Accreditation for the Nation

The changing status of accreditation within Government Departments

Preface

This short paper aims to provide the reader with a brief history of HMG Accreditation and how, over time, 'accreditation' of IT systems within Government Departments has developed, changed and created a challenge for government departments to maintain, and how one Department is aiming meet this challenge.

The author has been working as an Accreditor for a central government department and, for the last two years, he has been involved with the implementation of a new Accreditation toolset with a modern web-based interface that streamlined the Accreditation function without losing the ability to explore items in detail. It has also delivered enhanced benefits such as triage, management reporting tools and greater understanding and alignment of risk across the organisation.

In the beginning

There were no RMADS. There was no accreditation of HMG computer systems. It was up to each Department to decide on what where their requirements and what approach they would take to protecting the information they handled. These decisions were often devolved to the IT Departments because users felt that they did not understand the risks or what could be done about those risks.

Over a period of time HMG realised that due to increased reliance on ICT, increased electronic datasets containing citizen data and the general lack of a singular view of measuring risks, there needed to be a formal approach to assurance. This lead to the creation the Manual of Protective Security (MPS), latte to be called the Security Policy Framework (SPF) which mandated that Government IT systems had to be accredited.

So, in the 1980s, there was a requirement for new systems to prepare System Security Policies (SSP) which was set out in CESG's Memo 5 to be reviewed by the Departmental Security Officer. National advice was provided by CCTA (UK government agency providing computer and telecoms support to other government departments handling 'Unclassified but Sensitive' data) and CESG (who acted as the National Technical Authority and provided guidance to Departments handling Classified information).

HMG mandated that all systems holding Classified material to be formally accredited. In 1995 HMG renamed the classification marking scheme to the Protective Marking Scheme and removed the distinction between Classified and 'Unclassified But Sensitive' data.

By the late 1990s, with CCTA having been superseded, CESG was providing HMG with technical security advice and created a suite of formal documents that guided central government departments on aspects of information assurance. These documents fell into several categories including Memorandum, Good Practice Guides, Architectural Patterns and Information Assurance Standards. Two of these standards IS1 and IS2 (originally 2 separate standards before they were combined in the 2000s) were the Government policies on how to formally document and assess the risk management requirement for ICT systems.

Developed from CESG's Memo 10, IS1 was the formal Risk Assessment Method (which was heavily developed in its lifetime from a simple spreadsheet to a formal modelled method) and IS2 was the guidance on creating an Accreditation Document Set (ADS later renamed RMADS). The ADS was a five-document set - (Introduction, Risk Assessment, Risk Management, In Service / Decommissioning and Certificate).   The problem was that all this guidance was very technical to understand and labour intensive to follow.

Mind the Gap

In essence, there was not only a skills gap but also a labour gap as there were literally thousands of systems that needed to be assessed. Realising this, CESG created the CESG Licensed Advisor Scheme (CLAS).   At the time, most HMG systems were handling information with a maximum classification of RESTRICTED and it was these systems that CLAS consultants were normally called in to work on. CLAS consultants were at a minimum SC cleared, so could work on SECRET systems, but normally each department had few systems operating at this level and preferred to keep the Accreditation in-house (normally with the Accreditor directly working on them).

After a successful pilot, a partnership with industry professionals was launched — these consultants were vetted and trained (to ensure a baseline level of quality/understanding) were to be the workforce that HMG could call in to write the RMADS, liaise with the Accreditors who would in turn accredit a system. It is important to note at this stage that the core values of the scheme, that each CLAS consultant should've delivered included, Business Focus, Dealing with Change and Value for Money. We shall revisit these values later.

Each system would be reaccredited over time (normally 12 months), or if it was changed significantly (if the change altered the Risk Profile) or following a security incident. If all (or at the least, most) of the systems were formally accredited, over time each Accreditor (or Lead Accreditor) could manually create a Risk Register to gain an overall picture of the HMG Department's risk profile. Other important documents and policies could be derived from this information, such as Waiver Lists, Trend Analysis then later Risk Appetite.

