Accreditation

Accreditation is formal, third party recognition of competence to perform a specific task.

In the Government arena security accreditation is mandatory for all Information & Communications Technology (ICT) systems that handle, store or process protectively marked information or business critical data. The Cabinet Office sees accreditation as a business enabler and believes that the accreditation process provides important assurance (Information Assurance) that an organisation can accept the balance between business opportunity, risk and cost for any given information system.

Risks in a Government sense are assessed against the Business Impact Level (BIL) of the loss of Confidentiality, Integrity or Availability of information within varying business scenarios; whether direct or indirect endangerment to life (or multiple lives), political instability, maintenance of Critical National Infrastructure (CNI), public sector financial loss, reputational impact, etc.

Risks in the private sector will probably very much focus on financial impacts (loss of critical business data (IPR, etc), disruption of vital systems, etc), but, in accordance with UK law, should also include the risk of loss/misuse of Personal Data.

Assurance that these risks and therefore impacts will not materialise is provided by accreditation. Accreditation will consider the value of physical assets (e.g., IT hardware) and non-physical assets (e.g., business reputation); it will consider the threats / plausible compromise methods to those assets and any exposed vulnerabilities. Accreditation will then consider the proposed treatment or management of the assessed risks, and will usually call for an appropriate vulnerability assessment / penetration test scenario to provide the risk owners with technical assurance of the documented security controls.

Private sector organisations seeking internationally acclaimed certification for the security of their organisation, or system therein, may seek IEC/ISO27001 Certification. Government-employed systems / services are accredited more stringently than the criteria laid out in IEC/ISO27001, instead, they are accredited against the Security Policy Framework (SPF), of which the HMG Information Assurance Standards (1-2, 4, 5, 6 and 7) are a subset, and within which appropriate implementation of the Baseline Control Set (mapped to IEC/ISO27001) is prescribed – the level of implementation being dependent upon the BIL. Some Government departments, for example the Ministry of Defence (MoD), have their own security policies, which are more granular in context. In these cases,

accreditation will consider both Government and Departmental security policies.

The role of the Accreditor is to act as an impartial assessor of all risks that an ICT system or service may be exposed to throughout its lifecycle in meeting the business requirement and to formally accredit that system or service. This is conducted on behalf of the Senior Information Risk Owner (SIRO) (possibly the Chief Technology Officer (CTO), Chief Operating Officer (COO), etc), who must be a senior Board member. It is stressed the SIRO must be a Board Member as they must provide governance for the project (or business) and have the right to make Board-level decisions.

The Accreditor will advise and guide the project or programme team and will play a central role in any committees, panels and groups that are set up to support the accreditation process. An understanding of ICT related technology is useful but the role will not usually require deep technical expertise, more important is an ability to consider information risk management in the round to ensure that all required physical, personal, procedural and technical controls are balanced.

It is important therefore, that the Accreditor has access to people who have a technical understanding of the technologies involved, and other specialist skills to support the accreditation process. Accreditors are fully accountable for their decisions to the SIRO. Before granting an accreditation decision, the Accreditor must also consider wider implications that the system in question may have on other interconnected systems, and vice versa. In some cases, the Accreditor may choose to offer 'Conditional Accreditation' for a system that may lack specific, or a range, of security controls. Conditional Accreditation may be for certain components of the system, or for a brief period of time, after which they will review the improvements to the security model and may, if satisfied, offer a longer or wider-scoped accreditation decision. They can be called to account for their actions in a legal proceeding but are not liable in law. As part of the overarching Corporate IA Strategy, the Board must define an accreditation strategy that takes into account the need to demonstrate compliance with National (and where applicable International) IA Standards and policy and meet their legal and regulatory requirements. The board must also ensure that funding and resources are available to deliver the strategy.

Accreditation requires that the risks be reduced to a level defined by the organisational Harm Level/Risk Appetite. IA risks above the Risk Appetite, which cannot be mitigated by policy-prescribed methods, may be manageable by compensating controls, but will usually require sign-off by a higher authority. In business terms, this suggests that the SIRO must take the risk to the Board for sign-off. In Governmental terms, this will usually require sign-off by a representative of, or the, Chief Information Officer.

Accreditation should be seen as a business enabler, not a complex problem. Risk assessment, information security and assurance should be integral areas within the design, build and implementation of ICT systems and solutions so that accreditation can be a seamless process. For this to be possible it is essential to use the services of an experienced Accreditor, who will work with the business to ensure that risks are identified, assessed and dealt with effectively.

Regency IT Consulting employs experienced Accreditors with the skills, knowledge and training needed to provide accreditation and associated support services within your department or business area. As an independent assessor of risk, the Accreditor can give the business the assurance that an information system meets the Information Assurance requirements of the business. Based on Harm Level/Risk Appetite and management of residual risks our Accreditors will formally accredit the system on behalf of the Board of Directors.

By working with you and understanding your business area and the risks that are pertinent to your information systems, our Consultants' advice and support will enable risk owners to make properly informed judgements about how best to manage the residual risks that they own. By using one of our Accreditors, time and cost savings can be made by ensuring the solution is fit for purpose and complies with relevant legislation, policies and guidance from the outset.