10 Principles for Effective Information Assurance

A principle driven strategy in a less policy constrained environment

A White Paper from:

Advent IM Ltd Security Consultant, Chris Cope CISM, CISSP, MInstISP, CESG Certified Professional, PCBCM, ISO27001 Lead Auditor

ADVENT IM

Introduction

On 1st January 2015, CESG withdrew the mandatory requirement to use the Information Assurance Standards 1 and 2 (IAS1&2) when assessing the information assurance requirements for IT systems. Government departments could now adopt the risk management methodology they wished, but has this led to a rush of departments trying new methodologies? Well no, not really, since with the Government's Security Policy Framework to consider, i.e. the requirement to properly assure IT systems, many accreditors are currently sticking with what they know and advising departments accordingly. But with greater freedom, the information assurance community should consider what a new assurance methodology could look like.

Background

IAS1&2 had many positives; a requirement for risks to be properly assessed, good communication to all users via Security Operating Procedures (SyOPs), treat information assurance as a through life process and implement good governance. However, many of the positives were undone by the hugely process driven methodology in generating weighty Risk Management and Accreditation Documentation Sets (RMADS), complex language and a lack of flexibility when dealing with multiple systems within one organisation. CESG tried to address some of these concerns by calling for a risk managed approach to accreditation, but still the perception remained that the aim of accreditation was to generate impenetrable documents. Each organisation is different, hence the danger in prescribing one strategy designed to fit all, so it is important that information security managers and accreditors are able to shape the risk management strategy to fit the circumstances. If the brave new world means risk management becomes less process oriented, perhaps a better approach is to adopt a principle driven strategy? The following are 10 information assurance principles which will enhance the security of any organisation.

©Advent IM Ltd 2015

Principles for Effective Information Assurance in a less Policy constrained environment

Focus on the business. IT does not operate in isolation, neither does security. Both support the organisation in the pursuance of its business or operational objectives and any information assurance strategy must have the aims and objectives of the organisation front and centre of its thinking. Without this strategic overview, security solutions may not enable the functionality that the organisation is depending on. If an information security manager is at odds with the business leadership, security will be undermined as users ignore security controls, safe in the knowledge that the senior leadership is not fully on board. To be ultimately successful, senior management must completely support security, but this endeavour is made easier when information security managers fully consider the needs of the business. The aim is to assure the information held by that organisation so that it is secure enough, not to tick boxes.

Adopt a holistic approach. Information assurance is, even without considering the wider business interactions, a blend of physical, procedural, personnel and technical security. So to be effective, information assurance cannot just be about the technology. The increasing use of the term 'Cyber' has perhaps led to predominance towards the high-tech, yet the majority of the threats faced are human in nature. Even the most high-tech threats, such as Advanced Persistent Threats, heavily utilise human vulnerabilities, such as phishing, in the kill chain. So beefing up the firewall or investing in high grade encryption is not the whole solution. It is thus a concern that many information security managers spend a disproportionate amount of time concerned with technology, rather than strategy. Security works best when it is holistic, where defences are layered in depth, so a weakness in one is mitigated by the presence of another. It's also hugely important to ensure that security does not focus completely on confidentiality; both integrity and availability are equally important, sometimes more so.

Be risk driven, not adverse. This is the opposite of a compliance based system. Managing information assurance cannot just be a tick box exercise. Security controls cost money, they also restrict functionality. If a system is over protected, then financial resource has been wasted and users will over time lose respect for apparently pointless security controls that prevent them from doing their job. An organisation that understands the importance of its assets, including information, and is aware of what risk it is prepared to accept, will be able to make a more nuanced decision on which areas of the system require more protection than others. Controls can then be more focused, less expensive but more effective as a result. However, for this to work, organisations must truly embrace risk management. They must engage with the process and accept that the cost of doing business means taking some risks - reducing them to 'As Low As Reasonably Practicable', is the main objective. Organisations should also accept that things will go wrong. There will always being uncertainty because risk is not always predictable and cannot therefore be totally eradicated.

©Advent IM Ltd 2015

Build in good governance. Good governance was a cornerstone of the IAS1&2 policies and for a good reason. To be successful, an information assurance strategy needs to be owned and led. Without named positions in charge of the process, the chances of the strategy being successful are hugely reduced. But good accountability extends beyond merely signing documentation; the strategy must be supported and believed in. It must also be measurable. The saying 'what gets measured gets done' is correct. There must be quantifiable goals for any strategy, and this includes information assurance. Applying metrics against the delivery of ISO27001 controls, incident rates, access requests and security training information can all be useful in monitoring the effectiveness of the information assurance strategy, but only if attention is being paid to the results. Information assurance must be a routine management activity that is on the agenda at Board level and where the activities of the security practitioners are fully held to account.

