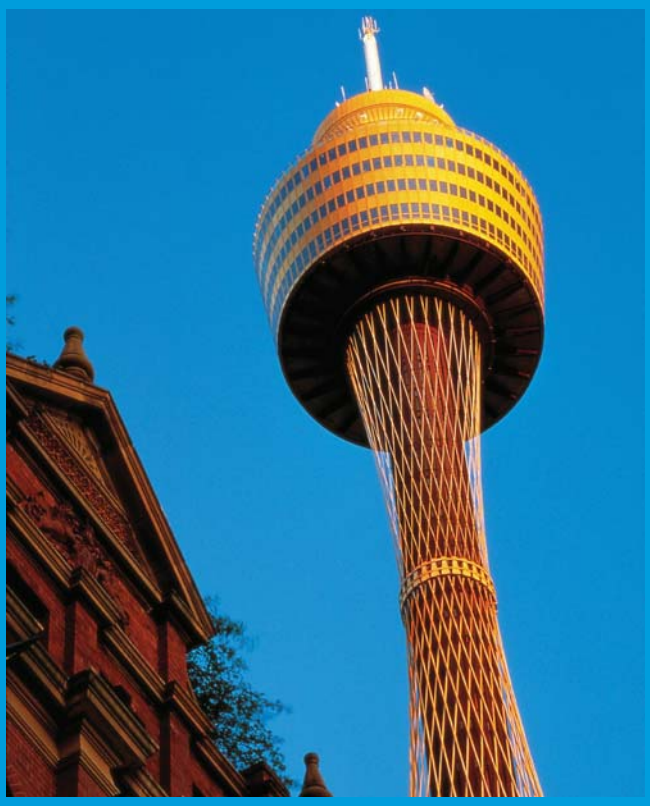


Security Policy

Information Security Policy & Framework Development

An organisation's information is rapidly becoming its most valuable asset. With advances in technology and business methods, risks are introduced on a wider scale and at a quicker pace than ever before. One of the major challenges an organisation faces is to find and employ an effective and proven model for information security. This model has to fit the organisation's business and also address many different facets: people, policy, process and technology.

Information Security Framework

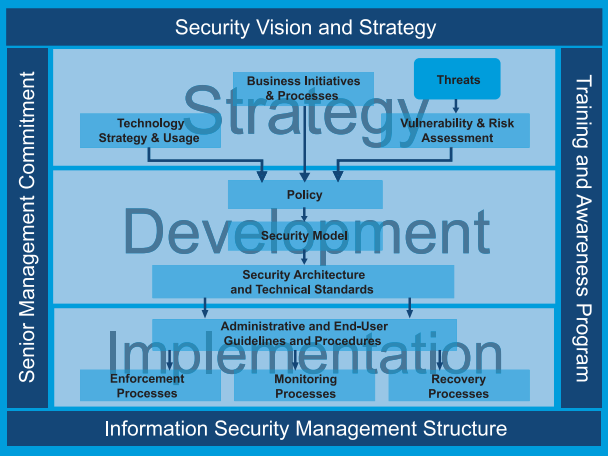
PricewaterhouseCoopers' information security framework is a comprehensive and proven model. It defines the various levels of security processes that need to be developed and implemented to ensure that the information assets of an organisation are effectively and efficiently secured.

The information security framework is developed to help understand an organisation's security challenges from a business perspective, and to provide a structured approach to support enterprise security management initiatives.

The Four Pillars

There are four pillars that support the information security framework. These four components must be in place to implement a successful information security programme:

- Senior management commitment
- Security vision and strategy
- Information security management structure
- Training and awareness



*connectedthinking

PRICEWATERHOUSECOOPERS

The information security framework, like any architecture, has many different building blocks that, combined together, form a solid foundation for addressing enterprise information protection. The result is a model for information protection that takes into consideration all of the aspects of an organisation, from business processes to technologies to individual employees. Enterprise security architecture defines the information security strategy that consists of layers of policies, standards, processes and procedures, and the way they are linked. The enterprise security architecture is crucial to a successful information security management program. Without an established security architecture to govern the infrastructure, adequate security cannot be achieved.

Risk Assessment

Risk assessment is the process of defining security requirements for information assets in each of the three risk categories: confidentiality, integrity, and availability. It involves defining control measures to ensure that security controls are appropriately identified, implemented, and maintained. The objective of risk assessment is to gain a sound understanding of the security risks associated with an information asset, and to agree on what safeguards are worth putting in place to reduce the level of risk or to lessen the impact of a potential security breach.

Information Classification

Directly related to risk assessment is information classification. With the explosion of distributed system environments and information flowing through extended corporate networks linked to suppliers, business partners and customers, classifying information is becoming a business necessity. Adequate information classification can aid in lowering the overall cost of information security.

Technical Control Standards

The technical standards are documented technology specific controls for all the major platforms within the organisation. Within the technical standards are the step-by-step implementation procedures for the controls. This documented set of controls forms the baseline configuration information necessary to secure technology platforms.

Conclusion

Organisations can avoid most of the negative security related events, and actually improve information access for their extended user communities as well, if they develop effective information security management practices and the related technological security infrastructures. By viewing security not as a cost centre, but as an enterprise-wide strategic enabler issue, organisations can begin the process of improved information security management in this age of increasingly converging digital communications.

To learn more about how we can reduce your company's security risks, please contact:

Pongsak Achakulwisut
Partner
PricewaterhouseCoopers
66 (0) 2344 1120
pongsak.achakulwisut@th.pwc.com
www.pwc.com/thailand