BRITISH TRANSPORT POLICE

Report to:	**Finance Group**
Agenda item:	**8**
Date:	**16 January 2013**
Subject:	**Disaster Recovery Phase 2**
Sponsor:	**Director of Corporate Resources**
For:	**Information / Decision**

1. PURPOSE OF PAPER

1.1 This is the Business Case for phase 2 of the Disaster Recovery Centre project in Birmingham and outlines the work needed to convert the existing 'cold' facility to a 'warm' facility.

1.2 This paper summarises the full DR Business Case. More detail can be found in the main document, along with cost breakdowns, benefit analysis and risks.

2. BACKGROUND

2.1 The role of any Disaster Recovery (DR) facility is to ensure that an organisation can survive the loss of its primary ICT centre and continue to operate. Few organisations can afford to duplicate all of their operational systems and services in a dedicated DR environment so it is usual to concentrate on providing a DR capability for core systems only and accept that, in a disaster, some services would need to be suspended, or significantly reduced, until normal service was resumed.

2.2 There are three broadly accepted levels of DR facility which are categorised by how quickly a DR facility can be brought into operation if the worst happens. The levels are referred to as 'hot, 'warm' and 'cold', or in ITIL terminology 'immediate', 'intermediate' and 'gradual'. Typical recovery times are 0-12 hours for hot standby systems (this can be immediate), 12-72 hours for warm standby, and over 72 hours for cold standby. Naturally, hot standby is the most expensive DR option and is usually reserved for mission critical systems such as Command & Control, or similar applications, where public safety is at risk.

2.3 It is important to note that Force's Command & Control system, supplied and supported by Capita, is protected by a 'hot standby' capability that is fully independent of the DR Centre in Birmingham and has already been the subject of a full-scale test. Similarly, the ICCS, Voice Telecommunications to the key locations, and dispatch of Airwave Radio Communications, are all protected by well established processes and equipment that are not associated with the core network so these are not at risk, nor part of this business case. And the Force Network is provided as a resilient managed service by BT and not part of this business case.

2.4 In its current state, the DR Centre in Birmingham already provides a fully functional 'cold standby' capability for all systems **plus** a 'warm standby' capability for all of the systems that currently utilise the Windows Virtual Environment and the Crime system. However, the lack of a functioning connection to CJX would seriously hamper operational policing and delivery of front line services should the Centre be invoked. Approval to connect the DR Centre to CJX had not been given during the Phase 1 project but that approval has now been granted.

2.5 The full list of mission critical systems and services, together with their desired and current levels of DR capabilities, is shown in the following table:

System/Service	Description	DR Level Required	Status
C&C	Command and Control	Hot	Done
ICCS	Integrated Communications	Hot	Done
Airwave	Airwave Radio Communications	Hot	Done
Voice	Voice telecoms into FCRL, FCRB, FCC and CRC	Hot	Done
Network	Network connections to FCRL, FCRB, FCC and CRC	Hot	Done
CJX	Link to national systems like PNC,	Hot	Done

	PND, ViSOR, etc.		
Crime	Crime Recording System	Warm	Done
Points	Tasking System	Warm	
FIS	Force Intelligence System	Warm	
Intranet	Force Intranet	Warm	Done
Email	MS Exchange System	Warm	
PNC	Police National Computer system	Warm	
DWH	Data Warehouse	Warm	Done
Station Check	Outlying stations voice log	Warm	
CuCase	Custody & Case Preparation	Warm	Done
Holmes	Major Enquiry System & Casualty Bureau	Warm	
Origin	HR System (including Duty Management)	Warm	

2.6 This proposal provides a series of tiered steps, some of which are optional, to deliver a 'warm standby' capability for the remaining mission critical systems as highlighted above.

2.7 Please note, however, that any DR facility is, by definition, work in progress because any changes made to the primary ICT facilities at FHQ (whether that is extra server power and storage capacity to meet organisational growth or new systems and services) needs to be reflected in the DR facility as well. Thus future business cases for new or modified mission critical systems will need to include costs and resources to replicate those changes in the DR environment.

3. OPTIONS

3.1 There are 9 options, presented as steps, some of which are optional:

- **Step 1**: connect the DR Centre to CJX and provide the requisite firewall protection for that link. This will enable the DR Centre to connect to PNC, PND, ViSOR, and

other national systems if invoked and is essential to provide the 'warm standby' capability required by the Force. As part of this work, BT will conduct a scoping study to determine what changes to the network would be required to share the second the CJX link during normal operations and to access DR systems on an individual basis.

- **Step 2**: the Force uses a product called Legato to backup all of its Unix based systems to a Quantum storage device, and a second Quantum device is currently being built at FHQ in order to provide an off-site copy of all of the backups. This second device needs to be transferred to Birmingham. Synchronised over the network, it will provide a secure, off-site copy of all Unix backups **and** a repository of system backups to be used if the DR Centre is invoked.
- **Step 3**: relocate the existing 'hot standby' server for the Force Intelligence System (FIS) from the FHQ Data Centre to the DR Centre in Birmingham. It will still continue to function as a 'hot standby' server for the primary server (should that fail) but will also then provide a DR capability for FIS in the event of a disaster at FHQ.
- **Step 4**: migrate Points and our PNC gateway software from the old Windows NT Domain to the new domain and then virtualise onto the new Windows Virtual Environment. This will have the immediate effect of providing a DR capability for Points and PNC because everything on that environment is automatically replicated in Birmingham.
- **Step 5**: provide a duplicate server environment in Birmingham for Microsoft Exchange (our e-Mail system) which currently has no DR provision at all. It had been intended to leave the provision of a DR capability for Exchange until the planned major upgrade to Exchange 2010 but that would incur delay and expose the Force to some risk. A duplicate server environment and storage needs to be provided in Birmingham to provide a 'warm standby' capability for e-Mail.
- **Step 6:** provide DR capabilities in Birmingham for the specialist 3rd party voice systems (Station Check and Firearms Voice Recording) which were out of scope of the original proposal.

