

ITDR What are the challenges for 2010?

Introduction to White Papers

TRICKS give an inside track of tools and techniques to solve the challenges we are all about to face.

TRICKS

Technical evolution; cloud computing, latency, dispersion, compaction

Regulation, contractual obligation and compliance

Information security: Confidentiality, Integrity, Availability

Cost during recession: outsourcing and right-sourcing

Kollaboration Integration, dependencies and supply chain continuity

Sustainability: Green computing

Synopsis of each white paper

Paper 1

Technical evolution; cloud computing, latency, dispersion and compaction.

Every organisation and home is increasingly dependent on technology. We have all experienced the frustration of a loss of data, connectivity, power or hardware/software failure. As IT evolves it becomes more resilient and reliable and yet all too often we suffer from disruptions. This paper delves into cutting edge technology but without being blinded by science. The real issues are what can go wrong and what do we need to have in place to continue or recover technology if and when it (or someone else) lets us down.

Paper 2

Regulation, contractual obligation and compliance

In every contract there is a Force Majure clause. Increasingly there are specifications for ITDR and business continuity. This is regulated in part of the world and in the UK is non-prescriptive but there is plenty of guidance from the Financial Services Authority. Customers require their suppliers to be able to keep going regardless of the circumstances. ITIL methodology, best practice, penalties and standards all converge on ITDR. This paper addresses how we comply. What measurements we should agree to and how we can demonstrate to prove our DR capability.

Paper 3

Information security: Confidentiality, Integrity, Availability

ISO27000 is being achieved globally. The UK government has adapted standards to protect national infrastructure and is providing advice to business. The degree of resilience and level of security can be costly and degrade performance. This paper explains how to address the balance of making data and systems available without the associated downside security risks. Clearly this is not just an IT issue but a wider organisational challenge.

Paper 4

Cost during recession: outsourcing and right-sourcing

Operational expenditure versus capital expenditure is a dilemma every CTO, CIO and CXO level executive faces. "Faster, cheaper, better" is the cliché however the reality is conflict between investing, making do and transferring the risk to someone else. This paper determines the metrics for decisions on outsourcing, internal right-sizing and self sufficient approaches to enable cost benefit analysis.

Paper 5

Kollaboration Integration, dependencies and supply chain continuity

Everyone depends upon someone else. The problem comes when you are let down. In some cases you can see it coming, in other cases failure comes as a complete surprise with no warning. Value chains, supply chains and network diagrams all illustrate links and often a critical path. This paper describes the relationships between organizations and what can be considered to protect their touch-points.

Paper 6

Sustainability: Green computing

The question of a sustainable environment can be seen in every school, home, business and government. We are all interested in carbon emissions and the future of Planet Earth. IT is at the very heart of the debate on energy consumption. This paper defines what can be done such as ISO14000 and what should be done at nil cost or as a quick victory in the Green Campaign.

White Paper 1 Technical Evolution

Technical evolution; cloud computing, latency, dispersion and compaction.

Every organisation and home is increasingly dependent on technology. We have all experienced the frustration of a loss of data, connectivity, power or hardware/software failure. As IT evolves it becomes more resilient and reliable and yet all too often we suffer from disruptions. This paper delves into cutting edge technology but without being blinded by science. The real issues are what can go wrong and what do we need to have in place to continue or recover technology if and when it (or someone else) lets us down.

Technical Evolution Top 10 on Tape Back Up

Some might argue the days of metal media tape back up are over. But for those who remember the days of batch processing overnight, nightly back up tapes and weekly back up tapes how many of you did or are;

1. Checking the integrity of the back up?
2. Performing a restore on a different tape drive, configured to a different machine after loading the appropriate software, with the correct version within the recovery time objective you set?
3. Storing the tapes off site in a secure but easily accessible location?
4. Rotating the tapes and renewing them regularly in accordance with a policy?
5. Reviewing and updating the back up regime every time there is a change control or new installation as ITIL would suggest?
6. Testing a restore with users accessing the data from remote or DR locations?
7. Reviewing the licences and versions in order to restore the platform to the current profile.
8. Ensuring the business (users) have their expectations managed on the recovery time objective.

9. Ensuring the business (users) have their expectations managed on the recovery point objective, are aware of and accept the potential for data loss.
10. The decision to invoke a DR restore is practiced by those who have the authority to take it and that they are familiar with their actions and consequences.

All simple pointers for good practice but have you evidence in your organization it is being done? Of course back-ups are old hat in the world of high availability. Why do we need to worry about restoring data when we have 99.999% availability? Technology has undoubtedly improved resilience. But five 9s availability costs a packet and so do Tier 4 datacentres so what are our new options?

