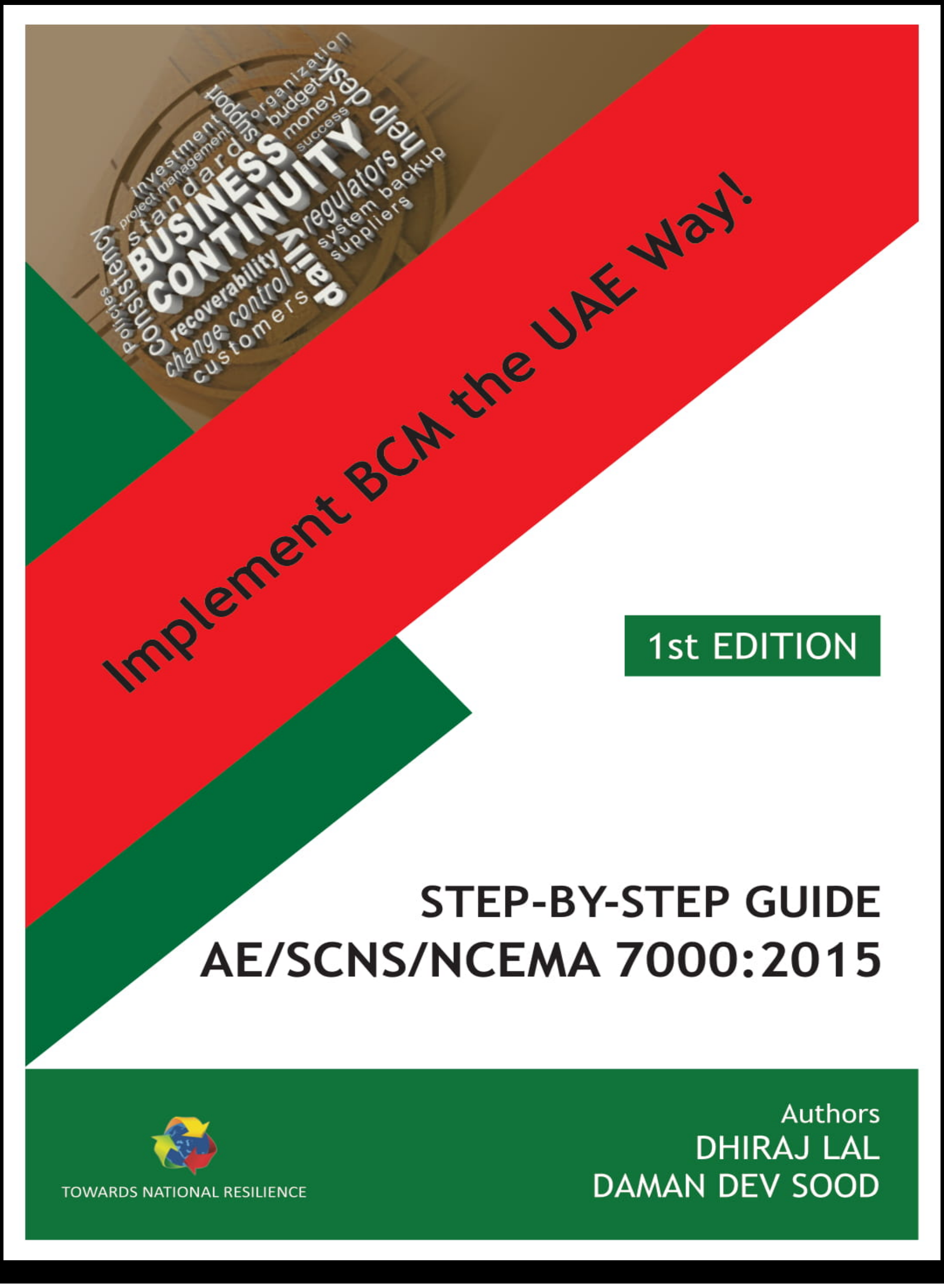


Implement BCM the UAE Way!

1st EDITION

STEP-BY-STEP GUIDE
AE/SCNS/NCEMA 7000:2015

TOWARDS NATIONAL RESILIENCE

Authors
DHIRAJ LAL
DAMAN DEV SOOD

*An extract from the Risk Assessment Chapter*

*Clause 8.2 of the NCEMA 7000:2015*

Read the "Step by Step guide to the NCEMA 7000" on the free kindle App or on your Kindle Reader. Available for purchase on the kindle store https://www.amazon.com/dp/B0846QZP7G

# Typical contents of each chapter in the book

## Additional information

# Sample contents from the Risk Assessment Chapter

## Overview

Clause 8.2 of the NCEMA 7000 document states that the organization shall establish, implement and maintain a methodology for risk assessment to identify, analyze and evaluate the risks which may disrupt continuity of activities. The organization shall:

- Identify and approve risk parameters and must be pre-approved by the top management.
- Identify the risks that can disrupt the performance of prioritized activities.
- Analyze the risks against predefined evaluation criteria.
- Evaluate the impact of the addressed risk.
- Take into account interdependencies related to the performance of prioritized activities.

## Explanation

The NCEMA 7000 BCM standard defines risk as “the impact of uncertainties on organizational goals.” The fact is that often certain factors may arise, which give rise to business disruptions, thus preventing the organization from continuing to deliver its key products and services. These uncertainties make it more difficult for the organization to meet its goals and business objectives.

The standard defines Business Continuity Risk Assessment as “the process in which risk is identified, analyzed and evaluated.” Therefore, Risk Assessment seeks to help organizations to equip themselves to manage risks.

## Objectives

In order to implement a robust business continuity program, it is critical to have a good understanding of any risks that may prevent the organization from achieving its goals. The organization should be able to manage those risks, so as to decrease any negative impact that they could have on the organization’s ability to meet its goals.

Ideally a BCM Risk Assessment seeks to:

- Prevent business disruptions from occurring.
- If indeed any disruption occurs, to quickly bring it under control, before it gets out of hand.
- Try to make sure that the disruption does not occur for long; at most, for just a short time.

Through a well-conducted BCM Risk Assessment, you would have prior warning of the possibility of things that may go wrong. This would give you an advantage to bring such situations under control, if they did occur. You would get time to think through the situation well in advance, evaluate many possible courses of action, choose your preferred actions, and then implement any agreed controls and solutions.

Let us take an example. If an organization knows that its office is in a low-lying area where water can collect and the area can be flooded, it can put in place advance planning to prevent any disruption that the flooding might cause. The organization may consider moving to a region with higher elevation, or to a higher floor in the same building. It may choose to install emergency power facilities in upper floors and not in the basement. It may choose to put in place the needed infrastructure to quickly pump out water in case of flooding. It could also set up advance notification protocols with the weather bureau so that they could get advance notice of disruptive weather situations like heavy rainfall. It may put in place arrangements so that staff can work out of other distant offices on days when there is likely to be heavy rainfall. All in all, with advance knowledge, planning and testing, an organization would be able to do many things to be able to deliver its products and services even in times of disruptive situations.

If the Risk Assessment activity is effective, then the entire cost and effort of activating Business Continuity can be avoided - which could be a huge saving of time, effort and resources.

But what makes the BCM Risk Assessment different from a traditional Risk Assessment that many organizations may already have been conducting for many years? This is a new question that BCM professionals love to ask, which is: “What if?” For example: What if our supplier did not deliver us the required raw materials? Would we still be able to produce our product and meet the delivery timelines we have promised to our customer? What if the telecom cable got cut? How would we communicate with the external world? And other such “What if” questions.

By asking this question, competent and inquisitive BCM professionals even in the most mature and professional organizations are often able to add huge value during the BCM Program implementation. They do this by highlighting risks that no one in the past had raised or addressed. For example, many professionals may feel relaxed once a control was put in place for a possible vulnerability. But the BCM professional may be worried and ask what is the backup plan if the control failed? The organization may realize then that there is no plan B, which gives rise to a new vulnerability, which also needs to be addressed, for the organization to be adequately protected.

So the prime objective of a BCM Risk Assessment is to protect the organization from the cost and effort of managing disruptions that can damage the organization ability to continue. Yet, Risk Assessment could also help increase the trust, faith and loyalty of your customers, who may now see the organization as forward-looking, proactive, and professionally managed. In addition, the BCM risk assessment activity can also help identify opportunities that can help enhance the organization’s productivity, efficiency, revenues and market share. This is because the Risk Assessment activity often identifies steps, procedures and controls where resources, money and effort are being spent, but it is leading to no tangible benefit. Those resources can be re-deployed to other opportunities where they can yield more benefits. By communicating the benefits of smart Risk Management solutions implemented, other departments can learn also, and the whole organization gains.

## Deliverables

The key deliverables from this activity are the:

- Risk Assessment Methodology Document
- Risk Assessment Report

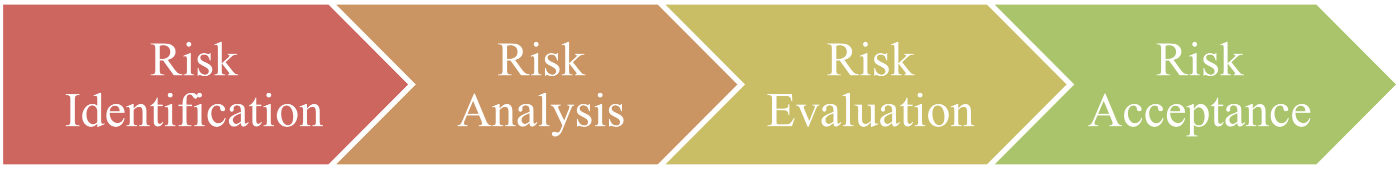
These are part of the 17 required documents as mentioned in the NCEMA 7000 standard.