- **Step 7 (optional)**: provide duplicate servers in Birmingham for the Origin-HR and Holmes systems which currently have no DR provision at all. It had been intended to provide a shared server for both systems in Birmingham under Phase 1, but the system suppliers would not give approval for shared or virtualised versions of their products and the work was suspended. Installing two separate servers (for the moment) will ensure that these systems have a DR capability in Birmingham.
- **Step 8 (optional):** consider upgrading the existing network connections from existing P2 sites into Birmingham as they are slower than the equivalent connections into FHQ. This lack of bandwidth would give rise to performance problems if the DR Centre were invoked, especially as many FHQ staff would need to relocate to a P2 site in London, adding to the demand at those sites. This will involve upgrading the existing 5Mb circuits to 10Mb. As the network is provided as a managed service by BT the work would be entirely undertaken by BT with no resource implications for BTP.
- **Step 9 (optional):** implement the recommendations of the BT Scoping Exercise (completed as part of Step 1) to allow the Force to share the second CJX link during normal operations and access DR systems on an individual basis.

3.2 There are some caveats and notes as follows:

- Step 1 includes a £2,000 Scoping Study from BT which will identify and make recommendations for changes to the configuration of the Force network to allow the second CJX link to be shared across the whole network during normal operations (not just kept on standby in case the DR Centre is activated) and to make better use of the network in general. The Scoping Study is scheduled for 22nd January and the costs of the recommendations (which will affect Step 9) will not be known until after that date.
- There is a small possibility that the increased replication and back-up traffic from FHQ to Birmingham (Step 2) may require an upgrade to the dedicated DR network connection (currently 100Mb).

- The cost of the new server for Holmes II (Step 7) is based on a worst case quotation supplied by Unisys but other Forces run the system successfully on smaller boxes so Technology will conduct further research with a view to reducing this cost.
- The cost of configuring Holmes II on the new server (Step 7) is based on a "will not exceed" quotation from Unisys but experience says that this work should take a lot less time and effort and we are expecting the cost to reduce.
- The cost of configuring Origin on the M4000 server (Step 7) is based on a standard quotation from Capita but seems excessive and may turn out to be less.

4. FINANCIAL IMPLICATIONS

4.1 This cost profile assumes financial approval in January to allow equipment and 3rd party supplier services to be ordered against the capital budgets before the year end. Annual maintenance payments will, for the most part, start in 2013/14. If approval is delayed then the profile may alter and some capital payments will be made in 2013/14. If options 1-6 are approved then the cost profile is:

Financial Year	Total Cost	Capital	Revenue
2012/13	**£64,600**	£62,800	£1,800
2013/14	£6,900	£0	£6,900
2014/15	£6,900	£0	£6,900

4.2 Options 7 and 8 carry significant cost implications for both capital and revenue but if all 8 options were to be approved then the cost profile would increase to:

Financial Year	Total Cost	Capital	Revenue
2012/13	**£217,406**	£213,606	£3,800
2013/14	£58,578	£0	£58,578
2014/15	£58,578	£0	£58,578

4.3 An additional figure of £10,000 to £20,000 should be set aside for contingency, depending which options are approved.

5. RECOMMENDATIONS

5.1 It is recommended that options 1 and 2 be implemented immediately as these are essential pre-requisites for any DR capability. This will enable the DR Centre to be used as a 'warm' DR facility for most core systems by providing the missing link to CJX and the outside world, and by providing a secure off-site storage mechanism for the back-ups that would be needed to reload those systems should the DR Centre be needed.

5.2 It is also strongly recommended that options 3 - 6 be implemented as this will close the existing gaps in the DR plan by providing DR facilities for those mission critical systems which were excluded from phase 1 of the project because of outstanding virtualisation work or upgrade plans.

5.3 Options 7 provides a DR capability for Origin-HR and Holmes, neither of which are currently defined as mission critical, but the Force may wish to reconsider that position as the impact of losing either system in the event of a disaster would be keenly felt and impact operational policing. There are significant costs however.

5.4 Option 8 is for debate as the costs could be deferred or avoided if the risks to the organisation were felt to be manageable. Again, there are significant costs attached to this option.

5.5 Option 9 is for debate depending on the outcome of the BT Scoping Study.

British Transport Police

Disaster Recovery Centre Phase 2
FULL BUSINESS CASE

BTP Department/Area: Technology

Authors: Alan Shrimpton, Sue Brown

Sponsor: Director of Corporate Resources

Version: 1.1

Date Issued: 14th January 2013

Departmental Approval

Department	Approved By	Title/Rank	Date Approved
Crime	No impact		
Estates & Facilities	No impact		
Finance	Charles Le Fevre	Lead Management Accountant	15th Jan 2013
Fleet	No impact		
HR	No impact		
Operations	No impact		
Procurement	Matt Hyde	Procurement Manager	14th Jan 2013
PSD	No impact		
SDD	Doug Ring	Head of PMO	8th Jan 2013
Technology	Originator		

Revision History

Version	Date	Comments
0.7	10th Jan 2013	Submitted to ACC Corporate Services for initial review
1.1	14th Jan 2013	Minor revisions, confirmation of final supplier costs
1.1	14th Jan 2013	Submitted to DCC and ACC Corp Services for review
1.1	14th Jan 2013	Submitted to Finance Group via Elaine Derrick

Table of Contents

British Transport Police

1 PURPOSE OF DOCUMENT

This is the Business Case for phase 2 of the Disaster Recovery Centre project in Birmingham and outlines the work needed to convert the existing 'cold standby' facility (see below for definitions) to a 'warm standby' facility.

2 BACKGROUND & DEFINITIONS

The role of any Disaster Recovery facility is to ensure that an organisation can survive the loss of its primary ICT centre and continue to operate. Few organisations can afford to duplicate all of their operational systems and services in a dedicated Disaster Recovery (DR) environment so it is usual to concentrate on providing a DR capability for core systems only and accept that, in a disaster, some services would need to be suspended, or significantly reduced, until normal service was resumed.

