



THE ICOR
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

Jodie Tappenden

Section 1: Multiple Choice. (1 point each)

- | | |
|-------|-----------|
| 1. A | 21. B |
| 2. G | 22. AG |
| 3. F | 23. D |
| 4. A | 24. A |
| 5. B | 25. C |
| 6. C | 26. D |
| 7. D | 27. B |
| 8. H | 28. G |
| 9. A | 29. A |
| 10. D | 30. C |
| 11. A | 31. C |
| 12. C | 32. A |
| 13. F | 33. B |
| 14. B | 34. D |
| 15. B | 35. D |
| 16. A | 36. A |
| 17. C | 37. A |
| 18. A | 38. B |
| 19. G | 39. D & D |
| 20. A | 40. B |



THE ICOR

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

Jodie Tappenden

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.

PLEASE SEE ATTACHED SHEETS
(7 PAGES).

1. ISO 19011 clause 7 lists competences required for Auditors such as clause 7.2.3 which covers the knowledge & skill set an Auditor should possess; clause 7.2.2 which documents the personal behaviour of an Auditor & compliance with the principles of Auditing; clause 5.4.4. which also refers to clause 4.2, the Auditor should be independent from the subject being Audited & be unbiased. These are important competences as they display objectiveness and impartiality as found in ISO 22301 clause 9.2.
2. ISO ~~clause~~ 19011 clause 5.3. provides guidance on establishing the Audit programme which covers the same required for an Audit plan. Clause 5.3.1. advises the identification of roles and responsibilities, which is needed to establish the roles ^{of the lead Auditor} ~~within the Audit team~~ and to identify the necessary procedures. Clause 5.3.3. requires the establishment of the extent of the Audit which is important as this is when the scope, objectives & duration ~~it~~ is defined (also see 5.4.2). Clause 5.3.6 is also important as the programme resources need to be identified to identify the availability of personnel & Auditors and to plan for financial elements like travel, accommodation and any others.
3. ISO 19011 clause Annex B provides information on different Audit methods, such as B.2. which involves reviewing documentation to ensure it is up to date and in line with the organisation's document management procedures as found in 22301 clause 7.5. This would also ~~allow~~ provide evidence for continual improvement of the BCMS. Interviews with individuals as per B.7. is also a valuable method to use as you can check personnel's awareness of the BCMS, the policy & objectives.

4. ISO 19011 clause Annex B.3. provides guidance on sampling. 2 sampling techniques are judgement-based sampling as found at B.3.2. which ~~provides the Auditor the technique to review the organisations requirements~~ requires the Auditor to have knowledge of the subject matter, giving them the ability to review, as an example, the BCMS and it's achievements of the meeting, the scope as defined in ISO 22301 clause 4.3. Statistical sampling as per B.3.3. is ~~another~~ the other technique which could be utilised ~~at~~ in reviewing BIA's as found in ISO 22301 clause 8.2.2 to check for validity and correctness in a large organisation. A sample of 10 out of 40 could be tested to provide a statistical figure of compliance.
5. ISO 22313 clause 4.2.1. figure 4 provides clear guidance for who is included in the process for determining the needs, such as top management and those who manage business continuity. An example of an interested party would be customers, they would need and expect value for money and a product to be delivered within agreed timescales. Another example would be regulators, these would expect to see the legal & regulatory requirements met, ~~and~~ adhered to and monitored by the organisation to ensure compliance, as seen in 4.2.2.
6. ISO 22301 clause 4.2.2 requires an organisation to have a procedure in place to access & review legal & regulatory documentation. As an Auditor I would review their BCMS scope (clause 4.3.1) and their BC Policy (clause 5.3) to identify ~~re~~ amendments, updates and reviews in line with any regulatory / legal changes. This should be documented & maintained in line with clause 7.5. in ISO 22301 for managing documentation.

