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

Matthew Hall.

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. A
11. A
12. C
13. F
14. B
15. B
16. A
17. ~~B~~ C
18. A
19. A
20. A
21. B
22. G
23. A
24. A
25. C
26. D
27. B
28. ~~A~~ G
29. ~~A~~ ~~C~~ A
30. C
31. C
32. A
33. A
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
Matthew Hall

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.

SEE ATTACHED SHEETS.
(8 PAGES)

MATTHEW HALL
07 APR 17
ASHORNEHILL, COVENTRY, UK

① 19011/7.2.3 identifies some of the key competencies for auditors. These include but are not limited to;

(a) Organisational understanding – enables auditor to understand the structure, culture, functions and relationships of the organisation.

(b) Knowledge of audit principals – individual must be able to apply the the best/appropriate methods in order to produce a detailed audit report

(c) Technical knowledge – up-to-date knowledge of key legal and regulatory standards is critical to ~~ensure~~ assess whether the ~~auditor~~ organisation is meeting ~~the~~ its legal requirements and meeting best practice.

② 19011/5.1 provides guidance of the key elements of an audit plan. These include, but are not limited to;

(a) ~~Ad~~ Audit Objectives – these define what is to be examined, any exclusions and the aim of the report without an objective the auditor is unable to produce a report.

(b) Selection of audit method – this should be appropriate to the organisation and chosen to ensure the best data is obtained. This will ensure an accurate report.

(c) Selection of team members – This should be in accordance with 19011/7.2.3 to ensure the correct level of knowledge + expertise. This will enhance the validity of the report.

MATTHEW HALL
07 APR 17
ASHORNE HILL,
COVENTRY, UK

4 19011/B.3 outlines 2 methods of sampling;

(a) Judgement based sampling (19011/B.3.2) - relies on the expertise of the audit team. It relies on the auditors knowledge to examine, analyse and report on the best form of data. This can be previous audits, changes in technology/legal requirements etc. It allows for flexibility in choosing the best data set.

(b) Statistical sampling (19011/B.3.3) - based on audit objectives and uses a sample selection from the organisation. ~~May work well with~~ Effectiveness is dependant on the size of the organisation, number of auditors, audit frequency etc.

3 19011/5.4.3 provides guidance on selection of audit method. 19011/Annex B identifies a number of methods;

(a) Contact - this involves interviewing employee's (either remotely or on site). Interviews can determine levels of training, competance and understanding of BCMS.

(b) Non-contact - this can involve documentation reviews to ensure the organisation is conforming to its own policy (as per 22301/5.3). It can provides documentary evidence of long term commitment, review and improvements

MATTHEW HALL
07 APR 17
ASHORNE HILL
COVENTRY, UK

(5) 22301/4.2 requires an organisation to understand the needs of interested parties and these should be documented (as per 22301/7.5). Interested parties could include

(a) Owners of business continuity procedures - they need to understand and have reviewed BIA's in order to ensure RTO's are met.

(b) Suppliers - would want to know the requirements/expectations of organisation and also inform them of their own BC procedures.

Those involved should range from Top Management to Line Management from accross the organisation and interested parties.

(6) 22301/4.2.2 requires the organisation have in place processes to understand, review and record (in line with 22301/5.3 and 22301/7.5) the relevant legal and regulatory requirements. Evidence that this is up-to-date and exhausite should be documented and available as per 22301/7.5.

(7) 22301/4.3 requires the organisation to set the scope with due reference to 22301/4.1 in detailing the issues (internal & external) that affects it ability to apply the BC policy (as per 22301/5.3) and also 22301/4.2 by understanding the needs and requirements of affected parties (as outlined in 22313/4.2.1 figure 4).

MATTHEW HALL
07 APR 17
ASHORNEHILL, COVENTRY, UK

(8) 22301/5 provide guidance to top management on its role within the BCMS. There are a number of ways this can be achieved;

(a) ensure that policies and objectives are clearly defined (as per 22301/5.3)

(b) ensure that adequate resources are allocated to implementing the BCMS Policy

(c) promote improvement to BCMS through planned exercising and testing.

(9) 22301/6.2 requires that top management ensure BC objectives are set, however this may be delegated in line with 22301/5.2 provided it's documented. This does not abrogate the need for top management to ensure they review and approve the BC objectives. The suitability of the BC objective would be assessed against the BC Policy (22301/5.3) ~~(10)~~ and the needs and requirements of the organisation and interested parties (22301/4.1 and 4.2) and legal/regulatory requirements 22301/4.2.2).

(10) There are ~~two~~ a number of methods available;

(a) 19011/6.2 – document review to ensure roles + responsibilities (as per 22301/5.4) are defined and recorded (as per 22301/7.5).

(b) 19011/6.7 – interviews with employees to ~~ensure~~ establish that they are aware of, and understand their roles + responsibilities

(c) 22301/8.5 – testing and exercising is regularly conducted to ensure competency (as set in 22301/7.2).

