

ICT Office, Office of the Prime Minister

Executive Summary

Student Consultant, Kenrick Fernandes
Community Partner, Tepua Hunter

I. About the Organization

The mission of the ICT Division in the Office of the Prime Minister is to serve as a governmental authority in the area of information and communication technologies for all government bodies.

The Office began serving the Cook Islands government in 2003, and the placing it in the OPM was intended to strength its role as a body with governing authority. Despite being a small office faced by challenges including lack of confidence in its abilities, funding constraints and limited manpower, the office has been working hard to build relationships across government. The major activities undertaken by the office include: installing and maintaining hardware and software services for the OPM and other ministries, providing recommendations for IT related projects, providing system and end user support, working with ministries on internal technology requirements and providing training to staff members to facilitate capacity building.

The staff members of the office fulfill three different responsibilities of strategic planning, system administration, and end user support. Despite technology planning and management being carried out on an ad-hoc basis, the advanced competencies of the staff in their individual areas, complemented by the office's small size allow them to manage the technology systems for all seven divisions of the OPM. This involves managing integrated systems for email, file sharing, backup and internet access across multiple devices.

In this regard, the staff are also pursuing the latest technologies for their systems, including the cloud, as a means of dealing with bandwidth bottleneck issues and ensuring the maximum flexibility of the office in dealing with change of the times and expansion of the government. In addition, while more advanced systems for information management have been explored, none have so far met the required criteria. Business systems and related finance procedures are manually handled currently.

II. Addressing the Need for Reliability in Technology Systems

In the functioning of government today, digital technology is becoming increasingly important. In the Cook Islands in particular, with a vision to move to e-government, technology is set to form the backbone of governmental operations. Accompanying this increase in dependency on technology is a set of unique risks including technical errors, hardware failures and perhaps most commonly, user errors which can lead to loss of access to data or loss of availability of services. The importance of government in the functioning of a nation makes it clear this risk is one that must be mitigated and business continuity be ensured. The way to address this is through having a backup system that acts as a redundancy measure or safeguard against loss of availability. The Cook Islands are also under

threat of natural disasters which have wreaked havoc on other divisions of government in the past. The lack of backup systems in government has also been addressed in external audits, and thus the design and implementation of a backup system appropriate for the situation is a top priority.

The outcomes involved in the task of creating a national backup system were:

- Surveying of all government entities to determine the current state of individual backup systems
- Collaborating with Telecom Cook Islands to utilize the options provided by the private sector and enhance the relationship of the office with the monopoly
- Evaluating the present technology infrastructure according to the information to identify the available options for a national governmental backup system
- Identifying the requirements to be met by the system

Communicating information and recommendations regarding work undertaken to the development partner was obviously integral to this. However, since the tasks involved in the outcomes were undertaken by an external consultant, the risk remains of the project failing to have a champion to carry it through government. In addition, the relationships built were through the consultant, and a human resource will be lost with the departure of the consultant, making it documentation of all outcomes through the process necessary.

Based on the analysis conducted through the information gathering phase, the need to introduce a centrally managed system of hardware and software purchase, in bulk, for the purposes of distribution to all government entities, was found to be advantageous. This has been recommended, along with the necessary procedures and the associated benefits. Implementation of this system can lead to large savings across government in the area of IT expenditure, as well as reduced strain on the finance managers and IT personnel within each government entity.

Consulting Partner

Tepua Hunter
pua@pmoffice.gov.ck

ICT Office, Office of the Prime Minister
Rarotonga, Cook Islands
http://www.pmoffice.gov.ck

About the Consultant

Kenrick Fernandes
kof@qatar.cmu.edu

Kenrick is a rising junior in Computer Science at the Qatar campus. His interests include technology entrepreneurship, music, people, good food, design and community development. He enjoys working in environments that allows for a symbiotic relationship between people and technology.

ICT Office, Office of the Prime Minister

Final Consulting Report

Student Consultant, Kenrick Fernandes
Community Partner, Tepua Hunter

I. About the Organization

Organization

The mission of the ICT Division in the Office of the Prime Minister is to serve as a governmental authority in the area of information and communication technologies for all government bodies.

The office itself is located in the compound housing the Office of the Prime Minister and the governmental entities under its frameworks. The ICT office performs many duties towards fulfilling its mission including installation and maintenance of information and communication technologies (such as digital phone systems, email servers, and other software and hardware support) for all departments of the OPM, as well as for other ministries (those that require support or do not have qualified personnel in-house or on contract); providing recommendations for technology-related projects, and coordinating purchasing and upgrading of IT equipment.

The Office began serving the government of the Cook Islands in 2003, and the purpose behind placing it in the OPM was for it to have a strong foundation to strengthen its role as a body with governing authority. In the words of the community partner, it is still in an incubation period.

Despite being a small office supported by only 3 people, its long term goals including overlooking ICT for all government ministries, so as to standardize technology across government, ensure better usage of shared resources, mitigate unnecessary duplications and errors, cut costs through centralized (bulk) purchases, and facilitate better management of ICT assets.

Since its inception, the Office has been working hard to build relationships with the other governmental agencies, providing support and training, besides working up to a legal framework allowing them to occupy the role of overseer of IT for the whole of government. Some of the biggest challenges facing the office include constraints in terms of funding, capacity, staffing, and building confidence with the other governmental entities, especially in improving the perception of the office's role and capabilities. This lack of confidence translates directly to governmental expenditure, since ministries that lack confidence in the ICT office work directly with the private sector for IT support and purchases, thus eliminating the scope for better coordination and large-scale savings.

Facilities

The ICT office shares a reasonably sized cabin with the Climate Change division of the OPM. In addition to individual workspaces with desk and computers, a common area with a meeting room and seats is also part of the space. This cabin also includes the main server room for all sections of the OPM, and the space is adequate and well ventilated. Natural light and breeze ensure a pleasant working environment.

With regard to provision of utilities, the office is assured an advance warning (approximately 48 hours) from the ISP in case of internet outage, and has an alternate power source which is critical for uninterrupted supply.

While the office space is inviting and not crowded, physical security is an area that could use improvement. During the day, the security of the office is guaranteed by the belief that no one would be brazen enough to break in to the OPM, as well as the watchful eye of the many offices surrounding the ICT office. However, during the nights and on weekends, security is not tight, and despite locks on the door of the office, and on the server room door, forced entry and theft are very real dangers. Furthermore, due to the wood used in the cabin's construction, fire damage is a threat that has no deterrent built in.