Cloud computing

Network architecture on a Local Area Network in the office and a Wide Area Network over a Virtual Private Network across the world provided their own resilience with diverse routing and separate circuits but suffered from single points of failure, could be insecure and had finite distances due to "Latency". The outcome for disaster recovery and business continuity was a headache.

On one hand best practice was advising datacentres or secondary locations to be a prescribed distance apart from the primary. Post 911 distance in the US was perceived to be 300 miles. This means in the European theatre Paris is too close to London and Manchester would not be able to site a secondary DR site on UK soil.

On the other hand technology permitted synchronous replication but only within a short distance because of latency. The speed of light is about the quickest speed we know of; but with "widgets" at each end split nanosecond delays force replication to be asynchronous and over a few miles this becomes a problem.

On the third hand (if there was one) most organizations plan to displace and relocate their staff to their secondary location which creates another business dilemma of how far and who and when. Enter work area recovery DR sites which can be purchased on a dedicated or syndicated basis again based on risk appetite, cost and degree of guarantee required.

Juggling with three hands is tricky especially when faced with business prioritization of who gets what first (in the trade called a business impact analysis). The threat of terrorism would lead us to conclude a strategy of dispersion is best. The trouble with dispersion is it is expensive and hard to control. The technical answer is compaction with blade servers getting smaller and real estate in data centers becoming less expensive. The opposite side to the same coin is the lobby for sustainable (green) computing. Compaction means more power. More power means more heat. Heat and power require more cooling. This is more expensive and not good for our emissions.

Cloud computing by definition has five essential characteristics:

- On-demand self-service,
- Broad network access,
- Resource pooling,
- Rapid elasticity,
- Measured service

It sounds better cheaper and faster but does it provide resilience and if it is compromised how is it continued and recovered?

Like in logistics "just in time" means there is no reserve (or redundancy) in the system. This can be true of "on demand" and "self service" – you get what you pay for. Ever visited a self service restaurant?

Broad network access is key as long as the system security is protected and only the approved users gain access. The broader the access the more exposure to intruders you offer.

Resource pooling makes economic sense as long as resources are not stretched beyond their capability. Sweating resources leads to overloading and subsequent failure.

Rapid elasticity such as burst capability on connectivity can be cost effective but often syndicated and shared services are not guaranteed.

"What gets measured gets done" however monitoring is not the answer. The human interface of a decision or judgment being made once an alert, alarm is vital to do something about the information or measurement that is being presented.

Homeworking Top 10

Working from home must be the solution of choice. Everyone has a home PC these days. But information security and business continuity remains an issue. Answer this from your homeworking strategy for contingency planning:

- a. Can you record calls and use your VOIP?
- b. Are you adequately supervised in the eyes of a regulator?
- c. Is the network degraded by the number of concurrent users?
- d. Have you issued enough keys, dongles and logins and those that have them are trained sufficiently to use them correctly?
- e. Are you going to issue everyone with a laptop?
- f. What are the health and safety implications?
- g. Can you enforce it in contracts of employment?
- h. Are there family or environmental distractions?
- i. Will the world working from home in Pandemic crisis overload the backbones of power and telecoms we are all dependent upon?
- j. Where is your Blackberry server, your email server, your web server, your shared files and print server and are they protected and resilient?

So finally a catastrophic thought...

Just to cheer you up and entice you to the ITDR Conference. Can the World Wide Web fail? All networks have dependency to some degree on 3rd party infrastructure. We have seen the effects of viruses (and the plethora of information security threats). We can't get away from facing the facts of human nature; that some of us deliberately meddle, some of us are criminals, some do things that are just plain stupid. Can we look to BS25777 on information communications technology service continuity for the answers?

Delivering our products and services in 2010 will rely heavily on technology. But we must learn to integrate technology with the other elements (or Ps) we depend upon; people, premises, processes, publicity and 'phones/public infrastructure.

White Paper 2 Regulation

Regulation, contractual obligation and compliance

In every contract there is a Force Majeure clause. Increasingly there are specifications for ITDR and business continuity. This is regulated in part of the world and in the UK is non-prescriptive but there is plenty of guidance from the Financial Services Authority. Customers require their suppliers to be able to keep going regardless of the circumstances. ITIL methodology, best practice, penalties and standards all converge on ITDR. This paper addresses how we comply. What measurements we should agree to and how we can demonstrate to prove our DR capability.

Regulation

Regulation in the UK is generally non-prescriptive. Regulators such as the Financial Services Authority (FSA) expect to see IT disaster recovery capability but without specifying the details. In the financial services industry there is a lot of guidance on business continuity, crisis management and disaster recovery see www.fsc.gov.uk from the Tripartite (FSA, HM Treasury and Bank of England).

