



## DTSL Totality Business Systems Checklist

### What is the checklist aiming to do?

Assist in:

- Identifying risks to business operations
- Avoid loss or minimise loss If a loss event occurs
- Prevent unauthorised system access and use of resources.
- Protect against injury

It is not possible to eliminate every possible danger

### The process:

There are four basic steps:

1. Acknowledge and identify risks prioritise risks
2. Select appropriate strategies to avoid risk
3. Evaluate results
4. Revise strategies

The following covers a number of areas for consideration, but can easily be extended

- Computer System Support
- Do you have a support agreement in place?
- What should the response time be?
- Do you use in-house IT support personnel?
- If yes, are their skills being kept up to date?
- What happens if they leave?
- Is there a contingency plan?
- What if IT staff are sick, is there someone to cover?
- **Insurance**
  - Is your computer equipment insured for fire, flood, theft, etc.?
  - Have you insured against data loss in the event of a disaster?
- **Disaster Recovery** - Is a disaster recovery plan in place?
- **Fire** - Does your Fire Alarm system provide sufficient cover?
- **Anti-Virus Protection** - Do you have anti-virus / anti-spyware software installed on ALL computers including laptops?
- Do you receive and install updates?
- What plans are in place to get help and or assistance for recovery?
- **Power Failure / Surges**
  - Do you suffer from electricity power failures?
  - Is critical equipment (ie server) protected by a UPS (Uninterruptible Power Supply)?
- **Computer Hard Disk Protection**
  - Do your file servers have protection against hard disk failure apart from a backup?
  - Do the hard disks have a level of RAID implemented?

Level 4, Citylink House  
53 Boulcott Street  
Wellington

Phone (04) 499 7534  
Fax (04) 499 7535  
Email [service@dtsl.co.nz](mailto:service@dtsl.co.nz)  
Web [www.dtsl.co.nz](http://www.dtsl.co.nz)



- **Data Security**
  - Is data theft covered in your employment contracts?
  - How do you protect sensitive commercial or confidential data?
- **Data Storage**
  - Do you have adequate data back up
  - Procedures in place?
  - Do you have a fire proof safe for on-site data storage?
  - Are further copies kept off-site?
  - When was the last test restore done and logged?
  - Are the back-up procedures documented?
  - Sources?
  - Who is allowed to delete data?
  - Who is responsible for archiving data?
- **Program Applications**
  - Do you have adequate data back up Program Applications
  - Who controls access to company software?
  - Do you have the right number of software licenses for each application?
  - Is all software purchased (including licenses) recorded on the company asset register?
- **People**
  - Do your Health and Safety procedures cover use of computer equipment?
  - Are there documented policies and rules re use of computers (eg access to computer based pornography or prohibited adult material?)
  - If computer equipment is loaned to staff (eg PC's, printers, notebook computers, PDA's etc). Are guidelines documented for the employees 'duty of care'?
- **Physical Security**
  - Do you have a security alarm system installed?
  - When were the codes last changed?
  - Who locks up at night?
  - Who has keys to the offices?
  - What happens if a key holder leaves the company?
  - Is the key holder list up-to-date?
  - If you recently took possession of new office space have the locks been changed?
  - Are laptops or similar left in vehicles, how are they secured?
- **Computer System Access**
  - Do you have a documented security section in the company IT policy?
  - Who has access to what, when and at what level (eg: Read-only)?
  - How often are they changed? Is this frequent enough?
  - Who knows the master (e.g. Administrator's) password?
  - Do screen savers require passwords to be re-activated?
  - What happens to passwords when staff leave the company?
  - Would you know if system security had been breached remotely?
  - Would you know if a breach of system
  - Do you have intruder surveillance activated on your network system?
  - Is there a software and/or hardware firewall in place?
  - Who has access to the firewall configuration?
  - Do you have anti-spam email software in place?