Please note that Disaster Recovery is about planning for a catastrophic loss of ICT services (such as the loss of the FHQ building to fire, flood or any other event that renders it unusable) and is not the same as Business Continuity which seeks to plan for the loss of individual systems and services.

In planning any DR facility there are three questions to be asked:

- which systems and services should be included in the DR facility?
- where should it be located?
- what level of DR provision is required?

The issue of where a DR facility should be located depends on space (is there a facility large enough to house the DR servers and storage), connectivity (can it be connected to the Force network with network connections that are fast enough to do the job), and cost (of the machine room and network connections – should they be insourced or outsourced). Many organisations choose to outsource their DR provision by paying for space in a commercial DR centre, and providing network connections to that centre, but this requires additional security considerations in a Police context that make it an expensive option. Consequently, and as BTP already had the capacity within its own estate and network connectivity could be provided via the WAN Upgrade project, Birmingham provided an appropriate location.

The question of which systems should be included in the DR Centre can be answered by looking at the agreed list of mission critical systems as defined in the Force's Business Continuity Plan and the out-of-hours support arrangements. They are:

System/Service	Description	Support period
Command and Control	Command and Control	24/7
ICCS	Integrated Communications	24/7
Airwave	Airwave Radio Communications	24/7
Voice	Voice telecoms into FCRL, FCRB, FCC and CRC	24/7
Network	Network connections to FCRL, FCRB, FCC and CRC	24/7
CJX	Link to national systems like PNC, PND, ViSOR, etc.	24/7
Crime	Crime Recording System	24/7
Points	Tasking System	24/7
FIS	Force Intelligence System	24/7
Intranet	Force Intranet	24/7
Email	MS Exchange System	24/7
PNC	Police National Computer system	24/7
MDA (see note below)	Mobile Data Service	24/7
DWH	Data Warehouse	24/7
Station Check	Outlying stations voice log	24/7

The first 5 systems and services on the list (shaded in blue) are already protected by their own DR facilities (C&C) or provided as resilient managed services with defined fall back options (ICCS, Airwave, Voice and Network) and are therefore outside of the scope of this business case.

The remaining 10 systems are in scope of the DR Centre, but please note that the MDA (Mobile Data Service) was excluded from the final DR requirements list by decision of the project board because of the cost and complexity of duplicating the O2 gateways and device management servers in Birmingham.

.

In addition, and given the expense of creating a DR Centre, it is suggested that the following non-critical but core systems should also be included within the scope of the DR Centre:

System/Service	Description	Support Period
CuCase	Custody & Case Preparation	Business hours
Holmes	Major Enquiry System & Casualty Bureau	Business hours
Origin	HR System (including Duty Management)	Business hours

The level of DR capability relates to how quickly a DR facility can be brought into operation if the worst happens and there are three, broadly accepted levels - 'hot', 'warm' and 'cold'. In the ITIL standard these are also referred to as 'immediate', 'intermediate' and 'gradual'.

A 'cold standby' or 'gradual' DR facility is the minimum cost option and provides a DR centre fitted out with servers, disk storage and network connections, but all powered off (cold). This is most commonly used by organisations whose business "can function for a period of 72 hours or more without IT services", but it would not be considered appropriate for an organisation like the Police Service providing 24x7 services. Recovery time is in excess of 72 hours.

A 'warm standby' or 'intermediate' DR facility is one where the DR centre is not only fitted out and connected to the network but powered up and running (warm) with duplicate copies of core systems running on the equipment. Live data from operational systems is normally copied over to the DR systems at regular intervals (typically overnight but more frequently for critical systems) or loaded from the last backup if the centre is invoked. This allows recovery time to be reduced to a few hours (and at worst a day or two) as IT staff need to transfer to the DR site and restore the latest data files or backups to the duplicate systems already running there.

A 'hot standby' or 'immediate' DR facility is one where the DR centre is not only connected and powered up but also receiving real-time data feeds from the primary site such that the DR systems are mirroring the operational systems. This is achieved by a technique called data replication which copies every change or update made on the live system and applies it directly to the DR system using a dedicated network connection. In such facilities, recovery time is measured in minutes, and in some sophisticated systems can even be seamless where the transition from live to DR environment goes unnoticed by the users. Naturally, this is the most expensive DR option and is usually reserved for mission critical systems such as Command & Control, or similar applications, where public safety is at risk.

3 CURRENT POSITION

As already noted, the Force's Command & Control system, supplied and supported by Capita, is protected by a 'hot standby' capability that is fully independent of the DR Centre in Birmingham and has already been the subject of a full-scale test (running for 50 minutes, though with some minor issues). A longer test is planned for the Spring.

Command & Control runs on a dual node system at FHQ with 'hot' fail-over to a third system in Birmingham if required. Activation of the DR facility is immediate.

It is also important to note that the ICCS, Voice Telecommunications to the key locations, and dispatch of Airwave Radio Communications, are all protected by well established processes and equipment that are not associated with the core network so these are not at risk, nor part of this business case. Likewise, the Force Network is provided as a resilient managed service by BT and not part of this business case.

The DR Centre in Birmingham, as currently configured, provides a minimum 'cold standby' capability that is fully connected to the Force Network and available for use 24/7. Given sufficient time, **any** system can be recovered into the DR Centre by procuring the appropriate server and storage hardware, installing the software on that equipment, and then reloading the data from the last available backup. However, whilst this may be appropriate for second tier systems, it is not fast enough for mission critical systems.

The DR Centre has, therefore, also been configured to provide a 'warm standby' facility for the entire Microsoft Windows Virtual environment using duplicate servers and storage, and real-time data replication services to copy database changes to Birmingham as they happen. The following systems are already protected by this facility:

Intranet	Force Intranet	Warm
DWH	Data Warehouse	Warm
CuCase	Custody & Case Preparation	Warm

A range of other non-mission critical systems are also available to run in the DR Centre, simply because they reside on the same Windows Virtual environment, and these include the ICCM Service Desk system, e-FINS Finance system and KIMS Property Management system.

