CENTRE *for* DOCTORAL TRAINING *in*
CYBER SECURITY

CDT Technical Paper

09/15

A pilot study investigating the process of risk assessment and re-accreditation in UK public sector systems

Michael Davies

A PILOT STUDY INVESTIGATING THE PROCESS OF RISK ASSESSMENT AND RE-ACCREDITATION IN UK PUBLIC SECTOR SYSTEMS

MICHAEL DAVIES

Centre for Doctoral Training in Cyber Security
University of Oxford

Abstract

The provision of security of information and its supporting ICT infrastructures within the UK Public Sector is long-standing and well established, underpinned by a wide range of standards and literature. For the many security practitioners that are employed in the sector, a number of important concerns have experientially emerged over several iterations of policy and standards that have been developed over time to govern this activity. The aim of this qualitative pilot study was to explore these concerns from the perspective of security practitioners employed in the sector. Data was collected from six security practitioners via semi-structured interviews. Subsequent transcripts were analysed using a Thematic Analysis approach that identified four significant themes that suggest that re-accreditation rarely occurs outside of the formal accreditation cycle, and point to the underlying reasons why this is the case.

Given that the National Technical Authority (NTA) is undertaking a comprehensive review of Information Assurance in the Public Sector, this pilot study is well-timed. This qualitative investigation of the issue is novel, and while aspects of these themes may be recognised anecdotally by consultants in this field, this pilot study provides an inductive, data-driven account of the issues with re-accreditation that transpired both within and across participants' transcripts. Finally, this study gives some indication of potential further research that could be undertaken in the area.

1 Introduction

For the large number of information security practitioners that are employed in the UK Public Sector, a number of important concerns have experientially emerged in the areas of residual risk assessment and accreditation, over the several iterations of policy and standards that have been developed to govern this activity. The main aim of this qualitative pilot study was to investigate these concerns from the perspective of the security practitioners employed in this area, and in the process attempt to answer the research question

Is there evidence that Public Sector organisations undertake the analysis of Residual Risk and system re-accreditation outside of the mandated accreditation cycle?

adfa, p. 1, 2011.

Accreditation is an assessment of an ICT system or service against its information assurance requirements, resulting in acceptance of residual risk, in the context of the business requirements and information risk appetite, and is in essence a precursor for the approval of a system to operate. The clear implication being that without a current and valid system accreditation in place, a system should not be operating.

The pilot study collected qualitative data of the experiences of consultants during semi-structured interviews (Myers & Newman, 2007). The subsequent transcripts were interpreted using Thematic Analysis and four superordinate themes were identified:

- System re-accreditation rarely occurs outside of the mandated accreditation cycle
- Key concepts and processes not understood at Senior Information Risk Owner (SIRO) level
- Under-resourcing in terms of sufficiently trained and experienced personnel in key areas
- Disproportionate nature of accreditation/re-accreditation in today's Information Assurance environment

Thematic analysis has enabled the issues considered by the participants as most relevant to emerge as themes in the data, with participants also providing insight as to what improvements they believe should be undertaken to the current processes. Finally, this study gives some direction on potential further research in the area.

2 Methodology

A qualitative approach to answering this research question was chosen based on the ability of such an approach to encourage participants to provide open and expansive responses to the range of question posed, and not be limited by trying to artificially impose quantitative values on their uniquely qualitative experiences. Information Risk consultants will have formed their own impressions and opinions of the way information risk is managed and communicated in organisations. In expressing these qualitative, personal impressions, the researcher anticipated, that the experiences of failures to fully utilise residual risk analysis in the decision to re-accredit, within these organisations, would be recalled, identified, and articulated by the participants to the researcher. The interview methodology selected for the study was a one-on-one, semi-structured interview based approach, where the participants were asked the same set of questions. The questions were phrased in an open-ended way and participants were encouraged to elaborate on their responses to each question while minimising the influence of the researcher. A complete script has been employed, but the questions posed to the participants have been designed to minimize the follow on inputs of the researcher, allowing the participants to freely explore and consider their responses to each question. Given that the participants all have considerable experience in this area of information assurance consultancy the researcher was confident in the ability

of the participants to respond positively to this approach, "the researcher may have prepared some questions beforehand, but there is a need for improvisation" (Myers & Newman, 2007). This semi-structured approach provides the opportunity to introduce a carefully planned and consistent interview schedule and range of questions to the participants, with the flexibility to probe deeper into participant responses of particular interest. McNamara (2009) has stated that this style of interview approach will enable the researcher to "ensure that the same general areas of information are collected from each participant; this provides more focus than the conversational approach, but still allows a degree of freedom and adaptability in getting information from the participant". This was the approach employed here.

