Community Links with Two Non-Profit Organisations: Technology Problem Solving or Proper Risk Management?

Christo Potgieter
Wintec
christo.potgieter@wintec.ac.nz

Jannat Maqbool
Wintec
jannat.maqbool@wintec.ac.nz

Abstract

This paper shares learning from initiatives by one tertiary institution to add value for two community organisations. Looking externally, Non-Profit Organisations (NPO) internationally and in New Zealand face significant challenges to enhance capacity for improving operations and community service (Thornton, 2009). The purpose of the project was to advise them on technical IT (Information Technology) matters, and so an assessment instrument was developed from ITIL (Information Technology Infrastructure Library) and other sources that are simple, generally available and free. Early field activities exposed the need to fully appreciate the operating challenges faced by NPOs and the accommodation of unique situation of each in consultation. It seems important for tertiary institutions to adjust approaches for the unique needs of NPOs, including accommodating sophistication but without available funding. Practicing auditors and consultants on risk management might consider covering the implications of increased use of Information Technology readily.

Key words: Student outcomes, completions, pass rates, examination, predictors, predictive efficiency

Introduction

Challenges for tertiary institutions and Non-Profit Organisations influenced this project. Fullan and Scott (2009) described broad changes internationally taking place in the tertiary environment, such as opening of access for students, changes in funding, growth of the export market, user pays with changing patterns of participation, changing expectations of students and maintaining academic standards. They carefully describe aspects of leadership roles involved in improving the alignment of tertiary institutions with the external environment.

The matter of challenges has also been explored in presentations at New Zealand conferences by Potgieter & Ferguson (2009). In some regards some institutions might already be far down the required road with changes but there are many things to do. A key aspect of the change is the enhancement of practice of frequent review, for alignment.

One of the important matters increasingly expected by Tertiary Education Commission (TEC) in New Zealand, is close alignment with industry. This covers a wide spectrum of matters, including ensuring qualifications are aligned with industry needs and close collaboration. Fulfilling roles from areas of strength in order to benefit the broader community, is highly valued. This aspect of transfer for upliftment, is one that Wintec strongly pushes via its strategy on Research, Development and Knowledge Transfer. One of the key aspects in this plan is delivering project-based problem-solving services to organisations. This paper summarizes the aspects of knowledge transfer and experience in doing this first project of the institution.

The environment includes various communities with a wide range of characteristics. While collaboration with the various industries is important, one should not neglect the "Not-For-Profit" (NFP) or "Non-Profit Organisations" (NPO). These entities are usually less able to compete with profit-making organisations for resources of tertiary institutions, starting from a weaker financial position. Wikipedia defines and describes these organisations as ones who do not distribute surplus funds to shareholders, rather using it to further pursue goals of the organisation. Examples include charitable organisations, trade unions and public and organisations, excluding government and its agencies.

Wikipedia also describes the challenges faced by NPO's, namely capacity building, Founder's Syndrome and Resource Mismanagement. Limited and unreliable external funding for operations especially impacts negatively on the spectrum of staffing processes and practices. Weak staffing capabilities and practices even impact on resource management, apparently contributing to increased risk exposure for the organisation. It would however be fair to say that this risk most often viewed as unacceptable, could be caused by lack of accountability but is most often caused by lack of skills of staff or very high workload typical of environments with volunteers.

The situation in New Zealand seems to be summarized in a key report that follows from a national survey of NPO's every two years. From the most recent report by Thornton (2009, p3): "Despite the current economic conditions there is no change to the three most challenging issues facing the Not for Profit sector: financing the activities of the organisation; fundraising; and the role of the board and other governance issues". Regarding technology, it is noted that "Website management and maintenance is an increasingly significant issue for organisations with 17% of respondents listing it as

one of the three most significant issues, up 8% from 9% in 2007" (p5). No mention is made of a Board Committee for IT (p17) and IT not mentioned anywhere else in the report.

The New Zealand Department of Internal Affairs provides useful reference material for the many community organisations in New Zealand. The Community Resource Kit (2010) is a practical "hands-on" resource to help organisations to get started and to develop good practice in the voluntary sector environment. Of twelve sections, one provides information on the use Information Technology, just the very basics of planning, obtaining and using it.

