

Introduction

Welcome to the first of a periodic newsletter aimed at accreditors. The Accreditors' Forum Steering Committee intends to use these newsletters to keep you, the accreditor community, informed of developments of interest to you.

Increasing Accreditation Capacity and Capability

At the last Accreditors' Forum a workshop was held to generate ideas on how an organisation's accreditation capacity and capability could be increased without increase in resources. Ideas that emerged from this workshop and elsewhere are outlined in the annex to this news letter. We would welcome views on how to further develop this guidance.

Accreditor Role Definitions

At past Accreditors' Forums we have discussed Accreditor Role Definitions (ARDs). The purpose of these is to:

- Drive professionalism of accreditation as envisaged by the HMG IA Competency Framework under development by Cabinet Office
- Enable greater mobility of accreditors between public sector organisations and to open up more career development opportunities

Your comments have been factored in to a new version which we aim to publish under Cabinet Office sponsorship by 19 Feb 2010 on the Cabinet Office IT profession website (<https://it.civilservice.gov.uk/>) and the CESG policy portfolio website (<http://cesgiap.gsi.gov.uk/index.php>). We will promote use of the ARD by:

- Proposing amendments to the HMG IA Maturity Model, HMG Security Policy Framework, HMG IA Standard No 2 and the OGC Gateway Review Process that require or encourage use of the ARD
- Writing to SIROs to encourage them to make use of the ARDs
- Participating in wider IA professionalism events

CESG Listed Advisor Scheme (CLAS)

At the last Accreditors' Forum, comments were made on the variable quality of CLAS consultants. CESG has been considering for some time how to address this perception. Whilst all applications for CLAS membership require written evidence of competency against the CLAS Framework (http://www.cesg.gov.uk/products_services/iacs/clas/newentrants.shtml) followed by an initial 3 day training course with annual updates, it is accepted that this is not as rigorous as the selection process for some professional bodies. Significantly raising the standards for the existing scheme, without giving members adequate time to reach those standards would be open to legal challenge. CESG is therefore considering other options for raising the bar. What ever option is chosen there will always be a need for clients of CLAS consultants to select their consultants carefully. IA is a broad field and nobody can be an expert in all areas.

Surviving & Thriving in the Economic Climate

As public sector funding cuts are being widely debated, IA could still be a growth area. Government initiatives such as Smarter Government and Digital Britain require public confidence in the public sector's ability to protect sensitive data.

The recently launched Government ICT Strategy sets out the Government's aim to create one secure, resilient and flexible network which will enable every area of government to adapt their ICT to best deliver for the public. In this environment, better IA can be a major business enabler. The full strategy is available on the Government IT Profession community space (www.civilservice.gov.uk/it) where you can post your thoughts and comments.

Further ideas on the relevance of IA in a cost cutting climate can be found at http://www.cesg.gsi.gov.uk/docs/IA_in_a_cost_cutting_climate.pdf.

IA as part of the HMG IT Profession

Over recent months, we have been working closely with the Government IT Profession to incorporate IA as part of their professional group. As IA professionals we all know that IA is not simply a subset of IT and that it includes much that is outside IT, but there are potential advantages of being part of a major Civil Service profession, including greater recognition of IA roles across the public sector.

IA professionals will also be able to register on the Government IT Profession community space (www.civilservice.gov.uk/it). Built with public sector IT professionals in mind it offers a single place to come together, share best practice, tap into development opportunities and increase your knowledge. The community space offers:

- a single point of access for information relating to IT professionalism and the wider IT landscape

- the opportunity to be part of online networks built around competency groups and areas of interest
- increased personalisation that will provide you with information, tools and learning relevant to your areas of interest
- access to contact details for IT professionals across the public sector, via the people finder, and
- a central place to exchange knowledge, share best practice, find jobs and opportunities, develop your skills and grow communities.

To join, complete the registration form, ensuring you are using a public sector email address as your primary email address. If you are unsure which competency group to select, IA falls under strategy and architecture.

A significant change that has already occurred is the move of the Cabinet Office lead on IA professionalism (Sharon Wiltshire) to work under the Deputy Director of the Government IT Profession (Kate Silver). Over the next few months CESG intends to present a paper on its vision of IA professionalism to the IT Profession Board and to the IA Delivery Group chaired by the Government CIO, John Suffolk. If this vision is accepted we expect IA to be formally announced as part of the Government IT Profession.

Use of ISO27001 across the public sector

In Nov 09, a sample of accreditors completed a short questionnaire to give an indication of how much ISO 27001 (Requirements for an Information Security Management System) was used across the public sector and whether it was useful. The survey indicated that between 1% and 10% of public sector organisations were certified to ISO 27001. Those that were certified found the Information Security Management System useful and that it nicely complemented the accreditation approach detailed in HMG IA Standards Nos 1 & 2.

