

Information Security Healthcheck

If you are running an information organisation, you no doubt spend money on information security. But how do you determine whether you are spending too little, or too much? If there have been security incidents, how do you tell what areas in your organisation need addressing?

IRM's Information Security Healthcheck service evaluates the security of all aspects of your business using established methodologies to assess the security of your people, process and technology. Most importantly, it evaluates you relative to other organisations in your business sector, giving you valuable information about the marketplace and your exposure to risk relative to your competitors.

The result is a clearer view of where your security is on target, where more focus is needed, and where you may be able to make savings for your business while maintaining appropriate levels of security.

A complete Information Security Healthcheck includes the following phases:

- **Information Appraisal**

During the first stage of the review, IRM speaks to senior executives such as the CIO and immediate reports to gain insight into the systems and data that the organisation holds. This allows IRM to understand what information the business manages and, looking from a high level business view, gauge the major threats to this information.

- **Cultural Appraisal**

This phase involves interviewing a range of employees across the organisation, in addition to any third party staff whose work may impact on the security of the client organisation. IRM works to understand how the organisation functions, and how employees view their role in the company, particularly from an information security point of view. Technologies and controls are discussed to develop an understanding of the technical controls in place within the organisation, and IRM gauges internal awareness of security through conversations about security responsibilities, internal processes and security policies.

- **Physical Appraisal**

A brief Physical Appraisal takes place, with IRM quickly gauging the overall physical security of the working premises and facilities in scope for the information security review.

- **Documentation Review**

IRM reviews the policies in place within the organisation, assessing their completeness. IRM will determine how the policies compare with the feedback from the cultural appraisal and information appraisal, determining where there are shortcomings in the policy set, and where there appear to be gaps in the understanding of policies and procedures internally.

- **Deliverables**

IRM will deliver a formal report including an executive summary, a summary of your organisation's security position in the context of people, processes, and technology, and recommendations to address shortcomings in the face of identified threats to the organisation.

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.