Obviously organisations vary in their use of IT, so dependence on IT might be low or even non-existent for some NPO's. In fact, IT is not even mentioned in the Code of Governance for the Australian Community Sector (2008), so it is most likely not very important for governance considerations and therefore probably operations. However, it is increasing and some NPO's have become very dependent on IT for daily operations. Considering a range of possible implications of failure in IT, it would be prudent to formally assess risk regarding IT and manage it appropriately.

One of the guidelines for practicing Chartered Accountants in Canada (Lindsay, 2009) includes IT as one of eight themes. Under question "What are the major risks and uncertainties facing the organisation?" is an example called "Inability to perform critical functions that depend on technology" (p7). Clearly they see aspects of the use of IT as a risk for NPOs that needs to be managed. Considering capacity building challenges mentioned in Wikipedia and the complexities with risks from ever-changing IT environment, it would be understandable if in-house skills re IT are not available – hence the need for oversight by governance structures.

From the above one could see good reason and opportunity for tertiary institutions to constrictively contribute to NPOs as matter of community service. Specific aspects could include knowledge transfer to solve problems and development to improve staff capability. These could improve resource management and reduce operating risks for the NPOs.

Background to this project

As part of Wintec's ongoing focus on research and "Technology Transfer" as a strategic priority and following a recent internal review of research processes and policies the organisation has developed a "Research, Development and Knowledge Transfer" (RDT) model designed to, amongst other things, improve Wintec's connection with the applied research needs of the region and shift some of the institutes RDT resource into the hands of the community.

This model includes a scheme whereby organisations are able to commission work into areas of their interest. The scheme attracted several ideas for the pilot with one idea involving a look at whether

businesses have adequate business continuity and disaster recovery plans in place. This was one of four ideas selected to have a research proposal developed, funded and implemented. Given that this project was a first for Wintec and considering available timeframes, the scope of the project was narrowed to ICT continuity within the local NFP and/or community services sector.

A draft high-level project plan was submitted in September 2009 with the detailed project plan being reviewed and approved in October 2009. The review commenced shortly after and was finalised with the presentation of a report on findings in December 2009.

Information and communications technology (ICT) continuity requires much more than just ensuring information is 'backed up' regularly - it is about identifying mission-critical business processes and having steps in place to ensure their continuance and/or restoration during and after a natural or man-made disaster. Such processes not only rely on hardware, software and communications infrastructure being available but also on stored data and/or information as well as people with the required skills and knowledge to operate the information and communications technology. Well documented procedures are fundamental as is having such procedures readily accessible when needed.

Larger enterprises are able to invest considerable sums of money in ensuring they are adequately prepared however such funds may not be available to smaller organisations such as those in the not-for-profit (NFP) and/or community services sector but for many such organisations business, including ICT, continuity is just as important and arguably more so given their importance to the wider community.

Aside from funding, many aspects of existing guidelines or resources available for use in establishing an ICT continuity plan may not be relevant to these organisations and New Zealand itself given its many geographical features may also present further challenges to ensuring adequate ICT continuity requirements. There may also be requirements specific to such smaller organisations.

Preparing for the project

The review firstly identified appropriate assessment criteria and then assessed two local NFP sector organisations against these criteria to ascertain whether they had made adequate provisions for ICT continuity, including those related to risk mitigation and documentation. The resultant findings were then reported to the client organisation and Wintec. The client organisation may then refer to this material to assist in ensuring adequate safeguards are in place to allow the organisation to continue to serve the community in the event of a major disruption. The review itself was limited to two local NFP sector organisations and where possible their selection was based on a moderate to heavy reliance on ICT and their capabilities in terms of establishing a sound and effective ICT continuity (and restoration) plan.

Furthermore, although wider business continuity practices were discussed or referred to during the review, the review was limited to an assessment of ICT continuity only. That is, it considered the continuation of the ICT including operational resource requirements but did not for example consider the availability of food and water should staff be unable to leave the premises in the event of a natural disaster, or whether the building itself would be accessible to staff in such a situation. These latter elements would fall within an organisation wide business continuity plan.

