

Security Policy, Standards and Procedures

Development and Review

For most organisations, maintaining security is an essential part of ongoing business. To reduce the likelihood of a security failure, the process of implementing security has to be formalised. The formalisation of security solutions takes the form of a hierarchical organisation of documentation sets with each level focusing on a specific type or category of information and issues.

- **Policies**

Security policies sit at the top of the documentation set hierarchy and defines the security needs of an organisation and how that organisation addresses those requirements. Policies are generic, non-IT specific statements of intent defined and owned at the highest of management/board levels, and are usually concise in their nature.

- **Standards**

Security standards define compulsory requirements for the use of hardware, software, technology, and security controls. Standards define steps or methods to accomplish the goals and overall direction defined by security policies.

- **Processes**

Security processes document, at a high level, the actions necessary to implement a specific security mechanism, control or solution.

- **Procedures**

Security procedures are detailed, step-by-step how-to documents that describe the exact actions necessary to implement a specific security mechanism, control or solution. Procedures are driven by upper layer policies and processes.

During a Documentation Set Review, IRM will first identify the exact documentation framework that has been adopted by the organisation. Each document will be reviewed against both security best practice and its applicability and suitability within the hierarchical layer.

During a Documentation Set Development exercise, IRM will initially engage with the business to understand and advise on any documentation framework that the organisation has in existence, or that the organisation should adopt going forward. Consultants will work closely with the client at all business levels in order to understand operation requirements and the business model in use. Once the framework and requirements have been identified, IRM will draft the relevant security documentation sets, transposing and merging business requirements with security best practices.

From a documentation set review, IRM will deliver a formal report including an executive summary, a summary of your organisation's documentation framework and overall position, and recommendations to address shortcomings in the documentation set. From documentation set development, IRM will produce a set of documents within an appropriate framework for the business.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.