Programs

As listed in the first section, the major activities of the office include: installing and maintaining hardware and software services for the OPM and other ministries, providing recommendations for IT related projects, providing system and end user support for technology under its supervision, and working with ministries on internal technology requirements such as databases/websites when appropriate. Yet another important function of the office is to provide training (both by spreading the word about trainings offered by regional organizations, as well as conducting its own) to staff members of all of the government's ministries, to facilitate capacity building in the ministries.

As of the present time, these activities directly support the mission of the organization, and in the future, it is foreseeable to have the office look towards the future of ICT in government as well, in terms of in-house development and technology upgrades. In the words of the partner, the main aim of the office at present is to work on building capacity within the ministries within the resource constraints.

Staff

Tepua's responsibilities include coordinating the dissemination of news and updates regarding ICT programs available in the region (Pacific countries and New Zealand) and ICT workshops being organized for the schools and ministries, reporting to regional organizations and funding agencies about long term projects, and providing reports to higher government authorities including the ministers for ICT and Telecom.

Mii's tasks include providing end user support – over phone and in person – and managing and providing training for the use of systems (such as Microsoft Office software) that are installed and administrated by the ICT office.

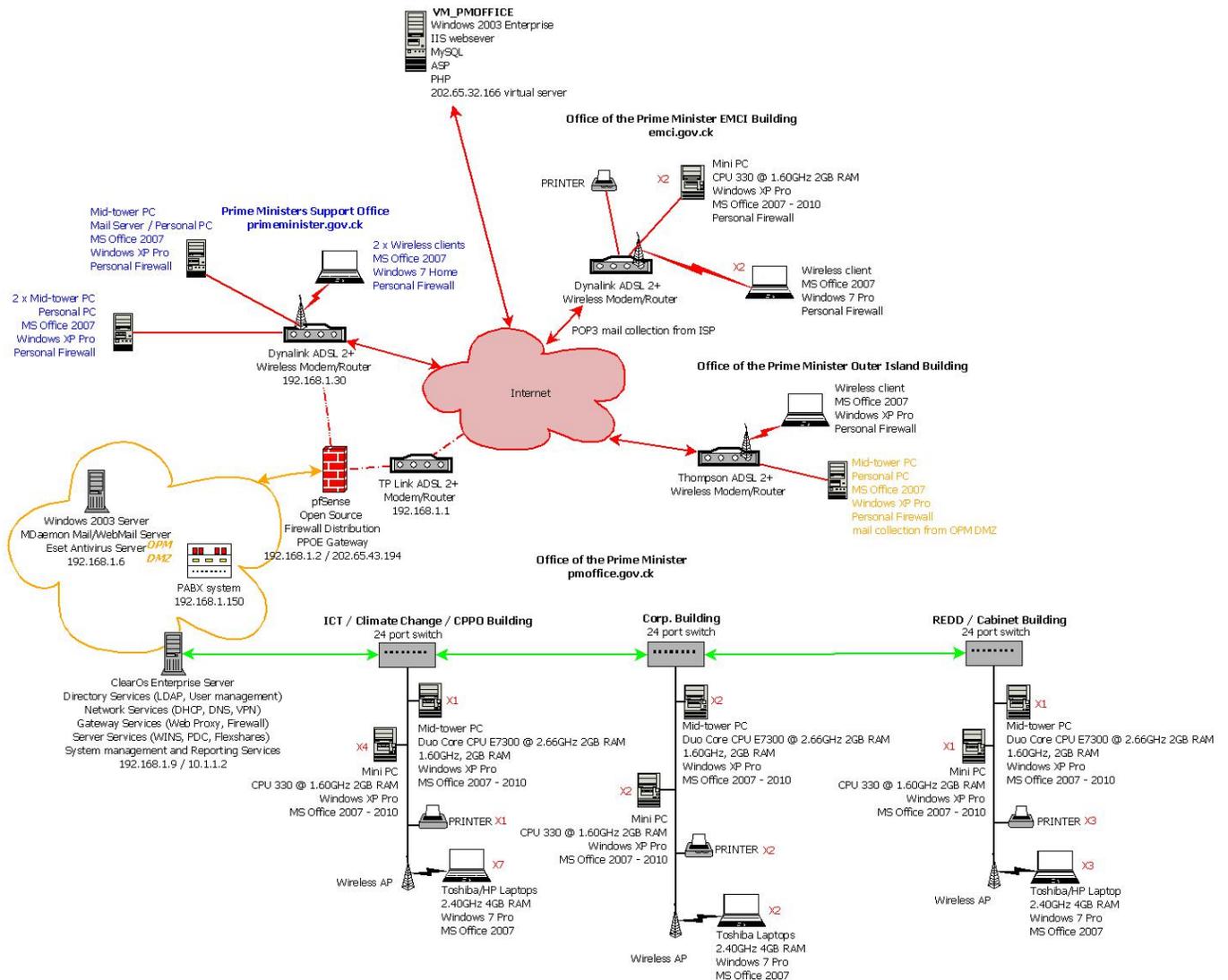
Mitchell's role encompasses a range of tasks including networking, systems installation and support, providing support to the other ministries for both internal projects as well as joint ventures with the private sector, liaison and services with the ISP, management of the phone system, and handling procurement and recommendations for other ministries.

Furthermore, special responsibilities of the office include planning and management of IT services and provision of IT support for events, such as sporting events (World Youth National Competition

and Pacific Mini Games), and the upcoming forum for Pacific leaders. Finally, management of the official government website is also under the purview of the ICT office.

Technology Infrastructure

Below is an informative and comprehensive diagram provided by Mitchell, the system administrator, which I have used for its clarity. The diagram provides an overview of every device on the OPM network, as well as its specifications (depending on relevance, hardware or software or both), to show the network structure



Technology Management

Being the ICT office, the expectation that technology is managed quite well is met and possibly exceeded. Of the 3 staff members, the supervisory role of the management of reporting, liaisons, and strategic planning is filled by Tepua. Mitchell is responsible for the installation and management of networking monitoring systems, predicting growth to anticipate required technology upgrades, and any other troubleshooting and support task requests of the office.

With regard to operational tasks, these are managed by Mitchell as well, and critical tasks such as data backup and software and antivirus updates and upgrades are all currently handled automatically, with Mitchell serving as the point of contact and supervisor.

From a strategic perspective, this is very much carried out as on an ad-hoc basis, simply because the number of staff involved is small, as are the number of people with the required technical expertise.

