

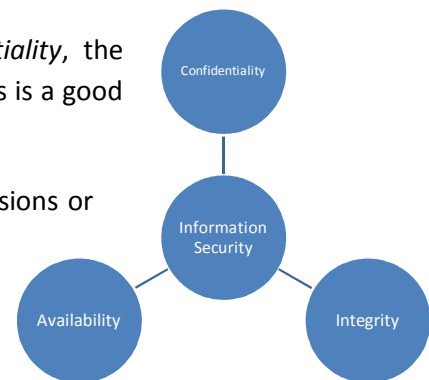
Information Security *is* Business Continuity

Securing corporate information has extraordinary implications across the entire organisation. It is very easy to think that a firewall, some good anti-virus software and password controlled access to IT systems is all that is required. It's a good start but there is a great deal more to deal with once you get into the detail.

If you consider that information security is about the *confidentiality*, the *integrity* and the *availability* of your data and applications, then this is a good place to start in thinking the process through.

Each of these areas requires careful consideration before any decisions or policies can be created or managed.

Confidentiality means ensuring that confidential, sensitive, possibly secret, information that resides on corporate systems remains just that by implementing proper access controls based on an individual's role and the status of the information. This would apply to both physical and logical access.



There is nothing worse than having incorrect information stored within the systems thus the *integrity* of the data is key to the business. If security has been compromised and the data has been altered in some way then this constitutes both a breach of security and a risk to the business. It could be simply mismanagement of a backup/restore procedure that has altered the data. In other words data integrity can be impacted by more than just security breaches.

Data *availability* constitutes the third element of information security. If a server, an application or the data associated with it is unavailable then again, a business risk is exposed. For many applications, the brief loss of availability does not constitute a major business risk, but in some circumstances it may. Consider the availability of SCADA systems in the real time control of oil or gas production, of that of a utility company such as Scottish Gas or Scottish Water. Any loss of availability of these systems could be a major risk to the entire organisation from a Health and Safety point of view, from an environmental point of view and, ultimately, from a financial point of view. The long term loss of availability of critical applications, even if they're not real time, will constitute a major risk to most organisations.

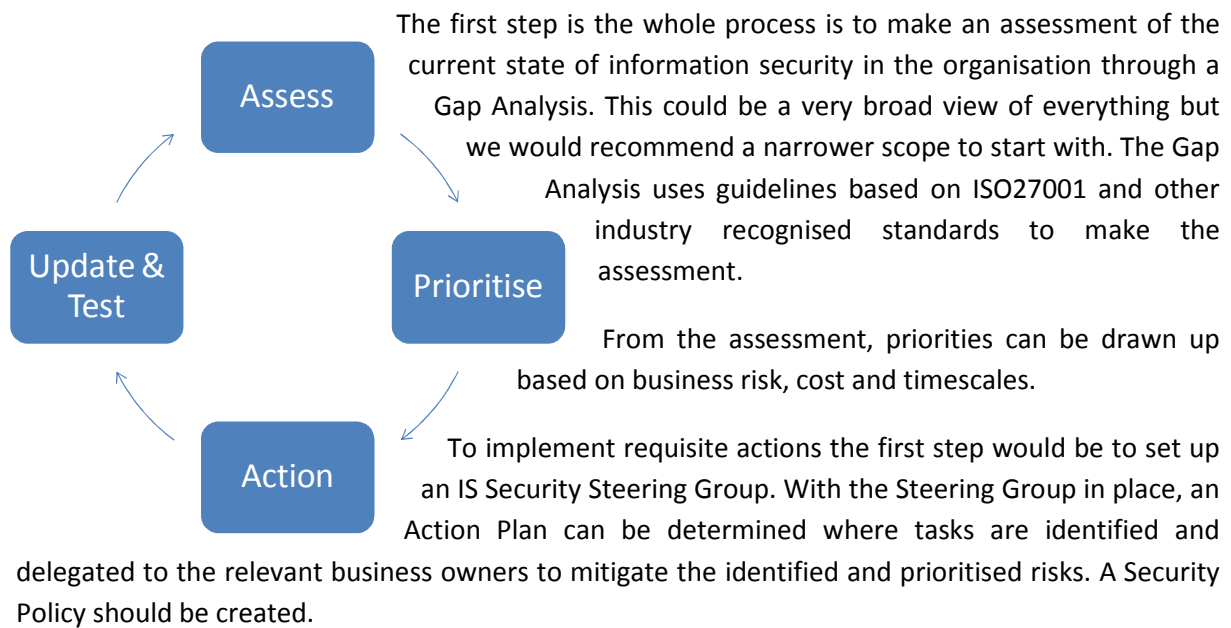
Organisational Structure

Information Security is often seen as the responsibility of the IS/IT department which, in terms of putting the relevant technology in place to ensure that confidentiality, integrity and availability are maintained, is not an unreasonable position. However, how do the IS department know what the business risk is and therefore know what level of security to implement to address that risk? There is clearly a balance between the potential cost associated with a risk and the mitigation of that risk. This is a business view, not an IT view. Once the costs are known and the likelihood of the risk

assessed then the cost of mitigation can be determined and IT (or other department) can take the necessary steps.

To achieve an effective information security posture, an organisation needs to have an IS Security Steering Group consisting of its senior figures (CEO, CIO, CSO etc). The Group will be responsible for defining what is and isn't an acceptable business risk, the objectives and strategies required to maintain this posture, and to prioritise, monitor and review all related activities.

Vioptim's Approach



Finally, procedures and processes are updated and put into action, IT systems updated in line with the mitigation strategy and tested against the security policy.

Vioptim and its partners will help guide you through this process providing consultancy, technical assistance with IT systems and the provision of the relevant solutions to comply with the security policy and mitigation strategy.

Information Security is Business Continuity

Often thought of in completely different terms, the reality of life in the business world is that the only way to ensure business continuity is to have a rock solid information security structure in place. Securing your information is ensuring the continuity of your business.

About Vioptim Ltd

Vioptim provides practical consultative services and solutions to effect positive change in IT systems by using virtualisation techniques, optimising existing designs and ensuring the security of information and applications.

Vioptim Ltd is registered in Scotland #356270

For further information please visit www.vioptim.com