The International Consortium For Organizational Resilience
Embedding the culture and systems of organizational resilience

BCM 5000 ISO 22301 Lead Auditor Exam 2016
Answer Form
Your Name
Rosemary Beech

Section 1: Multiple Choice. (1 point each)

1. a
2. g
3. f
4. a
5. b
6. c
7. d
8. h
9. a
10. d
11. a
12. c
13. f
14. b
15. b
16. a
17. c
18. a
19. g
20. a
21. b
22. g
23. d
24. a
25. c
26. d
27. b
28. b
29. a
30. c
31. c
32. a
33. b
34. d
35. d
36. a
37. a
38. b
39. c
40. b

The International Consortium For Organizational Resilience

Embedding the culture and systems of organizational resilience

BCM 5000 ISO 22301 Lead Auditor Exam 2016
Answer Form
Your Name
Rosemary Beech

Section 2: Short Answer (3 points each). Do NOT copy and paste clauses from any of the standards. Answer in your own words.

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.

FOR ALL ANSWERS PLEASE SEE ATTACHED SHEETS. 1–14 RB.

Rosie Beech pg 1 of 14.

① 19011 (4)
Auditors must undertake their role in an impartial manner to provide an objective view of the organisation they are auditing.

Auditors must ensure they are working within the legal and regulatory framework to demonstrate compliance with the law.

Auditors must adhere to confidentiality to ensure that the integrity of the organisation is not compromised and that all information gathered as part of the audit is not abused in any way.

② 19011 (6.3.2.2)

Firstly the auditor needs to establish the objectives of the audit to ensure that what they are reviewing with the auditee is in line with the audit programme and what elements of the organisation is to be reviewed.

Rosie Beech p. 2 of 14

The audit plan must also clearly set out the scope of the audit. This should include what area(s) of the organisation will be reviewed ie which locations or departments and also which of the organisations processes will be scrutinised as part of the Audit. By clearly defining the scope this sets out the expectations on the Auditor and Auditee to ensure joined up thinking for what is being reviewed and Audited.

My final example relates to the audit methods which are going to be used identifying what evidence is to be reviewed and how this will be collected. An example would be sampling as detailed in 19011 Annex B this will ensure that the Auditor and Auditee are both aware of how they will need to participate in the Audit ie provide information of evidence or ensure employees are available for attendance at interview mtgs.

3. 19011 Annex B. B1
The Audit methods used will depend on the scope and objectives of the Audit which will have already been defined. Two examples of Audit methods could include :-
* defined human interaction this could take the form of one to one interviews whereby the auditor could use a series of questions to be answered by the interviewee this could be undertaken on-site or remotely.
* the auditor could also review a variety of documented evidence to gauge opinion of the organisation's performance. Review of reports, previous audit action plans, conducting on-site visits and also observing working practices.

4. 19011 Annex B. B3
* Judgement based Sampling: this sampling method relies on the experience and knowledge of the auditor and audit team. The audit team may have previously performed audits on the organisation and therefore have

experience of the audit scope and knowledge of the requirements in order to meet the objectives. They may also have identified previous actions from the audit so will be able to review if those actions have been appropriately completed. As there is no statistical element to this audit method there may be less clarity over audit conclusions.

* Statistical sampling enables the auditor to review evidence against requirements of a procedure and can therefore use an attributes-based approach ie either the evidence conforms to the requirements or it does not (correct/incorrect)

5. ISO22301 4.2 identifies that the needs of interested parties must be considered by the organisation as part of their BCMS. this could include top management. ISO22313 4.2.1 provides examples of the types of interested parties 2 examples include shareholders and customers to the organisation. Both of these interested parties must have

have their needs considered and also their expectations determined including obligatory and ~~implied~~ stated requirements but also those that could be considered implied. Both shareholders and customers will need to have assurance that the organisation can continue to operate in the event of an incident and this should be included within the BCMS scope 301 4.3.1 and 4.3.2 and the BCM Policy 301 5.3.