The project involved a review only, not an audit, and as such detailed observation and testing to validate review responses offered by members of the client organisation and/or associated parties was excluded from the scope of the project.

Assessment of the resultant findings and the implementation of opportunities for improving existing ICT continuity arrangements within the organisation or the application of review findings to update relevant course material at Wintec also did not fall within the scope of the project.

The project: Approach and Instruments

The initial phase of the project was to identify appropriate assessment criteria. This involved a considerable amount of research given the numerous resources available in both hardcopy and on the Internet covering the topic of business continuity and disaster recovery, as well as the need to gain an understanding of the local not-for-profit sector and any requirements or considerations specific to organisations within this sector.

In response to increasing pressure to cut costs, increase efficiency and meet set timeframes organisations can be seen to be increasing their reliance on information and communications technology (ICT), and as this reliance grows so does the associated risk and hence the need to have procedures in place to continue and recover operations in the event of a minor or major interruption impacting the organisation. However, it may be easy for organisations to become complacent believing that nothing will happen and that an investment in being able to cope with an incident that is not likely to occur is not a good use of already limited funds. There may also be a lack of understanding as to how critical ICT is to delivering the organisations services. However, maintaining as close to ‘business as usual’ as possible, should an interruption occur, may not necessarily require a huge investment of time or money. It is simply about understanding the organisations individual requirements and then establishing solid continuity measures, including risk mitigation practices and having an ongoing management plan in place.

There are two elements, business continuity and disaster recovery. The first phase included understanding the distinction between the two. The research indicated that continuity planning and management differed from disaster recovery planning in that the latter was concerned with needing to

restore the original business facilities following a major interruption, where as continuity planning was focused on ensuring critical business areas and services continued to operate throughout the disruption (Security+ Certification for Dummies, p 271). Business continuity management refers to business continuity in the wider sense incorporating the whole organisation and all services upon which the business is dependent, where one such service is ICT (IT Service Continuity Management and Disaster Recovery Best Practice Handbook, p18).

There was certainly no lack of resources on the topic of business continuity providing not only definitions and general guidelines but also self assessment tool kits, ready to use templates, and detailed recommendations. The material was based mostly on widely applied measures including those within the Information Technology and Infrastructure Library (ITIL) framework and the ISO 27000 series, defined as the "Business Continuity" standard. There were also several organisations offering to develop business continuity plans for any organisation for a fee. It would be difficult however to simply apply what was available to any given organisation without firstly understanding the organisations ICT and service environment and assessing continuity requirements including maximum allowable downtime. In the absence of a strategy addressing these aspects the organisation may under or over cater to actual business needs thereby risking a misallocation of resources and/or adversely impacting stakeholders.

In considering the available resources it was important to keep in mind that the main purpose of ensuring effective continuity management was to ensure an organisation could continue to operate, serving its client base and other 3rd party stakeholders, during a disruption. The focus was therefore on business services and, albeit fundamental, technology was an underlying factor to the provision of such services. The project was also limited to a consideration of ICT continuity only. The ITIL framework focuses on transforming the management of ICT from a silo based re-active department to a service based pro-active driving force aligned with business objectives and goals. It therefore made sense to base the assessment criteria on the framework's ICT service continuity management module. The four stages of the business continuity lifecycle (Refer Appendix 1) were then further expanded to include other guidelines from the research including criteria that would be suitable for a small organisation and possibly specifically to the not-for-profit sector.

From the above a range of review areas regarding ICT continuity management were identified: Policy and Scope; Requirements and Strategy; Implementation (Risk mitigation, Emergency Response Plan, ICT Continuity Plans, Documentation) and Operational Management for Assurance (Format and Distribution, Education and Awareness, Review and Audit, Testing, Change Management, Training). Each was awarded a rate and point, as is described in the report below. As a first project for both Wintec and the particular organisations, this simple approach with subjective views could serve as base for further refinement.

Overview of the organisations for use during assessment

This project considered the ICT continuity requirements and practices of two organisations, called AAA and BBB, chosen from the not-for-profit sector given the importance of this sector, the limited resources organisations within this sector and the opportunity it presented for Wintec to contribute to the wider community. A further consideration in selecting the two organisations was their moderate to heavy reliance on ICT to deliver business services.

