CloudPolicy

STRATEGY.VISION.LEADERSHIP

CloudPolicy Document (Confidential)

Client:	Bank of Butterfield
Project:	Cloud Services
Prepared By:	Julian Box
Prepared For:	Mark Duddy
Reference:	Bank of Butterfield CloudPolicy

Table of Contents

Document Control

Document Control:

The following document is supplied to Bank of Butterfield to assist in the evaluation cloud based services and their appropriateness for use by the business.

It is based on the information provided to us in a series of meetings and via the collection of performance data.

Information contained in this document is accurate to the best of our knowledge at the time of publication and is required to be treated as confidential. It should not be reproduced or made available in any form to persons outside the group directly responsible for evaluating its contents.

Any performance data provided is based on relevant information made available to us/collected at the present time, and must (except where stated otherwise) be regarded as an estimate only, since the actual performance and functionality of any computer system will depend upon a variety of factors, not all of which are related to the products and services that may ultimately be supplied.

The master document is controlled electronically within the Supplier's DMS. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

This version: 1.0

Introduction

As part of Bank of Butterfiled's review of their future IT needs Calligo Limited has been requested to review the current infrastructure and the options that cloud computing offers.

There are several options available with a view to balance budget and functionality; the following document is a set of findings based on the analysis of Bank of Butterfield's current infrastructure, resources and the future requirements, which were obtained through reviews and discussions with members of Bank of Butterfield team.

Document Mandate & Purpose

The purpose of the document is to present a summary review of Bank of Butterfield's current envirnement, this will allow for a fully costed solution to be provided.

Executive Summary

This report discusses and outlines how Bank of Butterfield will benefit from a transition from the current environment of internally managed systems to a consolidated and managed service based on cloud computing infrastructure.

Cloud computing is achieved through the use of virtualisation technologies in a multi tenanted configuration. Multi tenancy refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organisations (tenants). With a multi-tenant architecture, a software application is designed to virtually partition its data and configuration, and each client organisation works with a customised virtual application instance. Virtualisation achieved mainstream adoption during the last ten years as organisations strive to eliminate the inefficiency created by the proliferation of x86 architecture that resulted from the huge expansion of server-based services in the 1990s. Cloud computing is an evolutionary step that allows virtualisation efficiency levels to be raised even further.

The analysis of the current estate has allowed Calligo to demonstrate how Bank of Butterfield can gain benefits from the use of cloud-based services to meet their business operations requirements.

This report recommends that Bank of Butterfield move forward using the following services and changes:

- CloudCore – A virtual datacentre hosted on Calligo's Jersey CloudCore platform for running all of Bank of Butterfield's back office applications including file sharing, SQL and the Jobstream Trust system
- CloudSafe – A disaster recovery virtual datacentre hosted on Calligo's Guernsey CloudCore Platform for use in the event of a problem at the primary virtual datacentre plus the resources are to be used for Test and Development to maximise the efficiencies available to Bank of Butterfield
- CloudCopy – Backup services that will run with two tiers of storage (short and long term) and with a primary backup set in Jersey and a second copy held within the Guernsey Datacentre
- CloudNet – Connectivity to the cloud via a managed Sure 1Gb dedicated connection with 1GB failover link managed by JT
- CloudBuilder – Professional services engagement to on-board Bank of Butterfield to the new environment
- CloudReady – Professional services engagement to help align Bank of Butterfield's IT service delivery to a cloud based model

The new model of managed infrastructure underpinned by cloud computing advocated by this report will provide Bank of Butterfield with a fully functioning system, which is accessible, reliable, secure and cost effective. This will have a dramatic effect on the overall efficiency of the on-going business's operation and enable new operational processes that will benefit the organisation and allow it to meet its business expansion plans through the use of an agile and responsive technology platform and strategy.

Cloud computing will also have a dramatic, positive environmental impact. Inefficiency is driven out of the server and virtual only based computing models, which enables a more effective scaling of resources to demand, a reduction in utility (power, heat) consumption and a consequent improvement in the carbon footprint.

Summary Matrix of the Pros & Cons of Cloud

Area Description	Positive	Negative
Only pay for what you use.	Allows alignment of costs to the businesses need and removes the needs to estimate future consumption which is mostly incorrect.	Can be difficult to generate long term cost models.
Internal costs associated with monitoring and upgrades.	Removes the need for Bank of Butterfield to maintain an infrastructure support team to its currently levels and redirect the costs into the businesses core focuses.	Perceived lose of control, but the business will still collaborate and plan with the cloud provider for all upgrades.
Agile IT Service	Cloud based services are able to increased and decreased as and when a business requires them.	None
Application Focus	Cloud based infrastructure allows businesses to focus on their core competencies. IT teams focus on business value based functions.	None
Time zone support	Cloud services are covered 24/7 removing the need for internal IT Teams include additional staff to truly support a global business.	None

Private Cloud (in house) - Estimated 5 year total cost of ownership

Public Cloud (outsourced) - Estimated 5 year total cost of ownership

Summary

The tables above takes the cost savings that Cloud Computing could yield and levels them against the cost of implementation realising a possible net saving of £999,999 over the five-year period. The reduction in expenditure would also realise massive operational benefits with the objective of an improved and agile disaster recovery becoming a reality.

Overview of Cloud Services within Offshore Jurisdictions

Offshore jurisdictions around the globe are having to respond to tighter regulations and increased competition. As such they have quite specific technology challenges, not least around data residency, security and governance. With one of Bank of Butterfield's long-term business objectives including expansion into other offshore jurisdictions this section looks in detail at the challenges and benefits in using cloud computing as the underpinning technology platform.

The changing nature of offshore business

The world of offshore business has changed substantially over recent decades, not just in the face of increasing regulation but also to recognise the changing nature of the global business landscape. In response, once-disparate jurisdictions with a specific financial focus have evolved into highly sophisticated business hubs for international and multinational companies.

Today's offshore centres – locations such as the Channel Isles and Grand Cayman, Luxembourg and Switzerland, Panama, Gibraltar and Malta, Singapore and Hong Kong – offer a range of services that extend way beyond their traditional remit. Most, if not all international companies use offshore facilities for some activities, for reasons including reduced operational overheads and labour costs, asset protection and data confidentiality, proximity to target markets and their growing reputation as business centres of excellence.

From a governance perspective, offshore jurisdictions now represent some of the most regulated locations in the world. For example, in response to concerns around money laundering (represented by the Financial Action Task Force on Money Laundering's '40+9' recommendations), leading offshore locations are now more tightly controlled than many onshore financial centres.

In this increasingly global marketplace, offshore jurisdictions face growing competition from onshore locations. The underlying principle – that organisations can benefit from operating in a country in which they do not trade – remains true whatever the country, onshore or offshore. Equally, the core financial benefits are only one factor in the decision process, which need to be weighed against other factors such as labour costs, access to resources, availability of suitable infrastructure, operational and logistical overheads, market accessibility and so on.

So, just as the decision to run an element of business offshore is not a simple yes/no, neither is it enough for offshore jurisdictions simply to 'be' offshore. Rather, organisations have to derive clear business benefit from doing so, beyond simple financial savings. Such increasing expectations are driving offshore providers to provide greater innovation and business flexibility, married with efficiency savings.

Can cloud computing respond to offshore needs?

While definitions of cloud computing may vary, they share the same core idea – that computing services can be delivered across the internet from providers more flexibly and efficiently than traditional, in-house infrastructure. Industry experts often compare this phenomenon with the way that electricity was generated and consumed a century ago, with regard to today – we can see a similar move towards delivering computing as a utility or as a service, rather than having to build and run computing capabilities in-house.

Broadly speaking, cloud computing is underpinned by the following three models:

- Infrastructure as a Service (IaaS) – provision of raw processing and storage resources.

- Platform as a Service (PaaS) – covering application and service building blocks.
- Software as a Service (SaaS) – the delivery of complete applications, usually with a web-based interface.

As part of any due diligence Bank of Butterfield must assess cloud providers to ensure they provide efficiency, flexibility and scalability. The key for the providers lies in the ability to support much larger numbers of users, and to do so far more efficiently than in the past. Technologies such as virtualisation, dynamic provisioning and distributed processing all play a part – but the key is that, given the scale of computer power available today, it makes greater economic sense to share computing infrastructure among larger numbers of users and workloads.

There is nothing to stop Bank of Butterfield from adopting similar capabilities by creating their own, 'private' cloud environments; equally, Bank of Butterfield may choose to access 'public' cloud services from a third party provider. Bank of Butterfield can also work with a hosting company to deliver 'hosted private' cloud services. To illustrate that cloud computing is not an all-or-nothing decision, many organisations choose a hybrid configuration – using a combination of public and private cloud services to meet their specific needs, this is an option reviewed by this report.

The core benefits of public cloud computing (for example scaling services on demand, paying only for what is used, benefiting from resilient third-partly infrastructure and so on) apply equally well to offshore as onshore organisations. Similarly, the levels of data security and business continuity protection offered by providers like Calligo tend to surpass all but the most resilient of in-house data centre environments. In principle, this makes public cloud computing of particular benefit to organisations like Bank of Butterfield that are looking to achieve the highest levels of data protection for themselves and their clients.

Among the offshore community, however, there remains a perception that cloud computing falls short of requirements. While providers have traditionally been quick to emphasise the economic benefits, they have not always been so responsive in two areas in particular – both of which matter a great deal to offshore businesses:

- Location guarantees – in that cloud providers have not always been able to state with certainty the exact location in which data is being stored, for a given customer. In the early days of cloud computing some providers took the line that location simply didn't matter – it was simply 'in the cloud'.

  This view quickly evolved when it was pointed out that a number of national laws (not least, within many European countries) required that sensitive data remained within country boundaries.

- Conflicting legislation – the location issue is further exacerbated by the realisation that national and international laws are not always aligned with the needs of data owners, nor with each other.

  For example, the fact that many cloud providers are US-headquartered means that they are subject to the US Patriot Act - which means that US agencies can be granted access to data stored by such providers, wherever it is located.

  In addition the US Foreign Intelligence Surveillance Act (FISA), which is the law used by the NSA within the US for the PRISM program and which has made the headlines in recent months, allows the US government to intercept communications such as telephone calls and emails between foreigners (but not US citizens), without a warrant.

For offshore organisations, these concerns are more than a nice-to-have as they frequently conflict with the regulatory frameworks of their chosen jurisdictions. Even where no such conflict exists, offshore organisations looking to offer confidentiality guarantees to their customers need to be completely sure that data is located within a chosen jurisdiction and is subject to its laws alone.

Given that some larger (often US-based) cloud vendors have been slow to respond to such issues, it is equally understandable that offshore organisations have been reticent to adopt public cloud computing. While some are creating their own private cloud infrastructures, the preference for many companies is to stick with traditional in-house models, even if they are less efficient and – not ironically – potentially result in increased data risk for customers.

The bottom line is that, whatever the benefits, Bank of Butterfield will only adopt a technology if it passes a basic threshold of adequacy in terms of data risk. Calligo's platform has been designed to tackle these issues and allow organisations like Bank of Butterfield to adopt cloud services that meet the challenges outlined above. Organisations running all or part of their business offshore have certain expectations of the jurisdictions in which they operate, which in turn set out the requirements to be met by their cloud service provider.

Data and trust requirements

For Bank of Butterfield, data is king. Cloud service delivery therefore needs best-in-class data management, to cover aspects such as:

- Data security, meeting stringent criteria of confidentiality, integrity and availability and offering protection against external attacks and internal breaches.
- Client privacy is of prime importance to offshore businesses, imposing restrictions on whether a provider can view the data contained on their servers.
- Data protection, backup and archiving capabilities to assure data can be recovered if lost, and to meet an organisation's data retention requirements.
- Data residency needs to be guaranteed on a jurisdiction by jurisdiction basis, including support for clients who have data in more than one location without reducing protection in individual locations.
- Data movement, in that some clients may have operations in more than one jurisdiction so should be able to move data from one to another.

A number of pan-industry initiatives are underway to address these areas, including the Trusted Cloud Initiative (TCI) from the Cloud Security Alliance. This sets out both key criteria for cloud service provision, together with approaches and tools to help organisations adopt cloud services in a way they can trust. However these still fall short in areas such as data residency and movement which requires additional due diligence on the part of Bank of Butterfield to ensure their provider delivers on the above data protection and privacy needs as well as meeting the business's expectations and regulatory requirements.

Service requirements

Alongside data guarantees, Bank of Butterfield needs to be sure that service levels meet expectations, particularly around such aspects as:

- Service availability and stability – for global businesses, the expectation is now 24/7 with minimal, if not as close to zero downtime.
- Service consistency – while offshore organisations may be small, they may support large numbers of clients. Performance, response times and the like need to remain consistent,

whatever the load and however many users are trying to access the service.
- Service scalability – it should be straightforward to scale a service up and down, (for example) adding or removing users, or increasing or decreasing storage capacity.
- Service management and monitoring – visibility is needed into the services that are being used, for planning and to pre-empt any problems should things go wrong.
- Architectural flexibility – providers should be able to support integration between in-house and hosted, on and offshore, and private/public cloud architectures.

Criteria such as these impose demands on providers to assure responsiveness and transparency, particularly around management and operational processes which themselves need to be tightly defined, followed and controlled/monitored.

Governance requirements

A provider must be able to demonstrate that it is in full compliance with the jurisdiction within which it is operating. This includes criteria such as:

- Data retention – including, for example, assurances around data deletion which can be fixed according to policies set by the offshore company.
- Data ownership requires clear stipulations and guarantees. SaaS providers have been known to change their terms and conditions to suggest they own the data being stored by their systems – which renders them unusable by offshore companies.
- Financial and structural stability - A provider not only needs to be able to demonstrate how it can assure continued delivery of service and data protection, but also set out recourse mechanisms in case the provider should no longer be able to operate, for whatever reason. For example, in terms of data, copies with a third party provider or data escrow procedures.

While this stringent set of criteria might not be so vital for onshore businesses or indeed for all data types, they set the bar at an acceptable level to meet the demands of offshore businesses today. It is clear that without such criteria in place, cloud services will always be subject to limited adoption by offshore businesses. Equally, offshore organisations need to ensure they have their own houses in order, or the benefits of cloud computing will not be achieved.

Making the most of cloud

There is no one size fits all with cloud. As mentioned, several architectural models exist such as public and private cloud; resources can be situated in-house or in a hosted facility; and finally, the term itself can refer to delivering infrastructure, platform or software as a service.

For offshore organisations like Bank of Butterfield who are looking to adopt cloud services, there is no simple button to be pushed; rather, decisions need to be made at every step from selection, through procurement to deployment and management. Below I've laid out a number of best practice lessons, which are designed to help offshore organisations realise the full potential of cloud.

- Put data (classification) first. Not all data is created equal – for example, building telemetry (access data, temperature, power consumption, etc.) does not have to be stored in the same way as customer details. As such, it is essential to have appropriate data classification mechanisms in place to enable cloud service procurement criteria to be set.
- Conduct due diligence. Cloud service providers are simply suppliers, which need to be treated with the same levels of due diligence as any procurement process. Even lower-cost (or even free) services could be considered for business-critical use and therefore need to be considered as such.

- Manage IT as a service portfolio. Cloud computing involves moving from a view of IT centred on supporting products, to one which is about managing services throughout their lifecycles. Both cloud providers and internal IT services can be managed together, or considered as part of a broader portfolio of IT service delivery.
- Take a comprehensive view of costs. When buying in cloud services, it is important to consider all costs of each service across its lifetime, not just the ticket price. These include, for example, internal overheads, supplier management and contingency planning costs, all of which add to the financial impact.
- Plan for cloud contingencies. With cloud computing, the nature of contingency planning changes. I have already mentioned the need for recourse mechanisms should a provider fail; other questions to be considered include what could happen should data find itself in the wrong place.
- Consider cloud proactively. Recognise that cloud computing is a symptom of how technology adoption is evolving. Organisations that do not incorporate cloud into their IT strategies could find themselves adopting cloud services on a piecemeal basis, increasing both costs and adoption risks.

Finally, it is important to consider cloud computing as an integral part of your IT capability. The questions you need to answer – what services do you want technology to provide, what data is required or created by those services, where is the best place for the service to run and who would be in the best position to manage it – go across all of your IT, cloud or otherwise. By seeing cloud computing in this way, you are in a position to make the right decisions.

Above all, you should be honest about your own capabilities – how many organisations would be able to say they have a completely clean sheet when it comes to service delivery, data governance and so on? While no organisation is perfect, these best practice tips should help you to choose the right partner and reduce the risks to a level commensurate with the needs of an offshore organisation.

Project Scope

The following items have been deemed as the objectives that Bank of Butterfield requires from the new IT solution.

This report details each separate element that is encompassed in the objectives given to Calligo and details how this can be achieved if the proposed solution were to be implemented.

Primary Objectives

Secondary Objectives

- Remove the need to host or manage infrastructure
- Reduce Hardware Maintenance costs
- Reduced running costs, power, cooling
- Reduction costs and improve efficiencies of Anti-Virus software management

Current Infrastructure Overview

The following information is a summary breakdown of the current technologies and services in place at Bank of Butterfield:

Current Infrastructure Utilisation

Overview

Many of the benefits of cloud are built around the core ability to utilise the available resource more efficiently and effectively. Cloud take the benefits of virtualisation which is essentially all about resource management and is in some ways a return of the methodologies of mid-range and mainframe computing models to another level through the benefits of scale via multi tenancy. Therefore to understand the areas that could benefit the most from cloud it is important to actually monitor and asses the current utilisation models.

Utilisation Detail

As part of the CloudPolicy process we have run the VMware Capacity Planner application to collect inventory and performance information over a four-week period. The statistics have been collated to help formulate a detailed view of the resources used currently with in currently environment.

We use the peak load values when considering cloud, not the weekly average. As statistics are received, they are evaluated to determine what hour of the day is the peak load. The peak load is determined by evaluating load for a minimum of three weeks. The hour with the consistently highest load will be deemed the peak load hour and its average value becomes the peak load for the server.

A guide to the measured statistics

Resources	Explanation
CPU Utilisation (MHz)	Calculating the peak average GHz load placed upon the existing server estate based on % utilisation against the total amount of CPU installed.
Memory Utilisation (GB)	A calculation of the utilised memory (RAM) in GB against the allocated resource
Disk Utilisation (GB)	A calculation of the utilised disk space in GB against the allocated resource
Disk IOPS	The total storage Input/output operations
Disk Reads/Writes (MBps)	The total of the IOPs with regard to read and write operations.
Network Traffic (Mbps)	A measure of how busy the server network card is, taken from the average data throughput in Mb per second.

Data Collection Periods

Week 1 - Data captured up to 06/09/2014

Week 2 - Data captured up to 13/09/2014

Week 3 - Data captured up to 20/09/2014

Week 4 - Data captured up to 27/09/2014

Entire Estate Performance Trends

Overview

This section of the report summarises the performance statistics that are critical when planning a transition to a virtualisation environment. This section of the report is split into the following subsections.

Performance Characteristics Overall Summaries

Each area of critical importance to virtualisation/consolidation is summarised complete with utilisation graphs. This includes the following areas;

- CPU Trends
- Memory Trends
- Disk IOPS Trends
- Disk IOPS data volume trends
- Networking Trends
- Storage Capacity Requirements

Average Virtual Machine Profile

Each area of critical importance to virtualisation/consolidation is utilised to create a 'Peak Load' average machine profile.

This is then compared to the 'Industry Average' calculation figures that are provided from VMware Capacity Planner for the purpose of comparison. This industry average is based on information submitted to the VMware Capacity Planner Warehouse

Current Infrastructure Operating Efficiencies

This area takes the measured performance characteristics and measures this against capacity providing an operating efficiency percentage figure for each element, including the following components;

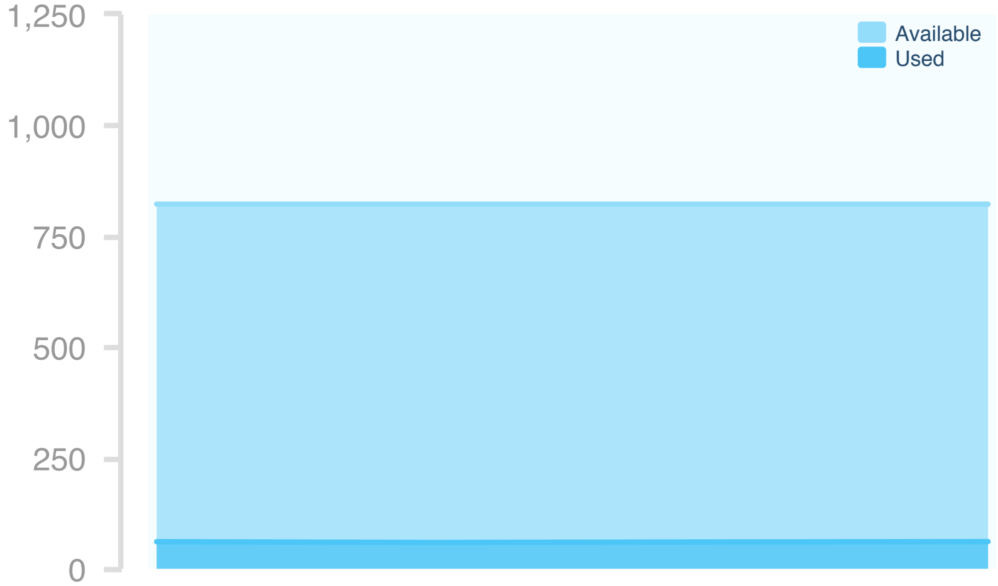
- CPU
- Memory
- Networking
- Storage Utilisation

By measuring over at least a 4 week period we are able to capture month end or periodic changes and incorporate these into the modelling.

It is important to capture the variations in the demand to ensure that enough resource is available for when the peaks occur and not leave services starved of capacity.

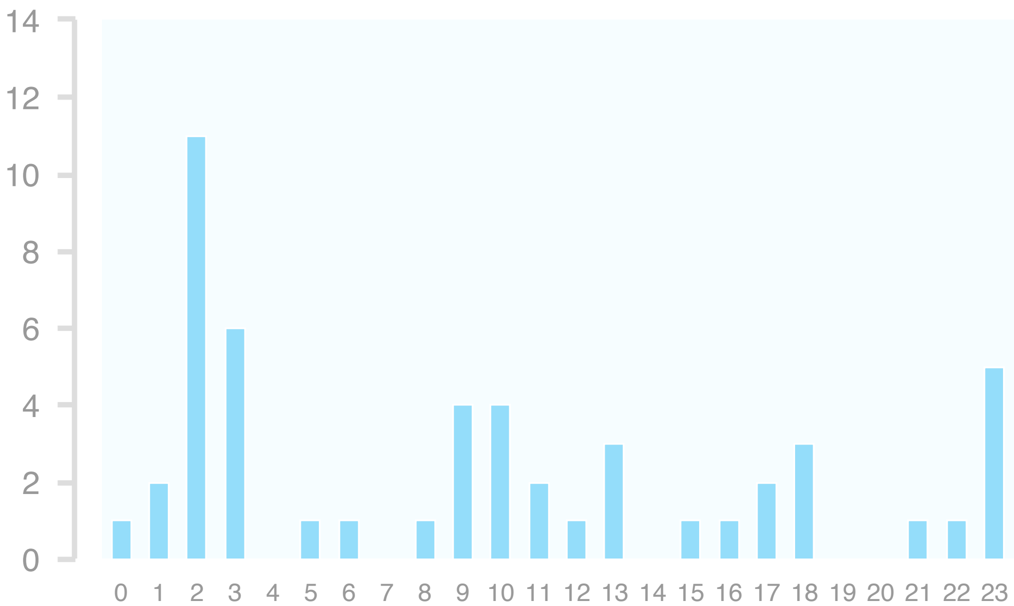
Cpu Utilisation (GHz)

Peak Values: *Available*: 822, *Used*: 61



The peak of CPU often occurs with the lowest demand for memory, this behaviour at first glance may appear odd but it is a trend that Calligo has observed before.

Peak Hour

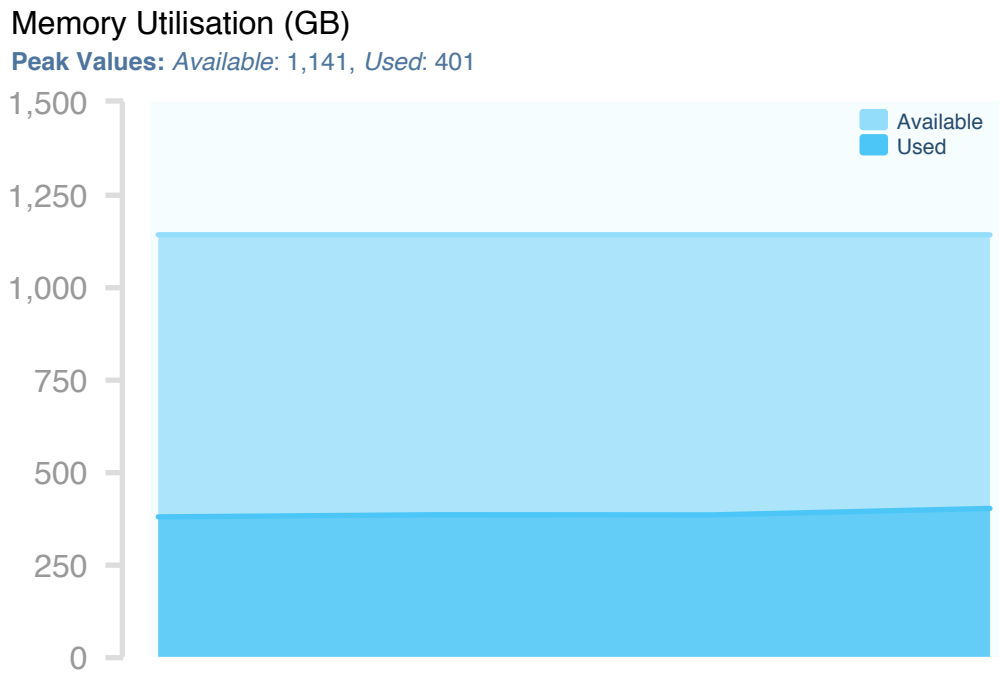


Ideally you are looking for an even spread of demand throughout the 24 hour period.

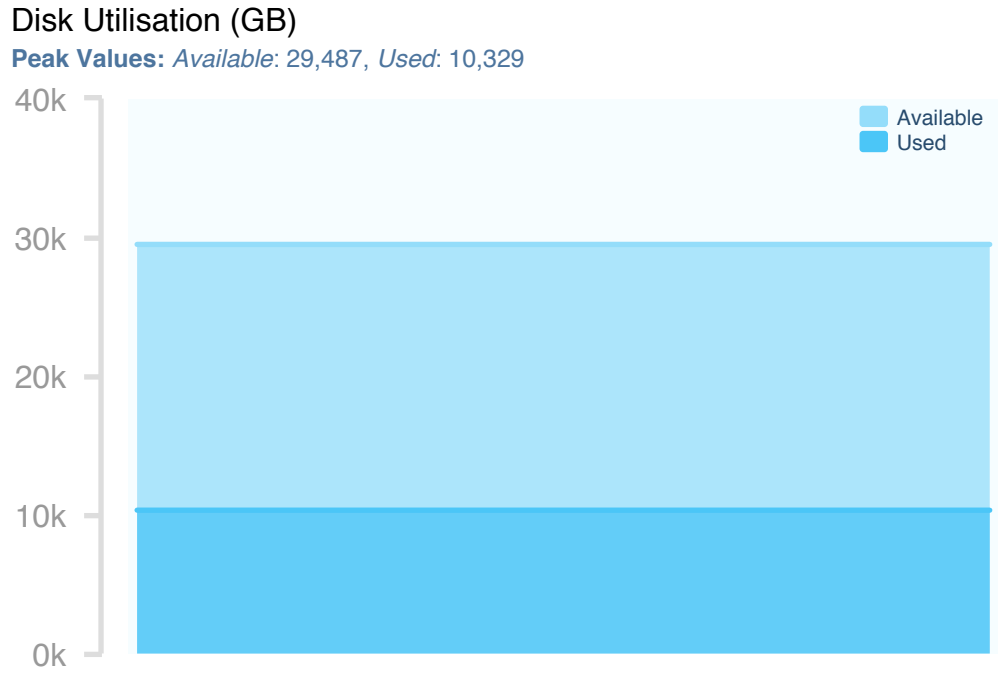
If there are concentrated periods of load being experienced this can be caused by some of the following activities:

1. Backup schedules
2. Anti Virus Scans
3. Update periods
4. Logon and Logoff

Calligo model on the load placed at peak average demand and therefore this load is catered for.



Calligo typically witnesses very little variation in memory demand and in most cases memory peak occurs at the time of least CPU demand.



By examining the week-by-week trends storage can illustrate the operational behaviour of an organisation, such as month end processes.

When the servers are moved into the virtualisation platform their disks will be presented via the Storage Area Network (SAN) and this will be used to consolidate resource.

Best practice requires a minimum of 20% additional free storage space.

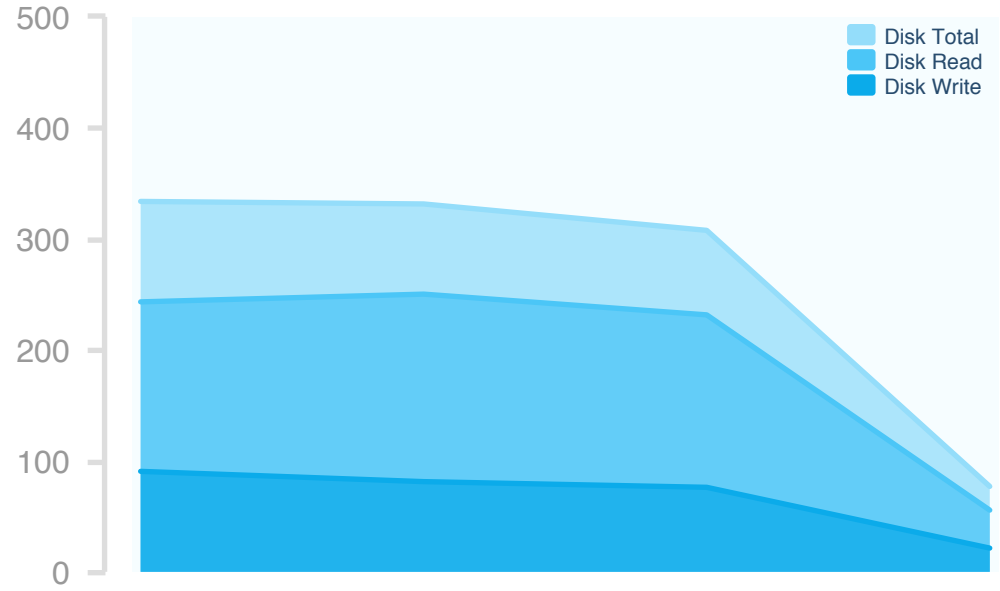
Disk IOPS

Peak Values: *IOPS*: 7,045

Storage input/output operations are monitored as the transition to Cloud based computing places a significant dependency on centralised multi tenanted storage, which needs to be capable of guaranteeing throughput.

Disk Reads/Writes (MB/s)

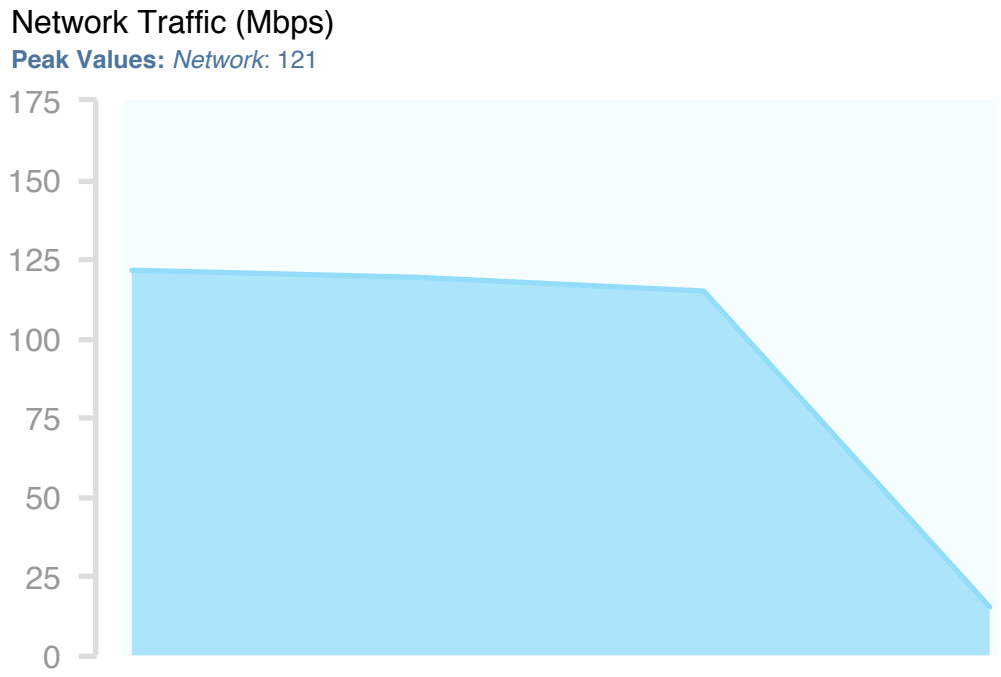
Peak Values: *Disk Total*: 334, *Disk Read*: 250, *Disk Write*: 91



Normal disk activity behaviour is to see significantly more disk read performance that write.

The graph indicates the volume of data being written out to the underlying storage. The cloud storage will need to be able to cope with not only the amount of transactions but also the volume of data.

The blend of the read and write transactions will have an effect on any storage not designed for use in a multi-tenanted platform.



Most physical machines have connection to the network via Gigabit network interface cards (NICs). When these machines are virtualised they will share network interfaces via virtual networking. Therefore it is critical that the networking layer is not overloaded causing machines to perform poorly.

In the consolidation hosts used by virtualisation, multiple physical networking interfaces will be bonded or teamed to provide higher bandwidth trunks into the main networking infrastructure and this will then be allocated to virtual machines via virtual network switches.

Detailed weekly performance analysis

Item	Totals
CPU Available (GHz)	Total CPU GHz available in the estate
CPU Utilised (GHz)	The total literal GHz consumption of the entire estate based on each individual servers consumption.
CPU Utilisation %	The percentage of CPU utilised in the estate
Memory Available (GB)	The total available GB of RAM in the estate
Memory Utilised (GB)	The total memory used in the estate
Memory Utilisation %	The percentage of memory utilised in the estate
Storage Available (GB)	The total available GB of disk space in the estate
Storage Utilised (GB)	The total GB of disk space used in the estate
Storage Utilisation %	The percentage of disk space utilised in the estate
Disk I/O	The number of disk input/output operations per second in the entire estate
Network (Mbps)	The total Mbps transferred on the network interface cards of the entire estate

Total resources across all hosts

Item	Week 1	Week 2	Week 3	Week 4
CPU Available (GHz)	822.2	822.2	822.2	822.2
CPU Utilised (GHz)	61.0	59.2	60.4	61.2
CPU Utilisation %	7.4	7.2	7.3	7.4
Memory Available (GB)	1,140.6	1,140.6	1,140.6	1,140.6
Memory Utilised (GB)	378.0	383.9	383.5	401.0
Memory Utilisation %	33.1	33.7	33.6	35.2
Storage Available (GB)	29,487	29,487	29,487	29,487
Storage Utilised (GB)	10,329	10,329	10,329	10,329
Storage Utilisation %	35.0	35.0	35.0	35.0
Disk I/O	6,652	6,772	7,045	4,275
Network traffic (Mbps)	121	119	115	15

Average utilisation per host

Item	Week 1	Week 2	Week 3	Week 4
CPU Utilised (GHz)	0.97	0.94	0.96	0.97
Memory Utilised (GB)	6.00	6.09	6.09	6.36
Storage Utilised (GB)	163.9	163.9	163.9	163.9
Disk I/O	106	107	112	68
Network traffic (Mbps)	1.9	1.9	1.8	0.2

Maximum modelled site

Item	Totals	Averages
CPU Available (GHz)	822.2	13.05
CPU Utilised (GHz)	61.2	0.97
CPU Utilisation %	7.4	7.4
Memory Available (GB)	1,140.6	18.1
Memory Utilised (GB)	401.0	6.4
Memory Utilisation %	35.2	35.2
Storage Available (GB)	29,487	468
Storage Utilised (GB)	10,329	164
Storage Utilisation %	35.0	35.0
Disk I/O	7,045	112
Network traffic (Mbps)	121	1.9

Optimised Private Cloud Resources

With the figures analysed for the virtual resources currently being utilised we can now specify the recommended resources to be secured for the optimised private cloud platform.

The following tables indicate the total available resource in each of the proposed VMware vSphere hosts to run the virtual servers.

The hardware specification below is a machine with 2 x 8 Core Processors running at least 3.00 GHz, with at least 64 GB of RAM in the both Data Centre. Modelling the statistics gathered this will require 8 hosts per site in order to provide full site failover fault tolerances.

The platform has been modelled with the following parameters:

- Most intensive processing week to provide CPU requirements
- Most intensive memory week to provide RAM requirements
- Additional host resource to cope with a failure to one host or for online maintenance
- Additional 10% loading for test and development functionality
- Additional 15% loading for immediate growth for existing projects

Host Resources Data Centre A (Primary)

Item	Host Total	Site Total
Processor (Hosts with 2 x 8 Core x 3.00) (GHz)	43.2	346
Memory (GB)	64	512
Network Bandwidth for ESX hosts (Mbps)	2,000	16,000

Host Resources Data Centre B (Disaster Recovery)

Item	Host Total	Site Total
Processor (Hosts with 2 x 8 Core x 3.00) (GHz)	43.2	346
Memory (GB)	64	512
Network Bandwidth for ESX hosts (Mbps)	2,000	16,000

Combined most intensive resource utilisation modelling

The following section takes the measured performance of the virtualisation candidates and overlays these onto the proposed consolidation resources and shows the utilisation.

Table A. Modelled candidate profile

Item	Host Total
Processor utilised (GHz)	0.97
Memory utilised (GB)	6.36
Storage allocated (GB)	0
Storage used (GB)	0
Disk IOPS	112
Network (Mbps)	1.93

Table B - Modelled site profile (using 10% annual growth)

	Utilisation Total	Proposed Total	% Utilised	Year 1	Year 2	Year 3
Processor (8 Hosts with 2 x 8 Core x 3.00) (GHz)	61.2	346	18%	19%	21%	24%
Memory (GB)	401.0	512	78%	86%	95%	104%
Network bandwidth for ESX hosts (Mbps)	121	16,000	1%	1%	1%	1%

Table C - Modelled site profile with the loss of 1 host (using 10% annual growth)

	Utilisation Total	Proposed Total	% Utilised	Year 1	Year 2	Year 3
Processor (7 Hosts with 2 x 8 Core x 3.00) (GHz)	61.2	302	20%	22%	24%	27%
Memory (GB)	401.0	448	90%	98%	108%	119%
Network bandwidth for ESX hosts (Mbps)	121	14,000	1%	1%	1%	1%

Summary

The 16 host systems would be utilised to 18% in year 1 from a CPU perspective. Based upon a growth rate of 10%, the platform would still be only 24% utilised from a CPU perspective after three additional years of growth.

Memory would be initially utilised to 78%. With a year 1 increase in demand of 10% this would occupy 86% of the 512GB RAM in the consolidation platform at each site. The platform reaches utilisation of 104% at year 3 which would require Bank of Butterfield to add further resources.

With the loss of 1 host system the remaining 7 hosts at each site would have their utilisation increased to 20% with respect to CPU resources and this increases to 22% when factoring in a year one growth of 10%.

The memory utilisation would increase to 90% with the loss of 1 host and this increases to 98% utilisation if the growth rate is 10%.

What is evident from these figures is that although the initial environment would cope with the loss of one host, the performance of the machines will in most cases be bound by the memory available to them in the event of a host loss rather than CPU.

In a two site setup the equivalent number of hosts needs to be added to the partner Disaster Recovery site to ensure resource is available in the event of the loss of one site.

What is not possible is to quantify into the figures are the likely decreases in consumed memory based on the advanced de-duplication facilities available within VMware vSphere Server with regard to duplicate memory pages.

The network demands are relatively low and would not cause a performance issue even in the event of a host loss.

Optimised Public Cloud Resources

Using the same figures for analysis as for the private cloud, we can specify the recommended resources to be secured for the optimised public cloud platform.

The following tables indicate the total available resource required in each of the proposed virtual datacentres to run the virtual servers. All resources are guaranteed and isolated for the sole use of Bank of Butterfield.

The virtual datacentres specification below for both data centres. Modelling the statistics gathered has allowed us to be specific to per site in order to provide full site failover fault tolerances.

The platform has been modelled with the following parameters:

- Most intensive processing week to provide CPU requirements
- Most intensive memory week to provide RAM requirements
- Additional resources for use in a Disaster Recovery situation
- Increase the Disaster Recovery resources from 10.00% to 20.00% to allow for test and development functionality
- Additional 15% loading for immediate growth for existing projects

Virtual Data Centre (vDC) Resources

	Total	Calligo Price Per Unit	Cost Per Month
Primary vDC CPU	61.2 GHz	£7.00	£428
Primary vDC Memory	401.0 GB	£13.00	£5,213
Primary vDC Storage *	12,394 GB	£0.20	£2,479
Primary vDC Storage Throughput	7,045 IOPS	£0.00	£0
Secondary vDC CPU	6.1 GHz	£7.00	£43
Secondary vDC Memory	40.1 GB	£13.00	£521
Secondary vDC Storage *	12,394 GB	£0.20	£2,479
Secondary vDC Storage Throughput	7,045 IOPS	£0.00	£0
Secondary vDC Bandwidth	10 Mbps	£55.00	£550
		PRIMARY SUB-TOTAL	£8,120
		SECONDARY SUB-TOTAL	£3,043
		vDC TOTAL	£11,163

* Best practice requires a minimum of 20% additional free storage space

Environmental Impact

Using estimated figures for the power used by physical, private cloud and public cloud infrastructure it is possible to compare the carbon footprint of each.

	Power Used (kW/year)	Carbon Footprint (tonnes/year)	Percentage Reduction	Equivalent number of cars removed *	Equivalent number of trees planted **
Current Physical	386,316	251.1	N/A	N/A	N/A
Proposed Virtual	224,256	145.8	42%	56	10,534
Public Cloud	10,709	7	97%	129	24,415

* Equivalent number of 1.6 Petrol MINIs removed (15km yearly mileage @ 127 g/km)

** Equivalent number of trees planted (10kg CO_2 removed per year)

Appendix A - Calligo Overview

Calligo is the Channel Islands' only dedicated cloud computing specialist and operates the most technically advanced and secure platform available within the offshore market. The team responsible for bringing virtualisation and cloud computing to the islands has over 10 years of practical experience delivering and running cloud services and over 50 years of combined cloud based technology knowledge.

Cloud computing based services represents such a paradigm shift in the way business systems will be delivered that many of the skills and disciplines required to correctly plan, design, implement and support such infrastructures are not found within the traditional server-based computing teams.

Calligo has established an unrivalled reputation built on delivering successful transformations where real strategic benefits have been delivered throughout the entire organisation.

Calligo is able to partner with their clients and, where needed, third party suppliers to develop a comprehensive, strategic, transformation plan.

To deliver the broadest range of services to its clients Calligo partners with other suppliers. Foreshore Limited provides data centre hosting services in Jersey. Sure International are a strategic partner that provides data centre hosting in Guernsey, intra-islands network connectivity and IP services to both data centres.

The following appendices provide an overview of Calligo's services. It is intended to support debate and evaluation by Bank of Butterfield. Calligo services can be configured in a variety of ways to support Bank of Butterfield's tactical and strategic needs.

Appendix B - CloudCore Overview

CloudCore is an underpinning technology that allows Calligo to deliver cloud computing services including Infrastructure, Platform and Software as Services along with other "as a Service" offerings including Disaster Recovery and Desktop. It also provides for centralised management of all the Calligo services including hybrid configurations.

CloudCentre is the unifying management layer developed by Calligo that allows Bank of Butterfield to capitalise on the flexibility and agility offered by cloud computing. Using a single management area Bank of Butterfield can provision resources across multiple cloud environments.

CloudCentre management layer

- Advanced architecture for the management of multiple cloud environments: hybrid, private and public.
- Single management environment that insulates the user from the complexity and diversity of the underlying architecture.
- Central access to support auditing of migrations, performance, change & configuration management and capacity plan.
- Management Information; a dashboard providing MI such as performance, utilisation, usage and cost.

Calligo's Infrastructure as a Service (IaaS) cloud computing service offers a secure, self-managed technology environment that gives Bank of Butterfield the flexibility to deliver computing resources when needed, as well as evolve and develop without any restriction on future decisions about operating systems, hardware or applications.

It also:

- Provides the freedom to choose the exact type of model wanted, while leveraging the existing infrastructure as your business needs evolve.
- Simplifies both provisioning and deployment, is cost effective, stable, scalable, reliable and enables a rapid response to business change.
- Eliminates unnecessary capital expenditure, reduces approval cycles and time-to-market, gives easy, self-service access and a sense of control.
- Enables Bank of Butterfield to allocate resource in a granular manner to gain maximum efficiency from the resources you procure.
- Provides 'elasticity', giving Bank of Butterfield the flexibility to acquire or release capacity on demand, have control over the whole technology environment and service levels, greater visibility into costs and greater automation through software with lower system administrator to server ratios.
- Provides the required security and control to help ensure Bank of Butterfield meet their security and compliance requirements.

Using technologies from several leading cloud vendors, Calligo offers an enterprise class architecture that leverages the power of cloud computing while retaining the flexibility, security, and open standards to support Bank of Butterfield's existing and future IT requirements.

A cloud service is enterprise class when it provides multi-tier security including physical, infrastructure and user levels, compatible management and security models to enable application portability to and from internal datacentres, and fast self service provisioning of resources. Some of the requirements of an enterprise class cloud service include business agility, auditable security, flexible service levels and

control.

Hardware

Calligo's CloudCore services are built to a standard design using VMware's vSphere and vCloud Director implemented on hardware from IBM, SolidFire, Netgear and Cisco, housed within Foreshore's datacentre in Jersey and Sure International's facility in Guernsey.

The physical infrastructure is designed with resilience built in so that single points of hardware failure are avoided and also makes use of VMware's high availability features.

Storage platform

Calligo exclusively use SolidFire's storage platform. This was specifically designed for cloud service providers and is entirely based on solid state drives. This provides an extremely fast disk system and enables Calligo to deliver, and guarantee, any level of disk performance whether high or lower (IOPS) without impacting on other clients using the CloudCore platform.

All data at rest within CloudCore is 128 bit encrypted. Our understanding is that we were the first cloud provider in the world to provide this. Encryption is managed at the hardware level so there is no degradation of performance.

VMware vSphere

VMware vSphere is the industry-leading virtualisation platform for building cloud infrastructures, offering the highest levels of availability and confidence when running business critical applications.

Calligo makes full use of the enterprise VMware features including vMotion and Distributed Resource Scheduler (DRS), ensuring resilience and performance at all times.

vCloud Director

Built on top of vSphere, vCloud Director provides the secure and scalable multi-tenancy which is a key component of an enterprise-class cloud. Calligo's CloudCentre enables Bank of Butterfield to access and consume their cloud resources quickly and simply. The self-service capability enables the provisioning, access, modification and consumption of cloud resources with maximum agility.

With the ability to provide for different tiers of service, vCloud Director enables us to provision your cloud environment with one or more virtual datacentres (vDCs). Within your own vDC, we allocate the CPU, RAM, storage and networking resources you need with complete perimeter network security between each customer's vDC provided by vShield Edge.

vShield Edge

VMware vShield Edge integrates with vCloud Director and vSphere providing features such as Firewall, IPSec VPN, NAT and DHCP services that provide the required perimeter security between the vDC and any other external networks. Customer configuration through the CloudCentre web portal offers virtualisation aware security, simplifying application deployment and enforcing the boundaries and edge security required by compliance standards.

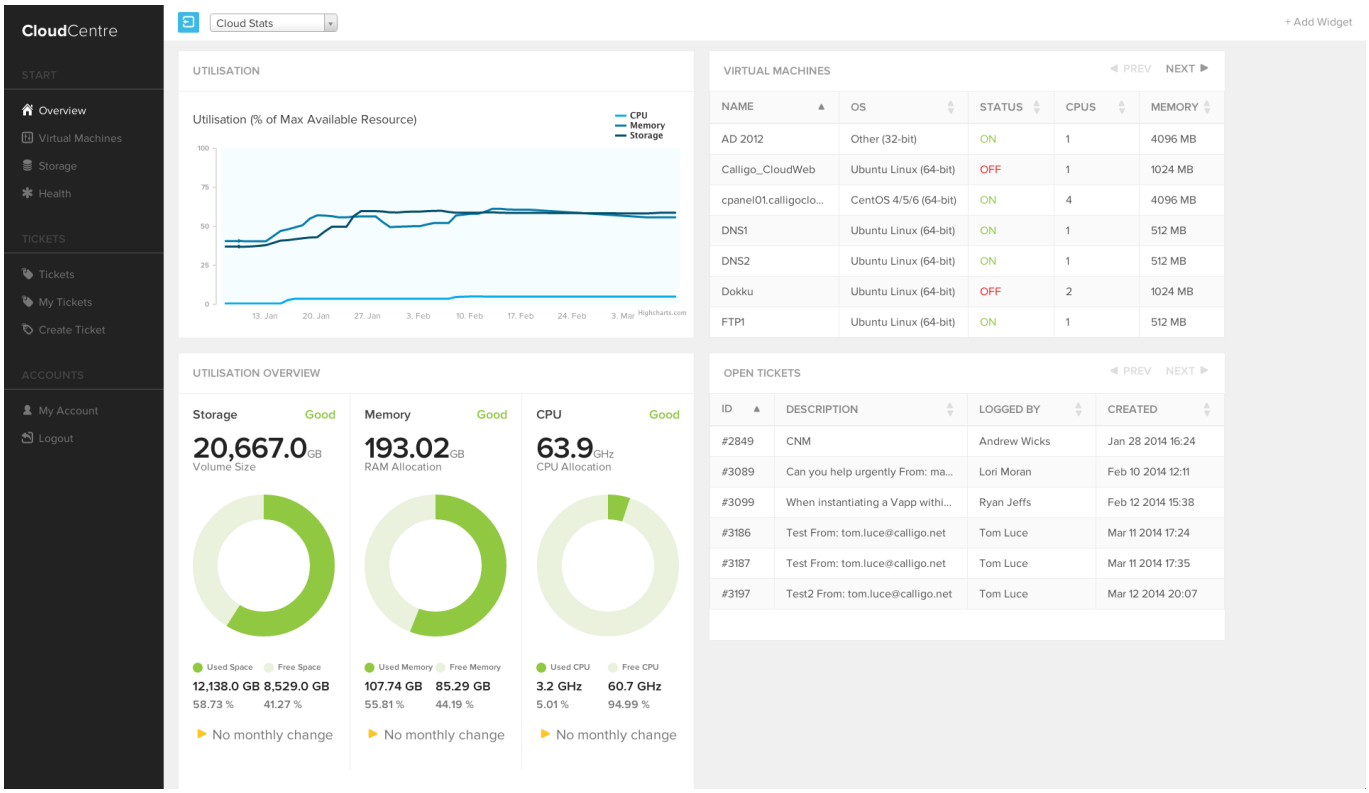
Catalogues

Customers can deploy standard services from catalogues through the CloudCentre web portal. Catalogues contain templates such as vApps (to deploy virtual applications containing one or more virtual machines), and media that they can attach to virtual machines to then appear as if a CD had been inserted. Catalogues are an important feature of a modern cloud computing environment. They ensure that standard machines are deployed that conforms to Bank of Butterfield's information security policy.

CloudCentre Portal

This has been developed by Calligo to provide an easy to use, highly visual tool for reporting and management. It can connect to multiple clouds (e.g. Calligo's CloudCore, a private cloud or a third party cloud) to allow consistent management of cloud resources.

This screen shot shows various performance and trend statistics and a real time view from Calligo's Helpdesk system.



Infrastructure as a Service (IaaS) Security

Calligo's CloudCore Infrastructure as a Service product is based on VMware technologies.

VMware offers secure and robust virtualisation solutions for virtual datacentres and cloud infrastructures, and has both the technology and the processes to ensure that this high standard is maintained in all current and future products.

VMware virtualisation gives you:

- Secure architecture and design: Based on a streamlined and purpose-built architecture, vSphere is considered by experts to be the most secure virtualisation platform.
- Third party validation of security standards: VMware has validated the security of their software against standards set by Common Criteria, NIST and other organisations. VMware

ESXi has Common Criteria EAL 4+ Certification.
- Proven technology: More than 300,000 customers – including all of the Fortune 100 as well as military and government installations – trust VMware to virtualise their mission-critical applications.

The implementation of VMware vSphere and vCloud Director and related technologies in the CloudCore environment has been performed following VMware and Calligo's best practice hardening guidelines along with the use of enterprise controls for security and compliance.

Isolation is provided by design for all aspects including:

- CPU & Memory: VMs have limited access to CPU, memory isolation is enforced by hardware, and memory pages are zeroed out before being used by a VM.
- Virtual Storage: VMs only see virtual SCSI devices, not actual storage. Exclusive VM access to virtual disks is enforced by VMFS using SCSI file locks.
- Virtual Network: No code exists to link the virtual switches, and virtual switches are immune to learning and bridging attacks.

VMware vShield Edge is used to provide comprehensive perimeter network security for virtual datacentres integrating seamlessly with VMware vSphere and VMware vCloud Director. It provides the essential security gateway services to safely share network resources by creating logical security boundaries that provide isolation for virtual datacentres in the vCloud environment. vShield Edge is deployed as a virtual appliance to provide firewall, VPN, NAT and DHCP services, delivering network security within the virtualised environments and providing the logging and auditing controls that are needed to demonstrate compliance with internal policies and external regulatory requirements.

Disaster Recovery

Cloud computing has many benefits that assist in the delivery of a Business Continuity plan including the ability to simplify and automate the tasks required to provide reliable and rapid disaster recovery. Using Calligo's CloudCore Bank of Butterfield will have an infrastructure platform where data and services, for the whole group, are replicated across two sites.

Technologies that are standard within the CloudCore product such as data replication, high availability and fault tolerance mean that Bank of Butterfield will be well positioned to survive the loss of a single device, multiple devices or even a whole site. In most cases services will continue to be delivered without any impact to end users.

The CloudCore service provides a highly available service with guaranteed service levels so the disaster recovery service would only be needed in extreme circumstance such as the loss of the whole site. Although it will be rare to invoke a disaster recovery service the nature of Bank of Butterfield business means that it is essential that it has reliable and tested business continuity and disaster recovery plans.

CloudSafe

CloudSafe is Calligo's disaster recovery option. It's a specially designed variant of CloudCore that allows clients to reserve the computing capacity they would need in a disaster scenario but only pay for it when it is needed. Assuming that Jersey site is hosting all production environments and CloudCore Guernsey is the DR site then only a percentage of the required (live) processor (CPU) and memory (RAM) are provisioned and paid for. On invocation or testing these will be increased. Disk always needs to be provisioned at 100%.

This is one of many scenarios. CloudCore offers great flexibility and a number of different DR scenarios become possible and will need to be discussed during the detailed planning and design phase.

CloudCopy

This is Calligo's backup service. Bank of Butterfield servers would be backed-up to Calligo's cloud and the backups are replicated across the two sites. CloudCopy removes reliance on tape or other less reliable backup media, reduces the internal effort required to administer traditional backup solutions and removes the need for physical tape storage. Delivered as a fully managed service it means that Bank of Butterfield staff can concentrate on other aspects of IT delivery knowing that the Society's data is continuously protected.

CloudCopy uses the market leading software from Asigra to back-up the widest range of servers. These can be physical or virtual and a wide range of operating systems are supported. In general the Asigra software is agentless and requires no client installs. An agentless approach removes compatibility problems caused by different combinations of agent, operating system and application revision levels. An agentless design is inherently easier to support and does not rob processing power from the core application of each machine that is being backed up.

The backup software encrypts your data in-flight and at-rest. Different encryption strengths are available including AES 256-bit with a 32 character key. Only Bank of Butterfield hold the encryption key. The backup software has achieved the highest level of independent accreditation – no one else can read your data whether on the fly or at rest.

Calligo has partnered with Databarracks to deliver CloudCopy. Databarracks has a 10 year history of delivering managed backup solutions; they have over 1,000 clients and protect in excess of 10PB of data.

CloudCopy is highly configurable so that it will deliver Bank of Butterfield's backup and data retention policy. It uses different disk systems to handle short and long-term backups. This allows for long term retention of data at an affordable price point.

Online Backup advantage

The CloudCopy service provides a highly reliable, automated backup and recovery service that assures fast and accurate restoration following data loss or destruction.

Instant offsite backup

- Immediately transfers backup data to two diverse and secure datacentres
- Online backups are conducted automatically and without human intervention
- This automated process, coupled with detailed reporting, provides a clear view of the chain of custody of stored information with rapid access should it be required.

Increased control

- Centralised management and control of all backup tasks
- Critical data automatically transmitted offsite to dual data vaults
- Only you can decrypt your data
- No risk of backing up to faulty tapes
- Calligo's support team monitors the backup service round the clock

- Detailed audit trail for every backup is emailed to the client every day
- Ultimate in equipment compatibility and data delivery for business continuity planning

Increased data security

- Data is compressed, de-duplicated and encrypted at the customer server prior to transmission – minimises data stored
- Data remains encrypted and protected in the secure vaults
- Various levels of encryption to choose from
- Data is never handled by a third party

Saves time

- Automatic process requires no manual prompting or on-going management
- No inventory management and shipping of backup tapes offsite for storage
- Only new files and changes to existing files are backed up, reducing bandwidth requirements and backup window
- Data is always available for restoration
- No need to retrieve tapes from storage to conduct a simple file restore

Saves money

- Dramatically reduces costly downtime
- No capital investment
- Reduces or eliminates upfront and on-going hardware and software costs
- Reduces in-house staff time managing tapes and backups
- Supports multiple operating systems and databases
- Capacity review
- Configuration/performance tuning
- Delivery of health check report
- Short & long term storage
- CloudCopy has two tiers of storage; one for fast retrieval of short term storage and the other for long term archiving.

Appendix C - Inter site failover

To achieve VM level replication between multiple datacenters we leverage VMware's vSphere Replication Appliances (VRA). This replicates VM disk level changes from one physical site to another, hence replication is configured on a per VM, not per LUN basis. The RTO for VRA replication is asynchronous and scales between 15 minutes and 24 hours at 15 minute increments, however it will endeavour to replicate in as near time as possible, bandwidth depending.

To facilitate a site failover a vCenter object dedicated to a pool of ESXi hosts has a stretched network between two or more sites with hosts spanning all sites. A site is considered dormant when Hosts within this site are in Maintenance Mode. Failover is achieved by shutting down virtual machines, waiting for VRA replication to synchronise between sites and re-associating virtual machine objects with dormant hosts in alternative sites.

Failover between sites can be automated through various scripting mechanisms, this can include a structured power-on of the site's VMs based on business roles and requirements for each service provided. For example; firstly virtual firewalls, followed by Domain Controllers, followed by database servers, followed by application servers and so on.

Dedicated Storage is required at each respective site as well as each site requiring full compute capacity to run the VM environment.

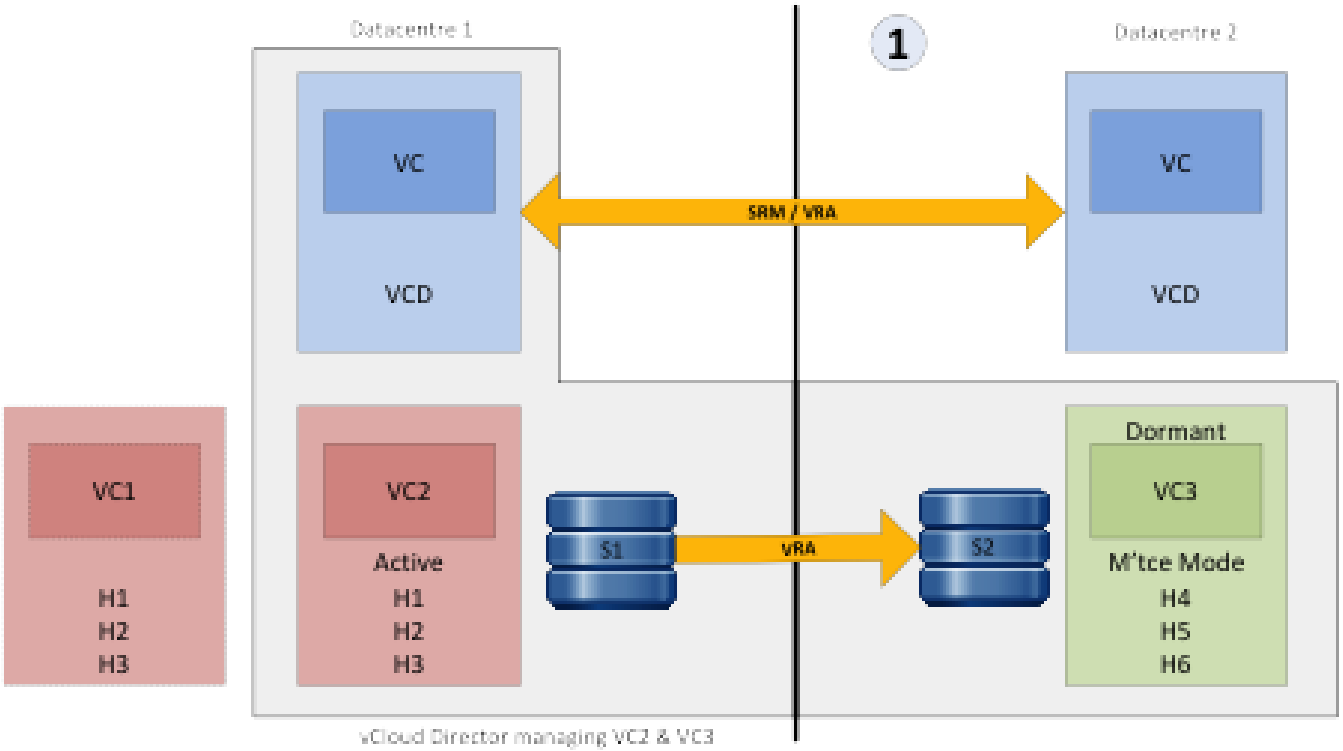
Protection of the vCloud is provided by SRM at the management layer, removing the single point of failure.

Consideration is to be made for the vSphere Replication Appliances within the estate; a minimum of one VRA per ESX host is required with recommendations for more dependent on the host workload.

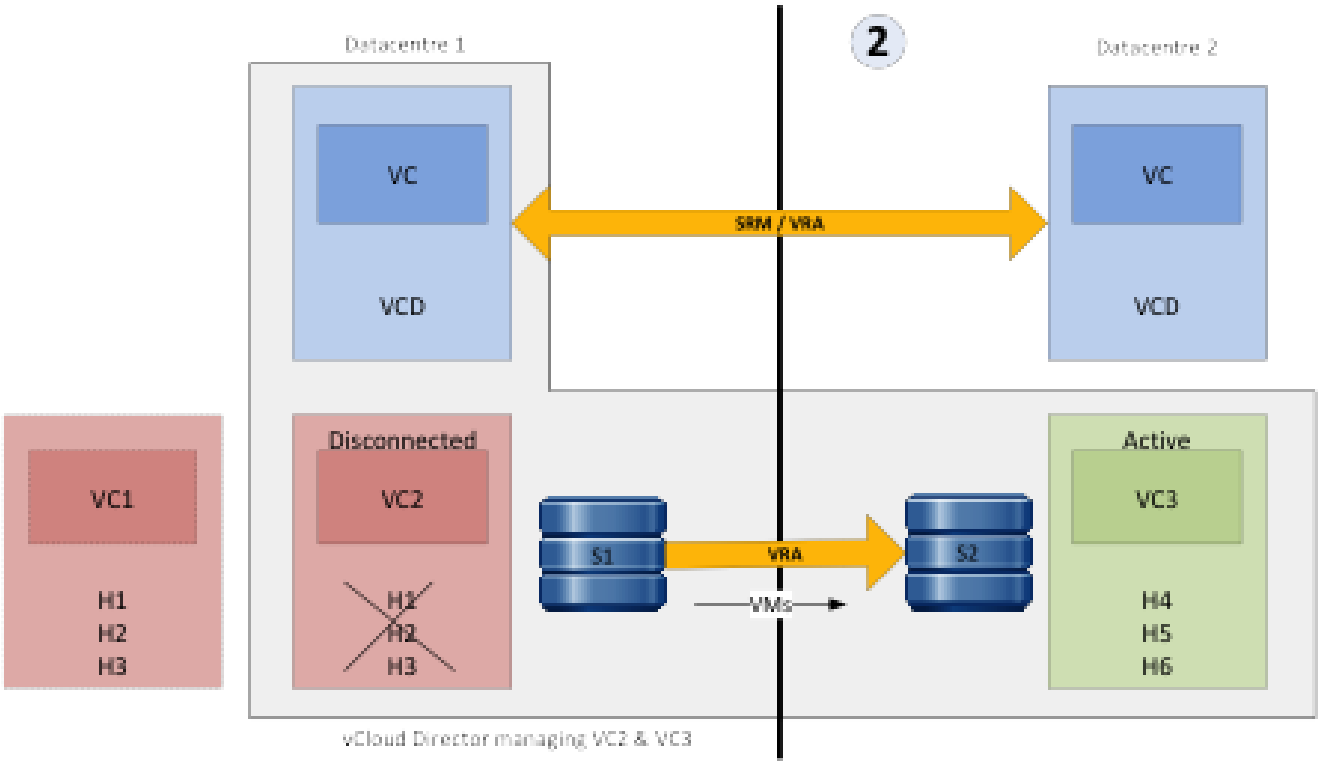
Failover times from site to site:

Action	Duration
Virtual Machine shutdown time	10-15 seconds + x minutes for OS shutdown
Wake dormant alternate site	2-3 minutes
Synchronise VRA changes	~15 minutes
Re-Register Virtual Machine with alternative site	2-3 seconds
Power up VM	3-5 seconds + x minutes for OS boot time

This is represented pictorially below.