The Risk Assessment Report would typically include:

1. Summary of the Risk Assessment activities conducted
2. Prioritized Risks, in order of potential disruption impact
3. Possible mitigants and controls

## Methodology and Tips

The Risk Assessment Process comprises 4 steps as clearly mentioned in the NCEMA Standard. These are:



Risk Identification

Risk Analysis

Risk Evaluation

Risk Acceptance

**Risk Identification:** As per the NCEMA Guidelines document, the following sources of risk shall be considered:

- Unavailability of staff
- Destructive loss of all or part of a building
- Major physical utilities (power, water, etc.)
- Loss of ICT functions (data center, servers, etc.)
- Unavailability of information
- National / international crisis or disaster
- Financial shortcomings
- Unavailability of transportation
- Any issues or problems with business partners and/or suppliers.

Ideally, the anything and everything that can cause a business disruption in delivery of the organization's prioritized activities should be considered in the Risk Assessment, as signed off in the BIA. Ideally the Risk Identification exercise should be extremely comprehensive and exhaustive. All the 3 techniques of conducting a BIA could be utilized also for a Risk Assessment – questionnaire, one to one interviews and workshops.

**Risk Analysis:** Once a list of risks has been put together through a comprehensive Risk Identification exercise, the need now is to analyse those risks in terms of their ability and impact to disrupt the organization from meeting its business objectives. For this, it is useful to put in place Risk Analysis Scales. A good way to do this is by categorizing all risks in terms of the following 2 elements:

- Likelihood/ Probability – how likely are the identified risks to occur?
- Impact – how big is the impact of the risk occurring to organization's business and to the objectives?

Table 1 (from the NCEMA 7000 document) shows an example of possible Impact scales used for Risk Analysis.

Table 1: Example of Impact Scale

| Impact Scale | | | | |
|---|---|---|---|---|
| Very High | High | Medium | Low | Very Low |
| 5 | 4 | 3 | 2 | 1 |
| The impact of this risk is very high. Its occurrence would be extremely negative for the organization, up to a total disaster | The impact of this risk is high. There are major disturbances or disruptions coming from coming from this risk | The impact of this risk is medium. It has some negative effect, but the overall damage is limited | The impact of this risk occurring is low. There is only a minor effect on the organization | The impact of this risk occurring is very low. There is no or negligible impact on the organization |

The second part of the risk analysis is the determination of the risk likelihood. For the risk assessment methodology, a quantitative approach may not often work, due to insufficient information available. Hence, we might sometimes need to use a qualitative (relative) scale. To identify an appropriate likelihood for a risk, it may be needed to consider objective information from records of past events. In the absence of this, interviews with stakeholders and employees can also be used to get a first impression. Table 2 (from the NCEMA 7000 document) as given below is an example of the way likelihood of each risk can be estimated using this scale.

Table 2: Example of Likelihood Scale

| Likelihood Scale | | | | |
|---|---|---|---|---|
| Very Unlikely | Unlikely | Possible | Likely | Almost Certain |
| 1 | 2 | 3 | 4 | 5 |
| Less than 1 in 5 years | Less than 1 per year | Once or twice per year | Between 3 and 5 per year | At least 5 per year |
| Extremely unlikely events, not expected to happen | Unlikely, but there's a slight possibility that it may occur at some time | The event might occur at some time. For example, there may be a history of casual occurrence in the organization | There is a strong possibility of the event to occur. There may be a history of frequent occurrence in the organization | The event is high likely and expected to occur. There is a history of regular occurrence in the organization |

**Risk Evaluation:** The results of risk analysis (also referred to as Risk Values) shall be compared with predefined risk criteria set by the organization to determine whether a risk is acceptable or needs risk treatment. The basis of the comparison is the risk calculation and the level of acceptable risk. Table 3 from the NCEMA 7000 document demonstrates a method to assess the overall risk criticality.

Table 3: Example of Risk Matrix

| | | | Risk Matrix | | | | |
|---|---|---|---|---|---|---|---|
| **Risk** | Impact | Very High | 🟨 | 🟧 | 🟧 | 🟥 | 🟥 |
| | | High | 🟩 | 🟨 | 🟧 | 🟥 | 🟥 |
| | | Medium | 🟩 | 🟨 | 🟧 | 🟧 | 🟧 |
| | | Low | | 🟩 | 🟨 | 🟨 | 🟧 |
| | | Very Low | | | 🟩 | 🟩 | 🟨 |
| | | | Very Unlikely | Unlikely | Possible | Likely | Almost Certain |
| | | | Likelihood | | | | |

**Value:** Once impact and likelihood has been calculated, they need to be interpreted. In the sample table shown below, the maximum risk value is 25 (5 by 5). Possible actions are also indicated below, on a sample basis.