Internationally, there are physical distances set between primary and back up data-centres. In some countries, regulators set timescales for Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) and Maximum Tolerable Period of Disruption (MTPoD) for data, applications and networks. There are even international examples of specified frequencies for testing and rehearsals.

Legislation

In the UK the Civil Contingencies Act (CCA) was passed in 2004. This created, for the first time, a law related to business continuity in the public sector. Category One responders such as Police, Fire, Ambulance, Coastguard and Local Authorities and Category Two responders such as Power, Water, Sewage, Gas and Telephony carriers are required to have a business continuity capability including the provision of IT Disaster recovery. Consider government departments and agencies who are audited under the CCA for example the NHS – your local Hospital or DEFRA's Environment Agency and their supply chain that provide the UK's critical national infrastructure. The CCA has had far reaching effects to promote and encourage disaster recovery.

UK Government

Key milestones going forward address a combination of good practice, adherence to the HMG Security Policy Framework specifically...

MANDATORY REQUIREMENT 70

Departments and Agencies must have robust, up to date, fit for purpose and flexible business continuity management arrangements that are regularly tested and reviewed and supported by competent staff that allow them to maintain, or as soon as possible resume provision of, key products and services in the event of disruption. These are:

- A BCM strategy endorsed and supported by Board level management.
- A BCM programme appropriate to the size and complexity of the department.
- Planning to proportionately manage the impact of events and recover from them.
- Communications that ensure that all staff are aware of the BCM arrangements and of their responsibilities within them.
- Key assets, products and services are identified and protected, ensuring their continuity.
- An incident (crisis) management capability is developed to provide an effective response.
- The organisation's understanding of itself and its relationships with other departments and organisations to include Local Authorities and the Emergency Services is properly developed, documented and understood.
- Staff are trained to respond effectively to an incident or disruption.
- Stakeholder requirements are understood and able to be met.
- Staff and stakeholders receive adequate support and communications in the event of a disruption.
- The organisation's supply chain is secured.
- The organisation's reputation is protected.

Standards

The take up for BS25999 the 2007 business continuity standard has been high, downloads of the Part 1 and Part 2 documentation reached record levels and motivated further standards in ICT Service Continuity (BS25777) Risk Management (ISO31000) Incident Management and has been aligned with BS27000 Information Security and a plethora of other related standards. This has applied a pressure for an international standard (ISO22301) with a number of countries developing their own standards and regulators developing their own regulations.

BS 25999 provides a basis for understanding, developing and implementing business continuity within an organisation. The standard comprises two parts:

- Part 1, the Code of Practice, provides BCM good practice recommendations.
- Part 2, the Specification, provides the requirements for a Business Continuity Management System (BCMS) based on BCM good practice and can be used to demonstrate compliance via an auditing and certification process.

ITIL

IT Infrastructure Library is a methodology which holistically addresses business continuity and disaster recovery as part of service management and infrastructure management processes.

Operational Layer

- Configuration Management
- Service Desk Management
- Incident and Problem Management
- Change Management
- Release Management

Tactical Layer

- Service Level_Management
- Availability Management
- Capacity Management
- Continuity Management

- Financial Management

Contractual Obligation

Invariably in contracts there has been a force majeure clause. This is to protect everyone from an unforeseen event such as an act of God for which there can be no risk management, no mitigation and no recovery. Since 911 "Terrorism" has been a separate clause on insurance policies outside of the all risks cover. Increasing business continuity is specified in a contract. Tenders require a demonstration of business continuity and disaster recovery. Most recently force majeure is being questioned, disputed and retracted because IT DR and business continuity specifications mean force majeure is no longer relevant.

Compliance

In the last few years there has been an "emergence of convergence". The glossary of terms for disaster recovery and the compatibility of legislation, regulation, standards and methodology has encouraged simplicity and measurement. As we know what gets measured gets done! What gets measured gets recorded and the records can be used as evidence to prove capability. Increasingly evidence rather than a simple tick box are included in tenders, service level agreements and contracts.

Questions like "Have you got a DR capability?" Have now been replaced by:

- a. What guarantee of data integrity and timescale can you fully recover your systems? (Please provide a copy of your RPOs and RTOs for critical applications). And/or
- b. When did you last test? (please provide a copy of the report proof and that revisions have been implemented).

An audit report validating attaining a standard (BS25777), adopting a methodology (ITIL) or meeting a regulatory requirement (FSA) goes toward proving the DR capability. The acid test is integrating the capability with your dependencies and rehearsing it in conjunction with the users (wherever they end up working from).