6) 22301 4.2.2. the organisation must ensure that all applicable legal + regulatory requirements are included in the BCMS and they must continually check & review any changes to these requirements that they operate within. An auditor you could review versions of the BC Policy 22301 (5.3) to ensure updates have been captured as relevant and review the scope of the BCMS (4.3.1) which should be available through the document management system as out-lined in (7.5).

(7). 22301 (4.3) outlines the requirements of the scope and the auditor should review if this aligns to the needs of interested parties (22301 4.2) and also aligns to the overall strategic aim of the organisation (22301 4.1) the auditor should also review the organisations risk appetite and review the Risk Assessment (22301 8.2.3). Exclusions from the scope should be documented and explanation given as to why they are excluded. Those exclusions should not affect the organisation's ability to ensure the continuity of its operations that are included within the BCMS scope 22301 4.3.2.

(8). 22301 5.2 management commitment can be demonstrated by aligning the aims + objectives of the BCMS with the strategic direction of the organisation. They can also ensure that communication is provided ~~to~~ throughout the organisation on the importance and requirement for Business Continuity. They are also crucial to the need to promote the aspect of Continual Improvement by supporting time out and

Rosie Beech pg7 of 14

attendance at Exercises and Rehearsals and ensuring that action plans + recommendations are implemented.

(9). 22301 6.2 states that Top Management should ensure that appropriate BC Objectives are identified and are communicated to key stakeholders within the business. The objectives must align to the BC Policy, must ensure that the key products + services can be maintained, objectives can be measured to ensure progress and must be reviewed. As an auditor I would want to review the BC Objectives against the Organisation objectives and that they have taken into account the needs of interested parties 22301 4.2 and the BCMS Scope (4.3.1/4.3.2)

(10). 22301 5.4 states how an organisation must assign roles to relevant staff to ensure that the needs of the standard and BCMS are being met and also that reporting performance to top management is available. Auditors could use interviews or observe those

Rosie Beech pg 8 & 14

with responsibility to gauge if they are undertaking their day to day responsibilities appropriately (19011 annex B) also reviewing or observing exercises and rehearsals to demonstrate how well an individual performs in their assigned role (22301 8.5)

(11). BCSM documents can include

22301 4.3 The Scope of the BCMS
22301 5.3 The BC Policy
22301 8.4 Business Continuity Plan(s).

22301 7.5.
All of the above should be stored in line with the requirements of 301 7.5 documented info within the organisation Record Management System. 7.5.2 outlines the requirements for all documents that they should have an identification and description. 7.5.3 outlines the control methodology for example how the documents should be stored, who can see them and how they should be used; version controlled, how long they should be kept for and the prevention of using out of date info.

Rosie Beech pg 9 of 14

(12) As an auditor I would expect to see a fully completed business impact analysis document as outlined in 22301 8.2. Further info on the content of the BIA can be found at 22313 8.2.2 explaining that the BIA should identify the organisation's key products + services and the processes or activities that they rely on and what the impact over time would be if those services were disrupted. I would also expect to gain an understanding of the interdependencies and the resources required to perform those activities.

(13) to verify the RA the auditor could review the scope of the BCMS 22301 4.3 and also the organisation's Risk Appetite 4.1(c) which would account for internal + external factors that could result in risk and also the auditor could review the organisation's risk criteria that has been used to categorise risks. The auditor should also consider if the needs and expectations of interested parties (4.2.1) have also been considered as part of the risk assessment process. The Risk Assessment itself should also be reviewed against the aims + objectives of the organisation (4.1).

(14). 22301 8.3 identifies that BC strategy should be as a result of the outputs from the Business Impact Analysis (8.2.2) and risk assessment (8.2.3)
The BIA is used to capture all the key products and services and also the processes that are required to complete them and also maps out over time what the impact would be if those key services were disrupted. BC strategies should then be identified to alleviate or reduce the impact of that disruption.

(15) 22301 (8.4.4) identifies the requirements of a BC Plan, however 22313 (7.5.1) sets out 'how' procedures should be documented. A procedure is defined as a specified method of completing a task or role. Therefore the BC Plan needs to contain very specific methods of how to carry out a determined task.

Rosie Beech pg 11 of 14

(16).