Ensure good communication. Any strategy depends on communication. The organisation's senior management need to understand what the practitioners are telling them, but perhaps most importantly of all, the ordinary users need to understand what is expected of them. Security education is critical, both in providing the required information that users need and in inculcating a positive security culture. Effective security education should take a variety of forms and must be designed around the needs of the users, i.e. what is important to them? What message will resonate best with them? If there is one element of RMADS that deserves to be kept, it's the SyOPs. This doesn't means the lengthy tomes that were impenetrable to ordinary users, but 2-3 pages of key information relevant to the user and the system is vital in reducing the human vulnerability.

Approach information assurance from the top down, and the bottom up. RMADS were criticised for being too system focused, which often means multiple RMADS across an organisation. A typical RMADS would acquire and document a significant amount of information on the wider organisation, as well as the system, so why not cut out the repetition. An organisational wide assessment of information assurance can be structured very effectively against any of the standards in existence, such as ISO27001. Individual systems do require their own consideration, but this should be in context of the wider information assurance eco-system and not in system isolation. Documentation for the system itself should only include that which is distinctly relevant to that system. Specific controls from ISO27001 (assuming that is the standard of choice) can be individually applied, allowing the higher level controls to be dealt with by the organisation. Also, why do a risk assessment for every system? An organisation wide risk assessment will deal with the vast majority of organisation's requirements. New systems can be assessed against the organisation risk assessment and, if it is felt that additional risks are presented, then the overarching assessment amended. Information assurance professionals must look to make the process fit the organisation, rather than the organisation fit the process.

©Advent IM Ltd 2015

Consider the full lifecycle. Here, IAS1&2 got it exactly right. Information assurance is a through life concept, not a one off exercise. Recent research by CESG has highlighted that security developed from the conceptual phase reduces costs by 40%, when compared to consulting a security professional for the first time just prior to release. Regardless of the development model employed, information assurance must be considered for the first time when the project is first considered as a concept. The initial information assurance plan should then be refined throughout development, with security professionals influencing design decisions. However, the work does not just stop when the eventual 'product' goes live. The information assurance strategy needs to continue throughout the in-service stage of the project, remaining flexible to deal with changes in technology or use. Finally, the disposal period is just as important as those that precede it. Permanently destroying information (or securely archiving it) must be an informed and methodical decision, again providing the assurance that the organisation's information is secure.

Remain adaptable. Remaining flexible is crucial. Information assurance procedures in relation to a specific system will change through its lifecycle and information assurance practitioners must be involved in day to day decision making. Very few systems remain stable during their use and decisions made for the initial deployment will need to be re-visited as either technology or its use changes. To ensure continued assurance, the strategy must be maintained to ensure that changes are carried out in a considered and secure manner.

Be inclusive. Inclusivity is essential. Information assurance covers a wide range of disciplines, and very few practitioners can realistically claim to be experts across the board. Not only does the strategy need to consider the input from the IT department, business leadership and risk management, but there are other critical areas to incorporate. Human Resources must be involved as many controls will involve incorporation into personnel contracts and alignment with any disciplinary system. There are a number of key areas of legislation which are imposing controls on organisations. The Data Protection Act (and forthcoming EU Data Privacy directives) places an onus on the organisation to properly protect sensitive personal data. But aside from legislation, the impact of security breaches on contracts must also be considered. With an increased understanding of information assurance standards such as ISO27001, what liability do you have to your customers if you have a data breach that involves them? Or a loss of service? Understanding the legal impact from information assurance incidents is becoming more important, particularly with regard to how much security is enough.

©Advent IM Ltd 2015

10

Plan for the unexpected. No matter how well protected you feel you are, any organisation can suffer an unexpected disaster. Protecting the enterprise from risks occurring in the first instance is only part of the story; ensuring robustness is just as essential for when incidents occur. If businesses understand which of their functions are truly important to them, they will be able to undertake a business continuity exercise which will offer genuine improvements in resilience. With IT being a key business driver, the potential for an IT incident to impact on the business output has grown exponentially. IT Incident Response Plans cannot be the sole preserve of the IT department; they must be intrinsically linked to the wider organisation, and vice-versa. Good resilience is the key to surviving incidents with the business intact.

Finally

There is no magic bullet to information assurance. With IAS1&2 no longer being mandated as the only accepted risk methodology, there is greater freedom in how organisations can provide their information assurance; but with greater freedom comes risk. Too much policy can result in a compliance based approach, too little and doubts over the efficiency of any solution come into play. Perhaps a principle based approach will be of more use to the wide array of government organisations, and private enterprises, trying to understand how to proceed in a less constrained environment.

©Advent IM Ltd 2015

ADVENT IM

10 Principles for Effective Information Assurance

A principle driven strategy in a less policy constrained environment

www.advent-im.co.uk

0121 559 6699

0207 100 1124

@Advent_IM