White Paper 3 Infosec

Information security: Confidentiality, Integrity, Availability

ISO27000 is being achieved globally. The UK government has adapted standards to protect national infrastructure and is providing advice to business. The degree of resilience and level of security can be costly and degrade performance. This paper explains how to address the balance of making data and systems available without the associated downside security risks. Clearly this is not just an IT issue but a wider organisational challenge.

The Security Dilemma

Ever been in a sweet shop full of children? They all want to look, many want to buy, some have purchased already and are eagerly eating their gains (of whom some will be disposing of their waste wrappers on the floor and worst a few disposing of their chewed gum under the counter). There will be a small proportion seeking to steal a sweet, some will get confused (or try to trick the shop assistant) and order more than they can afford, someone may drop their purchase on the floor (or were they deliberately pushed?) and the very bold might even get "organised" criminally to rob cash out the till or mug other children.

Welcome to the world of physical security. Theft, contamination, breakages, injury and waste could be solved very easily – lock the shop and admit no children. Of course as a business those kinds of barriers are unacceptable because it would kill profit from the majority of child customers parting with their hard earned (or easy come easy go). There must be layers of affordable and appropriate security to; prevent, pursue, protect and prepare.

In the real world these 4 Ps are the foundation for the UK's counter terrorism strategy and pillars within the HM Government's Security Framework. The adoption of a mix of physical and logical security is the key to information security and ISO 27000 – clearly not just IT security.

Linking back to the sweet shop case study now we can expand the example to consider electronic point of sale, supply chain issues, cyber crime, your reputation and all vulnerabilities. As a starting point, download the short video and booklet "Secure in the Knowledge" for advice. From a legislative perspective you must comply with the Data

Protection Act 1998. From a business perspective have a look at Confidentiality, Integrity, Availability... C-I-A.

Confidentiality; Ensuring your information is used appropriately.

Clear desk policy, ID badges, escorted visitors, personnel vetting

Computer passwords, Restricted Logical Access, Encryption

Physical locks, alarms/locked doors, CCTV/lighting, guards, laptop/mobile security and remote access (home-working) protocols

Network firewalls, DMZ, access permissions, information trails

Destruction (of hard drives, memory sticks, CDs/DVDs, paper)

Integrity; Ensuring your information is fit for purpose

Validate correct and accurate information/data from the source.

Prevent corruption or unauthorised changes whilst using or storing information including the media carrying the information.

Only use information for the purpose for which it was collected.

Do not pass information to unauthorised third parties.

Maintain your anti-virus and anti-spyware software.

Prevent unauthorised use of Internet, personal software and tampering with enforced policies and training.

Availability; Ensuring your information is there when you need it

Back up information regularly and test to restore it outside the normal environment.

Manage the amount of information you need and validate the sources.

Prepare alternative ways to present and access information should the normal environment become denied or fail.

Identify, prioritise and agree with users what is critical and the sequence of recovery.

Concept... Think of a balcony – people might jump off it deliberately, but that is very unlikely. You put up a safety rail to prevent accidents, not because you don't trust people. The same applies to information security.

Resilience and Preparedness

There are plans for a new ISO 22301 Business Continuity and Preparedness. Like the layers of an onion described in the layers of security there are also layers of resilience and preparedness. These can be combined in 3 dimensions linking security, continuity and sustainability.

The three dimensions are Hierarchy Integration and Time –

- Hierarchy – organizations are built on levels of authority. These must make sense i.e. be appropriate for the rank. Don't exceed your level by making strategic policies outside of your control.

Likewise ensure the resources are available in the right sequence to allow for functional priorities and a sensible sequence.

- Integration – We cannot do anything in isolation. We must collaborate, coordinate and integrate with everyone around us – the authorities, regulators, local community, press, supply chain and customers.
- Time - business is dynamic and things change over time therefore we need to adopt different measures, styles and responses for different times such as before, during and after an event.

The key is to embed information security into our culture. Imagine the power of the eyes and ears, the hands and feet, the communications, the brains for initiative and discipline of all those children in the sweet shop. If they were aware, alert (but not alarmed) well organised and empowered security would be a “piece of cake”. Anyone for a mint?

White Paper 4 Cost

Cost during recession: outsourcing and right-sourcing

Operational expenditure versus capital expenditure is a dilemma every CTO, CIO and CXO level executive faces. “Faster, cheaper, better” is the cliché however the reality is conflict between investing, making do and transferring the risk to someone else. This paper determines the metrics for decisions on outsourcing, internal right-sizing and self sufficient approaches to enable cost benefit analysis.

Recession

Recession has claimed many victims – we all read headline news of household names such as MFI, Woolworth and Lehman Brothers going out of business. We have all thought about relative job security, market forces and the global economy. With everyone looking for savings out suppliers, customers and competitors are all seeking an edge financially.

