Business Continuity

Current Offerings

19 October 2022

Contents

1 Description

This service is provided to ensure that all customer systems are available to the business during a required operational window, can survive damage or equipment failure and be recovered and returned to operation with an agreed time period and in accordance with agreed SLAs.

For a small organization, this facility is primarily ensuring the network is available and implementing backup and recovery of each device.

As an organization increases in size and complexity it generally gathers infrastructure, and if it has been in existence for some time, it is likely to have significant infrastructure which it needs to manage in the first instance and potentially replace.

1.1 Service Elements

1.1.1 Pre-requisite

It is a pre-requisite of this service that all equipment is managed through our remote management service which delivers an asset register.

1.1.2 The elements of this service are as follows:

a) We will first document and create diagrams that describe all the infrastructure, inter connectivity and locations of assets on the asset register that is not automatically documented using the remote management system.

b) We will ensure operational processes are in place to describe how hardware is procured, managed physically and replaced.

c) We will document the business processes of the organization, the systems that support those business processes and the path of transactions across the network and the systems to support an end-to-end process.

d) We will carry out a risk assessment so that the importance of each asset is documented. This risk assessment includes:

   i) Analyzing the risk of failure of the equipment.

   ii) Risk and impact of potential human errors.

   iii) Temporary loss of infrastructure facilities such as power, network or air conditioning.

   iv) Permanent or extended loss of any item or a site due to: criminal theft, storm, flooding, explosion, or other act of God or terrorism.

e) For each risk we will recommend appropriate mitigation strategies and contingency plans to minimize the risk of failure, ensure duplication so that in the event of a failure systems can carry on while the failure is resolved (for example by configuring mirrored disks so that one disk continues to work until the failed disk can be hot swapped or the system shutdown under control and the failed disk replaced).

f) We will agree with a customer their appetite for risk. For example, we will agree:

   i) Whether all data held is important and if it can be recovered from other sources so the level of protection required is minimal.

   ii) The maximum acceptable time to recover a system following a failure.

g) We will identify any design changes or enhancements to systems that are required to reduce the level of risk to an acceptable level, when the costs of such enhancements are considered, and we will implement those design changes once agreed.

h) We will then define the operational procedures for protecting all data and devices and for recovering from a failure.

i) We will ensure that all recovery plans are practiced to an agreed schedule.

1.2 Example risk strategies include:

1.2.1 Laptops

a) Ensuring an image backup of the OS is taken from time to time from which the laptop can be recovered.

b) Enabling backup of all changes on a laptop to either local storage or to the cloud.

c) Testing that a laptop can be recovered from its image and data backups.

d) Holding a supply of replacement laptops in store so that in the event that a laptop becomes corrupted but appears operational, it can be recovered from the disk image and data backups of another laptop.

e) Monitoring a laptop to ensure that no data is stored on the laptop.

f) Deploying a Windows server running remote desk top so that all business computing is carried out on a server rather than a laptop device.

1.2.2 Servers

a) Deploying all servers onto a VMWare environment running a high-end server with hot swap drives configured with redundancy.

b) Enabling a configuration that supports shared drives so that if a physical server fails, all virtual machines can be restarted on the alternate server.

c) Backing up servers to a cloud immutable store so that they can be recovered even in the event of attacks such as ransomware.

d) Minimizing the number of servers with stateful information such as an RDBMS, meaning that the server can be recovered from a historic working copy, immediately restarted and brought up into configuration in the organization.

e) Implementing high availability mechanisms such as data replication so that in the event of a failure control can be transferred immediately to the standby server without service interruption.

f) Ensuring an immutable backup of changes is maintained so that in the event of an operator error, lost data can be recovered from the audit trail.

1.2.3 Network access

a) Ensuring that there are two separate telecoms / broadband providers delivering separate services to each site.

b) Providing multiple domain controllers so that the failure of one machine does not bring down the DNS infrastructure of the organization.

c) Potentially offering multiple routers which can operate in parallel so there is no single failure.

d) Deploying switches to partition the network into separate security zones so that problems in one zone can be contained.

e) Configuring a mixture of RJ45 and Wi-Fi capability to ensure that there is no single point of failure.

1.3 These operational procedures would typically cover:

a) A plan to back up each system on a regular basis.

b) Where appropriate to ensure incremental backups are taken with an agreed frequency, so that in the event of a catastrophic incident all data (up to an agreed period, or immediately a change occurs) is backed up offsite.

c) Utilizing spare equipment maintained in place to enable recovery from backups to be practiced on the spare equipment to prove the integrity of the backup and effectiveness of the recovery process to completely restore a system.

d) Methodology for replacing failed equipment.

1.4 The service includes:

a) A risk monitor that generates alerts related to system health and flags up any events that indicate a heightened level of risk.

b) Carrying out preventative maintenance to replace items of critical importance early to minimize the risk of a major failure.

c) Maintaining a local supply of spare / replacement hardware to ensure all operational procedures are practiced and to minimize the recovery time in the event of a failed item of equipment.

d) Generally reserve equipment will be maintained on line so that all updates can be performed and the equipment maintained in an identical configuration to the equipment in production.