This pilot study employed a small number of qualitative interviews undertaken with 6 individuals who are practitioners in the area of UK Public Sector system accreditation or who have been closely involved professionally in public sector IT. Five of the six participants are certified as Security Information Risk Advisors (SIRAs) under the CESG Certified Professional (CCP)[1] scheme. One of the participants was a Lead Practitioner with extensive experience of Public Sector accreditation. The sixth participant was originally recruited to undertake a test interview, but with wide experience of information and system management in the Ministry of Defence (MOD), the contribution made during the interview was of considerable relevance to the pilot study and the researcher was of the view that data of such relevance should not be excluded. The interviews witnessed these participants discuss their broad range of experiences of system accreditation in the UK Public Sector, before being requested to consider in detail, the sub-processes of residual risk analysis and the decision making processes around re-accreditation.

The questions used in the study are provided below:

1. What are the main issues you have experienced when consulting to the UK Public Sector?

2. What specific issues have you encountered when undertaking residual risk assessments?

3. When consulting to the Private Sector have you experienced similar or different issues?

4. How was the "risk appetite" of the organisation communicated to you during the consultative process?

5. Have you ever known full re-accreditation of a system to be undertaken outside the accreditation cycle?

[1] CESG Certified Professional (CCP)

6. What were the key decision-making processes involved?

7. In your opinion what influence did the "risk appetite" of the organisation have on the decision-making process?

8. Can you identify ways in which the residual risk analysis process can be improved?

9. The National Technical Authority is currently reviewing the full Information Assurance process, what do you expect to see coming out of this review?

A formal test of the interview was undertaken using an individual who was originally unconnected with the project but who did have wide experience of the area of investigation. This test-run followed the structure of the planned interview sessions in detail, enabling the researcher to identify any weaknesses in the planned interview format in terms of timings and question content (Kvale, 2007). Some issues with the structure of the interview were discovered. Audio recording using a single device – a laptop – was found to be less than ideal being prone to accentuation of background noise. For the remainder of the interviews two audio recording devices were employed. Also, the format was revised to ensure the interview content was more focused on the subject area. Importantly, the answers provided to the suite of questions during the test-run interview were closely scrutinised to see if the questions did indeed enable a range of answers that would support the aims of the project. Feedback from the pilot study was employed to refine the interview question to ensure that they supported the aims of the project.

The interviews were audio recorded with participants granting consent for this on the Project Ethical Consent Form. Full written transcripts were produced with anonymisation provided for all participants. Following transcription the audio recordings were destroyed, in accordance with the Project Ethical Consent Form. Subsequent analysis of the transcripts was then undertaken to draw out the key themes from the participant responses.

Thematic analysis, given its flexibility and utility, was used to identify patterns across the range of data provided by the participant consultants, using coding and theme development to draw out the recurring and relevant themes in participant responses (Braun & Clarke, 2006).

3 Preliminary Results

The decision to adopt a Thematic Analysis of the transcribed data provided the opportunity to "*explore in detail individual and personal lived experience and to examine how participants are making sense of their personal and social world*" (Lyons & Coyle, 2007). The Information Assurance community in the UK is small with many

consultants, particularly those employed in the public sector, having many shared experiences. This facilitated the exploration of individual's experiences of residual risk and re-accreditation across a wide area of the public sector, and lead to the identification of criteria for the selection of illustrative quotations that identified key superordinate themes and sub-themes. A tabular summary of the key themes identified, and a selection of supporting statements provided by the participating consultants is provided in Table 1 below.

Key Theme 1. Lack of re-accreditation outside the cycle	Key Theme 2. Key concepts not understood by SIRO	Key Theme 3. Under-resourcing of key personnel	Key Theme 4. Accreditation Process inappropriate
I struggle to think where I have seen anything re-accredited on a 12-monthly cycle … there is no point in going back and re-accrediting the whole system if there hasn't been any major changes Never in my experience … I think resources are the main issue	SIROs aren't actually sufficiently educated to understand (residual) risk … the SIRO is often too remote doesn't understand it doesn't understand what he is being asked to sign up for There is a definite lack of understanding especially by the SIROs and even senior management what is the definition of residual risk	People with appropriate skills not being in positions … the government witnesses too many changes that the pace of government accreditors not keeping up that could be down to resources that could be down to people with appropriate skills not being in positions … Danger is we may be starting to rely on the service integrator doing risk management due to lack of roles within the department	… the RMADS which ends up as a door stopper it's a 300-page document that no one really uses it and in my experience I have spoken to lots of accreditors and pan-government accreditors and they have never found any practical use of that It has just ended up as a tick box exercise now basically you have got this whole stack of documents which are RMADS which no one looks at them You have a heavy duty workforce and policies to follow that makes it (re-accreditation) not impossible but it's almost it can take

			as long as the whole implementation

Table 1: Key Themes and supporting statements from participant interviews.