Table 4: Risk Interpretation

| Risk Value | | | | |
|---|---|---|---|---|
| Very Low | Low | Medium | High | Very High |
| 1-2 | 🟩 3-4 | 🟨 5-8 | 🟧 9-15 | 🟥 16-25 |
| No action required | No action required | No action may be required on some risks, but others may need to be treated. Decisions to be taken case by case | These risks could have a high impact on the organization, and definitely need to be treated | These risks could have a very high or catastrophic impact on the organization. These risks definitely need to be treated |

**Risk Acceptance Criteria:** In accordance with above, risks of high and very high level should always be considered for risk treatment, but can be accepted if one or more of the following criteria apply:

- The cost of risk treatment outweighs the impact of the risk occurring.
- The actions for risk treatment are not practical within the organization business, work environment or culture.
- There are no legal implications when this risk is accepted.
- There are only tolerable impacts on organization's business objectives.

For a comprehensive Risk Assessment, all possible sources of risks information should be considered, such as personal knowledge of experts, brainstorming sessions, existing Risk Register of the organization, Horizon Scanning Reports, etc. As an example, per the results of the Middle East BCM Survey conducted by CORE, the top 3 causes of disruptions were applications failure and network infrastructure failure (46% response), power outage (42% response) and human error (25% response)." This information should be considered by the team that is performing the Risk Assessment, which should then make their own judgement on the validity and relevance of this data to their own organization.

Post the Risk Assessment exercise, the team typically documents the findings in a report to Top Management. Proposed solutions are identified and suggested.

**END OF CHAPTER SAMPLE**

**Continuity & Resilience (CORE) provides**:

1. Consulting /Implementation – Save money by inviting our experienced consultants to implement for you.
2. Training – high quality instructor led training for all levels of your entire organisation, including senior management. Also, for individual professionals who want to get ahead. Provided online and in classroom (as permitted).
3. Finalise your BCP in 7 days – Typically for SMEs, vendors and small/medium corporates. Implement Basic readiness to meet minimum regulatory and customer expectations.
4. Mandatory annual audits - Annual internal audits as an independent control to meet compliance, regulatory and certification requirements.
5. Temporary and permanent staffing – hire our competent staff to implement your urgent projects.
6. BCM Automation – "Peace of Mind" efficiency tools for a world-class Business Continuity Management System.
7. Emergency Rapid Notification tools – Pass on critical communications in minutes to all your employees, customers, partners and key stakeholders.
8. Workplace Services – Flexibly operate from any close-by secure location which can change based on your requirements.
9. Awareness eLearning – State-of-the-art interactive 1-hour awareness module on BCM, including pandemic. Effective and intensive learning for your entire workforce, vendors and partners.
10. Learn more for less – Low cost Video-based learning for students and professionals.

**www.coreconsulting.ae**
**www.coreonline-certifications.com**

## *Step by Step Guide to NCEMA 7000 – Table of Annexures*

The following table shows all the annexures present in the book "Step by Step Guide to NCEMA 7000" to enhance readers' understanding of its chapters.

## ABOUT THE AUTHORS

**DAMAN DEV SOOD**
**CHIEF OPERATING OFFICER, CONTINUITY & RESILIENCE (CORE)**
**FBCS, AFBCI, CBCI, SMIEEE, MAIMA, ISO 22301 LA & Expert, IEEE Ambassador**

A former BCI Merit Award (Global) Winner and Business Continuity Manager of the Year in BCI's C&R Awards. Daman is a BCI approved Instructor from 2012 and he also serves as a member of BCI's speakers Bureau. He teaches and consults in BCM (ISO 22301/ NCEMA 7000) and related domains. He has served clients across the Govt sector, Energy, Oil and Gas, Infrastructure, IT, Banking, Finance, Insurance, Retail, Manufacturing, Automobile, Pharma, etc.

**DHIRAJ LAL**
**EXECUTIVE DIRECTOR, CONTINUITY & RESILIENCE (CORE)**
**MBCI, CBCP, CBCI, ISO 22301 Technical Expert, CISA, ITIL, ISO 31000, ISO 27001 Lead Auditor**

A former BCM Head and Sponsor, Dhiraj Lal is Asia's first BSI appointed BCM Technical Expert for BS25999/ ISO 22301 and has assessed 2 of the top 10 certified organizations globally. A Chemical Engineer with understanding of Oil & Gas and process industries, he has been consulting and teaching in BCM (ISO 22301/ NCEMA 7000) for over 20 years now.