Technology Planning

Technology planning is seen as a reactive process at this office, due to and driven by constraint rather than choice. Currently no formalized committees exist for the technology planning of the ICT office. However, the long term technology planning for the other ministries is handled by ad-hoc joint committees including the heads of ministries and key people from the ICT office. In terms of short and medium term technology planning, the staff sees themselves as dealing with problems as they arise.

The existing process for technology acquisition boils down to an approval by the Chief of Staff, and if finance is available, the purchase is made. A strategic plan is in place, however, encompassing the management of all ICT assets across government.

All ministries have had problems with use of technology in the past. From my perspective one of the dominant causes is the lack of redundancy or backup built into their technology systems, leading to near-total loss at the times of natural disaster. This is something all the ministries have had experience with, and hence the need for a backup system of some form is supported by a strong organic need.

Internal Communication

The Office is fairly modern in this aspect: internal communication occurs through email and a shared network drive for document storage. Data security is assured through directory service management for access privileges, firewall setups, and antivirus and proxy servers. A VPN is also in place to enable staff to work off site and still access documents and services. Total bandwidth is still paid for by the office, and due to its inherent limitations (in terms of bandwidth), overseas access is still slow.

With ambitious foresight, the office is moving towards a cloud based communication system, by setting up virtual machines for email servers overseas. The rationale behind this move is to diversify the available redundancy measures for access, as well as to overcome the bandwidth bottleneck that staff face when they go overseas. This pilot has already been tested in Germany successfully. In addition, the Office intends to move the whole of government towards a centralized contact

management system (like Exchange). In terms of broad strategy, the office is considering a move to a private cloud for the entire OPM, in collaboration with the local ISP to better utilize resources and promote a centralized approach to IT setup and management.

With regard to external communication, the Prime Minister's office currently has a domain registered at www.pmooffice.gov.ck, but no functional website is present.

Information Management

The OPM generates a significant number of documents on a daily basis, and these are all stored on the shared network drive. This centrally managed data is backed up regularly. Draft documents stay on local computers until they are endorsed, at which point they then enter the shared drive.

In the view of both the partner and me, a move to a central document and contact management system would be beneficial for capacity building and be a source of great support to the office as it expands. It seems that a variety of such systems have been trialed in the past, but so far none has been found to be feasible, either functionally or economically.

Business Systems

In terms of staff finance management, the staff members sign into a time book, which is managed by a central Finance department for the OPM. Dispensation of payment is then handled by the Finance department, as are other requests for purchases. Most of the processes in this regard, however, are still manual.

II. Backup Systems in Government

Motivation

In the functioning of government in the world today, digital technology (in this context, implying computers and networking/communication technologies) is becoming increasingly important, not just for reasons of economy and efficiency, but also for its ability to bridge divides and improve capacity to deal with complexity and information overload. In the Cook Islands in particular, with a vision to move to e-government in hand, technology will soon form the backbone of governmental operations.

Accompanying this increase in dependency on technology brings with it a set of unique risks, with regard to the availability of data and services. Technical errors, hardware failures and perhaps most commonly, user errors are part and parcel of working with this technology, and these can lead to loss of access to data or loss of availability of services. The importance of government in the functioning of a nation makes it clear this risk is one that must be mitigated as much as possible. The way to ensure business continuity - implying high levels or continuous availability of government data and services – is through having a backup system in place, that acts as a redundancy measure or safeguard against loss of availability.

In addition, the Cook Islands are under a heightened threat of natural disasters, including flooding, cyclones and hurricanes, which have, in the past, destroyed the systems of various government entities, at times forcing them to abandon operating or attempt to restore services from scratch. In multiple cases, this has led to the loss of irrecoverable data that must be gathered once again. This level of data security and availability is unacceptable for government entities, especially in times of natural disasters, when the urgency accompanying demands is often higher.

Finally, in terms of functioning as a business, the lack of backup systems in government has been addressed in external audits, and is a heavy burden on the minds of the administrators. From this perspective, since the problem exists across the whole of government, it practically necessitates a global, outside view to investigate it, and work on a solution.

Outcomes

Given the above motivation, my work progressed as described in the paragraphs below.

First and foremost, the problem and its requisite tasks were scoped and agreed upon in writing. The problem was identified as the lack of backup systems across government, and the need to put in writing a plan recommending a system to address this issue.

The primary step to outlining the design of a system was to gather information on the state of backup systems across government. Approximately 40 government entities were surveyed. This process involved calling the heads of each entity (from a rolodex of government was provided to me), working with them to identify the right person to meet with (which was challenging in the entities without formal technology personnel roles), and then arranging the logistics, including transport back and forth from offices. In general, this preliminary step enabled me to test the waters to discover what the feedback from the community was regarding the backup project, and there was definite approval from all entities.

Prior to the actual discussions, I spent a week researching backup policies and systems, looking at the kinds of backups and the different sample policies available, as well as the questions to be asked when designing such a policy. Drawing from this research, I crafted a questionnaire to be used in my interviews, which would take into account not just the backup systems in existence, but also the role of technology in the broader functioning of the entity, and the thoughts of the staff on the entity-specific backup requirements.

Putting this to test in the field through my interviews, the information gathering phase lasted for the duration of the next 6 weeks. As the time between interviews reduced, the need for putting in place tracking for progress, information requests and follow-ups led to the creation of documents describing the information obtained from the entities that had already been interviewed, as well as any further follow-ups. In addition, any special notes or questions for other entities to be taken into account before interviewing them were part of the document. Since a memo had been sent out to all the Heads of Ministries regarding my work, I was also able to use this opportunity to obtain feedback on the current role of the ICT Office, and the general perception held by the other entities regarding their functioning.

The details of the internal IT systems of each entity have been documented in the final report submitted to the development partner. This includes not just the current state of IT and backup systems, but also future plans in the area as well as information on their IT service provider. The

information gathering phase led to some interesting insights, especially the discovery that while many entities had a rudimentary form of backup, there were multiple entities that were running state of the art systems with cloud technologies, and one that had already begun the process of integrating and centralizing the IT of all government entities in close geographical proximity. Since the latter had had experience with cloud technologies, I was able not only to document the usefulness of these technologies in the context of the Cook Islands government, but also strengthen the capacity building approach by utilizing organic ideas in the design of a national backup system by an external consultant. In fact, the level of experience and testing already performed by 2 ministries was detailed enough to justify basing the technical system design requirements of the final report [See Appendix A] on their systems.

