Assure4
Technology Assurance for your Enterprise

White Paper

Technology Risk in the Not for Profit Sector

April 2015

Introduction

The Not for Profit (NFP) sector is a very important part of our current society that provides support services for a wide variety of people. NFP's can vary in size from the small to the very large. They typically have tight budgets, limited internal resources, and place significant reliance on volunteers.

Enterprises in the NFP sector often deal with vulnerable people, people with a mental illness and people with medical conditions and other situations that can make their personal information sensitive. These enterprises also often rely on public benefactors and donations for a significant part of their funding. Information relating to these matters may be stored within the information systems of these enterprises.

The board and senior management of any enterprise are responsible for the data that is collected and stored by the enterprise in order for it to achieve its mission. Significant reliance may be placed on the capability of their limited technical resources, but in many cases the board and/or senior management of the NFP may not have the appropriate technical resources available to discuss their concerns relating to the risks associated with their information technology assets.

Regulatory Environment

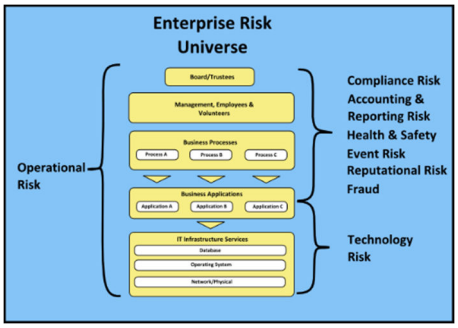
An NFP may be subject to a number of regulatory requirements such as Health Records, the relevant Privacy legislation and the federal government's Not for Profit legislation.

In July 2013, the Australian Charities and Not-for-Profits Commission issued governance standards for NFP's. These do not specifically require an NFP to adopt a risk management framework, however obligations placed on the governing body include:

- To ensure the financial affairs of the charity are managed responsibly;
- To act with reasonable care and diligence; and
- To act honestly and in the best interests of charity and for its charitable purposes.

Risk Management Program

Many NFP's have implemented Risk Management programs as a means of protecting the interests of the various stakeholders of the NFP. Like many enterprises, the Risk Management program will most likely be focussed on the financial and operational activities of the enterprise and not assess the risks associated with technology infrastructure that supports those activities.



Looking more closely at the operations of an enterprise, we see that the business processes utilised by the enterprise to achieve its objective rely on an underlying layer of technology infrastructure.

Any risks associated with the ownership and operation of the technology infrastructure should be reflected in the overall Operational Risk program, otherwise that program does not provide for the comprehensive management of risk in the enterprise. In too many enterprises today, this is not the case.

More recently, there has been an increased focus on the so called Cyberwar. Internet access provides a convenience for enterprise stakeholders, but access to the internet also means that the world potentially has access to your systems. Regulators are increasingly expressing concern about the potential for enterprises to suffer a cyber incident. Recent international experience has shown that the interests of the cyber criminals are not just focussed on the finance sector and big business, but they are looking at all organisations that may hold sensitive data, or that could be inconvenienced by a cyber incident.

A Risk Management program that includes an assessment of the technical environment will provide board members and senior executives with assurance that enterprise has taken appropriate steps to mitigate the risks associated with the utilisation of technology to enable the enterprise to achieve its mission.

About Assure4

Assure4 was established in 2004 to provide Technology Governance, Risk and Compliance services that focuses on the business. Assure4 has developed detailed methodologies to support the services they provide. These methodologies are customised to the particular requirements of each engagement as part of the project planning phase. Assure4 service offerings include:

- Technology Risk Management
- Information Security Management
- Application Control Reviews
- General Controls Reviews
- Business Continuity Management and Disaster Recovery Management
- Computer Forensics
- Pre-implementation Reviews
- Post-implementation Reviews
- IT Change Management Reviews
- IT Governance
- Project Risk Management
- Data extraction and analysis (CAATs)

To contact Assure4, call Tony Roberts on: 0411 229 396

Alternatively, you can email: tony.roberts@assure4.com