ISO 22301 8.4 and ISO 22313 8.4.1 describes how the organisation shall ensure they have documented procedures to ensure control and management of an incident. These procedures should be specific in terms of the immediate response to the incident; changeable to meet and respond to the incident and how it develops; and effective in that the actions taken are reducing the impact of the incident and anticipating of further changes.

(17). ~~IT teams~~ ISO22301 8.4.2. details the incident response structure however 22313 8.3.2.2 details the people that the organisation ~~should identify to respond to~~ should consider in the ongoing service continuity of it's operations. 3 teams that may be used in incident management could include a tiered management approach at a strategic level such as top management and then a tactical level to review communication and management of the incident and then an operational level

Rapie Booch pg 12 & 14

to resume business activities. Other teams could include the crisis communications team to ensure appropriate internal + external communications and a facilities team who could be preparing alternate locations to accommodate staff who are relocating. The BC team could also be assisting with management of the incident.

(18). ~~ISO22317 8.4 sets out incident comms requirements and steps~~ 22301 7.4 refers to comms in relation to the BCMS so as an auditor I would wish to review the BCM Policy (5.3) to understand what communication requirements have been included and how this will ensure the needs of interested parties are taken into account (4.2). I would wish to review examples of internal + external communications to assess content and the anticipated recipients and also as part of the audit interview or question recipients of communication to see if the comms given met their needs in line with ISO19011 Annex B.

Rosie Beech pg 13 of 14

(19). ISO301 8.5 relates to the requirements of exercise and testing as an auditor I would wish to see if the objectives of the exercise are appropriate to the size & complexity of the organisation. That there is a planned exercise schedule in place and that testing takes place at planned intervals. I would also like to see what changes or improvements have been made to the *BCMS as a result of the exercises so a review of any action plans and reports to Top Management (5.4)

* Scope (4.3.1) or objectives (6.2)

And a review of document evidence of changes to BC Plans that have been retained in (7.5) record management systems.

(20). ISO22301 10.2 states that improvement is part of the requirements of the standard to demonstrate the adequacy of the BCMS.

* The auditor can review the management review of the BCMS (9.3) to ensure that corrective actions as a result of audit or exercise rehearsals have been implemented and documentation updated. ~~Action plans ...~~

* Continual improvement action plans should contain what needs correcting, how it is to be corrected, timescales, and also the root cause so as to review if they may affect other areas of the organisation. All information ie action plans and updated documents should be maintained within the record management system (7.5) *the auditor can also review reports to Top Management to ascertain that continual improvement is part of the BCM reporting and that the scope of the BCMS is being regularly reviewed.

BCM 5000 ISO 22301 Lead Auditor Exam 2016
Answer Form
Your Name
Rosemary Beech

THE ICOR
The International Consortium For Organizational Resilience
Embedding the culture and systems of organizational resilience

BCM 5000 ISO 22301 Lead Auditor Exam Answer Form

The Examination contains a total of 60 questions. These questions are designed to evaluate your knowledge of BCM as well as your knowledge of ISO 22301, 22313, 17022 and 19011. The exam consists of two sections: 40 multiple choice and 20 short answer questions.

Multiple choice questions are valued at 1 point and the short answer questions at 3 points for a total of 100 points. The minimum passing score required to become an ANSI accredited BCMS Auditor is 80% or 80 points total and a minimum of 80% on each of the two sections. One free exam retake is available via ICOR's online exam system.

You will have *4 hours* to complete this examination. You may use all of your course materials.

Use this answer form to record your answers. Do not write the question, just answer the question. Do not copy and paste content from the standard. Use your own words and reference the clause number.

Student Information

Exam Score: **Pass / Fail**
Missed Questions:

Name: (as you want it on your certificate) Rosemary Beech

Address: (where you want the certificate mailed) 32 ERNEST FITCHES WAY LITTLEHAMPTON WEST SUSSEX BN17 7EP

Company Name: LEGAL & GENERAL

Email (work): rosie.beech@landg.com

Email (home):

Date of Exam: 07.04.17 Exam Location: ASHORNE HILL COVENTRY UK

Instructor Name: SCOTT CARVER