A task that ran parallel to the later end of the information gathering phase was the correspondence with Telecom Cook Islands, the local ISP, to obtain their infrastructure and product plans. The initial plan for the installation of the system had been to network all entities (willing to participate) through the existing infrastructure (all controlled by Telecom), and link them to the offsite location. This information was also necessary for the costing section of the final report, to make financial arguments for backup options.

As part of the system, the offsite backup location that had been suggested prior to my arrival, the National Archives, was also inspected to determine its feasibility as a site. This resulted in a fruitful discussion, and the outcomes have been documented in the report submitted.

The final outcome, which had also been an objective of the development partner prior to my arrival, was a report documenting the information gathered from the ministries that would list the options for the backup system, and make recommendations based on both financial and logistical grounds. Included in this task was the collation of information from all the individual interviews, follow-ups to clarify financial information, research for the technical system design, and analysis of ICT policies followed in government. The final report was edited multiple times based on feedback from the development partner, and is an appendix in this report. Through the process of compiling the information obtained from interviews, I was also able to identify other areas for improvement across the ministries (in the technology area) that were present across nearly all ministries. These were compiled into a separate document and submitted to the development partner, and are part of the recommendations made in this report.

Recommendations

The nature of the task undertaken was such that progress is in the hands of the development partner, and the final outcome (report) produced was a resource to be utilized to obtain funding for the initiative itself. This must be accounted for when making recommendations.

In the case of backup systems, the need for backup was clearly understood by all entities that participated in the information gathering phase, and most had at-least a primary onsite backup system demonstrating their commitment to the cause. In this regard, following through with the recommended plan (as outlined in the final report) will lead to the development of the entities abilities to deal with threats to their technology systems through backup.

A recommendation that has not been made in the final report, that would still be applicable, is that of outlining and distributing a plan to improve and standardize all onsite backup systems across government. Since each entity has varying levels of stability and flexibility in their onsite backup

system, using the approximate costs outlined in the report, a plan could be suggested of approximately the same financial burden (theoretically) that would involve a variation of a standard template plan developed by the ICT Office. In this manner, slight variations of the same onsite backup system with essentially the same hardware and software could exist across government.

The benefits of this would be felt both in terms of financial and human resources. Central purchases, of enterprise license purchases for software would lead to cost savings across government, as would bulk purchase of hardware. In addition, arranging this through a local private company would be an indicator of the pervasiveness and strength of the ICT Policy. Finally, in terms of human resources, for both the in-house IT personnel of the entities and the support staff (if they are from the ICT office), there would be a familiar routine and troubleshooting experience in place, as well as a community, and over time, resources to help troubleshoot problems with the systems. Thus, each entity would not have to re-invent the wheel with their system, and would have multiple options for troubleshooting. This would also simplify maintenance and upgrades across the board.

To pursue this recommendation, the following procedures would have to be undertaken:

1. Using available costing information and needs analyses of entities, calculate the upper and lower budget limits for the software and hardware.
2. Based on internal experience and reviews, identify the appropriate hardware and software
3. Negotiate bulk purchase deals with the providers based on the participating entities
4. Implement the system based on standard procedures
5. Configure settings on each installation based on internal requirements, according to the information already gathered regarding their backup needs.

The main resources needed for these are the documentation from the information gathering phase (which has been handed over to the development partner), relationships with the providers in the region, and some qualified personnel to install and configure the system in each location.

An expansion to this project that would help IT staff deal with troubleshooting issues would be the storage of system images for servers, especially those used to run critical services like email and file sharing. This would allow the systems to be restored quickly in the case of a crash, and imaging the system periodically would ensure minimal, if any, loss of data.

III. Additional Recommendations

Data Recovery Planning

A common theme that arose during discussions with both technical and non-technical staff in multiple ministries was the costs and stress incurred due to the loss of data or hardware failure on individual workstations. In these cases, while backup is definitely a solution, it would tie up more resources than required to solve the problem. The appropriate solution here is data recovery, which was an option that most personnel were unaware of. There were many stories of both financial and personal loss that a hardware failure brought, and the only known path was to handover the device to a local company that would simply format the machine.

To make a persuasive argument for introducing and spreading knowledge on data recovery requires an understanding of the means through which most, if not all, of the day to day problems of the entities can be solved. The spectrum of methods available for data recovery does include ones of greater cost, but the problems discovered in the information gathering phase could all be addressed via a couple of simple methods.

There are 2 main steps to be followed: the dissemination of information regarding data recovery through emails and workshops, and the provision of appropriate software tools to aid in the process. The former step would involve hosting workshops introducing the concept of data recovery, its methods and uses, and finally a few examples of relevant day-to-day problems that could be solved more efficiently and economically via data recovery. Many such presentations, for both laypeople and more technical audiences, are available for download online and could simply be used by the appropriate staff in each entity or the ICT office (to visit the site and deliver the workshop). For the latter step, it is important to note that nearly all the machines used in government run on Microsoft Windows, and resources are being recommended with this in mind. Winternals ERD Commander is an extremely useful tool, currently freely available, that can be used to create a boot disk that runs a live OS environment. Using this, data can be recovered from the hard disk. Given that the methods to use this software are freely available, it would be easy to burn a few disks for use and distribute them to the entities.

It is apparent from the means described above that implementing this recommendation would imply very light financial burden. Small amounts of skilled labor would be involved, and following through would help mitigate costs related to data recovery and result in less stress over lost data. This would be directly beneficial to the entities, but also in raising the level of knowledge and awareness of technical issues among the members of government. In addition, the ICT Office would gain positive exposure and improve its reputation among the sections of government.

Central Subscription and Purchasing

This is a concern that was voiced at multiple ministries. Staff repeatedly mentioned the high costs associated with purchasing subscriptions to software for daily use such as Microsoft Office, and many saw it as a heavy burden on their operating budget. In addition, those aware of the ICT Office and its role asserted that central license assignment with this office would be beneficial and expedient.

Simply put, purchasing software and hardware in bulk enables the buyer to negotiate better deals and prices, or take advantage of economies of scale. Given that the whole of government utilizes the same 2 or 3 software packages for reporting and accounting, central software subscriptions would certainly be of benefit. Furthermore, bulk purchase of ubiquitous hardware like user workstations, external hard drives and USB drives would lead to great savings across government, as well as improving the perception of the ICT office's role in governmental workings.

Putting this into practice would require understanding of enterprise licensing systems and their applicability to the Cook Islands government scenario, as well as research into the licensing package deals offered by the vendors for software like QuickBooks and MYOB. Consultation of legal frameworks to allow the use of this software across government would also be necessary. Finally, surveys to obtain the number of users, and hence licenses, required would enable accurate decision making and lead to better utilization of government resources. In all processes, looking at existing models in other governments or borrowing from existing legal constructs and contracts would be an easy way of launching this system in the Cook Islands government.