Finally, a separate DR server for the Crime system has been installed in Birmingham. This is a Unix based system and cannot use the data replication services enjoyed by the Windows environment, but database transaction logs copied to Birmingham overnight and applied to the DR database on the next day to keep it in step, thus providing a warm standby capability for this system as well.

Crime	Crime Recording System	Warm

The remaining systems, some of which were the subject of upgrades or virtualisation work at the time of the Phase 1 project and could not therefore be included in the Phase 1, still need to be implemented in the DR Centre:

System/Service	Description	Target Level
CJX	Link to national systems like PNC, PND, ViSOR, etc.	Hot
Points	Tasking System	Warm
FIS	Force Intelligence System	Warm
e-Mail	MS Exchange System	Warm
PNC	Police National Computer system	Warm
Station Check	Outlying stations voice log	Warm
Holmes	Major Enquiry System & Casualty Bureau	Warm
Origin	HR System (including Duty Management)	Warm

The CJX connection could not be implemented under Phase 1 because approval to do so had not been granted by the National Police Security Accreditor. That approval was withheld because the network security documents (called RMADS) had not been completed to the required standard by our network supplier. They have been reworked and approval has now been granted to connect the Birmingham DR Centre to CJX.

This is particularly important because the CJX link provides contact with national systems (such as PNC) and the outside world in the form of the Internet and external e-mails.

4 BUSINESS NEED

The proposal is owned by the Director of Corporate Services.

In its current state, the DR Centre in Birmingham already provides a fully functional 'cold standby' capability and a 'warm standby' capability for all of the systems that currently utilise the Windows Virtual Environment and the Crime system. However, the lack of a functioning connection to CJX would seriously hamper operational policing and delivery of front line services should the Centre be invoked.

The desired level of Disaster Recovery facilities for the Force has been defined as 'hot standby' for Command & Control, Voice Telecommunications into Control Rooms and Contact Centres, and Airwave, and 'warm standby' for the remainder of the systems listed on page 4. Much of this work has already been completed, but this Phase 2 business case addresses the provision of DR facilities for the systems listed on page 7 which were not covered by Phase 1.

The impact of not addressing the issues raised in this business case would be significant. If we lost FHQ tomorrow the only systems that would be immediately available would be Command & Control, Voice Telecommunications into the Control Rooms and Contact Centre, and Airwave Radio Communications. Primary published contact numbers (within the Control Rooms and First Contact Centre) are provided from a resilient platform outside of the BTP core network. In the event of a complete failure these can be recovered rapidly and call handling can continue, albeit at reduced capacity. The Force Contact Centre can operate in the event of a failure of the main call centre to approximately 75% of normal capability as long as the main telephony server and network in Birmingham is in place.

Whilst this is sufficient to take calls from the public and dispatch officers to incidents and crimes, most other core systems would be unavailable for a period of days or even weeks. Intelligence checks would have to be routed through other Forces by phone. Crimes would have to be recorded on paper and rekeyed into appropriate systems when they became available. Ditto Custody and Case Preparation which, in this electronic age, would result in delays to cases. There would be no e-Mail facilities for some time, probably around 2-3 weeks based on the experience of another Force who suffered a catastrophic loss of e-Mail services with no DR arrangements in place. Even shifting to paper based working, this would almost certainly impact the services we deliver to victims, their families and the wider community, and trigger one or more critical incidents.

This proposal provides a series of tiered steps, some of which are optional, to deliver a 'warm standby' capability for the remaining mission critical systems.

However, any DR facility is, by definition, work in progress because any changes made to the primary ICT facilities at FHQ (whether that is extra server power and storage capacity to meet organisational growth or new systems and services) needs to be reflected in the DR facility as well. Thus future business cases for new or modified mission critical systems will need to include costs and resources to replicate those changes in the DR environment.

5 OPTIONS

5.1 Summary of Options (presented as steps, some of which are optional):

- **Step 1**: connect the DR Centre to CJX and provide the requisite firewall protection for that link. This will enable the DR Centre to connect to PNC, PND, ViSOR, and other national systems if invoked and is essential to provide the 'warm standby' capability required by the Force. As part of this work, BT will conduct a scoping study to determine what changes to the network would be required to share the second the CJX link during normal operations and to access DR systems on an individual basis.
- **Step 2**: the Force uses a product called Legato to backup all of its Unix based systems to a Quantum storage device, and a second Quantum device is currently being built at FHQ in order to provide an off-site copy of all of the backups. This second device needs to be transferred to Birmingham. Synchronised over the network, it will provide a secure, off-site copy of all Unix backups **and** a repository of system backups to be used if the DR Centre is invoked.
- **Step 3**: relocate the existing 'hot standby' server for the Force Intelligence System (FIS) from the FHQ Data Centre to the DR Centre in Birmingham. It will still continue to function as a 'hot standby' server for the primary server (should that fail) but will also then provide a DR capability for FIS in the event of a disaster at FHQ.
- **Step 4**: migrate Points and our PNC gateway software from the old Windows NT Domain to the new domain and then virtualise onto the new Windows Virtual Environment. This will have the immediate effect of providing a DR capability for Points and PNC because everything on that environment is automatically replicated in Birmingham.
- **Step 5**: provide a duplicate server environment in Birmingham for Microsoft Exchange (our e-Mail system) which currently has no DR provision at all. It had been intended to leave the provision of a DR capability for Exchange until the planned major upgrade to Exchange 2010 but that would incur delay and expose the Force to some risk. A duplicate server environment and storage needs to be provided in Birmingham to provide a 'warm standby' capability for e-Mail.
- **Step 6:** provide DR capabilities in Birmingham for the specialist 3rd party voice systems (Station Check and Firearms Voice Recording) which were out of scope of the original proposal.
- **Step 7 (optional)**: provide duplicate servers in Birmingham for the Origin-HR and Holmes systems which currently have no DR provision at all. It had been intended to provide a shared server for both systems in Birmingham under Phase 1, but the system suppliers would not give approval for shared or virtualised versions of their products and the work was suspended. Installing two separate servers (for the moment) will ensure that these systems have a DR capability in Birmingham.
- **Step 8 (optional):** consider upgrading the existing network connections from existing P2 sites into Birmingham as they are slower than the equivalent connections into FHQ. This lack of bandwidth would give rise to performance problems if the DR Centre were invoked, especially as many FHQ staff would need to relocate to a P2 site in London, adding to the demand at those sites. This will involve upgrading the existing 5Mb circuits to 10Mb. As the network is provided as a managed service by BT the work would be entirely undertaken by BT with no resource implications for BTP.
- **Step 9 (optional):** implement the recommendations of the BT Scoping Exercise (completed as part of Step 1) to allow the Force to share the second CJX link during normal operations and access DR systems on an individual basis.

