
Overview

This Standard is about planning, managing and evaluating the incident response. It includes planning the incident response, managing the response in line with Business Continuity Management (BCM) plans and/or procedures and evaluating the response, using the findings to improve future plans and responses. It is for Business Continuity managers and/or other professionals who are responsible for managing the response to an incident.

**Performance
criteria**

Plan the incident response

- You must be able to:
- P1 identify all participants involved in the response process and their roles, responsibilities and authorities
 - P2 identify the trigger points for an incident, the lead and the person with responsibility and authority for invoking an incident response
 - P3 identify the main objectives of the response team
 - P4 confirm all types of resources needed for the response and access to those resources as necessary
 - P5 plan the use of all types of resources

Manage the incident response

- You must be able to:
- P6 manage and monitor the incident response in line with the organisation's BCM plans and/or procedures
 - P7 respond to the incident in a way that is proportionate to organisational goals, client-base and the services and products offered
 - P8 provide leadership and support to the incident response team
 - P9 consider the requirements and expectations of all interested parties
 - P10 use agreed processes to share information within the response team and wider organisation
 - P11 respond flexibly as the incident develops
 - P12 ensure that discussions, decisions, actions and communications are logged

Evaluate the incident response

- You must be able to:
- P13 debrief those involved in the incident response, offering appropriate support where necessary
 - P14 evaluate all aspects of the incident response
 - P15 use the evaluation findings to improve plans and responses to incidents

Knowledge and understanding

You need to know and understand:

- K1 current legal and regulatory requirements, Standards and good practice guidelines that apply to BCM
- K2 the organisation's BCM plans and/or procedures
- K3 the resources available for incident management
- K4 the process for invoking an incident and the roles, responsibilities and authorities of an incident response team, including who is responsible for invoking the organisation's BCM procedures
- K5 the competencies of those involved in the incident response
- K6 location of and contact details for team members and arrangements for contacting them outside working hours
- K7 interested parties and how and when to contact or involve them
- K8 methods of managing an incident response
- K9 how to lead an incident response team
- K10 the types of support that might be required by members of the incident response team
- K11 methods of communication during an incident
- K12 how to respond flexibly as the incident develops
- K13 different levels of criticality and how to respond appropriately
- K14 systems for logging discussions, decisions, actions and communications
- K15 how to debrief those involved and evaluate an incident response
- K16 the types of support that might be offered to those involved in an incident
- K17 how to use evaluation findings to ensure continuous improvement

CFABCM005
Manage the incident response



Developed by	Skills CFA
Version number	2
Date approved	November 2013
Indicative review date	November 2016
Validity	Current
Status	Original
Originating organisation	Skills CFA
Original URN	CFABCM8.0
Relevant occupations	Management consultants and business analysts
Suite	Business Continuity Management (2013)
Key words	Business Continuity Management plans; Business Continuity Management procedures; planning incident response; managing incident responses; evaluating incident responses; improve plans; monitor responses; incident response teams; invoking responses; roles; responsibility; authority