IT

In most organisations, IT supports the business, product or service. It creates efficiency by mechanising and digitising processes. In some organizations IT is the business and at all the ICT outsourcing companies recession has been perceived as a double edged sword. IBM, ICM, EDS/HP, Logica CMG, Atos Origin, Siemens all promote world class technical capability and cost efficiencies, but is outsourcing recession proof?

Purchasing DR

Disaster Recovery (DR) contract with a DR vendor or independent solution can provide the following:

Well supported, reliable and flexible DR management able to understand existing business needs and be able to meet future business growth

Dedicated seat opportunity within walking distance to meet all immediate denial of access issues

Potentially low risk syndicated or dedicated seating in an out of city site to accommodate during a major disaster

Quality out of city data centre with sufficiently available rack space and a well controlled environment to host core replicated systems

Highly resilient interconnected, multiple site infrastructure to allow data held in one building to be accessed easily by seats in another

Data centre to allow us to incorporate multiple telecom capabilities to act as backup to telecoms vendor

Managed data service opportunity to outsource all or certain elements of IT

Seats (work stations for work area recovery)

A 'seat' is effectively a desk in a DR suite which has a chair, a computer, mouse and keyboard, a monitor, a telephone and access to some other services, such as lavatories, meeting rooms, printers, photocopiers, food, accommodation, public transport, security and car park. It is networked to other seats in the DR suite and able to link to your applications and data.

DR vendors sell two types of contracts for seats:

Syndicated – suppliers of continuity services or as we refer to them DR vendors effectively provide a working environment to allow companies to deal with disasters effecting their primary office locations. DR vendors provide the seats in various office suite sizes and the underlying IT infrastructure and these 'resources' sit ready in office suites awaiting use.

Therefore to make money and mean they can provide clients with these resources economically a DR vendor must sell each seat a multiple of times to different clients. These seats are therefore referred to as syndicated and on invocation there is therefore a risk that the very seats/services you have subscribed to may not be available to you if other clients to whom the seats have also been sold have invoked before you.

Dedicated – to remove this risk there has been a big industry move towards permanent owned seats held as dedicated within DR vendor's buildings. This effectively provides a company with an additional office that is theirs to use for a majority of the year – to avoid landlord/lease issues the DR vendors reduce the number of day's actual use to below the full year's allocation but it's effectively a full-time available suite. The space can be used in real-time as part of business as usual or for testing and project work.

A Blend – the drawback of dedicated positions is that they are sold at a financial premium because they can only be sold once. To duplicate seats for an entire company's workforce it would prove expensive – comparable with your own work area costs (less for consumables such as power, water, aircon, telephone bill etc). Companies tend to blend the two types of seats and have enough core positions dedicated to continue immediately with business with an option to increase numbers with syndicated seats.

Home working is increasingly becoming a cost effective choice for business as usual operations and as an option for disaster recovery.

How to choose what is best

Risk – Essentially it all comes down to risk, understanding what these risks are, minimising them and deciding on a solution that is workable. For syndicated seating the risks are fairly clear in that the DR vendor's other clients affect our ability to get hold of those seats to which we have subscribed. All DR vendors have exclusion zones but these must be understood in order to weigh up the risks. In a disaster scenario involving just our building the exclusion zone will definitely preclude other clients in Primary site subscribing to your syndicated seats and the risk of your getting access is minimal. In this scenario the important factors are the speed with which our resources are made available to us and the length of time we can use those resources after an incident.

- Check whether there is an **equitable share** of syndicated seats during multiple invocations or if your vendor operates on **first come first served**.
- In a major incident the issue will be availability of those seats. To manage the risk DR vendors use a number of syndication management tools but essentially you need to know who are the clients sharing your seats, their industry, their location, and the resources under cover and the number of times these resources have been sold.
- The other risk of using a DR vendor is that of physical resources, i.e. are the DR vendor's staff and equipment able to cope with a large scale invocation or again will you be left without assistance and possibly short of equipment even though you obtain the seats.
- The sites themselves also need to be physically secure and at least environmentally equivalent to the primary site.

If the DR vendor has multiple well connected sites and all connected to your out of city data then they can potentially house you anywhere within the infrastructure loop at any of their buildings. There would obviously be a short time delay to get and whilst the client organisation can name (specify) a secondary site, they may end up at any DR location that has space available.

Staff Demographics

When considering out of city sites and even alternate city sites it is useful to review the locations of staff's homes. Core staff required for critical processing or invocation duties need to be able to get to the DR site physically and logically in short timescales. DR sites may be located conveniently in the commuter zones in suburban areas. Transport links are vital to consider as is parking, physical security and welfare of staff.