This page intentionally left blank

5.2 Step/Options Appraisal – Summary Table

Step/Option	Benefits	Cost	Risks (of not doing this)
1: Connect the second CJX link and protect it with appropriate firewall and security software. **As part of this work, BT will conduct a scoping study to determine what changes to the network would be required to share the second the CJX link during normal operations and to access DR systems on an individual basis. See Note 1 below.** **It should also be noted that we will be obliged to conduct a Network Penetration test after establishing the new link and this cost is accounted for at item 5.**	In the event of a disaster the second link will provide BTP with an accredited link to the Police National Network and key national databases including PNC, PND, ViSOR, NFLMS, NCALT, NBD etc.	**Capital Costs (one-off):** 1. Install CJX Link £2,000 2. Firewall connectivity £8,400 3. Network routing / load balancing Scoping Exercise £2,000 **4.** M86 proxy security £11,400 **5.** Penetration Test £2,000 **Total one-off costs £25,800** **Revenue Costs (ongoing):** 1. Annual Maint. £3,000 p.a. 2. Travel and hotel £200 *See Note 1 below.*	Loss of primary ICT services at FHQ would result in: • loss of access to PNC, PND, etc. • loss of access to NCALT • loss of access to the Internet • loss of all external e-Mail communications
2: Complete the implementation of the second Quantum back-up storage device in Birmingham. Set this device to synchronise with the primary device at FHQ over the Force network. **This equipment has already been purchased.** **It is envisaged that some 3rd party support may be needed to set up recovery procedures from the Quantum box to the DR servers.**	On a day to day basis this device will provide a secure off-site copy of all the Unix systems back-ups currently managed using the Legato software and stored on the original Quantum device at FHQ. In the event of a disaster at FHQ, this off-site copy of all the Unix based systems will be used to reload data from the last backup onto the DR servers providing a 'warm' DR capability. This option avoids the need for procuring expensive database replication software for the Unix based systems (though this can be evaluated as a future enhancement).	**Capital Costs (one-off):** All the equipment has been purchased already. 3rd Party Supplier Implementation for individual systems £2,000 **Total one-off costs £2,000** **Revenue Costs (ongoing):** Travel and hotel costs: £200 See note 2.	Loss of primary ICT services at FHQ, which would include the primary and secondary Quantum Storage device, would mean that the only remaining backups of the Unix based systems would be in held on tape.

3: Relocate the existing hot standby server for the Force Intelligence System from FHQ to Birmingham. Synchronised over the Force network, it will still continue to function as a hot standby server for the primary server (should that fail) but will also provide a DR capability for FIS in the event of a disaster at FHQ. **It is envisaged that some support may be needed from Memex to implement and test network synchronisation between the two servers.**	Provides a DR facility for the Force Intelligence System where there is none at present.	**Capital Costs (one-off):** No equipment required. Memex support for implementing network synchronisation £2,000 **Total one-off costs £2,000** **Revenue Costs (on-going):** Travel and hotel costs: £200	Loss of primary ICT services at FHQ would result in complete loss of FIS services until such times as new equipment could be procured and installed in Birmingham, system software reinstalled by the suppliers and then data reloaded from the Birmingham Quantum server (assuming Option2 had been implemented). Likely outage would be in the region of 2-3 weeks.
4. Migrate Points and our PNC gateway software from the old Windows NT Domain to the new domain, and then virtualise onto the new Windows Virtual Environment. This will have the immediate effect of providing a DR capability for Points and PNC because everything on that environment is automatically replicated in Birmingham. **It is envisaged that some support may be needed virtualise Points and PNC from Northgate and NDI.**	Provides a DR facility for Points where there is none at present. Allows the Force to finally shut down the old Windows NT services and associated domain which will simplify the network and support requirements.	**Capital Costs (one-off):** No equipment required. Northgate support for virtualising POINTS £3,000 NDI support for virtualising PNC Gateway £1,000 **Total one-off costs £4,000** **Revenue Costs (on-going):** No additional costs.	Loss of primary ICT services at FHQ would result in complete loss of Points services until such times as new equipment could be procured and installed in Birmingham, system software reinstalled by the suppliers and then data reloaded from the off-site backups. Likely outage would be in the region of 2-3 weeks.

5: Build a duplicate server environment in Birmingham to provide DR facilities for MS Exchange. Appropriate servers and storage can be supplied from spares released by the Windows Virtualisation programme. **Backup tapes from FHQ will be couriered to Birmingham to provide the 'warm' start data if needed, and Tape Library system will need to be provided in Birmingham. Replication is not currently possible with this old system (although options are under investigation).** **3rd Party Support will be required from OSCL to configure the DR e-Mail system.**	Provides a DR facility for MS Exchange where there is none at present.	**Capital Costs (one-off):** 1. Configuration services from OSCL £5,000 2. Server licences £1,000 3. Fibre cards for SAN £6,500 4. SysOp tape Library £2,000 **Total one-off costs £13,000** **Revenue Costs (on-going):**. 1. Additional Tapes £500 p.a 2. Travel and hotel £1,000	Loss of primary ICT services at FHQ would result in complete loss of MS Exchange services (e-Mail, Calendar, Contacts and Tasks) until such times as new equipment could be procured and installed in Birmingham, system software reinstalled and then data reloaded from existing backup tapes. Likely outage would be in the region of 2-3 weeks.
6: Provide DR facilities in Birmingham for the specialist 3rd party voice based systems such as Station Check and Firearms Voice Recording.	Provides a DR capability where none exists at the moment.	**Capital Costs (one-off):** 1. Servers, storage and other specialist equipment for Birmingham £14,000 2. Configuration services from Azzurri and Bitea £2,000 **Total one-off costs £16,000** **Revenue Costs (ongoing):** 1. Annual Maint. £2,100 p.a. 2. ISDN Rental £1,300 p.a. 3. Travel & Hotel £200	Loss of primary ICT services at FHQ would result in complete loss of these services until they could be re-supplied in Birmingham from scratch. Likely outage would be in the region of 3-4 weeks.