7. ISO 22301 clause 4.3 captures the requirements for defining the BCMS scope. When Auditing the scope would need to be reviewed to ensure the needs of third parties have been met and internal & external issues have been captured and taken into account (4.3.1.). The scope should also be aligned to the parts of the organisation identified as included along with the objectives, products & services provided / required. Exclusions should be clearly documented within the scope and should not affect the organisations responsibility & ability to operate & provide continuity to the business as defined / captured by the BIA and/or risk assessment (8.2.2, 8.2.3.). I would expect to see documented reviews as well as per clause 7.5.

8. ISO 22301 clause 5.2. provides examples of how top management should demonstrate its commitment to the BCMS, such as having a business continuity policy in place; ~~implementing~~ ensuring plans and objectives from the BCMS are implemented, and, for those who work with business continuity management, they have clearly defined roles & responsibilities, along with ~~these~~ necessary competences to deliver and maintain business continuity.

9. ISO 22301 clause 6.2. states that top management are responsible for ensuring the BC objectives are developed. This requires them to determine the resources required, assigning the responsibility of developing & maintaining the objectives and evaluation of their effectiveness. The suitability of the objectives would need to be aligned to the business continuity policy (5.3), be measurable, acknowledge & align to the acceptable minimum service & product levels and be updated as per 7.5. This would satisfy my requirement as an auditor.

10. ISO 22301 clause 7.3 requires all personnel working within the organisation's remit to have an understanding of their roles and responsibilities in contributing to effective BC management, the implications of non-conformance and what their role is if an incident was to occur. As per clause 5.2, top management are also to assign roles and responsibilities for management of the BCMS and 5.4, any other roles are assigned. As an Auditor I would refer to documented Terms of Reference (as per clause 7.5.) for inclusion of any BCMS roles and check they are reviewed & maintained. I would also use the interviewing method as per ISO 19011 Annex B.7.10 speak with personnel to ascertain their understanding.

11. ISO ~~22301~~ 22313 clause 7.5.1 provides a list of examples of documentation you would / could see as part of the BCMS, such as the BCP business continuity policy (5.3), BIA's and risk assessments (8.2) and BC objectives (6.2). As per ISO 22301 clause 7.5.3 documentation should be held in the organisation's records management system and should be controlled in line with their document management policy, including version control, access levels and restrictions.

12. ISO 22301 clause 8.2.2. provides ~~examples of~~ information relating to the BIA process which requires the organisation to document and establish the objectives, priorities and measurable outcomes / targets for an activity. I would expect to see the activities which support the designated service / products identified, the impact assessment if the activities were not performed, briefframes in prioritised order for resumption to an acceptable minimum level, accounting for the level which is unacceptable and any resources & dependencies required for the activity.

13. ISO 22301 clause 8.2.3. provides information on the risk assessment requirements of an organisation, which details the need for a process to be in place with formal documentation of the risk assessments undertaken. As an Auditor reviewing an organisation's Risk Assessment I would review the BCMS scope to confirm the internal & external issues, as well as third party needs, had been met and considered. I would check the risk acceptance criteria as defined by top management (clause 5.1). I would review the BC Policy (5.3) and BC objectives (6.2) to check alignment with the treatments identified.

14. ISO 22301 clause 8.3. covers the business continuity strategy process. When determining a BC Strategy a process which could be followed inline with ISO 22301 is to firstly use the BIA and Risk Assessment to address any findings, aligned to the BC objectives (6.2). From this the prioritised activities can be identified and protection measures established. Utilising the identification of any dependencies and/or products, identification for ways to continue or recover these as well as resumption, continuation or recovery of the priority activities. Lastly I would identify any mitigations and have measures / methods in place to deal with impacts. Resources would need to be determined to implement the strategy along with any other mitigating and protecting measures to prevent disruption.