Launching a Community Forum

The inspiration for this was provided by the conversations conducted with the various technical personnel in each of the government entities. A common theme seen throughout was the person with a fixed role and set of responsibilities in the organization, who worked with technology as a hobby, overstretched to deal with the technical problems of the organization because budget was either unavailable or unassigned for the purposes of technology in the organization. The only thing driving these people was their passion for technology, and a common complaint was the lack of knowledge about the various options "out there" in different areas, and lack of availability of updates about progress in the technology world as well as training for their skills. To this end, a community forum with the purpose of providing these technically able people with the required knowledge, support and news about the progress of technology in the Cook Islands and around the world, and a place for them to work together to better themselves would enable them to add new value and meaning to their dedication to technology.

The steps to launching this are straightforward: create an event design, based around either the creation of a new product or service, the training of attendees towards a new skill, or a brainstorming session for news, updates and so on. Once local sponsors for this are found, spreading the word among interested parties and focusing on the pride in "Going Local" for technical talent will help encourage people to attend. Momentum will be gained over time. In terms of resources, some time was spent working on a document describing the forum and its purpose, as well as a partial list of event design concepts that could be used in government as well. A few

meetings were also conducted with the target demographic to determine the feasibility of the idea, and it became clear that while the idea was intellectually captivating, many felt that the focus on using their skills to earn their livelihood would prevent them from participating whole heartedly in the initiative. The fierce competition to dominate the IT service provider industry in the Cook Islands was also cited as a reason for disinterest. On these grounds, further exploration of the idea was halted.

Benefit-wise, setting up such a forum would provide a place for the talent of the Cook Islands to develop organically, and encourage sharing of knowledge and experience across the boundaries of organizations. It would also provide a social motivation factor for the participants, as well as a heightened recognition, which would further encourage others to get involved. Having the ICT office spearhead this would show its proactive approach to addressing its responsibilities to the community as a whole, as well as its capability to function through creative initiatives, which are in line with its vision to act as an authority on ICT, even the human resources side.

About the Consultant

Kenrick is a rising Junior in Computer Science at the Qatar campus. His interests include technology entrepreneurship, music, people, good food, design and community development. He enjoys working in environments that allow for a symbiotic relationship between people and technology.

Appendix A – Final Report (submitted to partner)

Executive Summary

This report was commissioned by the ICT Office in the Office of the Prime Minister to examine the problem of a lack of backup systems in government, and to examine available options to solve the same.

With the rapidly increasing importance of IT services and digital data in the operations of the current government, the need to ensure the reliability and availability of these is becoming more urgent. Prior audits of government operations, as well as natural hazards have harshly exposed the lack of backup that currently exists, and the aftermath clearly demonstrates the criticality of having a backup solution for IT systems.

With this need in mind, an initiative was launched to gathering facts and information from all government entities regarding the current state of backup systems, analyze the results of these discussion and recommend a solution to the problem, keeping in mind the need for a managed, proactive backup system, be it centrally managed or not.

This report contains the summarized results obtained from the mission, as well as an analysis of the 2 options that emerged: of setting up a centrally managed data center for backup, and working with Telecom to utilize their data center as a client.

The analysis performed compares the options on the basis of financial concerns, flexibility, responsibility involved, knowledge and skills available, alignment with ICT policies, and benefits gained by the community. The comparison leads to the recommendation of the latter option of utilizing Telecom's data center, highlighting its advantages on all fronts.

Introduction

This report on the work undertaken for a national governmental backup system serves a dual purpose: to illuminate the state of technical affairs - with a special emphasis on backup - in all governmental agencies; as well as to propose and argue for a specially designed national backup system (NBS). This report represents the work undertaken by an external IT consultant to analyze the state of technology usage in each government entity (GE), and contains recommendations by the consultant to the purpose of the NBS. It must be kept in mind that the NBS initiative was launched not with the intention of bringing the whole of government's IT under a single umbrella, but with an aim to provide an essential service that is encompassed by the mission statement of the ICT office.

Problem Statement

In the 21st century, the role of ICT in government is rapidly shifting from a support option to that of an integral component of tactical and strategic operations. ICT, in the context it is used in this report, refers to both the raw data and information stored and utilized by GEs as well as the services, such as

email and file sharing, that form the backbone of a collaborative work environment as required by the GEs. With the increasing usage of computers and other digital-interface-enabled devices in all fields worldwide, the criticality of the smooth and correct functioning of these devices is rising as well. Being an important part of the organization structure directly implies the need for a guarantee on reliability.

With this in mind, the issue of business continuity is what digital backups address. There are multiple emergency scenarios applicable in the context of Rarotonga, from fire and thefts to cyclones and flooding. Members of government reading this report need no convincing regarding the threats posed by natural disasters such as hurricanes. Multiple GEs have already been affected by such circumstances and had to face loss of data and services that was critical to their operation. With the growth of government, both in terms of size and complexity, such operational blackouts become even more intolerable and intensify the need for business continuity systems that ensure the ICT aspect of the business systems is reliable and guaranteed. A widely accepted method for this is digital backup, which involves creating copies or “mirrors” of mission-critical data and services, which can be quickly and easily restored on available hardware, in the same state as they were prior to the emergency.

In addition to the natural need for backup as explained previously, the importance of the need to address this issue is further highlighted by the results of multiple audits that have pointed at the lack of backup systems [CITE] in place for government. This also brings issues of quality control and standardization into the picture, which are essential for maintaining both the professionalism of government as well as the national image and pride that the government fuels in the hearts of the people.

Last, but not least, the government has an ambitious e-government strategy in place, the implementation of which relies on the increased usage of ICT in all areas of the government’s operations. Having this plan in place also serves to highlight the urgency of the need for backup systems to support the e-government plans.

Objective

Having established the need for a backup system for government, the ICT Office in the OPM began planning the NBS initiative to address the issue, bringing in an external consultant to undertake surveys of all government entities, design a national backup system and examine the feasibility of the proposed system in this report.

It must be emphasized that the initiative did not have in mind the creation of a centralized NBS on beginning the project. It was open to the possibility that the current backup systems of individual ministries might be sufficient, and forcing a move to the NBS was not included in the intended set of actions. The primary phase of the project was based on information gathering and collation, to determine economic and strategic feasibility.