AAA is a disability services provider, based here in Hamilton, providing both contracted and charitable services nationwide. The organisations vision is to enhance independent living for its clients. BBB was formed over 20 years ago and is today a leading service provider assisting people with intellectual disabilities and their families throughout the Waikato.

The CEO at each organisation was contacted to introduce the project and both responded positively nominating relevant staff within the organisation to be available to provide input. It was apparent that each CEO was committed to ensuring adequate ICT management. An initial meeting was held with the individual responsible for ICT management within the organisation and in both cases they were a member of the senior management team and were also not from an ICT management background but managing the ICT portfolio as one of their many key responsibilities. Each senior manager was provided with an engagement letter for review and sign off which introduced the project, its purpose and briefly summarised the review plan and specific exclusions and conditions. In both cases the managers acknowledged that they were keen to participate in the activity and to benefit from Wintec's research and community focus. The meeting then progressed to a high level overview of the assessment criteria to identify other staff and also 3rd parties who would be needed to provide input in order to gain an understanding of the ICT environment, risk mitigation practices and ICT continuity.

Following on from this initial contact and prior to commencing the actual review an understanding of the organisation, critical business services and the ICT environment was gained through discussions with appropriate staff, suppliers and partners.

In BBB's case the Business Support Manager employed an ICT Administrator who was responsible for the efficient management, maintenance and day to day operation of the organisation's ICT. The ICT Administrator at BBB is supported by ICT-BBB (an ICT vendor company). However, AAA outsourced their ICT management and maintenance to ICT-AAA (another ICT vendor company) and had done so for over 10 years. Although the ICT Administrator at BBB is supported by ICT-BBB the support very much excludes day to day responsibilities, unless ICT-BBB is required to assist or to stand in for the ICT Administrator urgently, which is a considerable part of the role. These tasks are prioritised as much as possible however even then not everything is attended to as ICT operational and

procedural documentation was largely non-existent and a number of arguably fundamental risk mitigation practices had not been put in place. There is however awareness within the organisation of the ICT services and their importance and an understanding of the role of the ICT Administrator is achieved through regular interaction with staff and support responsibilities.

At AAA, a member of the ICT-AAA team visits the office at least 2 to 3 times a week checking in, reviewing logs and/or undertaking maintenance tasks. However interaction with staff and day to day operations within the organisation is limited. ICT-AAA are able to provide resources including back up resource as required to cater to AAA's requirements however given ICT management is outsourced although there is an awareness within AAA as to services being highly reliant on ICT there is very much a disconnect between ICT management and internal operations. For example in terms of ICT continuity there was some confusion between what ICT-AAA thought was happening with daily backup tapes and what actually was taking place or thought to be taking place at AAA.

Both organisations are heavily reliant on the individual responsible for ICT management having 'things under control' and effectively managing the relationship with suppliers, internal staff in the case of BBB, and related stakeholders. However, in both cases major decisions regarding the ICT environment, including ICT continuity did involve the CEO and in AAA's case the senior management team was also consulted. At AAA a meeting was held with the managers responsible for three services identified as critical to the organisation as well as the Account Manager at ICT-AAA, the Managing Director of another ICT vendor organisation and two additional staff members responsible for general business administration and finance. At BBB it was possible to meet with the Business Support Manager and ICT Administrator as well as discuss emergency response and ICT continuity overall with the CEO and briefly cover various general workflow aspects with the Human Resources Manager. Respondents at both organisations were happy to make themselves available for the review and provide input. It was useful to talk to various levels of staff and also to relevant external parties as it provided different perspectives and views of what should be a uniform approach to ICT continuity. A more detailed review would benefit from discussion with more hands on staff to ensure wider awareness and assess compliance at an operational level.

Observations about the organisations

The review addressed the 5 components of ICT service continuity management as provided within the ITIL framework. Respondents were asked a number of questions related to each area and as appropriate additional questions and or discussion arose including with respect to wider elements of continuity management. Observations were also made during visits to the offices. Table 1 below provides a summary of the assessment findings.

The assessment was not an audit and was therefore largely subjective, based on an understanding of the business and ICT environment gathered through interviews (and follow up questions) with relevant staff, partners and suppliers of the client organisation as well as a minimal amount of observation. Detailed observation and testing to validate responses was not included within the scope of the review due to time limitations.