MATTHEW HALL.
07 APR 17
ASHORNE HILL, COVENTRY, UK.

(11) Examples of BCMS Documents include;

(a) 22301/5.3 BC Policy
(b) 22301/~~5~~.4. Organisational roles and responsibilities
(c) 22301/7.2 competancy levels for those with defined roles and responsibilities.

22301/7.5 provides guidance on how these can be stored e.g hard i.e printed paper or soft i.e electronic. 22301/7.5.3 provides guidance on how document should be controlled and requires organisations to have in place procedures & processes to enable correct appropriate access, change control, reintention and destruction amongst others 22313/7.5 provides guidance in more detail.

(12) In establishing activity priority & service levels i.e RTO the organisation should be able to demonstrate links/reference to Business Impact Analysis (22301/8.2.2) and risk assessment (22301/8.2.3). The BIA & RA should align with BC Objectives as set out in the BC Policy (22301/5.3)

(13) The auditor should be able to identify a clear link ~~or at least refer~~ between the RA (22301/8.2.3) and the BC Policy (22301/5.3). Further evidence would be how/whether the Incident Response Structure (22301/8.4.2) is able to deliver/met/manage the stated BC objectives in the RA. Additionally the documented Risk Appetite will provide further evidence of conformity to 22301.

MATTHEW HALL.
07 APR 17
ASHORNEHILL, COVENTRY,
UK.

(14) ~~I~~ 22301/8.3.1 requires an organisation to be able to demonstrate that it has determined and selected a strategy based on the product of the BIA (as per 22301/8.2.2) and Risk Assessment (22301/8.2.3). The strategy should also identify the resource requirements (as considered with reference to 22301/8.3.2.a-h). For any residual risk the organisation should demonstrate adherance to 22301/8.3.3.

(15) 22313/6.2 outlines the content of BC Plans and links in to 22313/8.
Key elements include

(a) ~~op planning~~ 22313/8.1.a - Op Planning + control
(b) 22313/8.1.b - BIA + RA
(c) 22313/8.1.c - Business continuity strategy
(d) 22313/8.1.d - BC Plans
(e) 22313/8.1.e - Testing + Exercising.

All the above should be documented in line 22310/7.5 and reviewed in line with 22301/9.3

(16) 22301/8.4 sets out the BC procedures an organisation should follow / be able to demonstrate in the event of an incident;

(a) 22301/8.4.2 - Incident Response structure - The organisation should have in place procedures & a structure that can respond with trained personnel who authority to make decisions.

(b) 22301/8.4.3 Warning & communication - organisation shall be able to detect, monitor receive and respond to information & support / inform interested parties.

(c) 22301/8.4.4 BC Plans - organisation shall have in place established documented response procedures.

(17) 22313/8.4.2 provides guidance of the types of team an organisation may wish to use during an incident. Examples are below but are not limited to;

(a) 22313/8.4.4.3.1 Incident Management Team
(b) 22313/8.4.4.3.2 Communications Team
(c) 22313/8.4.5. Recovery Team

(18) 22301/8.4.3 ~~provides~~ requires an organisation to have established implemented and maintained procedures to be followed during an incident. These should be documented within the BC Plan. The requirement to test & exercise (22301/8.5) will establish whether these are fit for purpose and Top Management review (22301/9.3) will ensure ~~the~~ any changes are approved in line with the BC Policy (22301/5.3)

MATTHEW HALL
07 APR 17
ASHORNE HILL, COVENTRY,
UK.

(19) 22301/8.5 provides guidance to the auditor on the effectiveness of the exercise program. The organisation should be able to demonstrate.

(a) Test & objectives match BCMS scope & objectives (22301/8.5.a)
(b) Are conducted at planned intervals (22301/8.5.g)
(c) Are based on relevant & appropriate Scenarios (22301/8.5.b)
(d) Production of Post-Exercise Reports (22301/8.5.e)
(e) Reports are reviewed by Top Management (22301/8.5.f and 22301/9.3)

(20) 22303/10.2 requires an organisation to be able to demonstrate continual improvement. Evidence includes, but is not limited to;

(a) Continually renewed and updated BCMS documents
(b) Implementation of exercise recommendations.
(c) conduct of internal audits.

All the above should be conducted over a period of time (ideally no more than 3yrs) and be documented in line with 22301/7.5.

BCM 5000 ISO 22301 Lead Auditor Exam 2016
Answer Form
Your Name
Matthew Hall

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) Matthew Hall

Address: (where you want the certificate mailed) 34 Osborne Road, Warsash Southampton, Hants, SO31 9GG

Company Name: West Sussex County Hall

Email (work): Matthew.Hall@westsussex.gov.uk

Email (home):

Date of Exam: 07 APRIL 2017 Exam Location: ASHORNE HILL, COVENTRY, UK

Instructor Name: SCOTT CARVER