Furthermore, an important element to the design of a backup system is the amount of redundancy, and the number of backups available. In this context, having a backup that is physically at the site of or close to the data is referred to as the onsite backup, and backups that exist at a different physical location, generally distant from the data source, are referred to as offsite backup locations. The purpose

of having an offsite backup is to ensure that if disaster strikes a physical location and both the data and the onsite backup are destroyed, the data is still available due to multiple layers of redundancy.

Results

The following table will summarize the results of the information gathering phase, highlighting the state of backup in each GE, the provider of IT services including backup, and the associated costs of the backup service. It is important to bear in mind that since backup is a subset of essential technical functions, figures provided are approximated as best as possible, and the relevant contextual facts are emphasized as necessary. N/A has been recorded where obtaining a separate cost for backup functions is not representative. Finally, in multiple cases, the data is based on taking unit prices and calculating the total costs of multiple units (in this case, for external hard drives), and should be taken as a ceiling.

(references:

Offsite option equivalent: external hard drive being taken offsite physically

Internal: IT personnel exist within the organization

)

Entity	State of Backup	Current Service Provider	Associated Costs (approx. in NZ\$ and averaged where necessary)
Airport Authority	Different sections back up separately. Are currently planning to install an offsite backup location which will require the installation of fiber under the runway.	Internal	800 in fixed costs, as well as 1 hour /day of labor The upgraded system will cost 2500 in fixed costs, as well as 100 / month. Similar costs apply for labor hours
Ministry of Justice	Some sections are backed up, but significant quantities of paper-based information have no backup. An offsite backup location is desperately needed.	Internal	1000 in fixed costs, as well as 1 hour /day of labor
Ministry of Infrastructure and Planning	Backup is done intermittently on personal equipment. Certain sections may remain unaccounted for, and hardcopy documents have no backups in place.	Internal	1000 in fixed costs, as well as 1 hour /day of labor
Office of the Prime Minister	Being backed up with multiple layers of redundancy. Offsite	Internal	

	backup does not exist.		
Ministry of Agriculture (including BioSecurity division)	Backup systems are not in place, and MoA depends on MFEM and OPM for storage of certain data.	ICT Office, OPM	1000 in fixed costs, as well as 0.5 hour /day of labor
Audit Office	Technical Systems are merged with MFEM – backup does exist, including an offsite that is physically close by.	MFEM (in the past – HiTek)	See MFEM
Bank of the Cook Islands	Comprehensive backup policy and systems in place, including an offsite location.	Internal	
Business Trade Investment Board	Backup systems do exist, but no offsite location.	ICT Office , HiTek, some internal support	3000 in fixed costs, as well as 250 / consultation
Cook Islands Investment Corporation	Technical Systems are merged with MFEM – backup does exist, and a good offsite location is being considered	MFEM	See MFEM
Cook Islands Tourism Corporation	Backup systems and an offsite equivalent do exist.	Internal	4500 in fixed costs, as well as small labor costs as required
Crown Law	Backup systems exist, as well as an offsite equivalent option. An additional offsite location is being considered.	The Computer Man	1000 in fixed costs, including 80 / consultation visit
Ministry of Culture (including National Archives)	Hardware resources have been allocated for the purpose of backup, although process monitoring is personally enforced. An offsite equivalent option exists.	The Computer Man (primary), Summerfield Systems	2000 in fixed costs, as well as 250 / consultation visit
Ministry of Education (including National Human Resources Department)	A comprehensive and advanced backup system exists. Offsite option is not available.	Internal	1800 in fixed costs, covering multi-purpose hardware not solely dedicated to backup
Electricity Department	Onsite option and offsite equivalent option do exist. Setup of an additional layer of redundancy is being considered.	Independent Contractor	
Environmental Services	Personal backups of	Summerfield Systems,	N/A

	information are the only option – no others exist	Telecom	
Financial Supervisory Commission (including Financial Intelligence Unit)	With the recent integration of FIU into FSC, the FIU is merging technical systems with the FSC and their provider. Onsite backup and offsite equivalent option exist.	Summerfield Systems	800 in fixed costs, as well as 145 / consultation visit
Financial Services Development Authority	Onsite and offsite equivalent options exist.	Telecom	N/A
Head of State	Onsite and offsite equivalent options exist. However, there is an urgent need for an additional offsite location for backup of certain official documents.	Telecom, Internal	600 in fixed costs, as well as small labor cost where required
Ministry of Internal Affairs	Onsite backup systems exist, however an offsite location is urgently required.	The Computer Man	400 in fixed costs, as well as labor costs
Ministry of Transport	Onsite backup is in place, however offsite options do not exist.	Independent Contractor	N/A
Met Services	Personal backups are the main option, followed by a central onsite backup. Offsite options do not exist.	Internal	600 in fixed costs, as well as labor costs
Ministry of Foreign Affairs and Immigration	Technical Systems are merged with MFEM – backup does exist, and an offsite location is available close by (under MFEM)	MFEM	See MFEM
Ministry of Finance and Economic Management	A comprehensive and advanced backup system exists for the IT systems managed by the MFEM (including others merged with MFEM). An offsite option nearby is being utilized, but an additional distant offsite location is being considered.	Internal	800 in fixed costs, as well as 8 hours for setup labor

Ministry of Marine Resources	Despite an acknowledged lack of comprehensive IT systems, sufficient onsite backup systems are in place. An offsite location is being considered as well.	Summerfield Systems	(overseas)
Office of the Ombudsman	Onsite and offsite equivalent options are being utilized. The office is also dependent on MFEM for the offsite option and certain data storage.	The Computer Man	500 in fixed costs, as well as 75 / consultation visit
Cook Islands Parliament	A basic onsite backup system is in place, but it is critical to improve this system due to the important of Parliament. An offsite option is also urgently needed.	Summerfield Systems, Internal	N/A
Cook Islands Pearl Authority	Comprehensive onsite and offsite backup options exist. The offsite option is dependent on the ANZ bank.	The Computer Man	400 in fixed costs
Cook Islands Police	A single layer of onsite backup exists. An offsite backup system is urgently needed.	Internal	(overseas)
Cook Islands Port Authority	Onsite and offsite backup options exist with multiple levels of redundancy. An improved offsite option is recommended.	Telecom	
Office of the Public Service Commissioner	This office is currently in a move to the MFEM building, and will be integrating with the MFEM-managed building-wide IT system.	MFEM	See MFEM
Cook Islands Superannuation Fund	Comprehensive onsite and offsite backup options with multiple layers of redundancy exist. Offsite backup	Internal	400 in fixed costs, as well as 200 / month for leased line facilities. Small labor costs as required

	options are through a venture with Telecom.		
--	---	--	--

Primary Conclusions

From the above table and collected information, there are some very significant observations that can be made:

1. The lack of a comprehensive backup system in multiple ministries whose role in government is mission-critical
2. In many cases, the personnel bearing the responsibility for IT systems are not dedicated for this purpose. It is done in addition to their existing duties within the organization and leads to additional stress and overstretching, which rapidly destroys productivity.
3. While there are many ministries with insufficient backup systems, there are a few that have advanced technologies in place, and have already tested them over sufficient time periods.