Independent (In House DR)

A less traditional but cost sensitive disaster recovery option is to create an internal solution. The existing telecoms provider may need to provide

an alternate telecoms point of presence (POP) to ensure separate circuits or diverse routing. There may be existing space in the property portfolio with room available that is not in use and would potentially make suitable dedicated space. Space might be available at a very low rental cost for a quick lease in an area convenient for demographics, on a separate utility grid and outside the police or county boundary. There are possibilities for utilising the space for training/storage to offset the cost. In certain cases there is an opportunity to sell on the space for revenue as a mini DR vendor however risk and revenue should be carefully balanced regarding internal and external multiple invocations.

Even then we must know what to do when faced with the unexpected. Come to the conference and find out how others are facing these challenges. You may have been stimulated by this paper to make a comment or ask the experts a question which will be answered at the conference too.

BCI VOLUNTARY SUPPLIER RISK DECLARATION

Customer Name:	Abc plc		
Contract Reference:	xxxxxxx	As at:	Date
Client Site:	Site: 1 of 1	Primary Recovery Site:	
Xxxxxxxx		Xxxxx	
Xxxxxxxx		Xxxxx	
Xxxxxxxx		Xxxxx	
		Xxxxx	

We continually monitor the risk profile of services supplied to our clients. As a subscriber to our services you will receive a Voluntary Supplier Risk Declaration at commencement of your contract and an updated Declaration every subsequent year on or around your contract anniversary. This important information enables our clients to regularly evaluate the risks associated with outsourced services against their appetite for such Risks. A traffic light system has been used to highlight the service risk status and areas of potential concern. (GREEN – Acceptable, AMBER – Requires Attention, RED – Warning)

RECOVERY SITE STATUS

Recovery Centre Size:	xx,000 square feet	Site Dedicated Seats:	xx at issue date
Secure Recovery Suites:	x	Site Syndicated Seats:	xx
Workplace invocations at the centre during the last 12 months:		Site Dealing Positions:	xx
Total Number of contracted Seats	xxxxx	Site Utilisation is calculated as a multiple of the number of syndicated seats at the site (as shown above) by the maximum syndication limit per seat (as stated below), divided by the number of contracted seats sold to all subscribing clients.	
Centre Utilisation (at issue date):	xx%		

CLIENT RISK STATUS

Risk with explanation	Supplier Statement	Current Position at Review Date
Service Basis The basis of the service you have contracted for the above Client Site.	The service is a Syndicated Service. The service is shared with other subscribers and may not be available in the event of multiple invocations.	To mitigate risk, syndicated services are provided to monitored exclusion zone & subscription rates as disclosed below
Service Allocation The method by which your contracted services are allocated if there are multiple invocations.	Syndicated Service is made available on a 'first come first served' basis whereby legitimate invocations are allocated resource in the order in which they are received (time logged).	Met throughout year, no contract exceptions.

<p>Risk Statement</p> <p>The risk metric associated with the Client Site and the total number of sites supported by the supplier using the same asset or Recovery Site.</p>	<p>Each Client Site, based at a defined post code, is classified as a full subscriber on a 1:1 basis. The total number of these subscribers will not exceed the Syndication Rate applicable to the Service.</p>	<p>Subscriber Rates have been maintained during the year.</p> <p>Total number of risk sites supported</p> <p>from the recovery centre are xx</p>
<p>Syndication rates</p> <p>The number of times each item of equipment or workplace position (seat) can be sold to different Clients Sites.</p>	<p>Each asset may be sold up to a maximum of 25 subscribers per asset. Each subscriber will be located in an agreed exclusion zone area.</p>	<p>X:1 (workplace positions & PC's)</p> <p>X :1 (dealing facilities)</p> <p>X :1 (servers and peripherals)</p>
<p>Standard exclusion zones</p> <p>Distance between your sites and another Client or Clients syndicated to the same equipment or workplace position</p>	<p>Within 250m of the above address</p> <p>Within 250-500m</p> <p>Within 500-1000m</p>	<p>x other subscribers</p> <p>x other subscribers</p> <p>x other subscribers</p>
<p>SLAs (Service Level Agreements)</p> <p>Adherence to contracted SLA's</p>	<p>SLAs as stated in contract</p>	<p>Service Levels were met</p>
<p>Alternative Sites</p> <p>Alternative Recovery Centre available in the event the Primary site is unavailable and the basis of access to those sites.</p>	<p>Other sites may be made available on a reasonable endeavours basis only, subject to availability and outside of the Agreed SLA.</p>	<p>B Site x (xx seats xx miles)</p> <p>C Site x (xx seat xx miles)</p> <p>D Site x (xx seats xx miles)</p>
<p>Invocation Notification</p> <p>Making clients aware when equipment or workplace positions they have syndicated rights to have been invoked</p>	<p>Workplace – E-mail within 24 hours of invocation.</p>	<p>Standard met – issued within 24 hours</p>
<p>Testing</p> <p>Client contracts contain adequate test days for technology & staff rehearsal.</p>	<p>3+ days per annum minimum</p> <p>6+ days per annum recommended</p>	<p>xx days per annum</p>
<p>Testing</p> <p>Test days are appropriately utilised</p>	<p>IT tests minimum</p> <p>Business User tests recommended</p>	<p>None undertaken</p> <p>None Undertaken</p>

