IT Risk Assessment Checklist

The checklist contains a number of elements each of which addresses a different aspect of computer security or risk and is important for protecting your organisational data and computing resources. The elements are presented below in the initial checklist, each with a question to prompt consideration.

After reviewing the element, record your initial assessment by checking the appropriate box on the checklist:

- **OK** - the element has been addressed by the organisation action or policy. All the detailed questions can be answered affirmatively.
- **Review** - The basic issue has been addressed, but further review is warranted. Not all the detailed questions can be answered in the affirmative.
- **Requires Immediate Attention** - The element has not been addressed or recently reviewed. Few, if any, of the detailed questions can be answered in the affirmative.

Upon completion, the checklist provides a profile of your organisation's data and computing resources security. Those elements assessed as "Requires Immediate Attention" constitutes the organisation's primary security vulnerabilities and should receive prompt attention. A majority of "Review" or "Requires Immediate Attention" assessments suggests the organisation would benefit from a more systematic risk assessment and analysis.

Element	OK	Review	Requires Immediate Attention
Physical Security • Is our computing equipment properly secured? • Is there public access to our systems – and is it secure?			
Account & Password Management • Do we ensure only authorized personnel have access to our computers? • Do we require and enforce appropriate passwords? • Do we have appropriate permissions on folders and/or files?			
Virus Protection etc. • Do we use, and regularly update, anti-virus software? • Do we use and regularly update anti-spyware software? • Do we have anti-spam measures in place?			
Data Backup and Restoration • Do we periodically backup individual and organisation's data? • Do we test restoring data from backup media? • Do we keep backups offsite? • Do we keep onsite back ups in a secure, fireproof area?			
Operating Systems • Are the operating systems we use on our workstations and servers updated with current security "patches" and service packs?			

Element	OK	Review	Requires Immediate Attention
Application Software • Are our common applications (e.g. databases, accounts package) configured for security?			
Confidentiality of Sensitive Data • Are we exercising our responsibility to protect sensitive data under our control?			
Disaster Recovery • Do we have a current disaster recovery plan? • If we have one, has it been tested?			
Security Awareness and Education • Do we have safe computing policies and procedures in place? • Is our management committee/board aware of the issues? • Are we providing information about computer security to our staff?			
Network and server security • Do we have a firewall on our broadband connection? • Does our server have redundancy e.g. mirrored hard drives, RAID, redundant power supplies? • Is our network fully documented? • How good are we at managing our user accounts e.g. deleting ex-staff members accounts, changing passwords regularly? • Is our wireless network secure? • Is our remote access/VPN secure?			

Email security • Do we have an email policy (possibly as part of an Acceptable Use Policy)? • Is confidential email being encrypted? • Are our staff aware of phishing attacks and what to do? • Do our users know what to do if we receive a potential virus attachment			
Mobile data • Are staff using mobile devices such as USB memory keys, hard drives, PDAs, smartphones etc aware of the security implications?			
Hardware failure • Do we have anyone we can contact in case of hardware failure? • Is our support contract good enough to withstand a serious hardware failure			
Hosted services • Is our website account securely password protected? • Is our website backed up by the host provider? • Are we aware of our domain registration details including due payments?			

Checks carried out by _____

Date _____