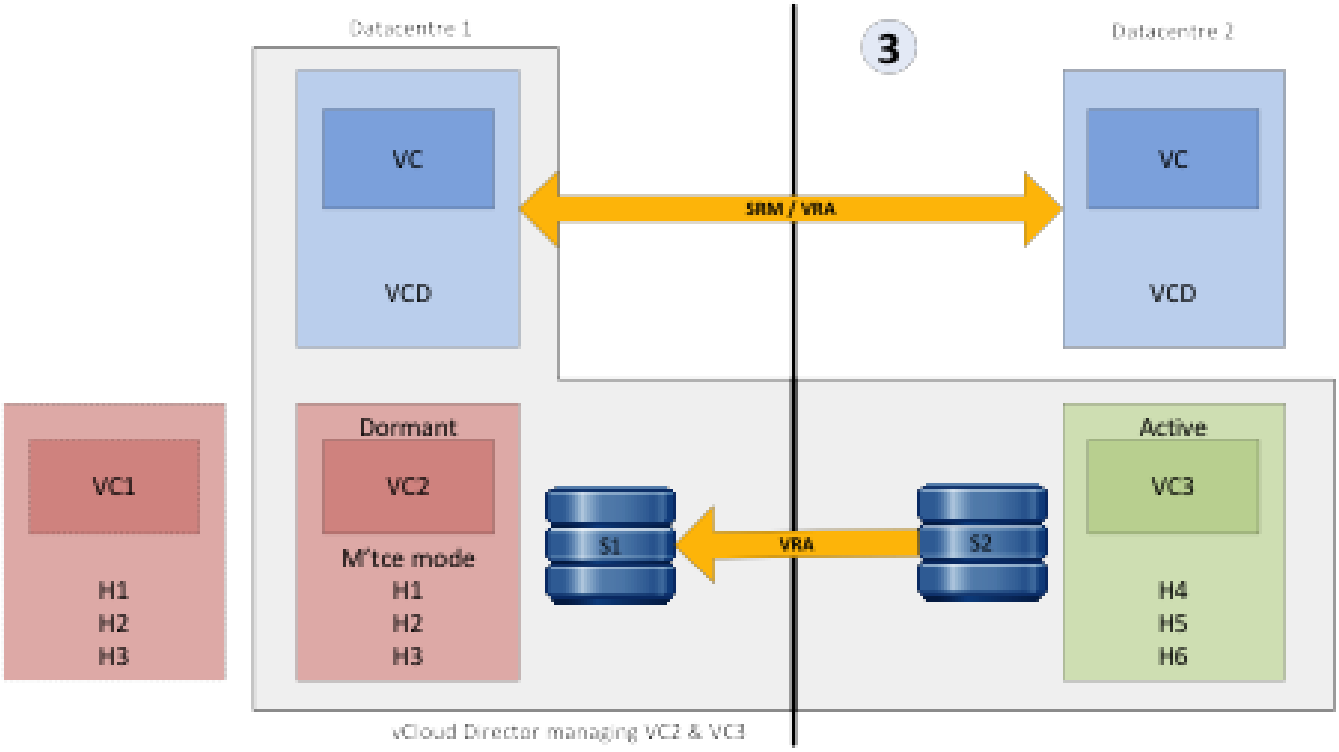
- vCloud Director is protected across two sites using SRM.
- vCenter 2 (VC2) (the active compute cluster) is replicating across sites.
- VC3 is dormant and in maintenance mode.



This is the process of making VC3 the active compute cluster.

- Disconnect VC2
- VRA has replicated the active VMs to Site 2.
- Make VC3 the active compute cluster.

- VMware HA registers the replicated VMs to now active cluster.



- Site 2 is now Active – VC3 is now the active compute cluster.
- VC2 cleans configurations, goes dormant and to maintenance mode.
- VRA is reversed – now replicating storage from Site 2 to Site 1.

Appendix D - Governance and Information Security

Calligo is an Accredited Quality Management System (QMS) company as specified in ISO 9001:2008. The scope of Calligo's QMS comprises Service Delivery, Project Management, HR and Supplier Management. Calligo employs a Compliance Manager, who is professionally trained as a lead auditor, to maintain and improve its quality, both internally and to its clients.

Constant integration of best practice and operational conformance to its published policies and procedures is undertaken.

ISO 27001:2005 standards are now being finalised. This is a more prescriptive standard than ISO 9001 and defines the information security management system that an organisation must operate. We anticipate assessment and accreditation to be completed by end 2013. Beyond this Calligo will be adopting the STAR standards that are now being scoped and developed by the Cloud Security Alliance, these standards are international recognised, as the de facto standards that cloud services providers should adhere to. These extend the ISO standards and reflect best practice that is specific to cloud service providers.

Appendix E - Data Centre Overview

Jersey

Foreshore is an international class Internet communications company that has been operating since 2000 in the Channel Islands and since 2001 internationally.

Foreshore's major shareholder is the Jersey Electricity Company (JEC) which is a public company and is listed on the London Stock Exchange. The JEC's major shareholder is the States of Jersey (Jersey's government). Foreshore's primary datacentre is housed at the JEC's Queens Road facility, which is a converted power station. This location is ideal as it naturally provides the ability to connect to different parts of the JEC power distribution network.

Foreshore's multi-site, resilient Internet backbone offers the very high level of reliability, scalability and security that is vital for businesses to thrive in today's challenging economic environment. The design of the backbone ensures there are no single points of failure and no reliance on any single service provider.

Foreshore holds an ISO 27001 certification covering its datacentre operations and is also accredited as a PCI DSS (Payment Card Industry Data Security Standard) Level One Service Provider.

Foreshore's operations team works on a full 24x365 shift rota to provide cover 24 hours per day, 365 days per year. The operators are trained in incident management and escalation through defined procedures. Infrastructure and systems are monitored from within the Network Operations Centre (NOC) and include security cameras, door access control, datacentre air temperature and humidity, fire detection equipment, critical power unit status and network status.

Power and environmental provisioning

All critical systems in the datacentre are fully redundant with power provisioning and distribution providing 2N resilience and air conditioning N+3 resilience.

Infrastructure design includes the following:

- Two independent sources of electrical supply from separate transformers
- Two distribution restoration standby generators on site
- 2N UPS systems including maintenance bypass
- Power distribution utilising critical power distribution units connected with static switches and including maintenance bypasses
- Dual radial individually fused circuits from separate distribution boards to client racks and equipment
- N+3 full function, downflow DX, self-contained and close control air conditioning units with remote condensors
- Temperature and humidity monitoring and control to maintained 21° centigrade +/- 2° and 50% relative humidity +/- 10%
- Water leak detection system
- System monitoring by IS1000 building management system

Guernsey

Located in Sure International's facilities at Centenary House, La Vrangue, St. Peter Port the purpose built Sure Data Centre is 25m above the highest recorded sea level, is built in an area free from any recorded seismic activity, is 4.2 miles from Guernsey Airport and is not on any airport flight path.

Sure Data Centres, surrounding and adjacent buildings:

- Do not contain hazardous or heavy industrial operations
- They present no risk of explosion or leakage of chemical irritants or fire
- There is no risk of flooding from rising costal tides or other bodies of water
- There are no large thoroughfares, roadways or railways adjacent or which bypass the site.

The Sure Data Centre in Guernsey already hosts many customer platforms annually certified and audited against the International Security Standard ISO27001 and the Payment Card Industry Standard PCI DSS. Sure is now engaged in completion of its own accreditation, of Data Centre services, and this will be completed by September 2013. This initiative confirms Sure's commitment to maintaining its position as a leading provider of communications and hosting services and solutions to the offshore and Channel Islands community.

Calligo's services are based in Sure's newest data centre buildings – the result of an investment of some $20m with a focus on security and resilience. Calligo's services leverage Sure's hosting and facilities management expertise:

- An onsite 24x7x365 network operations centre
- High power and cooling infrastructure
- Building management systems
- Security control systems
- Environmental management systems
- Fire suppression and detection tools
- A resilient ring power supply with multiple onsite substations
- Resilient UPS's, battery backup's
- Resilient diesel generators, 36 hours of diesel storage onsite and guaranteed offsite diesel storage with 24x7x365 guaranteed supply to site.

Appendix F - Core IP Network

Calligo leverages Sure Internationals IP network which is provided over 4 x diversely supplied 10Gbps (gigabit per second) fibres over 4 diversely routed and independent submarine cable systems (Hugo North, Hugo South, Hugo East and VTL Wavenet), the Sure Cisco-powered network consists of multiple diverse Guernsey Points of Presence (PoPs) connected directly to multiple Sure Guernsey PoPs within the heart of London and Paris telecommunications networks. Global IP connectivity is guaranteed by connecting multiple Tier 1 IP transit providers delivering world class levels of performance, resilience and quality of service to Sure Guernsey.

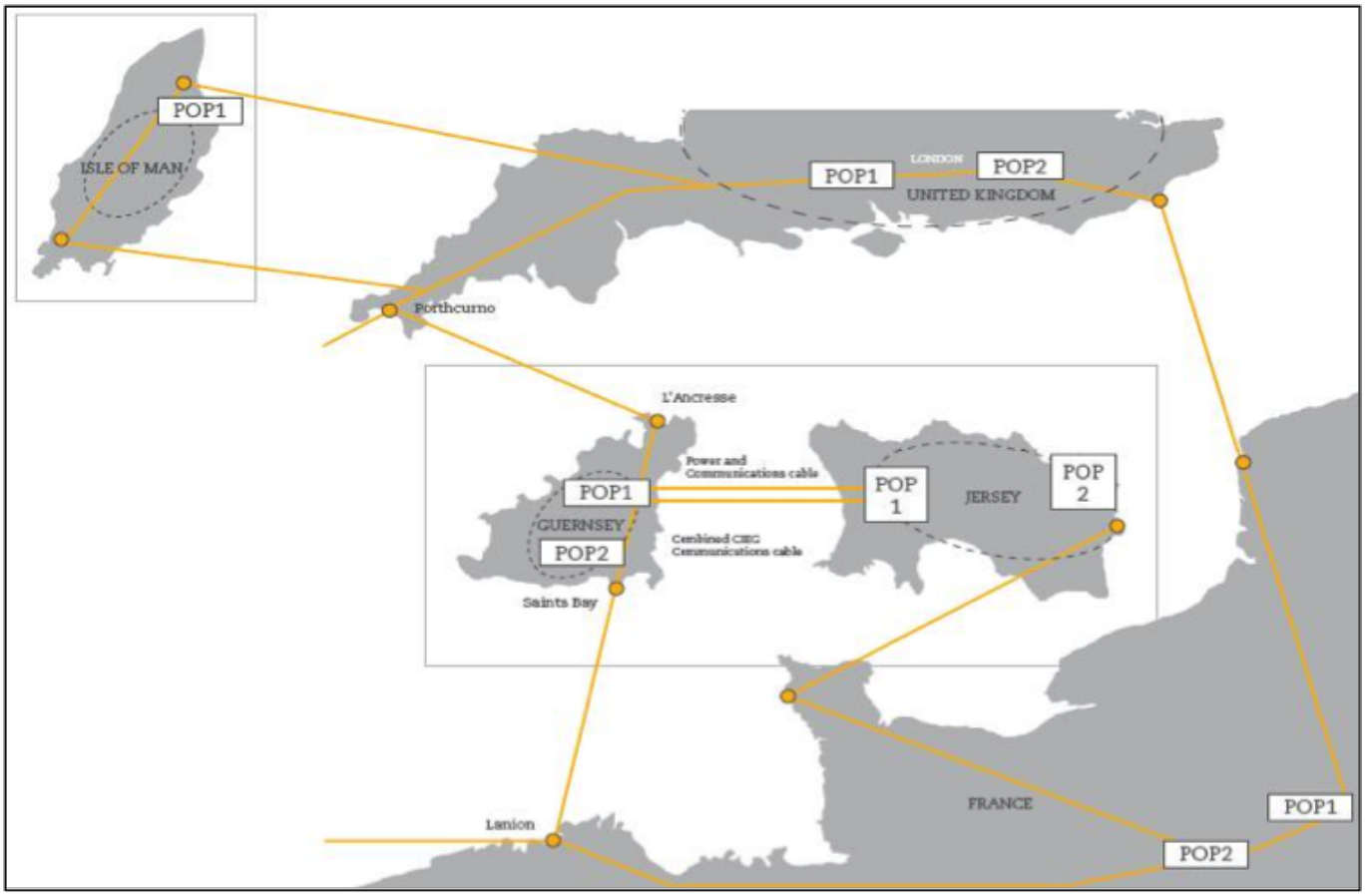
A summary of the key design criteria employed in IP network build are as follows:

- >99.999% core availability, including planned outages and DDoS attacks
- The core network is specified to recover from failure at the IP layer within 50ms allowing customer applications to be wholly independent of internet architecture deficiencies, and the associated multi-minute network (BGP) convergence times.
- <20ms latency between the UK internet backbone and the hosting facility
- <20ms latency between the Paris internet backbone and the hosting facility
- <0.03% packet loss between the private network edge and the hosting facility
- <10ms jitter between the UK & Paris internet backbone and the hosting facility
- Scalability and flexibility. The network is engineered for fast upgrade to allow integration of additional high capacity fibre links or Tier 1 IP transit services.
- Resilience. The off-island network is delivered over multiple carriers' fibre backbones, each with guaranteed diversity at four core fully resilient PoP locations in London, Paris and Guernsey.
- Upstream Internet connectivity will be provided via multiple direct connections to Tier 1 IP transit providers and can also include multiple Public Internet Exchanges.

