

COBIT 5 Toolkit – Control Objectives for Information and Related Technology

Level 1 – Plans, Policies & Procedures	
1.	ICT Strategic Plan
2.	ICT Implementation Plan
3.	ICT Internal Audit Plan
4.	Information Plan
5.	ICT Governance Policy
6.	Risk Management Policy
7.	Information Security Policy
8.	Change Management Policy
9.	ICT Continuity Policy
10.	ICT Governance Charter
11.	ICT Strategy Committee
12.	ICT Steering Committee
13.	ICT Operational Committee
14.	ICT Portfolio Management Framework
Level 2 - BCMS and ISMS Documents	
1.	Business Continuity Planning Procedure
2.	BCMS Policy Statement
3.	Document Control
4.	Information Security Classification Guidelines
5.	Internal Audit Schedule
6.	Internal Audit Report Lead Sheet
7.	Non Conformance Report
8.	Non Conformance Report Log
9.	Business Continuity Communication Plan
10.	Information Transfer Procedure
11.	Information Labelling Procedure
12.	Information Classification Procedure
Level 3 - Formats & Templates	
1.	ICT Champion Job Description
2.	ICT Manager Job Description
3.	Resource Manager Job Description
4.	Relationship Manager Job Description

5.	IT Risk Register
6.	Change Management Request
7.	Meeting Agenda Template
8.	Meeting Minutes Template
9.	Procedure Template Schedule
10.	Service Level Agreement Template
11.	Work Instruction Template
12.	Business Continuity Contact Log
13.	Internal Audit Action Plan
14.	Management Review Meeting Agenda

Contents

1	Introduction	4
2	Information Labelling Procedure.....	4
2.1	Printed Reports	4
2.2	Screen Displays	5
2.3	Recorded Media	5
2.4	Electronic Messages	5
2.5	File Transfers	5

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

Introduction

The purpose of this document is to set out how information assets will be labelled according to the information classification scheme in place within Organization Name. For details of the scheme used and the criteria for classifying information assets, please see the Information Classification Procedure.

The labelling of information assets is a key control which will allow the appropriate level of protection to be applied. Unless information is clearly marked, employees and third parties cannot know whether the information is sensitive or not, particularly as this can change over time.

It is a responsibility of everyone involved in the organization to carefully consider how the information they produce, handle and dispose of can always remain effectively labelled.

Information Labelling Procedure

In order to ensure that the correct controls are applied to the information assets of the organization, a system of protective marking will be used so that all employees and third parties (where applicable) are aware of how that information must be managed.

Printed Reports

Where possible, a printout of information that carries a security classification will display the security marking as a watermark, clearly visible on every page of the document. Where this is not possible, one of the following methods will be used:

1. The classification will be shown clearly on the front page and in the header of every subsequent page
2. Pre-printed paper showing the security classification will be used
3. A stamp will be used to mark each page with the security classification

Screen Displays

Computer systems which allow an authorized user access to classified information will include a warning of this fact upon logon which requires user acknowledgement of some form. Where feasible, users should also be warned upon entering an area of the system which contains a higher classification of information than most other areas.

Recorded Media

Strict controls are placed on the use of removable media such as CDs, DVDs, tapes, external hard drives and USB memory sticks within the organization. Where these are legitimately used to store classified data, they will be labelled externally with the security classification of the most sensitive data on the media, together with the date of creation.

Contents

1	Communication Plan.....	4
1.1	Purpose	4
1.2	Topics of Communication	5
1.3	Methods, Frequency and Audiences of Communications.....	5
1.4	Communication Procedures.....	5
1.5	Feedback About Communication	5

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Communication Plan

1.1 Purpose

Organization Name has in place a Business Continuity Management System (BCMS) which is compliant with the standard. This BCMS helps to provide governance and control of the business continuity measures it has in place.

As part of the BCMS there is a need to communicate with various third parties who may have a role to play in assisting the BCMS to fulfil its objectives and promote continual improvement.

This document describes:

- What will be communicated
- When it will be communicated
- With whom we will communicate

This is in addition to the communication that will take place during the course of a disruptive incident which is described in a separate document, Business Continuity Planning Procedure. Communication by top management to employees is set out in Top Management Communication Program.

1.2 Topics of Communication

As part of regular communications information will be disseminated and obtained in the following main areas:

- Enquiries regarding the objectives and intention of the BCMS from third parties, including customers, suppliers, the local community and the media
- Progress reports and updates to third parties on the scope and readiness of the BCMS
- Information from national and regional threat advisory systems and bodies
- Updates from national and local authorities on relevant plans and procedures, including levels of fire, ambulance and police cover
- Revised legal and regulatory requirements that must be met by the BCMS

1.4 Communication Procedures

Procedures will be established for each of the communications methods identified so that they are performed in a managed, repeatable way.

1.5 Feedback About Communication

For each interested party, a designated relationship owner will be agreed who is responsible for obtaining feedback on the success of communication and managing the relationship on an ongoing basis. Relationship owners are shown in the following table.

CHANGE MANAGEMENT REQUEST				
Change Description/Change Request Filename:				
Change Request No:		Project:		
Requested by:		Date:		
Department/Location:		Telephone:		
Description of the Change:				
Change Needed by (Date):				
Reason for the Change:				
Requestor Sign Off:				
Approval of Request:				
Change Impact Evaluation:				
Change Type:	Application	Hardware	Network	Operating System/Utilities
	Database	Procedures	Security	Schedule Outage
Change Priority:	Urgent	High	Medium	Low
Change Impact:	Minor	Medium	Major	
Environment(s) Impacted:				
Resource requirements: ☐ Personnel ☐ h/w ☐ s/w				
Test Plan Description:				
Rollback Description:				

Change Approval or Rejection	
Change Request Status: ☐ Accepted ☐ Rejected	
Comments:	
Change Scheduled for (Date):	
Implementation Assigned to (Names):	
Change Control Committee Sign Off:	
Change Implementation	
Staging Test Results:	
Implementation Test Results:	
Date of Implementation:	
Implementer Sign Off:	Date: