CAPITA

Technical Whitepaper

Risk Assessment and Risk Management in the changing HMG Information Assurance Landscape

Introduction

The Cabinet Office Security Policy Framework[1] requires that all ICT systems that manage government information or that are interconnected to them are assessed to identify technical risks. Following on from the introduction of the new Government Security Classification in 2014, Cabinet Office published an intent paper around the changes to Risk Management at OFFICIAL. This document effectively set the scene for the end of the IS1-2 risk management approach, Risk Management Accreditation Document Sets (RMADS) and Baseline Control Sets. In March 2015, CESG published a beta version of a Guidance paper "Principles of effective cyber security risk management"[2] which elaborates on this further but shows that this area is still a work in progress.

In making these changes, Cabinet Office stated, "We observed that the existing methods and tools used for risk management, though important, are not the most crucial success factors. What we found to be essential was for the business to create a culture and environment in which their risk management activities were effective."

The new guidance lays out eight fundamental principles of an effective approach to risk management:

1. Accept there will always be uncertainty
2. Make everyone part of your delivery team
3. Ensure the business understands the risks it is taking
4. Trust competent people to make decisions
5. Security is part of every technology decision
6. User experience should be fantastic – security should be good enough
7. Demonstrate why you made the decisions – and no more
8. Understand that decisions affect each other

However, it is important to note that the guidance, and the accompanying series of guides, do not mandate which risk management process should be used. In fact, it states that no single risk management process and accreditation process fits all scenarios. It is now the responsibility of the organisation to decide on the most appropriate risk management approach.

Capita ITPS uses ISO 27001:2013 to build Information Security Management Systems (ISMS) in order to deliver operational and real time risk management systems. The ISMS is used to provide security documentation – thereby replacing one off RMADS with ongoing security and risk management processes.

Risk Assessment Methodology

At Capita, we take a three-stage approach to risk assessment:

Discover

- Understanding the context and objectives
- Asset identification and valuation

Develop

- Developing the threat model
- Assessing vulnerabilities, likelihood and impact
- Producing the Risk Assessment

Deliver

- Control analysis
- Risk appetite
- Risk reporting

[1] https://www.gov.uk/government/publications/security-policy-framework
[2] https://www.gov.uk/government/publications/principles-of-effective-cyber-security-risk-management

©2015 Capita PLC All rights reserved

Using Risk Tools

It is important to define the distinction between the various phases of risk activity before discussing the attributes of tools:

1) **Risk Identification** – includes information asset identification, understanding the risk environment, analysing other related internal and external risk assessments, identifying the vulnerabilities of your information assets and the risks they face.
2) **Risk Assessment** – applying a methodology to the identified risks, either qualitative (based on information and intelligence, common sense and analyst's experience) or quantitative (based on metrics, numerics and matrices) or a combination of both, to produce quantifiable results (risks grouped by high / medium / low or numeric equivalents). Note that regardless of methodology, the results must be quantifiable in order for business risk decisions to be taken.
3) **Risk Management** – includes risk mitigation, risk appetite or tolerance, risk acceptance, operational and/or project risk review and management process, reporting upwards.

A fit for purpose tool will enable all of these activities, however some concentrate on specific aspects of the process. One definition may be:

> **A tool which automates the risk assessment process and delivers outputs in order to support the justification and the selection of information security controls.**

There is a vast array of 'risk assessment tools' available, ranging from Enterprise GRC tools such as SAS and SAP that provide enterprise organisational risk insight, to Security Information and Event Management (SIEM) solutions that provide very low level network level insight.

What to consider when selecting a risk tool

The following high level requirements should inform and drive the selection:

Integration

The tool should be flexible enough to be tailored to the local environment and speak the same language. It needs to be an integral part of and integrate into the wider organisational risk management processes. This is the key challenge of most tools. A general rule of thumb is that the more you invest in setting up and configuring the tool for the local environment, the more value it offers in terms of insight.

However, this needs to be balanced against the type of project, see Scalability.

This feature is particularly important when it comes to setting key variables such as impact levels. The tool should communicate risk levels in a format that the organisation is familiar with, whether that is words, a numerical scale or a colour code.

Scalability

The requirements and the nature of the project are key here. A one off ISMS with a specific, relatively small scope, will require a different tool to the outsourcing of a large business process which requires Governance, Risk and Compliance reporting and management across the programme.

For example, if the rough scope is less than 5 sites, 50 assets and 200 staff, then a spreadsheet or in-house tool may be sufficient, depending on the complexity of the scope. If the scope is larger or more complex, consider a software solution instead.

In general, if the enterprise architects are using enterprise tools to manage the design of the solution, then assurance ideally should be using enterprise tools to assure the solution.

Transparency

The tool will need to be transparent. Any tool which takes input, processes it and gives an output without a clear explanation of how it got to that output step by step should be avoided. For example, some tools have proprietary 'asset type – threat' mappings built in. It is important that these be available.