Armed with this information the Accreditor could start to influence Department policy with the overall aim of lowering the risks to its most valuable asset, the information that it handles.

In turn this information could then be reported to forums / central government functions / parliament and in theory a total picture of HMG's information assurance could be read and as such Government could decide on where and on what needed funding or developing. The value of current information and benefit at the highest level was indicated by the fact the Permanent Secretary signs off the annual security statement for Cabinet Office.

The Calm before the Storm

And so over time, systems got accredited, the CLAS scheme grew, CESG developed its policies and generally life was good, but all good things must come to an end. Initially the much of the guidance was marked RESTRICTED and was difficult to get hold of, resulting in a dip in expertise and understanding. With a less effective RMADS process, in 2014 the CLAS scheme folded (to be replaced with the NCSC Certified Cyber Security Consultancy Scheme); later CESG would be completely consumed into GCHQ and specific proscriptive guidance was no longer created.

Departments were left to manage their own affairs based on their own policies and risk appetites — what guidance there was, was based in ISO 27001 and budgets were tightened. Seasoned Accreditors were either moving into industry or retiring and external expertise was seen as an expensive overhead. So, the creation of RMADS documentation, as method of achieving accreditation was falling out of favour. It was seen as expensive to maintain whilst offering little benefit.

That is not to say that Risk Management and Information Assurance functions ceased, rather each department had to adapt from having external expertise on tap delivering documentation for consumption to back up in-house expertise to a situation where each Accreditor had to choose to deal with what was urgent and not necessarily what was important. It became more reactionary and as such many systems documentation sets were left to become outdated and irrelevant, essentially leaving systems unaccredited and unreviewed.

Those core values that were mentioned earlier were ebbing away. 'Business Focus' was fading as the Accreditation became more high level, 'Dealing with Change' was becoming less measured and reactionary and although 'Value for Money' was occurring in terms of financial savings, the overall value of Accreditation was being reduced as departments could no longer solely rely on the accuracy of its management information for creating policy.

Fast Forward

By 2010 many Government Departments fire-fighting to keep a handle on the accreditation statys of the systems that were operating. There weren't the resources to maintain the RMADS documents. New systems were dealt with immediately but then poorly maintained or left to lapse. Existing systems were dealt with based on their importance (size, number of users, changes or functions) to the Department. It got to the point where even that wasn't working, and the Information Assurance sections in Department were not delivering what was needed. Sooner or later there was going to be another incident similar to the HMRC data loss of 2008 and a radical rethink was needed.

The Department where the author was working started working with a commercial partner, who was able to take their COTS web-based solution and customise it to the Department’s particular needs. The Information Assurance team led the development, which involved interviewing all of the Department’s Accreditors, researching their approach to IA, their wants and needs and perhaps more important what they didn't want.

To cut a long development story short, the result was a through life information threat and risk tool that has digitised the Accreditation lifecycle within the department. Its modular nature has enabled the integration and delivery of various IA related business processes and outputs, thereby minimising and/or targeting effort, streamlining processes and improving the overall information security risk picture across the organisation. Thus, meeting the original core values which that are still believed to hold true today.

In a modern and agile ICT environment with multiple interconnected systems, all requiring risk management, the old Accreditation process is no longer fit for purpose. This Department has had to develop the grouping of systems together into logical groupings based on environment and the use of robust management tools. These tools must not only support the Accreditation process but also the on-going risk management and management risk reporting requirements.

Brave New World

The Department were the author worked opted not to go for a big bang approach. It dual ran both systems for 6 months. Maintaining our old Excel spreadsheet and manual documentation, whilst a select few users got to grips with data migration and pilot of the tool.

In the past, an IA consultant or skilled member of staff would liaise with the Accreditor, conduct interviews and write an RMADS. It would then be manually assessed, then reassessed, finally accredited and then mined for data on risks for a Risk Register. To deliver the required benefit (as recorded above) it was time consuming, labour intensive and expensive.

To tackle this, the department scoped and conducted an Overarching Risk Assessment that baselines the risks that the core business faces and allows constant evaluation of how those risks are mitigated. In an ideal world if everyone did a risk assessment they should all come out with similar results, however in practise this doesn't happen. The use of an Overarching Risk Assessment means that everyone is working from a common set of assessed risks.

Additionally, by having an Overarching Risk Assessment that has already been signed off by senior management it avoids unnecessary repetition by RMADS writers in undertaking that Risk Assessment.

Now with the web-based solution, any member of staff can request an Accreditation. They are guided through the approved and repeatable process using forms that are aligned to the departments Accreditation policy and ISO 27001.

The process is as follows:

- Accreditation Request — User fills out Basic Information.
- Triage — Accreditor selects the method of Accreditation (Full/Fast Track /Summary) based on system size/users/complexity.
- Submit — User fills out the forms relevant to the Accreditation method, the screens allow the User to have little hands on IA experience, but rather be knowledgeable about the system in general.
- Access — Accreditor access forms.
- Review — Optional Step if the Accreditor requires re-work.
- Escalate — Escalate to Senior Accreditor if Risks are Too High/Outside Appetite.
- Decision — Accredited / Declined.

The initial form is for basic system information, the latter forms ask the user to make a statement of compliance for the system against each control, whereby on review the Accreditor can accept, reject, refer back or escalate. These forms are the basis of each system's Accreditation Record.

The Accreditation Record as a line item on the screen has a unique number, Accreditation State, Expiry Date, Named Accreditor and Author and can be sorted filtered on any combination of the above.

Within each record there is a fully auditable notes section which the User and Accreditor can notate. It also records all key decisions made along the path of Accreditation.

Once the Accreditor is satisfied with the forms and is able to accredit, they fill out the Certificate Box. This box sets the level of Accreditation (Full/Interim) and the Expiry Date (as set by the Accreditor).

Once Accredited the Record is finalised as a snap-shot and one month before expiry an email is sent to the System Manager and Accreditor with let them know that re-accreditation is required. This helps with planning and scheduling.

Accreditation with Benefits

Not only does this web-based solution deliver a proportionate and effective end-to-end risk Accreditation management tool. It also enables the automated delivery of unambiguous, proportionate and consistent information through its reporting tools which enables the Accreditors to once again influence policy and advice.

It offers a greater cohesion of IA related information, enabling the provision of a comprehensive information risk picture across the department and the production of associated MI. This was once a labour-intensive trawl and scrape of the RMADS/Risks Assessments whereas now the trend analysis is up to the minute at the click of a button. The system also provides an efficient model, leading to savings in security and Accreditation processes as well as enhancing Accreditor/User experience.

Perhaps most importantly through its modular design the ability to develop IA services that can be operated on in the same way such as vulnerability management, risk balance and physical security.

Conclusion

Accreditation had become a dirty word in Government Departments. RMADS were seen as a handle turning exercise that no longer provided value for money. The implementation of this new system has reinvigorated the Accreditation Function for this government department. Accreditation is quicker, holistic, interactive, up-to-date and most of all proportionate. With more staff members being involved it also has the benefit of more staff being aware of IA activities as a whole.

As a former CLAS consultant the author is pleased the values to the scheme live on in this system.

- Business Focus — It is the business that is actually hands-on with its own Accreditations.
- Dealing with Change — The system is proactive and provides up to date MI.
- Value for Money — Accreditation is done in-house, repeatable, quicker and now provides greater tangible benefits.

In a modern and agile ICT environment with multiple interconnected systems, all requiring risk management, the old Accreditation process is no longer fit for purpose. Our organisation has had to develop the grouping of systems together into logical groupings based on environment and the use of robust management tools. These tools must not only support the Accreditation process, but also the ongoing risk management and management risk reporting requirements.

About the Author

Max Allen has worked in the Information Assurance industry for over 20 years. Max is a former CLEF Evaluator and CHECK Team Member, he was a CLAS consultant from the scheme's inception till 2014 when the scheme was wound down. Max currently holds Senior Level CCPs in Accreditation, Audit and Risk and is a founding Full Member of the IISP. In 2005 Max co-founded Platinum Squared Limited, a niche consultancy providing information assurance services to HMG and the private sector.