7: Build new live server environments in FHQ for both ORIGIN (HR +DMS) and HOLMES and ship the current servers to Birmingham to provide DR facilities for both systems. **This will require the purchase of a new server for HOLMES (quotation obtained) and re-use of the M4000 server purchased for the UNIX Virtualisation project for ORIGIN.** **Both new servers will need to be implemented by the appropriate supplier – Unisys and Capita.** **This will provide a 'warm' DR facility using the backups stored on the 2nd Quantum Storage Device (option 2) to reload the live system if required.**	Provides a DR facility for Origin and Holmes where there is none at present. Use of the much more powerful M4000 server for ORIGIN (originally proposed for the UNIX Virtualisation project) may address some of the current performance problems being experienced by Origin users because of the complexity of the system. Use of the backups on the Quantum Storage Device avoids the need for expensive database replication software.	**Capital Costs (one-off):** 1. Purchase new Holmes server and storage £39,000 2. Holmes configuration services from Unisys £30,000 3. Memory expansion for existing M4000 for Origin £8,000 4. Origin configuration services from Capita £25,000 5. Ship both old live servers to Birmingham £1,000 **Total one-off cost £103,000** **Revenue Costs (on-going):** 1. Annual Maint. £4,500 p.a. 2. Travel and hotel: £2,000 *See notes 3, 4 and 5 below.*	Loss of primary ICT services at FHQ would result in complete loss of ORIGIN (both HR and DMS) and HOLMES services until such times as new equipment could be procured and installed in Birmingham, system software reinstalled by the suppliers and then data reloaded from the Birmingham Quantum server (assuming Option2 had been implemented). Likely outage would be in the region of 2-3 weeks. Loss of Duty Management scheduling for the same period. Live Holmes events would need to revert to paper for the same period and then rekey data into the system once available.
8: Review and upgrade the existing P2 site network bandwidth provided to Birmingham (5mb) and upgrade to the same bandwidth as that provided to FHQ (10M) to avoid degradation of service if the DR Centre is invoked. Upgrading the P3 sites en masse was considered but is too expensive (see options below). **Bandwidth is purchased from BT under the WAN contract so this option requires only approval of the additional expenditure. BT will make the changes to the network.**	Provides the same network speed to FHQ and Birmingham so that the DR Centre (if invoked) can be used without degradation of services. If the DR Centre were invoked in anger then the P2 sites would be critical to the success of the operation as the staff who normally work at FHQ would decamp to pre-arranged P2 sites according to their departmental business continuity plans where desk capacity could be provided.	**Capital Costs (one-off):** 1. Design work, BT project management and installation fees £47,806 **Total one-off costs £47,806** **Revenue Costs (on-going):** 1. Additional recurring charges for faster circuits £47,178 p.a.	Loss of primary ICT services at FHQ would result in all other sites on the BTP Network reverting to their slower bandwidth connections to Birmingham to access the DR Centre. It is unlikely that the same volume of work could be processed across these slower circuits requiring local prioritisation decisions or some systems to be turned off. Extra load at P2 sites caused by the influx of staff from FHQ could cause operational problems.

9: **Implement the recommendations of the BT Scoping Exercise (completed as part of Step 1) to allow the Force to share the second CJX link during normal operations and access DR systems on an individual basis.**	The second CJX connection will provide resilience should the primary CJX link experience problems, and an opportunity to do some 'load balancing' between the two links to ease pressure at peak times. The Scoping Exercise will also recommend changes to the Force Network configuration and routing tables to allow load balancing across the whole network and access to individual systems within the DR Centre without invoking the whole centre.	**Capital Costs (one-off):** Unknown pending outcome of the Step 1 Scoping Study **Total one-off costs £t.b.a.** **Revenue Costs (on-going):** Unknown pending outcome of the Step 1 Scoping Study	None. These are added benefits and there are no risks to the network in not doing them.

Notes:

1. Step 1 includes a £2,000 Scoping Study from BT which will identify and make recommendations for changes to the configuration of the Force network to allow the second CJX link to be shared across the whole network during normal operations (not just kept on standby in case the DR Centre is activated) and to make better use of the network in general. The Scoping Study is scheduled for 22nd January and the costs of the recommendations (which will affect Step 9) will not be known until after that date.

2. There is a small possibility that the increased replication and back-up traffic from FHQ to Birmingham (Step 2) may require an upgrade to the dedicated DR network connection (currently 100Mb).

3. The cost of the new server for Holmes II (Step 7) is based on a worst case quotation supplied by Unisys but other Forces run the system successfully on smaller boxes so Technology will conduct further research with a view to reducing this cost.

4. The cost of configuring Holmes II on the new server (Step 7) is based on a "will not exceed" quotation from Unisys but experience says that this work should take a lot less time and effort and we are expecting the cost to reduce.

5. The cost of configuring Origin on the M4000 server (Step 7) is based on a standard quotation from Capita but seems excessive and may turn out to be less.

This page intentionally left blank

.

5.3 Option Recommendations

It is recommended that steps 1 and 2 be implemented immediately as these are essential pre-requisites for any DR capability. This will enable the DR Centre to be used as a 'warm' DR facility for most core systems by providing the missing link to CJX and the outside world, and by providing a secure off-site storage mechanism for the back-ups that would be needed to reload those systems should the DR Centre be needed.