Preliminary analysis of the important themes identified by the participants pointed to an emerging relationship between these themes, which is hierarchical in nature. This relationship is shown in Figure 1, and considered in the Discussion Section below.

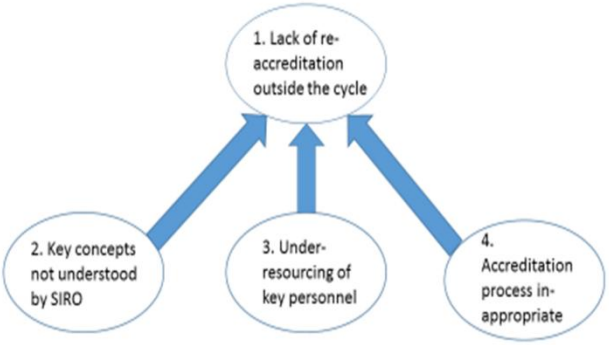

Figure 1: Inter-relationship between the four superordinate themes identified in the Pilot Study.

4 Discussion

The first emerging theme identified the common practice of failure to re-accredit systems outside the formal accreditation cycle. This process is supposed to be undertaken in response to any one of a series of mandated conditions for re-accreditation being met, and is compulsory, and not optional. The relationship of this theme to the subsequent themes identified is shown graphically above, and represents the idea that these are in fact the underlying causes for re-accreditation not being undertaken. For example, in the second theme there was a perceived causal relationship between the lack of re-accreditation and the fact that key concepts and processes are not well understood at the important senior stakeholder level of SIRO. If this is the case, there is the further related consequence that there will be a subsequent detrimental effect on the communication of key risk information in organisations and therefore on the effectiveness of decision making. Theme 3, which identified issues around the under resourcing of sufficiently skilled and experienced personnel is not contentious, reflecting the frequently observed shortage of skilled information assurance practitioners faced by all sectors. Finally, Theme 4 considers the inappropriate nature of the full accreditation / re-accreditation process in today's information security environment. The focus of all of the participants here was on the process of Risk Management Ac-

creditation Document Set (RMADS) generation, in support of the accreditation decision. In the fast moving rapidly evolving cyber security environment that challenges government departments and agencies today, the consultants all agreed that a process that can take months to undertake, and that can be undone by some form of offensive cyber activity in seconds, has possibly had its day.

Conversely, as shown by some of the consultants interviewed, there are occasions when re-accreditation *is* undertaken within the mandated accreditation cycle. This occurs when some significant change to a system has occurred, and where not to re-accredit would represent an obvious organisational failure to follow mandated standards and guidelines. At what level within the organization the decision to re-accredit is actually taken would provide an interesting area for further research.

5 Conclusions

This pilot study examined some of the issues associated with current processes around re-accreditation in the UK Public Sector. Based on this study there are clear indications that Public Sector organisations do undertake analysis of residual risk and risk appetite to support the decision making process for ICT system re-accreditation, but usually *only* for situations where some significant change has occurred. Where system re-accreditation should have, and has not been undertaken, Public Sector systems may be operating in an unsafe state. In the second theme there is a perceived causal relationship between this lack of re-accreditation and key concepts and processes not being understood at senior stakeholder level (SIRO), in Public Sector organisations. There is also the suggestion that this has a subsequent detrimental effect on communication of important elements of risk information and on decision making. These would appear to be suitable candidates for more extensive research. Moreover, the results identify measures that could be undertaken, such as enhanced training for SIROs, and more effective recruitment and retention of key personnel, which could be adopted in the short-term to address some of the issues identified.

6 References

Good Practice Guide (GPG 47), Information Risk Management. The document, although UNCLASSIFIED is subject to Crown Copyright and is available via the Information Assurance Portfolio at CESG

Anon, 2005. Risk Management and Accreditation of Information Systems, also released as HMG Infosec Standard No2

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology, (August 2015). http://doi.org/10.1191/1478088706qp063oa

Kvale, S. (2007). *Doing Interviews*. *Methods* (Vol. 2). http://doi.org/10.4135/9781849208963

Lyons, E., & Coyle, A. (2007). *Analysing Qualitative Data in Psychology*. Sage Publications Ltd.

McNamara, C. (2009). General Guidelines for Conducting Research Interviews. Retrieved from http://managementhelp.org/businessresearch/interviews.htm

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. http://doi.org/10.1016/j.infoandorg.2006.11.001