Therefore, accounting for point 3 above, it is the recommendation of the author that a capacity building approach be used for the NBS, utilizing organic ideas to serve the initiative. Essentially, the scope of the work remaining will be in a technical analysis of backup methods on a case by case basis, which must follow the comparison of multiple offsite locations. Providing this offsite option, however, is not a replacement for installing onsite systems. These onsite systems can be speedily deployed using standard off the shelf products without interruption of the ongoing processes of the respective ministries.

Budgeting

A point to emphasize is that in all cases, the fixed costs include costs for storage devices, which are prone to failure, and need to be replaced every few years. In addition, these must be tested for reliability and wear and tear regularly. Use of this method for backup also requires trained labor.

Furthermore, it is easy to see the fairly hefty costs associated with consultations arranged with external contractors. While bearing in mind that these are for all technical problems and not just backup, having a comprehensive backup system in place to address both hardware and software failures would ensure added resiliency of the IT systems in place.

Solutions

From the fact finding and analysis carried out, 2 options have emerged as possible solutions to the problem of a centrally managed backup system. Both options are detailed below. It is important to note that for both options, the task of setup of backup systems and processes on the government entity's

side is an additional process that will have to be carried out. This has been omitted from the option analysis due to the fact that the only cost involved is that of trained labor, which is already present in the ICT office.

Option 1

This would involve the ICT Office being responsible for the design and construction of its own offsite backup system for all the ministries. The following processes would be involved:

Process	Cost	Progress and Implications
<p>Identification of suitable location in terms of physical security, environmental feasibility and other relevant factors such as power and internet</p>	<p>Requires coordination between Telecom and the ICT office, as well as an analysis of multiple sites on these grounds</p>	<p>The National Archives site has been reviewed as an offsite location. Given its location and the nature and age of the building, the workflow of this process would be burdensome.</p>
<p>Purchase, installation and maintenance of infrastructure to support the backup system</p>	<p>Based on the approximation of 200 GB's of data for each government entity included, for 40 such entities, the costs would be (approx..) 2000 for the storage space (based on costing obtained from Ministry of Education). (and approximately 1500 in server costs)</p> <p>In addition, purchase of networking bandwidth to support the transfer of data to the offsite location (using Telecom's VLAN option) would, at 350 fixed costs, and 30 / site / month, total at 2500 (ceiling) in fixed costs and 1200 /month.</p> <p>For both the above, approximations can be tightened by accounting for the fact that MFEM currently coordinates a centralized backup system between 6 of these entities and are planning an expansion, which when accounted for reduces the monthly totals to 1400 / month.</p> <p>Finally, we can estimate an average of 100 / month for maintenance and upkeep, as well as 1 hr /day in terms of labor costs.</p> <p>Outside of this, installation of the infrastructure and initial setup</p>	<p>The main implication to be considered here is that this would involve preparation of invoices for the appropriate equipment, space planning for the chosen location, as well as regular maintenance and security. Since this will be a centralized location for government's data, around the clock security is also a must.</p> <p>With regard to the National ICT Policy (which encourages the private sector led expansion of ICT), this initiative would lead to a drop in their revenues due to the loss of associated government clients for the backup service. This could be interpreted as contrary to the spirit of the policy.</p>

	<p>and configuration will require 8 – 10 hours (at minimum) of trained labor for the location itself, not accounting for labor associated with the setup at each site. Labor at each site would vary based on their current status, but can be averaged at 3 hrs / site, leading to the estimate of 120 hours of labor to setup the distributed components of the system</p>	
--	--	--

System Design

Since the provision of the VLAN facility is undertaken by Telecom, trained labor will be required for the setup of a private cloud facility at the offsite location. As mentioned in the Primary Conclusions section, this approach to backup has already been initiated by the Ministries of Finance and Education, both using different technologies to implement a cloud based backup system.

The software associated with this setup are : XenCenter (or) vSphere Client (coupled with Veeam).

This solution option would have to meet the following requirements:

1. Ensure uninterrupted power supply, as well as the availability of backup power systems to maintain environmental conditions such as temperature, to the location
2. Put in place 24/7 physical security to protect from natural and human threats
3. Systems in place would have to support redundancy technologies (such as RAID for file storage and Virtualization for servers) to ensure smooth and speedy restoration in the case of expected hardware failures
4. Technically trained personnel (at least 1) would have to be available 24/7 (or optionally, a secondary person for off times) and be capable of dealing with day to day maintenance tasks such as hardware replacements and environmental stability upkeep, as well as broader analysis and improvement tasks such as software deployment and configuration and system health monitoring.

Option 2

This option involves establishing a client relationship with Telecom and utilizing their data center. From discussions with Telecom, it has been determined that a data center is currently available in Avarua, and another is under construction in a more geographically stable and protected location in Aroa. The projected costing details obtained from Telecom are given below. Telecom is also open to negotiation on prices and discussion regarding the flexibility of the arrangement, and discounts and reduced rates would also be applicable for larger requirements.

With this option, the setup and maintenance of the data center would be the responsibility of Telecom, and the processes involved with this option are:

Process	Cost	Progress and Implications
Purchase of required computing resources from the data center, and installation of required software systems	A virtual machine (VM) with the following specifications: dual core, 8 GB RAM, 500 GB HD, is estimated to cost around 600 / month. The purchase of 2 machines in this case is sufficient, and colocation of equipment in the center is possible. Therefore, 1200/month would be a ceiling, and there would be no fixed costs involved.	Utilization of both data centers would provide a flexible and resilient onsite and offsite backup option to all entities participating. In addition, 99.9 % uptime is guaranteed and the responsibilities and costs associated with maintenance, upkeep and utilities would all be borne by the provider.
Installation of connectivity between each government entity and data center (costing already carried out in Option 1)	Purchase of networking bandwidth to support the transfer of data to the offsite location (using Telecom's VLAN option) would, at 350 fixed costs, and 30 / site / month, total at 2500 (ceiling) in fixed costs and 1200 /month.	With regard to the National ICT Policy (which encourages the private sector led expansion of ICT), this initiative would lead to an increased business for a major technology company in the country, thus showing the strength of the ICT office's commitment to the policy.