	AAA		BBB	
Review area	**Assessment**	**Points**	**Assessment**	**Points**
• **Policy and scope**	Partial	1	Partial	1
• **Requirements and strategy**	Partial	1	Adequate	2
• **Implementation**				
• Risk mitigation	Partial	1	Partial	1
• Emergency response plan	Partial	1	Adequate	2
• ICT service continuity plan	Inadequate	0	Inadequate	0
• Documentation	Partial	1	Inadequate	0
• **Operational management for assurance**				
• Format and distribution	Partial	1	Partial	1
• Education and awareness	Partial	1	Partial	1
• Review and audit	Partial	1	Partial	1
• Testing	Adequate	2	Partial	1
• Change management	Adequate	2	Adequate	2
• Training	Adequate	2	Partial	1
Overall (out of 36)		14		13
Average	Partial	1.16	Partial	1.08

Rating & points		**Assessment**
Complete	3	Agreed with more than 100% of the appropriate assessment criteria
Adequate	2	Agreed with between 75% and 99% of the appropriate assessment criteria
Partial	1	Agreed with between 50 and 75% of the appropriate assessment criteria
Inadequate	0	Agreed with less than 50% of the appropriate assessment criteria

Table 1 – Summary of the assessment findings.

A detailed assessment of each organisation was provided to each, and included an overview of existing practices and provisions as compared to appropriate assessment criteria for ICT service continuity management. The assessment was accompanied by any relevant recommendations where appropriate. However, any identified opportunities for improving existing ICT continuity arrangements were fully covered by disclaimers regarding “at own risk” – the client organisations were invited to assess and independently evaluate recommendations prior to considering their implementation.

Part 3 of the business continuity lifecycle addressed ‘Implementation’ and included a review of risk mitigation practices. This involved a brief risk analysis whereby relevant staff and/or suppliers were asked to assess the probability of a list of incidents occurring and if they did occur the likely business impact, with both items requiring a ‘high’, ‘medium’ or ‘low’ assessment. Albeit brief this enabled the identification of areas where the organisation should focus risk mitigation efforts. As the review progressed various industry standard risk mitigation practices were discussed however in the absence of a detailed analysis and an assessment of acceptable levels of risk it was difficult to provide a list of detailed recommendations appropriate for the organisation and ICT environment. Albeit high level, the analysis did reveal a number of deficiencies with respect to the ICT service continuity framework and a number of general recommendations were identified with respect to specific risk areas.

The ICT Administrator at BBB also had access to a recent audit document provided by ICT-BBB which identified similar areas of concern however given existing workloads it had not been possible to date to implement such initiatives. BBB may therefore benefit from a fixed term project with additional resource focused on completing a detailed risk analysis and implementing appropriate risk mitigation practices, involving external parties and internal stakeholders as appropriate. The same could be said for AAA however given their ICT management is outsourced a more suitable approach maybe to discuss requirements with ICT-AAA for additional service and support resource.

Concluding comments about the organisations

The review highlighted the need for additional investment in ICT service continuity management at both organisations and a number of related areas that would benefit from more in-depth analysis. For example, risk mitigation, emergency response procedures and documentation practices including the implementation of a documentation framework to ensure effective ongoing management and maintenance of the ICT environment and operational policy and procedural documentation.

Managers at AAA had confidence in the Senior Manager responsible for the ICT portfolio and their effective management of the portfolio but did feel that ICT continuity (and business continuity overall) had not been addressed as much as perhaps needed to be given the organisations ever increasing reliance on ICT and the importance of services provided by the organisation. It was apparent that the continuity of services was a priority at BBB given they had recently undertaken a contingency planning exercise in the event that they may be widely impacted by an epidemic. A focus on ICT elements was however limited to noting that they were the responsibility of the Business Support Manager as a member of the Emergency Response Team. It was not apparent that AAA had undertaken a similar exercise however it was clear that some thought had been given to ICT not being available for whatever reason as regular electronic backups had been put in place and ICT-AAA was looking to move to further improve overall back up management practices in the near future. BBB is

however heavily reliant on the ICT Administrator given the Business Support Manager only assumed the role in May of the same year and at the time of this review had not been fully informed as to some aspects of the ICT environment and in particular some ICT continuity and risk mitigation practices.

