Midlothian

Appendix 1

Midlothian

ICT Business Continuity Plans
Testing Strategy

Author	Name Ian.Wragg@midlothian.gov.uk
Owner(s)	IT Services - Corporate Resources
Date	11/06/2013
Date Printed	29/01/2013
Version	1

Ref: ICT Business Continuity Plan – Testing Strategy
Issued By: Ian Wragg
Post: Information Security Officer
Dept: IT Services
Issue Date 29th January 2013
Issue No. 1

Document Control Information

Revision	Date	Revision Description
Version 1	29th January 2013	Final

Table of Contents

Section 1 – Introduction

Section 2 – Testing Process

Section 3 – Proposed order of testing

Section 4 – Real incidents

1. INTRODUCTION

The accuracy and suitability of IT Business continuity (BC) and disaster recovery (DR) plans can never be known until you test them. Fortunately, many types of tests are possible, ranging from simple to very complex. The key to business continuity testing success is to incorporate testing as part of the overall business continuity/disaster recovery management process. This can be achieved through working closely with the Councils Contingency Planning Group (CPG)

But testing can be a major challenge. That requires not only IT support but business management support, time for preparation and execution, planning and a structured process from pre-test through test and post-test evaluation.

This strategy focuses on the applications and systems identified as business critical by the CPG.

2. TESTING PROCESS

2.1   Test Objectives

The objective of testing Midlothian's IT business continuity plan(s) is to be sure that if a disaster or failure occurs, of whatever type, the plan will work correctly and effectively and the Councils business critical operations will be restored within the required agreed timescales. Thus, testing will confirm that the plan reflects the agreed business recovery strategy, that the resources, facilities, services, etc. required are available and correct, and that the plan is:

- *comprehensive*, i.e. that it addresses all of the Councils business critical functions and will deal with most types of disaster and failure,

- *accurate*, and will be effective and viable in use,

- u*nambiguous* and easy to follow – including by personnel who may not be familiar with the plan and supporting facilities, nor the local environment, i.e. that its use is not dependent upon in-depth knowledge of particular persons.

2.2 Test Management

In managing the testing of the IT business continuity plan(s), The IT Infrastructure Manager, Senior IT Support staff, supported by other CPG team members as required, is responsible for ensuring that the:

- plan addresses the Councils business critical functions and is fully tested,

- test results are properly documented, agreed, and if necessary, changes made to the plan,

- plan is reviewed following the testing to see if any changes are required to the Councils business continuity plan, accommodation and/or IT.

- relationships with other business continuity plans (e.g. interdependent systems) are catered for, and dealt with effectively,

- plan is reviewed on personnel changes relating to roles assigned responsibilities e.g. if IT support staff responsibilities change.

Ref: ICT Business Continuity Plan – Testing Strategy
Issued By: Ian Wragg
Post: Information Security Officer
Dept: IT Services
Issue Date 29th January 2013
Issue No. 1

Page 4 of 7

- right consideration is given to re-testing on a periodic basis, to ensure that the plan remains in line with the current business operations,

- tests are monitored, including ensuring that the designated persons for using the business continuity plans if a disaster or failure were to occur are fully involved.

2.3 Test Structures

Each test will be structured to maximise the value obtained from the resources involved. There is no point in involving a large number of people, and possibly outside resources, for a day for an initial test that is likely to fail within the first 10 minutes. Tests will therefore be clearly focused.

Initial tests will be short and self contained, with limited objectives. Only once simple basic tests of a limited number of tasks are shown to work will a test be extended to cover groups of previously tested tasks together. The approach is to start simple and only gradually increase the complexity and scope as previous tests prove satisfactory. As a guide to the structuring of tests, earlier tests will be with small groups using simple scenarios, use of the experienced personnel designated within the plan to perform the actions, use of personnel from one area only (e.g. someone familiar, but perhaps not with primary responsibility for the system), and restricting tests to read-through and scenario desk tests. As relevant, later tests will be with larger groups facing more challenging scenarios with surprise 'events' being introduced during a test. Large scale hands-on tests of parts of the plan will also be conducted and this is likely to include the business system owners.

2.4 Test Steps

2.4.1   Introduction

The steps in the testing of the Councils business continuity plan are to plan the test - critical to the success of the testing programme, test the plan, review the test and modify the plan.

It is emphasised that this is an iterative process and the steps will need to be undertaken repeatedly until it is agreed that the test objectives have been achieved. The steps are described in the following sections.