Recommendation

Taking into account the current situation regarding the availability of funds and experienced labor, the author recommends Option 2 for the following reasons:

1. National ICT Policy : Given that the policy encourages the development of ICT via partnerships with the private sector, this option will enable the development of a multi-faceted relationship between Telecom and the ICT office
2. Perception of the role of the ICT Office: Option 2 will help position the ICT office as the technology authority in the government, not just in policy, but also in perception due to their work on the initiative, as well as their level of involvement with the initiative. While Option 1 will also have a similar effect in this regard, the establishment of a public-private partnership involving the ICT office and a powerful IT service provider will help boost confidence in the feasibility and reliability of the initiative
3. The governmental entities themselves will be secure in the knowledge that they are being provided a service that is supported by multiple leaders in the Cook Islands technology arena, and this will bolster confidence and support
4. Costing : Financially, option 2 allows the elimination of a large expense in fixed costs, the value of whose assets will depreciate rapidly over time (as is common in the technology sector) and must be maintained and upgraded frequently
5. Ease of Setup, based on Present State of Labor : Option 2 will greatly reduce the additional responsibility that will have to be placed on the shoulders of current employees, or equivalently, eliminate the need for the creation of jobs that will be an additional strain on the finances of the office
6. Industry Relationships : Building a partnership over a sensitive project such as this will result in not only image boosts for the stakeholders, but also for a more connected technology

community, providing the intangible benefits of human relationships and additional opportunities for creativity and expansion

Conclusion

The above recommendation has been made after careful consideration of data collected during the information gathering phase, as well as a cost-benefit analysis of the available options. Special effort has been made to include the more “soft” or intangible benefits afforded by each option, which is especially important in a relatively small-sized environment like the Cooks, with a nascent technology industry. The recommendation of the report is to pursue a partnership with Telecom, and utilize the option of their data center, which would result in a smoother and more financially feasible solution to the problem of backup systems posed to spark the initiative.

Appendix A – Backup Systems Table

(SAN- Storage Area Network, NAS – Network Attached Storage, EXHD – External Hard Disk)

Entity	Backup System
Airport Authority	NAS
Ministry of Justice	EXHD
Ministry of Infrastructure and Planning	EXHD; On Server
Office of the Prime Minister	EXHD; On Server
Ministry of Agriculture (including BioSecurity division)	Backup systems are not in place
Audit Office	see MFEM
Bank of the Cook Islands	
Business Trade Investment Board	EXHD; using Acronis software
Cook Islands Investment Corporation	See MFEM
Cook Islands Tourism Corporation	NAS; using Acronis software
Crown Law	EXHD
Ministry of Culture (including National Archives)	EXHD
Ministry of Education	NAS; Backups done

(including National Human Resources Department)	with virtual machine hypervisor XenCenter, and with Windows Backup
Electricity Department	
Environmental Services	Personal backups of information – flash drives
Financial Supervisory Commission (including Financial Intelligence Unit)	EXHD; On Server
Financial Services Development Authority	EXHD
Head of State	EXHD
Ministry of Internal Affairs	EXHD
Ministry of Transport	EXHD; On Server
Met Services	EXHD; On Server
Ministry of Foreign Affairs and Immigration	See MFEM
Ministry of Finance and Economic Management	Done using virtual machine hypervisor VMWare, and Veeam software on server
Ministry of Marine Resources	On Server
Office of the Ombudsman	EXHD; On Server
Cook Islands Parliament	On Server
Cook Islands Pearl Authority	EXHD; On Server
Cook Islands Police	SAN
Cook Islands Port Authority	Tape; On Server
Office of the Public Service Commissioner	See MFEM
Cook Islands Superannuation Fund	At Telecom; Offsite at NZ; Local On Server

Appendix B – Costing Breakdowns

(approx. in NZ\$ and averaged where necessary – where the table cell is blank, cost is either zero or a special case has been described in the original table in the report body)

Where the table cell states “See MFEM”, this refers to the special case of the centralized IT system operated by MFEM.

Entity	Fixed Costs	Labor Costs	Additional Associated Costs
Airport Authority	800	1 hour / day	The upgraded system will cost 2500 in fixed costs, as well as 100 / month. Similar costs apply for labor hours
Ministry of Justice	1000	1 hour / day	
Ministry of Infrastructure and Planning	1000	1 hour / day	
Office of the Prime Minister			
Ministry of Agriculture (including BioSecurity division)	1000	0.5 hour / day	
Audit Office	See MFEM	See MFEM	See MFEM
Bank of the Cook Islands			
Business Trade Investment Board	3000		250 / consultation visit
Cook Islands Investment Corporation	See MFEM	See MFEM	See MFEM
Cook Islands Tourism Corporation	4500	As required	
Crown Law	1000		80 / consultation visit
Ministry of Culture (including National Archives)	2000		250 / consultation visit
Ministry of Education (including National Human Resources Department)	1800		
Electricity Department			
Environmental Services			
Financial Supervisory Commission (including Financial Intelligence Unit)	800		145 / consultation visit
Financial Services Development Authority			
Head of State	600	As required	
Ministry of Internal Affairs	400	As required	
Ministry of Transport			
Met Services		As required	
Ministry of Foreign Affairs and Immigration	See MFEM	See MFEM	See MFEM
Ministry of Finance and	800	8 hours	

Economic Management			
Ministry of Marine Resources			
Office of the Ombudsman	500		75 / consultation visit
Cook Islands Parliament			
Cook Islands Pearl Authority	400		
Cook Islands Police			
Cook Islands Port Authority			
Office of the Public Service Commissioner	See MFEM	See MFEM	See MFEM
Cook Islands Superannuation Fund	400	As required	200 / month for leased line facilities. Small labor costs as required

Appendix B – Alternate Solution Researched

As part of researching the option of setting up a standalone data center managed by the ICT Office, I obtained targeted geographic information from Telecom Cook Islands regarding their infrastructure on the island. Below is a map of the infrastructure facilities (including cables and exchanges) on the island. Telecom currently supports broadband access as well as VLAN facility over this infrastructure.



In addition, the inspection of the National Archives building to determine its feasibility as a data center yielded these pictures (showing the current state of the space):



