

IT RISK MANAGEMENT

IT Risk Management is more than just the latest jargon emanating from the IT sector. It is a complex issue, and this article provides an overview of its importance as a component of the operations process in a successful practice. It is particularly important with the release of the new RACGP standards (3 edition) which now has an emphasis on IT security in general practice.

Essentially, IT/IM Risk Management is the process of identifying risks/threats in the IT infrastructure of a business and implementing a strategy to eliminate/minimise the risks. Many businesses' IT infrastructure has developed on an ad hoc and needs basis. However, this exposes the business in numerous ways given that there are no consistent checks and balances in place. In particular, there are no assurances that critical business information and confidential patient information is protected. Section 4 of the Health Act (VIC), stipulates that the practice must provide "reasonable care" in relation to patient data. Whilst the term "reasonable" is contentious, what guarantee is there that the IT infrastructure of your practice fulfills the set requirements? Furthermore, extravagant expenses are often incurred when IT engineers are "investigating" somebody else's problem – how often does a hardware problem turn into a software problem and vice versa?

Enter IT/IM Risk Management. It provides a cohesive IT strategy designed to overcome the problems involved with ad hoc IT implementations. It can be specifically tailored to SME/SMB operation and is therefore cost effective, easy to implement and operate. And finally, any effective IT/IM Risk Management strategy needs to be reviewed on an ongoing basis. This is the only way to ensure that potential risks and problems are eliminated and/or minimized. The ongoing strategy translates in an increase in business efficiency and productivity, cost savings and peace of mind.

The following is a sample of the areas that may be incorporated in an effective IT/IM Risk Management Strategy for your practice:

- Patient Access Control
- Server Administration Control
- Anti-Virus Policy
- Email/ISP Policy
- Firewall Policy
- Intrusion Detection Policy
- Standard Operating Environment (SOE)
- Backup/Disaster Recovery/ Data Integrity and Redundancy Policy
- IT/ Site Documentation Policy
- Preventative Maintenance Policy

By Jim Doumakis
Jose and Associates www.jose.com.au jdoumakis@jose.com.au 03 9850 1350

© Copyright

The material contained within this document or file, the software, the design, the text, the processes, the systems, the tables, the compilation expressed in words, figures or symbols, the logic and the graphics comprised in this document or file as well as the selection and layout of this document or file are owned or licensed by Jose and Associates P/L and protected by the laws of the Commonwealth of Australia and the State of Victoria, including copyright laws. You may view and utilise this material for non commercial purposes only. Apart from this use or any use permitted under the Copyright Act (Cth) 1968, all other rights are reserved. You must not otherwise reproduce, transmit (including broadcast), adapt, distribute, sell, modify or publish or otherwise use any of the material except as permitted by statute or with the prior written consent of Jose and Associates P/L.