

PUBLISHED DOCUMENT

PD 25666:2010 Business continuity management – Guidance on exercising and testing for continuity and contingency programmes



This publication is not to be regarded as a British Standard.

PUBLISHED DOCUMENT

Business continuity management – Guidance on exercising and testing for continuity and contingency programmes

This publication is not to be regarded as a British Standard.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2010

ISBN 978 0 580 67840 0

ICS 03.100.01

The following BSI reference relates to the work on this standard:
Committee reference BCM/1

Publication history

First published July 2010

Amendments issued since publication

Date	Text affected
------	---------------

Contents

Foreword *ii*

0 Introduction 1

1 Scope 1

2 Terms and definitions 2

3 Programme management 5

4 Planning an exercise as a project 6

5 Exercises 8

6 Exercise preparation 11

7 Conducting an exercise 12

8 Post-exercise/real incident and disruptive events activities 14

Annexes

Annex A (informative) Roles of the participants 17

Bibliography 20

List of tables

Table 1 – Choosing an appropriate method of exercise 10

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 20, an inside back cover and a back cover.

Foreword

Publishing information

This Published Document is published by BSI and came into effect on 31 July 2010. It was prepared by BSI panel, BCM/1/-/9, under the authority of Technical Committee, BCM/1 *Business continuity management*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a guide, this Published Document takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

It has been assumed in the preparation of this Published Document that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions in this Published Document are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

The word “should” is used to express recommendations of this Published Document. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Published Document is not to be regarded as a British Standard.

0 Introduction

This Published Document gives appropriate guidance to all organizations on performing exercising, including testing activities, for continuity and contingency programmes. Arrangements for information technology (IT) systems also fall under this general guidance. This guidance is intended to be read and used in conjunction with BS 25999, BS 25777, ISO/PAS 22399 and BS ISO/IEC 27001 and the other relevant BSI documents.

This Published Document provides a framework for, or signposts to, good practice for any organization that wishes to engage in exercising activities.

Although there are operational differences between contingency and continuity programmes, it is suggested that there is synergy in exercising activities between these disciplines.

NOTE For the purposes of this document, the term "contingency" includes the disciplines of emergency, crisis, security, safety, resilience, incident and disaster management. It may also include disaster recovery activities from the field of IT.

BS 25999-1 has this to say about exercises:

"Exercises provide demonstrable evidence of a business continuity and incident management competence and capability. Time and resources spent proving BCM [business continuity management] strategies by exercising BCPs [business continuity plans] will lead to a fit-for-purpose capability. No matter how well designed and thought-out a BCM strategy or BCP appears to be, a series of robust and realistic exercises will identify areas that require amendment."

In "*Emergency preparedness*" [1], the UK Cabinet Office gives the following guidance:

- a) "... regulations require that plans include provisions for carrying out exercises", which
- b) "....means that the plan itself must include reference to an exercise programme, which will maintain its currency and validity."

The guidance in this document has been developed from a practical perspective and is designed to aid delivery of cost-effective and efficient exercising activities.

1 Scope

This Published Document (PD) establishes the principles and terminology of exercising and gives guidance on the processes and methods for developing or improving continuity and contingency capabilities.

NOTE For the purposes of this PD, testing is defined as a particular type of exercise that incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned. Accordingly, the term "exercise", where used in the PD, might also refer to testing activities.

The purposes of this PD are to:

- a) provide a basis for understanding, developing and implementing an effective exercise programme within an organization;
- b) provide confidence in the organization's ability to conduct exercises and tests with internal and external stakeholders;

- c) assist the organization in developing and assessing its exercising and testing capability in a consistent, cost-effective and risk-assessed manner that reflects good practice; and
- d) encourage constant improvement in contingency and continuity programmes within an organization.

This PD is intended for use by anyone with responsibility for operations or the provision of services, whether in public, private or not-for-profit organizations, from top management through all levels of the organization; from organizations with a single site to those with a global presence; from small to very large organizations.

2 Terms and definitions

For the purposes of this Published Document, the following terms and definitions apply.

2.1 brief

document (or oral instruction) which explains the exercise rules to exercise participants, and/or gives them background information about the scenario

2.2 debrief

occasion for exercise participants or incident responders to review and provide feedback relating to functional effectiveness, efficiency and resilience, usually after the exercise or incident is over, with the purpose of identifying lessons and participants' feelings that could provide learning opportunities

NOTE Usually, this is a facilitated discussion and a record is kept of the lessons identified. Debriefs immediately after an exercise are also known as "hot debriefs" (or "hot wash up"). Debriefs are an essential part of learning the lessons of an exercise or incident.

2.3 directing staff

NOTE See Clause 7 and Annex A for guidance on the roles of directing staff.

2.3.1 controller

exercise participant with overall control of part or all of the exercise and responsibility for:

- managing role-players and observers;
- coordinating improvised responses for issues that are not covered by the exercise script; and
- exercise administration generally, including health and safety

2.3.2 director

exercise participant with overall control of part or all of the exercise and responsibility for:

- ensuring that the exercise achieves its objectives; and
- starting and stopping the exercise

NOTE See Clause 7 for greater detail about the role of the director.

2.3.3 observer

exercise participant who watches selected segments as they unfold, whilst remaining separate from player activities

NOTE Observers play a crucial role in the debriefing and reporting process following an exercise. The term is also used for “VIP observers”, who usually visit the exercise for only a short time, largely for internal or external PR purposes, and do not take part in the debrief. Observers differ from umpires in that they are passive, while umpires are active participants.

2.3.4 role-player

exercise participant who creates or simulates a scenario by acting out the role of someone who would be involved in a real incident, but is not otherwise involved in the exercise

2.3.5 safety officer

exercise participant, usually in “live-play” exercises, who is tasked with ensuring that any actions taken are performed as safely as possible

2.3.6 umpire

exercise participant with the ability to intervene or adjudicate in the exercise to ensure that it progresses towards the aim or objectives

NOTE Umpires are often used to evaluate particular objectives which have been pre-designated in the exercise design. The umpire may also act as safety officer.

2.4 types of exercises**2.4.1 drill**

coordinated, supervised activities usually employed to exercise a single specific operation, procedure or function in a single agency

NOTE See 5.1a).

2.4.2 exercise

planned rehearsal of a possible incident designed to evaluate an organization’s capability to manage that incident and to provide an opportunity to improve the organization’s future responses and enhance the relevant competences of those involved

NOTE A test (see 2.5 and 5.1) is a particular type of exercise, which incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned.

2.4.3 live play

exercise activity that is as close as safely practicable to the expected response to a real incident

NOTE See 5.1e).

2.4.4 seminar (or syndicate) exercise

exercise in which the participants are divided into groups to discuss specific issues

NOTE See 5.1b).

2.4.5 simulation

exercise in which a group of players, usually representing a control centre or management team, react to a simulated incident notionally happening elsewhere

NOTE See 5.1d). Sometimes referred to as “command post exercise”.