BRITISH TRANSPORT POLICE

Report to:	**Audit & Risk Assurance Committee**
Date:	**31 May 2013**
Agenda item:	**6.5**
Subject:	**Disaster Recovery Phase 2**
Sponsor:	**Interim Director of Corporate Resources**
For:	**Information**

1. PURPOSE OF PAPER

1.1 To update Audit & Risk Assurance Committee on the rationale for the decision to undertake three levels of testing in relation to the Disaster Recovery Centre instead of the full failover test as recommended by Tribal following their audit on Disaster Recovery in 2012.

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 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 It is important to note that BTP'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.

3. DR FAILOVER TESTING

3.1 A previous internal audit recommended that a full failover test to the DR site in Birmingham should take place to test the capability of the system. The impact of such a

requirement to test the capability to support the Force should a disaster occur is substantial and needed to be reviewed.

4.2 Previous experience of disaster recovery at other forces and organisations is that a “big bang” test is rarely undertaken and that the operational impact would be very disruptive and significant from both a time and cost perspective.

4.3 Within the business case the level of criticality regarding systems and their DR capability was set out. Any testing will need to mirror the capability that has been put in place.

4.4 Three status levels of DR Capability were outlined in the business case being Cold, Warm and Hot and it is these that will need to be considered when deciding on the most effective testing scenario for BTP.

4.5 There are three levels of testing that are associated with these types of status levels.

- **Paper based** – The mechanism to restore the data to these “cold” servers will be documented and, if required, the servers will be livened up and the Application and Database restores carried out.
- **Application Test** – Regular back ups will be taken of the data bases for these applications and the data will be transferred to the DR Centre. The Application will be rebuilt and the Application Manager will be asked to carry out testing to prove that the system could be used if required.
- **Failover** – These are for those systems considered mission critical that have been set up with a Hot capability. Testing for these will be a switch over to the DR capability and full capability running will occur.

4.6 The key applications that have been deemed as critical have had “Hot” failover capability built and these should be tested on an agreed frequency. The testing for these applications would be on a complete failover basis. The applications deemed critical and therefore requiring a “Hot” failover test are listed in the table on the following page.

System/Service	Description	Target Level	Test
Command and Control	National Command and Control system	Hot	Failover
CJX	Link to national systems like PNC, PND, ViSOR, etc.	Hot	Failover
PNC	Police National Computer	Hot	Failover

4.7 Those system that have been deemed as “Warm” will have infrastructure in place and the appropriate backups will be being made on a daily basis. Testing of these applications should be on an application by application basis with the application manager undertaking tests to prove that the service has been restored. The applications deemed as “Warm” are as follows.

System/Service	Description	Target Level	Test
Points	Tasking System	Warm	Application Test
FIS	Force Intelligence System	Warm	Application Test
Station Check	Outlying stations voice log	Warm	Application Test
Holmes	Major Enquiry System & Casualty Bureau	Warm	Application Test
Origin	HR System (including Duty Management)	Warm	Application Test
Intranet	Force Intranet	Warm	Application Test
DWH	Data Warehouse	Warm	Application Test
CuCase	Custody & Case Preparation	Warm	Application Test
Crime	Crime Recording System	Warm	Application Test

4.8 All applications that have had a status of “Cold” will be the subject of a paper based testing scenario.

4.9 Timescales regarding this work are subject are currently being planned, in line with the delivery of the relevant systems and will progress will be reported on in further updates.

5. RECOMMENDATION

5.1 It is recommended that the Committee note the update provided in this paper.