Please note that the complexity and hence cost of developing a business continuity design for an organization can vary hugely depending on the size of the business, the asset base and the information held by the organization.

A key part of designing a BC/DR plan will include recommendations to reduce or transfer risk to a third party better suited to manage it in your behalf, for example by moving from hosted exchange to office 365 in the cloud and hence reduce the cost of our Service over time.

2 Commercial Terms

2.1 Design process charges

The design process will be charged on a time and materials basis.

2.2 Infrastructure equipment needs

Equipment required for the infrastructure shall be procured either by the customer to our specification or by us and resold to the customer and will remain owned by the customer after purchase.

2.3 Third party services

Third party services such as backup storage shall be charged based on the underlying charging model of the underlying service, for example volume of disk space.

2.4 Maintenance charges

Charges for maintaining and the managing the infrastructure and recovering any item of equipment in the event of a failure, in accordance with our operational procedures, shall be charged on a fixed price basis per machine under management provided we have operational control of all equipment and associated administrative passwords.

If the customer wishes to retain operational control of the equipment, then we will charge on a fixed price / device basis for routine activities to protect the environment but effort to manage a recovery shall be on a time and materials basis.

2.5 Hardware purchase

You pay for any hardware that we agree is required for the design.

There is also a charge for any works required to implement the network, for example to lay cable, to deploy the Wi-Fi hubs or to build a secure cabinet for your network equipment, though you may have a preferred supplier who can complete these works at your direction.

2.6 Monthly costs

You pay a single monthly subscription charge for each device you plan to have on the network. In the first year this includes an uplift to cover our initial design work, set up and configuration.

We review this charge on the anniversary of the service starting. Typically, the uplift would be removed if the level of support required by us during the year has been within any limits that we agree with you.

This charge is based on the standard protections we configure with you on the router as part of the design. If you need additional protection features from time to time then we can include them at a modest additional cost based on the underlying cost of adding the facility to the router.

Your charge is monthly in advance for payment within 15 days. We can take check or credit card but request you set up regular ACH payments to minimize administration and costs for both parties.

A small discount is available for increased long-term commitment or annual payments in advance provided payments are via ACH.

2.7 License costs

You do not directly pay for or own any underlying perpetual licenses or third-party subscriptions for our service. We manage all of the underlying technology.

2.8 Minimum commitment

When you take our service there is an initial 3-month commitment. You can terminate use of the service completely giving 30 days' notice on completion of the 3-month commitment.

If you terminate there is a small termination charge based on the period outstanding to the end of the anniversary of the contract because the router you own retains a dedicated untangle license to the end of that license period, and during that time while the full untangle license is active you will retain full functionality of the advanced router and firewall features.

2.9 Equipment management following termination

If you terminate the service then we stop managing your network and have no further responsibilities to you. The equipment is yours and remains in place and we will provide you the appropriate details for you to manage it yourself.

3 Service benefits

The benefits of taking this service are:

a) The senior leadership team has a real time understanding of the risks to their business and the status of all equipment with regard to those risks.

b) Where investment has been made to reduce the impact of any failure, they can view the incidents that have occurred and identify the reduction in the impact arising so that the investment made can be justified.

c) They have peace of mind that there are contingency plans in place which are practiced on a regular basis and therefore known to work, so that it is known that the organization can recover from any failure.

d) Where the business has accepted a risk, they can monitor the ongoing probability and impact so that if either change, they can review the situation and consider additional mitigation or contingency.

e) Essentially, the business can monitor the level of risk, where risks have materialized and been managed and any “near misses” suggesting further investment.

f) Based on hard facts, and changes in the underpinning resources available, the senior leadership team can constantly review how infrastructure risk is managed and adjust up or down the level of investment as appropriate.

g) In the event of a catastrophic failure, there are practiced plans with supporting information necessary to enable the organization to recover.

4 Deploying and Operating the Service

4.1 Start of the service

The start of the service is a project which will be run by us but which will involve a member of your senior leadership team who is responsible for business continuity and who has the authority to sign off the risk review and business continuity plan.

We acknowledge that “perfect is the enemy of good”. The business has lived with a level of risk to date. A proposal that required huge change implemented rapidly is inevitably expensive. It will almost certainly require significant investment in training and replacement equipment to implement rapidly.

Generally, a risk review will identify a number of risks that need resolution. However, our approach to delivering this service is to agree a plan for progressive implementation over time. For example:

- We are unlikely to recommend rapid and wholesale replacement of equipment.

- We might though recommend that in the future a standard corporate configured laptop is always purchased for consistency and simplicity of backup and recovery.
- Similarly for organization hosing their own applications, we might recommend the deployment of VMWare and the transfer of any stand-alone servers to a VMWare host on site, and then a progressive migration to the cloud in an ordered manner, rather than a big bang change.

4.2 Our commitment

We will operate the monitoring service on your behalf and provide you regular reports on the status and level of risk on the system.

We will ensure that roles and responsibilities are defined and terms of reference are documented so that the operation of this service is clear.

We will provide reports in accordance with the operational procedures to provide point in time records of the performance of the service.

Setup requires equipment to be installed in an appropriate environment.