Communications Among Accreditors

Another topic that has repeatedly been raised at Accreditor Forums is how we can improve the sharing of information between accreditors. In the last year we have launched networking groups among accreditors but we agree that something more sophisticated is required, preferably something that is already widely used. The HMG IT profession website (<https://it.civilservice.gov.uk/>) provides useful facilities including discussion threads but is not intended to protect sensitive information and is outside our control. The CESG GSI website currently offers fewer facilities (although that could be changed) but, as part of the GSI, is fit to protect Restricted information. We hope to make a recommendation on the way ahead at the next Accreditors' Forum.

Next Accreditors' Forum

The next Accreditors' Forum will be at MoD Main Building on 23 March 2010. The theme of the forum will be managing the shared risks of shared services. We expect to have a variety of speakers to outline the increasing challenge this poses to the accreditation community and a discussion session on how we should respond to it. In addition there will be the usual round up of new CESG policy and guidance plus views from Simon Kershaw, Head of Accreditation Specialism. If you have received this newsletter by e-mail direct from CESG you will be sent further details in due course. If wish to have your name added to the event distribution list please e-mail Events@cesg.gsi.gov.uk.

The following Accreditors' Forum will be on 29 June 2010, also in MoD Main Building.

IA10

IA10, arguably the largest public sector IA event of the year, will be held on 14 – 15 September at Park Plaza, Westminster Bridge, London. Requests for content from the accreditor community are welcome. Please forward them to Events@cesg.gsi.gov.uk.

Chris Few, CESG

On behalf of the Accreditors' Forum Steering Committee
Simon Kershaw, MoD, Chair & Head of Accreditation Specialism
Adrian Price, MoD
Chris Buckle, DWP
George McLeod, SPSA
Kevin Law, IPS
Lucky Afzal, CESG
Nick McKeown, HO
Peter Bonninga, BIS
Roger Hamilton, CPNI
Roger Millar, NIO
Sharon Wiltshire, NSG & Cabinet Office
Steve Lockert, MoD
Tammy Archer, MoD

Annex A - Increasing Accreditation Capacity and Capability

Given the unrelenting pressure to achieve more with less, below are suggestions from the last Accreditors' Forum and other sources on how to achieve this. These shouldn't be taken as new policy or guidance; they are just ideas for improvement from those active in accreditation.

Process

- Ensure IA is built into the procurement process so that security requirements and the accreditation process are factored throughout the system lifecycle including into contracts to deliver information systems.
- Ensure project managers are aware of the need for accreditation. This can be achieved by establishing IA in the project governance mechanism through workshops, briefings to the project management community or through additions to written project management guidance.
- Refine the local accreditation process so that it is better tailored to local requirements.
- Encourage SIROs to include IA in the overall business risk management.
- Provide training and mentoring to accreditors to enhance their effectiveness.
- Operate an accreditation triage process so that the accreditation of the riskiest Information Systems (IS) receive the most rigour and low risk IS follow a more streamlined accreditation process.
- Delegate as much of the routine work involved in accreditation as feasible to the client project; eg production of documentation, risk analysis and development of risk treatment plan. It should be noted that the proportion of the work that can be effectively be delegated to the project depends on the accreditors' confidence in their competence to carry it out.
- Develop a generic Risk Management Accreditation Document System (RMADS) for IS deployed into a common environment. This RMADS captures the controls applicable to the whole environment. System specific controls can then be captured in system specific RMADS and reference the generic RMADS. This avoids having to repeat content that is the same for each IS RMDS.

- Consider the scope of Targets of Accreditation. Can you accredit systems of systems rather than just systems? Increasing the scope may mean that the risk treatment is less finely tailored to IA requirements, but is a price worth paying if it enables accreditation of all IS.

People

- Self certified accreditation – are there any conditions under which you would trust project teams to accredit their own systems; eg experienced teams delivering low risk systems with sample checking by the accreditor? If not, what could be done to enable this?
- Can accreditors explain risks in terms that business managers understand? It helps them reach a consensus with clients faster.
- Accreditors need a variety of influencing skills to maximise their effectiveness; eg listening, communicating, negotiating, assertiveness, self-awareness. Consider training and mentoring to improve these.
- Be careful when recruiting and selecting CLAS consultants. They aren't all the same. Assess their suitability for your needs through scrutiny of CV and interview.

Technology

- Accredit infrastructure elements as being fit for a particular impact level to avoid reaccreditation within each application.
- Use shared services where feasible, it reduces the overall accreditation workload.