Feedback in both cases indicated that the review was well timed given that in BBB's case the organisation was in the process of implementing a number of ICT initiatives that would result in a considerable improvement to the existing ICT environment and ICT services and AAA had recently increased its reliance on ICT to manage the delivery of critical business services and was also looking to send out a RFP to relevant suppliers in the new year to ensure effective management of its ICT environment. Wintec's involvement was also well received given polytechnics are generally viewed as having a more practical approach to areas of study and therefore respondents were confident that both the review itself and any outcome would be beneficial in themselves.

The benefit of an independent 3rd party addressing the review was somewhat apparent as the lack of familiarity with the organisation resulted in questions and commentary that may not have been approached had the review been undertaken internally. The review prompted additional discussion with respondents indicating elements of a process/procedure that were perhaps routine with less apparent association with ICT continuity or ICT risk mitigation. Respondents started seeing matters from an outsiders perspective, identifying that their closeness with a process or procedure might have caused them to become complacent as to whether ICT continuity and risk mitigation requirements had been adequately covered. It was also important that the reviewer was not an expert as such in ICT continuity as it enabled staff to be more involved and therefore benefit more.

It is envisaged the review itself and review findings will prove beneficial to the organisations involved however given the limited scope of the current project and the many areas of ICT management and business continuity in the wider sense that were not considered there is definitely an opportunity for Wintec to approach these two and other organisations in the future with respect to further reviews in order to further benefit the sector and the members of the community that they serve.

Observations about this project for community alignment

It was very noticeable how these two community organisations are increasingly reliant on properly functioning Information Technology. In fact, disaster situations will significantly constrain their daily operation and community service. It is not clear that the extent of exposure was previously understood by senior staff, but it is likely not to feature high on priority lists in the very resource constraint environments of each organisation. It might be valuable to cover risk exposure due to Information Technology, in the annual audit processes typically conducted by chartered accountants, as recommended in the guidelines for practicing Charted Accountants in Canada (Lindsay, 2009).

This project helped the organisations to learn about their situation and Wintec to learn about community, specifically NPOs. For example, it confirmed the pressure NPOs experience regarding lack of resources and skills shortage, thereby identifying areas where Wintec might also contribute in future. It was also noticed that the organisations could make some changes once they understood risks and possible solutions. Also, collaboration on the project resulted in relationships being formed, which is leading to further projects. In this way, skilled staff from this tertiary institution can continue to be involved in solving industry problems via knowledge transfer.

Involving several organisations complicated the project significantly, since it became clear that NPOs could differ significantly. It was intended to have three NPOs', but the withdrawal of one NPO for internal reasons, was very fortunate in the end. Understanding the unique situation of each organisation in order to ensure value via relevant problem-solving approaches, required a noticeable amount of extra time. The approach to use generally available free material wherever possible was good, since it helped with simplicity, but the fact remains that assessment of two very different organisations complicated the project.

Conducting the project exposed the need for project management methodologies that significantly emphasize situation assessment, business analysis and feasibility analysis before so-called solutions are applied. Spending sufficient time during early stages of the project to understand business needs in order to avoid "scope creep" with associated project failure, is one of the big challenges for systems development. These small projects require more than one A4 page with project motivation, several days should be spent to scope the project properly after gaining an understanding of the field situation.

Acknowledgement

This project was funded by Wintec through the Voucher Scheme of the Research, Development and Knowledge Transfer (RDT) initiative, up to $5,000 (total cost). The project would also have not been possible without the participating organisations and the willingness of both management and employees to contribute to the review sharing their thoughts and responding to the questions raised.

References

Arnell, A. (1990). Handbook of Effective Disaster/Recovery Planning, McGraw Hill.

Bennett, J. (2010). Leveraging ITIL to improve business continuity and availability. Retrieved from http://www.continuitycentral.com/feature0586.htm.