To ensure maximum redundancy and circuit resilience and to deliver fully protected connectivity solutions, Sure's undersea fibre interconnect is built with guaranteed diversity (4 x 10Gbps links) - see Diagram 1. Fully resilient Layer 3 IP connectivity is then provided upon a fully resilient Cisco 12000 series and ASR9000 series core – see Diagram 2.

Furthermore, having implemented BGP Pre?x Independent Convergence (PIC) Sure's network is designed to recover from failure at the IP layer within 50ms, allowing hosted applications to be wholly independent of internet, fibre and network architecture deficiencies, and the associated multi-minute network convergence times historically required by BGP. Sure's enhanced core network is designed to provide 99.999% availability of internet bandwidth and is now also protected at its high capacity network edge by Sure's own fully integrated multi-layer and multi-vendor DDoS protection system supported by a specialist 24x7x365 DDoS security operations centre (SOC).

Diagram - 1 High Availability Submarine Fibre Routing



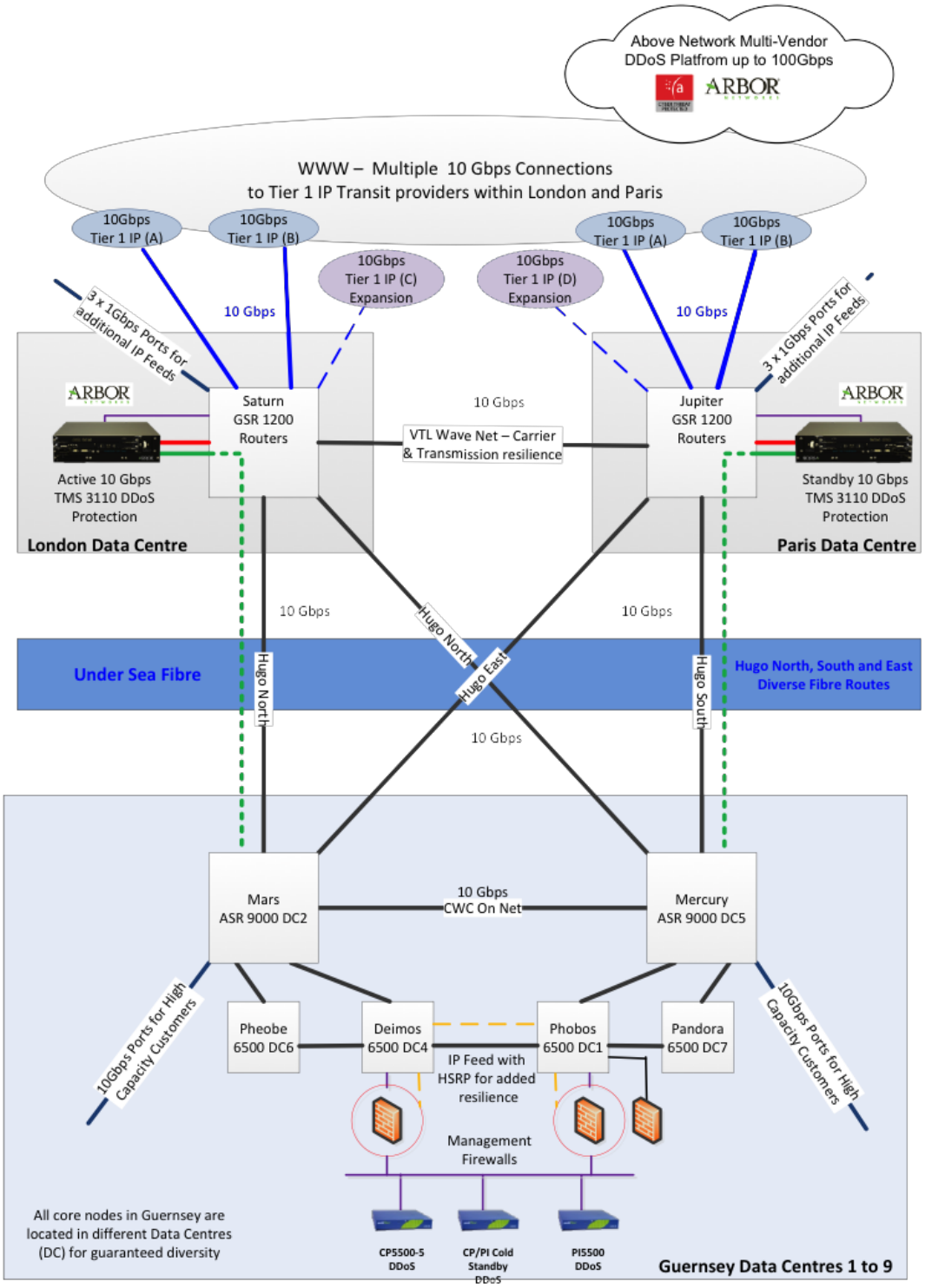
This diagram shows the undersea cables relating to Channel Island connectivity over the Hugo network – North, South and East. These cables systems are wholly owned by Sure.

POP locations indicate logical rather than physical network points for business connectivity.

DWDM termination equipment allows for multiple wavelengths on the cables providing near limitless bandwidth. A summary of the networks key design criteria are as follows:

- 4 x Submarine Cable systems
- True international connectivity
- Xtera DWDM hardware
- Cienna Core Director Mesh
- 80 x 10Gb EU/US transit links lit and carrying >100Gbps through the channel Islands

Diagram 2 - High Availability Layer 3 IP Network Design



A summary of the networks key design criteria are as follows:

- Built on Cisco GSR 12k carrier routers
- Implementation PIC technology <50ms convergence
- On-net Arbor DDoS Mitigation 2 x 10Gb
- Above-net DDoS mitigation up to 100Gb (Arbor & Adversor)
- Award winning designs (eGaming Awards – Best Connectivity Provider)
- Independent of Layer 2 network – built on dedicated 10Gb wavelengths
- Multiple Tier 1 IP transit peers & access to key internet exchanges
- Dedicated Layer 3 IP network, High Capacity International Private Lease circuits are available over a completely separate Sure Layer 2 network.

This diagram shows the core network nodes that Guernsey is physically connected to. The redlines indicate STM64 connections. Core Directors shown in green form part of this Global physical mesh. This mesh is provided over a highly resilient, self-healing, evolution of SDH. Multiple STM64 routes connect North, South and East from Guernsey into the Global mesh network.

Guernsey is a key point in the Cable and Wireless's worldwide global network providing part of the ring/mesh that connects the UK and Europe to the US. Typically 80Gbps of transit traffic bound for the US passes over this link at any one time. A summary of the networks key design criteria are as follows:

- Cienna Bandwidth Services
- Sure Alcatel Lucent MPLS Core
- No IP backbone services on this network
- Ethernet Services
- Point to Point and Point to Multi Point
- Full restoration on SDH and clear channel (optical services also available)

Appendix G - Cloud Computing Explained

Cloud computing covers several layers of technology and business process. The first of these layers is Infrastructure. This is an evolutionary step forward from virtualisation, which is a technique for managing IT resources so that the needs of users, rather than the physical configuration of hardware, are paramount. Cloud computing takes this technology and massively scales it to allow even greater levels of efficiency through the use of multi-tenanted techniques, which also incorporates true client isolation.

In practice it involves presenting users with a logical rather than just a physical or virtual view of available resources, according to their function, regardless of their physical layout or location. Conceptually, this is achieved in one of two ways:

- One physical resource (e.g. a server) can appear, from the user's point of view, to be servicing multiple 'virtual' resources.
- Alternatively, multiple units of resource (e.g. disks) can appear to the user as a single virtual unit.

For example, with cloud computing one physical server can service a number of different clients' virtual servers, each meeting the needs of a different client and within that client's groups of users. To all the different clients and users, it will appear as though they are working with entirely separate servers, which are grouped together based on the client but kept completely isolated from each other: the fact that a single hardware unit is servicing all of their needs is irrelevant, and not visible by the user.

This means that resources such as storage, memory and processors can be allocated dynamically and changed as and when requirements change, which is more efficient than using a number of discrete physical servers or a dedicated virtual based solution, each with resources dedicated to it. With separate physical or dedicated virtual infrastructure, if one of them is not required for a period its resources are wasted by lying idle; however with cloud based services, whenever a virtual server or application is inactive the resources previously allocated to it can be immediately diverted to other parts of the Cloud that require them.

However, cloud computing is not limited to infrastructure, although that is the best-known context in which this approach is currently used. The same principles are also applied to applications that are Cloud based whether they are delivered through the Platform or Software as a Service models.

Infrastructure as a Service is the most widely understood utilisation of cloud computing, where Amazon has been leading the adoption of this area. Infrastructure as a Service is where the raw resources of computing like CPU, memory and storage are bought and used on a pay as you go basis.

Platform as a Service provides a computing platform and solution stack as a service. It utilises the resources provided by an underlying Infrastructure as a Service offering, facilitating the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and usually provides all of the facilities required to support the complete life cycle of building and delivering applications.

Software as a Service (also referred to as 'on-demand software') is a software delivery model in which an application and its associated data are hosted centrally (normally via a Cloud platform) and are typically accessed by users using a web browser over the Internet.

Headline Benefits of Cloud Computing

Issue	Cloud Computing Solution	Benefit
Data Centre Costs	By using the physical resources more efficiently the asset is worked to higher levels (typically taking utilisation from sub 10% towards 80%) and therefore less hardware is required which reduces the costs associated.	Power, cooling, space and maintenance costs can be significantly reduced.
Operational efficiencies	Servers that were previously hardware based are presented as software and therefore deployment of servers can be achieved far more rapidly and reliably. Typical commissioning of a server that used to take 2 days (operating system and patching only) can be reduced to minutes by deploying standardised templates of virtual servers that are hardware independent.	Server deployment can be completed in significantly less time and with higher degrees of standardisation. Standard templates mean consistency of build and a lower risk profile.
Service Levels	Aligning business service levels to hardware-based solutions can be complex and costly. Areas such as business continuity and high availability can result in duplication of resources. Cloud Computing has such solutions built into the underlying architecture and therefore solutions can be standardised and costs are reduced.	Costly bespoke high availability solutions are not needed resulting in reduced expenditure and lower complexity. The solution can be made available to entire data centres.
Environmental Benefits	High power and cooling consumption of underutilised servers results in higher carbon emissions. Cloud Computing can significantly reduce these.	Massive savings in carbon emissions.
Planning for future requirements	The inefficiencies of the physical model places a high emphasis on accurate predictive planning. Whilst Cloud Computing does not advocate less diligence in the	Far more flexible and dynamic solutions that are more in line with the nature of an organisation's on demand model

Issue	Cloud Computing Solution	Benefit
	planning process it does enable greater flexibility by being able to share resources and prioritise allocation based on service level decisions.	
Dynamic Provisioning	Cloud Computing through all its forms allows the dynamic management of physical and virtual resources to meet the demand, this allows organisations to build for now but expand effortlessly for the future.	Matching I.T. strategy to organisational agility.