On behalf of Supplier, I warrant that the information is correct as at the date above.

Supplier Signature _____

White Paper 5 Kollaboration

Kollaboration Integration, dependencies and supply chain continuity

Everyone depends upon someone else. The problem comes when you are let down. In some cases you can see it coming, in other cases failure comes as a complete surprise with no warning. Value chains, supply chains and network diagrams all illustrate links and often a critical path. This paper describes the relationships between organizations and what can be considered to protect their touch-points.

Splendid Isolation is a myth

Welcome to the world of globalization. There is no such thing as splendid isolation. In information and in particular IT Logical security we endeavour to set ourselves up as an "island castle" where we can pull up the drawbridge for protection. But that siege mentality prevents us from doing business. Doing business is a risk, it has upside and downside. We aim to buy cheap and sell expensive to make a profit and that positions us in the supply chain. We all have suppliers and customers. We have to collaborate to negotiate price, service, quality and schedules. But our risk perception affects how well we feel about our suppliers.

Do we negotiate with our doctor, solicitor, policeman or accountant? We see them as trusted professionals and have a very different opinion of a used car salesman, estate agent or headhunter. Applying this risk perception to ITDR provides some options. We can outsource and as the cliché goes, "Nobody ever got fired for hiring IBM". But are IBM best value? Could they let us down or could a supplier to IBM let them down and cause a ripple effect that lets us down?

Single Points of Failure

When conducting business impact analysis the focus is on process. We process map the internal and external dependencies, we can see critical path analysis and all the touch-points along the way. Single points of failure are discovered. The good business sense about single points of failure is that they are cheap – no investment in redundancy, reserves or alternatives, if the single point doesn't fail we are quids-in. Whether you call it risk management or a gamble the role of the IT department is to advise and let the business make the judgment regarding the business case.

Continuous availability and high availability quite rightly are a big investment. With 99.999 availability guaranteed (5 minutes or so downtime per year) surely there is no need for further DR strategies or back up. We could save money by canceling back up. Sadly that will not provide the amount of investment for five nines. When faced with the bill for outsourcing HA the business may well have a change of heart and suddenly accept more downtime than previously (when they insisted they could afford no downtime at all!).

Supply Chain Continuity (Surveys are too often meaningless)

Weary of filling out questionnaires from existing customers, prospects during ITT, insurance renewals and regulatory returns can we have any confidence in our suppliers? Just because they have said they have plan for pandemic influenza, or an information security policy or a disaster recovery contract which they test annually these tick box surveys prove little capability.

The 6 Rudyard Kipling questions to ask are: Who, What, When, Where, Why How

1. How can we integrate our incident management escalation?
2. Who will inform us of a disruption in your supply chain by which means to allow us the maximum time to react?
3. Where are we (relative to your other customers) in the pecking order to receive continuity or recovery capability?
4. What is the level of continuity or recovery we can expect expressed in measurable terms?
5. When can we expect resumption of some and all services?
6. Why can't you share any intelligence or monitoring of your upstream supply chain in return for downstream pricing and volume intelligence or monitoring?

This is not a survey blindly emailed to everyone on the approved supplier list. This is a conversation, an understanding, collaboration with a capital K. Those survey forms admittedly are rarely investigated – remember Y2K... specifically have you any embedded chips, have you done remediation, have you tested the rollover, have you got a contingency

plan? We are asking the wrong questions to get reassurance. When was the last time you visited a key supplier or key customer without a salesman or auditor in tow? Wouldn't it be refreshing and much more useful to discuss capability what could be shared, who to communicate with and how to increase warning time. Would it be better to know you are last on the list to have supplies resumed and that means you get nothing for 3 days than confidently assume a supplier that has completed a survey saying truthfully it has, "A tested DR plan and can recover its critical applications in 4 hours". 4 hours to you (to recover an application) does not necessarily mean 4 hours to your customer when they receive business as usual service.

Communications

When we travel on a train and the train stops we are desperate to know why. We have a dependency with the driver to get us to our destination and notify us if there are any challenges. The passage of communications is critical for us to make informed decisions. The same applies to IT service continuity and the effects of a disruption within the supply chain. Everyone needs to know how to escalate, who can give advice. Information is power and communicating the status is vital but all too often the power is either abused or the message is not passed on.

Mapping value chains

It's not the plan but the planning

Failing to plan is planning to fail

Know your enemy

White Paper 6 Sustainability

The question of a sustainable environment can be seen in every school, home, business and government. We are all interested in carbon emissions and the future of Planet Earth. IT is at the very heart of the debate on energy consumption. This paper defines what can be done such as ISO14000 and what should be done at nil cost or as a quick victory in the Green Campaign.

Believe it or not

The scientific jury may be out on the reasons for global climate change but the evidence is overwhelming that it is happening, and happening fast. As ever the media have presented Climate Crisis which has to be taken seriously whether you believe the Kyoto Agreement will make any difference or that volcanoes and cows create more CO2 emissions than cars and aeroplanes. No need for research and analysis on the energy required to run IT systems or the heat that is created from the electrical power we all know servers get hot! We also cannot deny we are using more power and blade servers and compaction has resulted in smaller sizes using greater power. What a few years ago was term combined heating and power CHP in facilities management circles is now called CCP combined cooling and power.

Energy Consumption

There is a finite amount of power that can be consumed and turned into heat in a standard server cabinet. Racks amplify the problem and blades that can be bolted on to increase computing capacity devour electricity at an alarming rate. For those of you in the hosting business you will recall the relative change in pricing strategy as the cost of bandwidth for connectivity has dropped and the cost of power has increased disproportionately. Fans for air cooling are being replaced by pumps for water cooling net result, more power required. As components get smaller and can be fitted into tighter boxes, more space is required between hardware boxes to allow cooling.

Measuring the energy consumption is a tricky business if you aim to single out ICT. Power to the data-centre, server room or comms room can be calculated. But what of the hidden costs off site at the exchange, hosting center or the user at their desk even the user in their home? Calculating the real cost of energy could include the peripherals; monitors, telephony (mobile device chargers too), printers and copiers, shredders and the Aladdin's Cave of electrical "gizits" on every desktop.

UPS and generators as well as mains are in the equation and so it SDR testing at secondary and third party locations and the times you test the generator under load. Weekend working and night-time maintenance keeps the lights on and kettle boiling (and pizza's coming by scooter cooked in electric ovens). The case is made that everyone is part of the problem and therefore can make changes to become part of the solution.

ISO14000

The ISO for sustainability follows the same Plan Do Check Act methodology as every other standard. If you are considering certification to BS25999 BCM, ISO 27000 Infosec or ISO 9000 Quality save time, money and clearly energy by combining them and achieving them in parallel in preference to in sequence.

First you need a policy, some tools and techniques and some measurements to monitor and calculate progress. The aim is to inspire a cultural change like the constructive force of health and safety where everyone accepts their personal responsibility and are empowered to do something positive.

Quick Victories at Nil Cost

Top Ten ways of reducing power consumption

1. Turn off monitors
2. Turn off desktops
3. Turn off peripherals (printers, copiers and Aladdin's Cave)
4. Seasonally adjust CHP/CCP to the climate not the luxury of the operators.
5. Stop printing unless really necessary (and recycle waste)
6. Influence your suppliers to use less energy/packaging/visits
7. Use less travel and more conference calls or video conferencing
8. Use more email and less snail mail
9. Stop spam, distractions and improve time management
10. Visualise consumption so users can monitor and influence their consumption

Green Continuity

Off site is off balance sheet and lost carbon emissions. ICT service continuity management converges the benefits of best price, lowest risk, highest availability and lowest carbon footprint. Home-working transfers some risks and transfers some emissions. With children out at school and parents out at work household bills for daytime heating, lighting and computing are negligible. Home-working is a valuable contingency planning tool but not without green choices for the individual and organisation. Not using the car for work reduces CO2 but offsets home electricity only for large cars on long journeys. Will the facilities or IT department not only provide office furniture, desktop computing and broadband... but consider a solar panel, wind turbine generator or heat exchanger for the home to reduce corporate emissions?

Have you asked about the sustainability of your DR vendor? Syndicated work area recovery must be more carbon friendly than dedicated work area; of course only when it is in use.

The memory stick which is reusable (for data storage) and could last for years is greener than the equivalent of paper even recycled paper or DVDs. Next time you upgrade desktops consider "Computers 4 Africa" or other secure and sustainable disposal/recycling scheme.

The final word is about culture. We must encourage personal responsibility toward sustainability. Make choices for efficiency combined with emissions reduction. In just the same way as everything else in IT, what gets measured gets done.