

PRUDENTIA

Information Security Standards-based System and Methodology

Information Security Governance – Overview

Security threats to information assets are increasing. Organisations today have an obligation to comply with various industry related regulations and legislative requirements, and have a duty of care to safeguard their information holdings. They must provide credible assurance that they are doing so.

From a business perspective, organisations depend on their information. How effectively they manage and protect information assets can be critical to their survival. Various risks may affect the security – **confidentiality, integrity and availability** – of these assets. And, because it's impossible and impractical to achieve total security, the practise of sound information security governance is founded on the principle of effective risk management.

The overall objective of an information security program is to ensure that risks to an organisation's information are properly identified and effectively and efficiently managed. This emphasises that information security is a management issue and a matter that includes people, policy and process. It is not merely a technical problem. Deploying appropriate technical measures is necessary but insufficient to ensure continuing information security. When identifying possible threats, a broad 'business' approach must be taken when it comes to the value of an organisation's information assets. Identification and assessment of the main risks enables suitable management arrangements, key policies and roles and responsibilities to be established. These provide the information security governance framework. Once this framework exists, critical risks can be assessed more thoroughly and other risks considered through an appropriate methodology.

Standards-based Information Security Methodology

Prudentia has developed a **unique standards-based database and methodology offering** (including reports and forms). It specifically addresses the need for a simple and practical "step-by-step" approach to managing an information security program within an organisation.

The methodology has been designed using KnowRisk®'s "Method & Steps", is **aligned with the AS/NZ ISO 31000 Risk Management Standard** and has the **ISO 27000 international Standard series at its core**. It includes best practice that is built into its content thereby enabling it to practically form part of an overall information security governance framework. The standards for information security adopt a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security status.

PRUDENTIA

The heart of this methodology is the risk assessment and treatment process - the overall process of risk analysis, evaluation, treatment and control improvement - which benchmarks an organisation against the 11 security categories, 39 control objectives and 133 controls included in the ISO 27001 and 27002 documents. Most of the security controls will be applicable to all organisations and provides a minimum baseline or starting point for implementing an information security program.

This offering is aimed specifically at helping companies manage risk and alleviate the intensive and onerous ongoing compliance requirements of an effective information security program. It significantly reduces the complexity, time and cost in operational risk and control assessments. KnowRisk® enables dynamic real-time management reporting of the controls implementation status including cost management for all identified and managed risks throughout the organisation.

Value Proposition

The key value proposition of this offering is that it is **standards-based**. Governance is enhanced by making the process of **securing business-critical information** and compliance more manageable and practical in day-to-day operations. The process **establishes a culture of risk awareness amongst employees** and ensures that **sound risk management practice** is devolved throughout the operational level of the business. Compliance does not simply become a “tick-in-the-box” activity, but is **fully aligned and integrated with core business objectives and processes**. Information security risks are linked to business and organisation objectives. **There is assurance that the organisation’s information is well managed and secure.**

This is achieved by automating and integrating the assessment process into an employee’s everyday work related activities. The system can be quickly implemented in an existing work environment with minimal application and user training requirements. The use of “**Forms**” enables the administrator to present information for review, assessment and data capture to employees in a practical way that is familiar to them. They don’t have to change the way they work. As they already understand and are aware of the processes that relate to their duties and responsibilities, they can quickly and easily identify risks, review related controls and effect changes as and when it is appropriate to do so. They do not need to become “experts’ in the disciplines of information security and risk management.

Benefit

The result is that executive management can be **updated quickly and concisely** as to the current status of key information security risks and related controls and the manner in which they are being managed. This will afford them the **confidence and assurance** that **compliance is being practically managed** and achieved, **information assets are properly secured** and that **unwanted surprises do not eventuate!**