It is also strongly recommended that steps 3 - 6 be implemented as this will close the existing gaps in the DR plan by providing DR facilities for those mission critical systems which were excluded from phase 1 of the project because of outstanding virtualisation work or upgrade plans.

Options 7 provides a DR capability for Origin-HR and Holmes, neither of which are currently defined as mission critical, but the Force may wish to reconsider that position as the impact of losing either system in the event of a disaster would be keenly felt and impact operational policing. There are significant costs however.

Option 8 is for debate as the costs could be deferred or avoided if the risks to the organisation were felt to be manageable. Again, there are significant costs attached to this option.

Option 9 is for debate depending on the outcome of the BT Scoping Study.

5.4 High Level Cost Profiles

This cost profile assumes financial approval in January to allow equipment and 3rd party supplier services to be ordered against the capital budgets before the year end. Annual maintenance payments will, for the most part, start in 2013/14. If approval is delayed then the profile may alter and some capital payments will be made in 2013/14. If options 1-6 are approved then the cost profile is:

Financial Year	Total Cost	Capital	Revenue
2012/13	**£64,600**	£62,800	£1,800
2013/14	£6,900	£0	£6,900
2014/15	£6,900	£0	£6,900

If all 8 options were approved then the cost profile would increase to:

Financial Year	Total Cost	Capital	Revenue
2012/13	**£217,406**	£213,606	£3,800
2013/14	£58,578	£0	£58,578
2014/15	£58,578	£0	£58,578

An additional figure of £10,000 to £20,000 should be set aside for contingency, depending which options are approved.

5.5 Testing v Rehearsal

Individual components of this business case will be tested as they are delivered using a combination of external verification (as in the Pen test for the new CJX link), in situ tests for new servers and hardware, and trial recoveries from back-up conducted with the support of the relevant 3rd part suppliers.

The Phase 1 Business Case for DR proposed a full-scale test which was scheduled to run for a period of 3 weeks during February 2013. However, this approach is not recommended because the DR Centre is designed to provide a recovery capability for mission critical systems only, and because there will be some limitations using the DR service due to the slower network connections from P2 and P3 sites and Birmingham. There are also practical considerations around moving the Force over to run on the DR systems and then, more importantly, moving the data accumulated on the DR systems back to the primary systems at FHQ at the end of the trial period. A 3 week test would make this a major exercise.

For all of these reasons, any full scale test of the completed facility should be treated as a full Disaster Recovery Rehearsal and should be planned in conjunction with Force Operations Planning to ensure that there are no other planned operations scheduled for the same period and with due consideration to impact on the Force and the duration of the test.

It is outside of the scope of this project.

5.6 Future Options

It should be noted that there is an option to upgrade the network connections to some of the more modern P3 sites, as per Option 5 for the P2 sites, but the total cost (for the 79 sites that could be upgraded) would be over £110,000 in one-off charges and an additional £55,000 p.a. in rental costs for the faster circuits. It would be more cost effective for the Force to consider which P3 sites should be designated as being required during a DR scenario, and accept that the remainder will have only limited IT services, and run a separate project to just upgrade the network bandwidth to those designated sites. This could be run as a separate project at any time in the future.

There is also an option to engage with BT to automate the process of transferring control to the DR Centre in Birmingham as this is currently a manual process. However, we are not able to determine what the costs might be to automate this until BT have explained how the current network functions (a meeting has been set for the end of January 2013) so this option has been excluded from the Business Case at this stage.

6 IMPLEMENTATION

6.1 Responsibilities

The following people have overall responsibility for these proposals:

- **Project Sponsor**: The Director of Corporate Resources is accountable for the delivery of this project
- **Project Manager**: An experienced Technology project manager will need to be appointed to manage the project, either from within Technology or by recruiting an interim project manager.
- **Senior Supplier**: Alan Shrimpton, Interim ICT Transformation Manager, will be responsible for agreeing the objectives and ensuring that the project manager has the appropriate resources to deliver the project.
- **Technical Lead Networks**: Jim Lamberton, Assistant Technology Manager Networks, will be responsible for key deliverables in the project related to BTP's network, including technical liaison with the primary supplier, BT.
- **Technical Lead Communications**: Philippa Brown, Assistant Technology Manager Communications, will be responsible for key deliverables in the project related to BTP's voice communication services, including technical liaison with party suppliers such at BT.
- **Technical Lead Servers and Storage**: Ross Powell, Assistant Technology Manager DAMSS, will be responsible for all deliverables related to servers, storage and back-up environments.
- **Business Continuity:** Aminur Rahman, BTP Business Continuity Manager, will oversee the Technology DR plans and advise on all business continuity matters within the project.

6.2 Implementation Approach

Project set-up:

- The project will be established using the BTP project management methodology as set out by the BTP PMO.

- A project board will be established will be established under the direction of the project sponsor to deliver the project and govern the actions and decisions made in the project.

- A dedicated project manager will be appointed to manage the delivery the project.

- Regular highlight reports will be provided to the project board at a frequency to be determined by the board. Issue and risk logs will be maintained by the project manager.

Project approach:

- The project will be broken down in to work streams each with a clear scope depending on how many of the 8 options are approved.

- A Project Initiation Document (or PID) will be produced outlined the detailed proposals for the delivery of each option, applicable quality standards and acceptance testing.

Financial management:

- The budget will be controlled by the project manager using capital and revenue cost codes assigned by Finance. All purchase orders will be raised and tracked by Stuart Charters, Finance Liaison Officer for Technology.

Business change:

- This project will deliver changes to the DR infrastructure that will be largely invisible to the rest of the Force until such time as the DR Centre needs to be invoked. Changes will be made in the DR Centre in Birmingham and should not impact normal ICT operations being run out of the primary data centre at FHQ. All change management will therefore be routed through Technology's internal Change Advisory Board.