Multiple factors

Some tools (such as IS1) do not really take into account human, natural and physical factors. IS1 was a technical risk assessment only and did not include risks such as flooding. The tool should be holistic and cover all factors pertinent to information security.

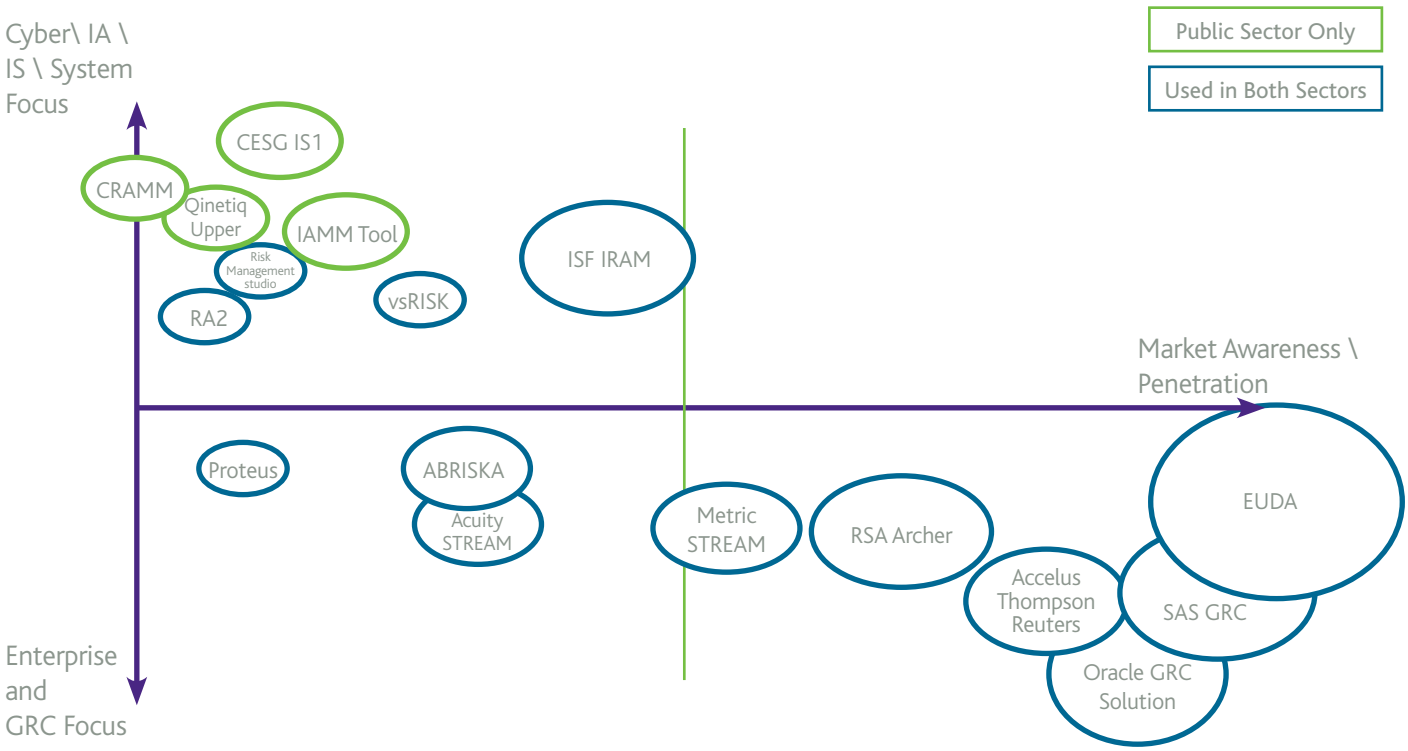
Dynamic, iterative and responsive to change

A tool should not be a one off exercise. Rather, it should be updateable, based on new information and new ways of working. In the simplest sense, most tools can do this, but there are few tools on the market that have the ability to take snapshots of the present and then model or simulate changes, such as the loss of a building or key asset.

©2015 Capita PLC All rights reserved

The diagram below presents our analysis of the Cyber Security tool market at the time of writing.

Cyber Security 'Tool' Market



At Capita, we have a wealth of experience in providing consultancy services relating to HMG Information Assurance and the requirements of the Cabinet Office security policy framework. The Capita IT Professional Services Information Security team provides expert ISO 27001:2013 consultancy and has developed an agile ISMS Methodology. All our consultants are experts in the Information Assurance field, are all qualified with CLAS (CESG Listed Advisor Scheme) and hold CESG Certified Professional levels across a range of security disciplines.

Noel Hannan
Information Security Consultancy Manager

For further information about these services please contact:

Email: **marketing.itps@capita.co.uk** | Tel: **+44 (0) 8456 077466**
www.capita.co.uk/itprofessionalservices

©2015 Capita PLC All rights reserved