2.4.2   Plan the Test

The first task is to establish the objectives and scope of each test, ensuring that all interested parties are informed, and then create the business continuity plan test plan. The list of items to be included in the test plan is as follows:

- test reference number - a test reference number
- business area/team - the name(s) of the business area(s) or team(s) under test (e.g. IT Service lead and business unit contact.
- types of test - whether it is read-through, scenario desk or hands-on,
- test objectives - the actual objectives of the tests against which its success can be measured after completion. These can be general objectives, and specific to the test,
- scope/boundary of the tests - a description of the scope/boundary, limitations, etc. of the tests,

Ref: ICT Business Continuity Plan – Testing Strategy
Issued By: Ian Wragg
Post: Information Security Officer
Dept: IT Services
Issue Date 29th January 2013
Issue No. 1

Page 5 of 7

- scenarios - a description of the sets of circumstances within which the tests are set, covering the disaster or failure that has occurred and the extent of damage, unavailability of service, absence of staff, etc.,
- date, time and location of tests - the date, time and location where the tests will be carried out (and/or where participants should meet initially),
- scheduled duration of tests - the planned duration of the tests so that participants can schedule their participation in with their other duties,
- test manager - the person responsible for calling, planning and co-ordinating the tests (i.e. the IT Infrastructure Manager or one of his/her team),
- "independent" test observers - the names of any 'independent" observers who will observe the conduct of the tests,
- 'in-house' test observers – as relevant, the names of any observers from other business areas/teams or senior management where there is an interface to them,
- test participants - the names of those participants required to take part in the tests. Depending on the test scope and scenario set, this list may or may not include all those members of the particular business area/team being tested,
- Parts of the plan to be tested and, if relevant, where there are to be constraints on the tests (e.g. only test access and resource availability.
- resources required - a list of resources, other than the actual business area/team members themselves. This may include specific physical resources, such as assets held off-site or specific documents,

Once the test plan has been completed and authorised it will be circulated to all participants and observers. Where relevant, arrangements will be made to notify business owners and if necessary other organisations so that they are aware of what is to take place.

The IT Infrastructure Manager will provide logs for himself and any other observers to record issues, observations and actions during the tests. Further, unless a test is to establish whether the business continuity plan itself can be retrieved in an emergency, a copy of the relevant parts of the plan will be provided.

2.4.3   Test the Plan

An initial briefing by the 'test manager' will precede the tests, outlining the reason for the tests, the scenarios of and background to the tests, the rules of conduct of the tests, and the roles of those personnel present who are not members of the business area/team being tested. The 'test manager' will then manage the test environment, allowing those under test to carry out the actual tests. That the tests should only be conducted with the resources available as part of the tests (e.g. a paper copy of the internal telephone directory cannot be used to locate someone if the scenario is an individual operating off-site without a copy of the directory). As necessary, the 'test manager' may act in a coaching role. Similarly, if the 'test manager' is aware of a deficiency in the plan under test they may guide the test team to discover this deficiency (e.g. by asking how a particular action is to be achieved where there is no corresponding step and procedure with the plan). The 'test manager may introduce unforeseen 'events' to test the ability of the team using the plan to react to changes of events.

2.4.4   Review the Test and Modify the Plan

Following completion of the tests, the IT Infrastructure Manager will chair a formal test review meeting with the observers and designated personnel involved in the tests, with the date, time and location as indicated on the original test plan. The meeting will consider whether the stated objectives of the tests have been achieved, any problems, omissions, deficiencies, issues, etc. discovered by the test personnel and observers, and the lessons to be learnt from the tests.

Subsequently, a plan should be produced identifying those areas of the business continuity plan tested that require modification ensuring that all modifications are made and, if necessary, re-tested. In addition, a short report should be produced for circulation to relevant individuals, describing the conclusions on the conduct and effectiveness of the tests, the key issues and deficiencies, the action plan, and the requirement for further tests.

Ultimately it is the named individual with business continuity responsibility who needs to ensure that business continuity plans are accurate and fit for purpose.

2.5 Frequency of Testing

During initial development of the business continuity plan, testing will be an iterative process until such time as the plan is judged to be fully fit for use. Once the plan is in place, further tests will take place when there are significant changes to in the character of the Council's business operations and the supporting facilities (IT, voice, etc.) and/or to the plan itself. The resources required for such tests will depend on the extent of change. In any event, periodic re-testing will take place to be sure that the plan remains in line with current Council business operations and requirements.

A testing schedule matrix has been created to identify the business critical application and IT systems and required testing frequency.

3. PROPOSED ORDER OF TESTING

The order for the testing and related test schedule is as follows. This encompasses testing those systems identified as business critical by the CPG first and then, as relevant, testing of others.

4. RESPONSES TO REAL LIFE INCIDENTS/NEAR MISSES

Following a real world incident or near miss, business continuity plans should be reviewed and if necessary re-tested to ensure completeness.

Ref: ICT Business Continuity Plan – Testing Strategy
Issued By: Ian Wragg
Post: Information Security Officer
Dept: IT Services
Issue Date 29th January 2013
Issue No. 1

Page 7 of 7