Community Resource Kit. (2010). Publication by Department of Internal Affairs, New Zealand . Accessed on 27 July 2010 at http://www.community.net.nz/how-toguides/crk/

Fullan, M., & Scott, G. (2009) *Turnaround Leadership for Higher Education*. San Francisco: Jossey Bass

Gregory, P. (2008). *IT Disaster Recovery Planning for Dummies*, Wiley Publishing.

IT Service Continuity Management and Disaster Recovery Best Practice Handbook. (2008). *Art of Service*. Retrieved from http://theartofservice.com.

Lindsay, H. (2009). 20 Questions Directors of Not-For-Profit Organizations Should Ask about Risk. *Chartered Accountants of Canada in association with Institute of Directors, 2009*. Retrieved from http://www2.unitedway.ca/UWCanada/uploadedFiles/Learn/20QuestionsNonProfitsShouldAskAboutRisk.pdf.

Miller, L., & Gregory, P. *Security+ Certification for Dummies*, Wiley Publishing.

Potgieter, C., & Maqbool, J. (2010). R&D Vouchers: Business Continuity of IT. Poster presentation at *1st Annual Conference of Computing and Information Technology Research and Education New Zealand, 6-9 July 2010, Dunedin, New Zealand*. Retrieved from http://www.naccq.ac.nz/index.php/conference-2010.

Potgieter, C., & Ferguson, B. (2009). Rebel with(out) a cause?! Presentation at annual conference of *New Zealand Applied Business Education*, Rotorua, New Zealand, 28-29 September 2009.

Steinburg, R.A. *Surviving ITIL*, Trafford Publishing, 2007

Thornton, G. (2009). Pressing issues impacting New Zealand's Not for Profit sector. *Grant Thornton not for profit survey 2009/2010*. Retrieved from www.grantthornton.co.nz

Wilder, D. (2008). *The new business continuity model, Version 1.0.*

Wintec Research, Development and Transfer Plan, May 2009.

Wintec Research Development and Transfer Plan – Scoping Paper, 2009.

Appendix 1 – Assessment criteria: ITIL, ITSM, ITSCM

The IT Infrastructure Library (ITIL), originally created by the UK government and adopted internationally as best practice for the provision of ICT services, is a series of documents organisations can use to adopt a service management approach to ICT effectively aligning ICT with the business. IT service management (ITSM) is concerned with the implementation and management of quality IT services to satisfy organisational needs. Focused on standardizing practices, ITSM can effectively mitigate human error and ICT failure, both of which are at risk of being the primary source of an interruption. Service level management is one of ten ITIL processes in Version 2.0 of the framework.

IT service continuity management (ITSCM) is another process within the ITIL framework. ITSCM supports the wider business continuity strategy by ensuring critical ICT services are available in a

timely manner following an interruption; until such time that standard levels of service can be restored (Servicing ITIL, p144). A critical service is considered in the context of business operations and goals as opposed to from a purely technological perspective. Furthermore, strategies and processes put into place as part of ITSCM must be based on a thorough analysis of organisational risk, costs and associated benefits (IT Service Continuity Management and Disaster Recovery Best Practice Handbook, p 60).