15. ISO 22301 clause 8.4.4. covers the areas required to be covered in BC plans. Procedures within BC plans should be documented ~~by way of a~~ by utilising the BIA (8.2.2) ~~to~~ for identification of priority activities and the BC Strategy (8.3). The BC plan should include the scope & reason / purpose, have procedures documented for activation in ^{an event} ~~events~~ ~~for example~~ and have a comms plan. This should be stored, maintained and updated in line with clause 7.5. with the organisations record management system & policy.

16. ISO 22301 clause 8.4 provides information relating to business continuity procedures. An incident response structure is needed (clause 8.4.2) which helps the organisation to prepare, prevent/mitigate and respond to an incident. There should be procedures in place to warn personnel of an incident and communicate by way of for example an incident communication facility* so the BC and incident team can continue to manage the incident (clause 8.4.3). BC Plans (clause 8.4.4) should be in place to provide documented procedures & processes for responding to an incident and resuming activity once the incident ends.

17. ISO 22301 clause 8.4.2. discusses the incident response structure. It also provides examples of teams who might respond to a disruptive incident such as an incident management team, a welfare team and a communications team. In smaller organisations one team may cover the roles of the teams above mentioned.

18. ISO 22301 clause 7.4 covers communication requirements. As an Auditor I would check to see if an organisation had a comms plan in place. I would review the internal & external communications, utilising the requirement for documented processes to be in place as per 7.5. I would also review their exercises & tests (8.5) to check if their comms for use in a crisis or incident have been tested. I would check if interested parties had been communicated with when scoping the BCMS as per clause 4.2. I would also review the communication undertaken with the relevant parties as per the operation element of ISO 22301, for example engagement during the BIA & Risk Assessment process (8.2). and when establishing & implementing BC procedures (8.4) to ensure they are fit for purpose and meet the needs of those involved. Lastly I would confirm the BC Policy (5.3) has been communicated across the organisation.

19. ISO 22313 clause 8.5. ~~X~~, depicts that BC plans and procedures cannot be reliable unless they are tested & exercised. As an Auditor I would review the organisation's ~~Audit~~ ^{exercise} programme against 22313 clause 8.5.2 and ISO 22301 clause 8.5. As defined in 301 clause 8.5 the exercise programme should align with the BCMS scope (4.3) and ~~BC~~ objectives, clearly defined aims & objectives are documented for exercise / testing scenarios, disruption to operations is at a minimum and are formally documented in post-exercise reports which capture actions for improvements, outcomes and any further recommendations. The exercise programme must be conducted at planned intervals within the organisation & gradually increase in complexity and scale over time. I would expect to see all of this documented and maintained ~~being~~ managed in accordance with clause 7.5.

20. ISO ~~claus~~ 22301 clause 10.2 states continual improvement is required and 5.2 states top management should promote continual improvement. An Auditor could evaluate whether an organisation has demonstrated continual improvement or not by checking top management have promoted continual improvement (clause 5) by reviewing exercises & tests undertaken for attendance and any sign off on changes made in line with recommendations. I would check the BC actions for addressing risks and opportunities at clause 6.1 to ensure continual improvement was demonstrated when reviewing the effectiveness in the management of the risks & opportunities. I would also review in line with clause 9 an organisations performance & evaluation procedures to see continual development made when implementing any actions from an Audit, any amendments made to strengthen the measurement of performance and the management review of the BCMS for amendments / changes to ensure it is up to date and strengthened. All the documentation should meet the guidance in clause 7.5.



Embedding the culture and systems of organizational resilience

BCM 5000 ISO 22301 Lead Auditor Exam 2016

Answer Form

Your Name

Jodie Tappenden.

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) JODIE TAPPENDEN

Address: (where you want the certificate mailed) 15 BLAKE ROAD, GOSPORT, HAMPSHIRE, PO12 1PT

Company Name: MINISTRY OF DEFENCE

Email (work): jodie.tappenden536@mod.uk

Email (home): jodie.tappenden536@outlook.com

Date of Exam: 6 7TH APRIL 2017

Exam Location: ASHORNE HILL, COVENTRY, UK

Instructor Name: SCOTT CARVER