- Changes to the Technology Business Continuity plans as a result of implementing this new capability will documented by the project and communicated to the Force Business Continuity Manager.

- There are no training implications for this project as it seeks to implement DFR copies of existing systems.

Procurement and supplier management

- No formal tenders are required for this project as the additional equipment can be purchased through existing national framework contracts, and the 3rd party implementation and configuration services (where required) can only be purchased from the suppliers that own the applications. A provisional procurement plan has been agreed with Matt Hyde, subject to which options are approved.

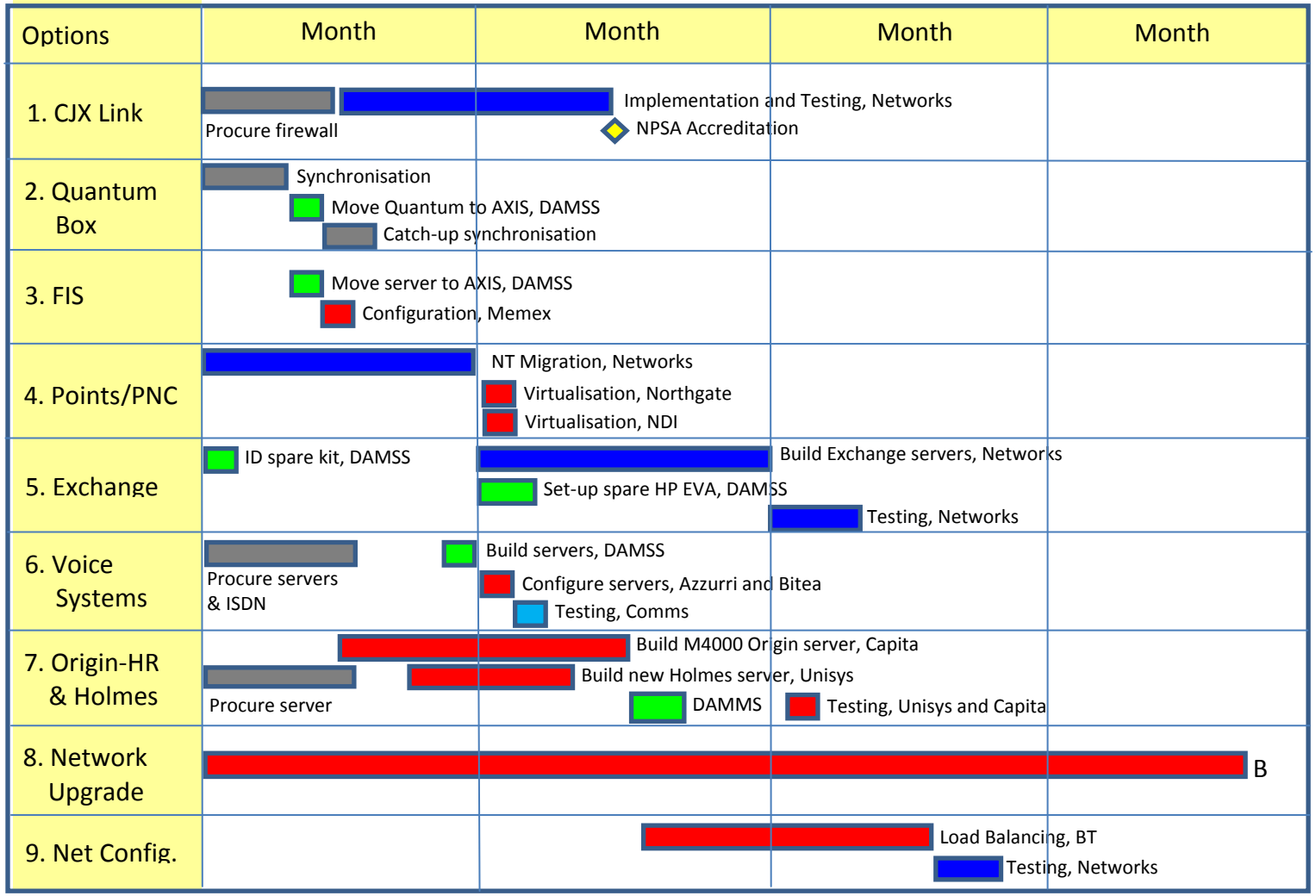
6.3 Key Milestones

See next page for detail.

If approval to proceed is granted in January 2013 and work commences on 4th February 2013 then options 1-6 would be in place and working by mid-April.

British Transport Police

Disaster Recovery Centre Phase 2
Full Business Case



This page intentionally left blank

7 IMPACT & ACHIEVABILITY

Department, name and position of consultee	Impact on proposal	Date Departmental sign off achieved
Business Continuity, Aminur Rahman	To ensure that the plans are consistent with the general Business Continuity plans for BTP. Business Continuity Manager was part of the Project Review team that agreed to go to a Phase 2 business case and has ben copied in to the Business Case for information.	Feb 2013
Finance Charles Le Fevre	To agree the budget figure noted in the document and approved by the appropriate body. To define how the approved budgets will be accounted for and ensure appropriate procedures are in place to control expenditure against those budgets. Initial discussions were held on 15/1/13.	Jan 2013
Procurement Matt Hyde	That any required procurements are checked and approved. An outline procurement plan was agreed on 14/1/13. All procurements are either via standard framework contracts (for hardware) or designated suppliers for specific software applications where they own the IPR for those applications. Matt will help Technology conduct mini-tenders across existing framework contracts where required.	Jan 2013
Individual Application Owners	To make them aware of the level of and disaster recovery and return to operation times agreed as a result of the proposals.	Feb 2013
Information Security Manager, Mike Clarke	To ensure that the implementation of the second CVJX link is properly documented and approved by the National Police Security Accreditor (now down), and that the new network link is penetration tested to the appropriate standards as required by the NPIA.	Jan 2013
PMO Doug Ring	To obtain quality assurance sign off the project proposals. The document was reviewed with the PMO on 8/1/13.	Jan 2013