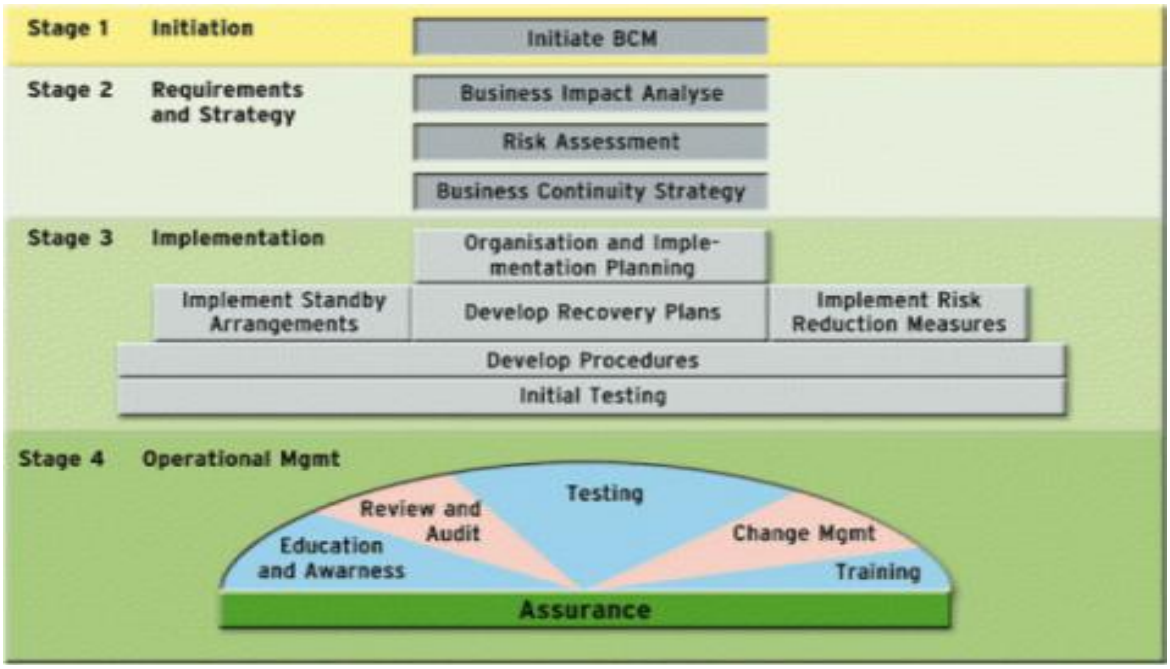

Figure 1 - The new business continuity model. Version 1.0 (Dan Wilder, 6 October 2008)

Figure 1 illustrates the four stages of Business Continuity Lifecycle as referred to in ITIL and applied in developing the assessment criteria used within this review (IT Service Continuity Management and Disaster Recovery Best Practice Handbook, p22).

In addition to the ITIL Version 2.0 framework, the following resources were referred to in developing the assessment criteria and risk mitigation matrix used within this review.

(ISO 17799) ISO 27002 - Code of Practice for Information Security Management: An information security standard originally published by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17999 and subsequently renamed as ISO/IEC 27002 (Wikipedia). The business continuity management component relates to protecting, maintaining and recovering business-critical processes and systems.

The New Zealand equivalent standard is NZS ISO/IEC 27002:2006: The ISO 27000 series is defined as the "Business Continuity" standard (The new business continuity model. Version 1.0) and lists certain existing standards including BS 25999 Business Continuity Management.

BS 25999 Business Continuity Management: A BSI's (British Standards Institution) standard in the field of Business Continuity Management (BCM) in two parts; the first providing a Code of Practice as a general guidance to establishing processes, principles and terminology; and the second, a Specification for implementing, operating and improving a documented Business Continuity Management System (BCMS) (Wikipedia).

Appendix 2 - Review plan

The objective of this review is to assess whether the client organisation has made adequate provisions for ICT continuity, including related risk mitigation and documentation, to ensure the continuance of critical business services in the event of a disruption.

Firstly appropriate assessment criteria were identified, including a focus on ICT continuity related risk mitigation and documentation. The assessment criteria were based on relevant elements of the ITIL Version 2 framework and further consideration was given to related industry standards and recommendations as outlined in the previous section. The review itself was undertaken as follows –

Area	Review
ICT service continuity management	Understand ICT continuity requirements Identify ICT specific aspects of any existing continuity management practices, including any documented ICT service continuity plan Compare practices to appropriate assessment criteria and assess Identify any opportunities for improvement
Risk mitigation	Identify - possible risks to the ICT environment, the probability of the risk occurring, the impact of the risk. (Identify any opportunities for improving existing risk mitigation practices associated with identified risks)
Miscellaneous	Additional points associated with business continuity and/or ICT specific continuity may arise for discussion/assessment as the review proceeds. In keeping with the methodology outlined in this document, where possible appropriate assessment criteria will be identified for comparison and findings will be summarized in a similar manner, including the identification of any opportunities for improvement.

Note - the assessment is not an audit and is therefore largely subjective, based on an understanding of the business and ICT environment gathered through interviews (and follow up questions) with and responses of relevant staff, partners and suppliers of the client organisation together with a minimal amount of observation. Detailed observation and testing to validate responses is not included within the scope of this review.