Once configured, this should be transparent to the people in your organization in most respects.

We will provide you with regular reports and alert you to any activity of interest for which management action might be required.

5 Supporting Documentation

As the operation of this service is transparent to your organization, there is no requirement for extensive documentation on the service itself.

We provide a short operations manual describing:

a) Our understanding of your environment.

b) Your responsibilities to inform us in good time of any changes that might impact our management of your network.

c) Mechanisms for requesting reports and the meaning of the reports we deliver to you.

d) The operation of our support system, how you can track any issue that has arisen and the SLAs and KPIs by which you can measure our performance.

We also provide an operations manual describing how to carry out critical onsite tasks to replace items of hardware to restart a device to that you can undertake basic functions for us as we work remotely.

6 How Support Works

6.1 Support mechanism

The following is a brief description of our support mechanism. This is explained fully in our support manual:

a) When an issue occurs on your network that is automatically reported to us then we document then triage that problem.

b) A new issue is then raised in our service desk environment, on behalf of the nominated user associated with the item of equipment concerned.

c) We may merge incidents reported for many devices if they are fundamentally the same problem, and particularly if you take on some of our other services that would report problems with the network.

d) You may raise a support issue directly for any item of equipment we are managing by using the Cysure icon on your machine. As soon as this appears on our service desk environment, you can then add further comments or information related to the problem.

e) All information related to the issue should be entered via service desk but we will accept calls to escalate urgent/serious issues by email or phone.

f) Once an issue is raised, you can then track the issue through to resolution.

g) Our operational procedures define what constitutes a material incident that should trigger forming an incident response team to manage any event that has the potential for a major impact on the business.

h) Any significant action, such as the taking down of a system and initiation of a recovery process requires authorization from the incident management team.

6.2 Hours and location of support provision

Support is provided during the working day between 0800 and 1800. Optionally you can purchase extended support for out of hours or 24 x 7.

Onsite support is not included as part of this service: we work with your onsite representative. However, we are able to provide onsite support as part of our Equipment Managed service offering.

At the end of each month, you are provided with a report describing our performance against agreed KPIs.

Our service desk is available at the following URL

https://cysure.atlassian.net/servicedesk/customer/portal/2

7 What is not included

The cost of hardware required to implement the agreed BC/DR design is not included in these costs so either we will procure that for you and charge you, or require you to procure it to an agreed specification and arrange delivery to your site.

Our remote monitoring service is a pre-requisite for this Service.

If you wish to retain administrative rights over your equipment rather than delegate them to us, then we cannot guarantee the configuration of those devices. As a consequence, effort to recover these devices following a failure is not included in the fixed charge and we will separately charge you on a time and materials basis for effort to recover a device that you have modified or have the capability to modify.

8 How we may change the service from time to time

The level of risk may change and we shall advise you of this. It may be that due to a heightened level of threat, additional mitigation and contingency spend is required to reduce the probability and impact of a risk to a level that is acceptable to you.

This spend will be required by you and if you decline to make the necessary investment, we may be unable to protect the equipment to the SLA previously agreed. We inform you if there is a change to the SLA and in the worst case if we are unable to protect the equipment, we may have to decline to provide business continuity support for a system component.

We have a standard price list for basic business continuity protection of devices.

Our service includes the use of underlying software licenses and subscriptions which we then use to deliver the service. In particular this includes the use of tools to provide backup and recovery to the cloud. From time to time the technology vendors of these products increase their prices and we need to similarly increase our prices.

We will publish any revised prices on our website and will notify you of any price rises giving you 3 months' notice of such price rises. By taking this service you agree to accept any such price rises. You may terminate the service if you wish.

We may change the products we use to provide this service at any time. It is then our responsibility to ensure that the change of product has no impact for you. Note:

- the most likely reason for a change would be that an alternative product either provides significantly more functionality at a comparable price, or is more cost effective for the capability delivered.
- As we would bear to cost of any transition, this is not something we would do lightly!

9 Terminating our service

If you decide to terminate our service, then for this service you must provide us 90 days' notice of termination. This also extends the termination period of any underlying services that we provide and on which this service depends.

You many terminate this service without terminating other services that do not depend on this service.

On termination and provided we have received payment in full on all outstanding invoices, we will provide to you details of all passwords and other confidential information related to the provision of this service which is not shared with you to ensure that that no unauthorized changes can be made.

If you terminate our service then any backups made and held on our cloud environment will be deleted.

One month after termination, or sooner if you request, we will remove details of the devices from our management platform and then remove all details of your organization from the platform related to this service. We will continue to manage any data required to provide other services that you continue to pay for.

It is your responsibility to archive any reports important to you before you terminate as once we remove your organization from the platform all historic data is deleted.

If you require any assistance from us when terminating, for example to transfer your equipment to an in-house solution or to an alternative vendor, then as a responsible supplier we will assist you in this process if requested and charge you at our standard professional services rates on a time and materials basis for any effort to assist you to

successfully transfer any historic backups. This assistance should be requested during the 3-month notice period and completed before termination of the service is effective.

If you request to purchase our business continuity training package, we can deliver this training and show you how to manage the integrity of your environment.