

BECOMING RESILIENT

THE DEFINITIVE GUIDE TO
ISO 22301 IMPLEMENTATION



THE PLAIN ENGLISH, STEP-BY-STEP HANDBOOK
FOR BUSINESS CONTINUITY PRACTITIONERS

DEJAN KOSUTIC

Dejan Kosutic

Becoming Resilient:

The Definitive Guide to ISO 22301 Implementation

*The plain English, step-by-step handbook for business
continuity practitioners*

EPPS Services Ltd
Zagreb, Croatia

Copyright ©2013 by Dejan Kosutic

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the author, except for the inclusion of brief quotations in a review.

Limit of Liability / Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. This book does not contain all information available on the subject. This book has not been created to be specific to any individual's or organization's situation or needs. You should consult with a professional where appropriate. The author and publisher shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

First published by EPPS Services Ltd
Nazorova 59
10000 Zagreb
Croatia
European Union
<http://www.27001academy.com/>

ISBN: 978-953-57452-3-5 (eBook)

ISBN: 978-953-57452-4-2 (printed book)

First Edition, 2013

CONTENTS

LIST OF FIGURES	9
PREFACE	10
1. INTRODUCTION	11
1.1 WHY BUSINESS CONTINUITY?.....	11
1.2 WHY IS PLANNING IMPORTANT?	12
1.3 WHAT BUSINESS CONTINUITY IS NOT.....	13
1.4 ISO 22301 PUTS IT ALL TOGETHER	15
1.5 WHO SHOULD READ THIS BOOK?.....	16
1.6 HOW TO READ THIS BOOK.....	17
1.7 WHAT THIS BOOK IS NOT	18
2. A FIRST GLANCE AT ISO 22301	20
2.1 INTERNATIONAL REACH.....	20
2.2 TERMINOLOGY	21
2.3 WHERE DOES BUSINESS CONTINUITY BELONG?	24
2.4 SHORT HISTORY OF BUSINESS CONTINUITY STANDARDS AND FRAMEWORKS	25
2.5 ISO 22301 AND ISO 22313.....	27
2.6 HOW IS ISO 22301 STRUCTURED?	28
2.7 WHICH ORGANIZATIONS CAN IMPLEMENT THIS STANDARD	31
2.8 HOW TO LEARN MORE ABOUT THE STANDARD	32
3. GETTING THE BUY-IN FROM YOUR MANAGEMENT (AND OTHERS)	35
3.1 IT'S ALL ABOUT BENEFITS	36
3.2 HOW TO PRESENT THE BENEFITS TO YOUR TOP MANAGEMENT	38
3.3 RETURN ON INVESTMENT (ROI)	40
3.4 DEALING WITH LINE MANAGERS AND OTHER EMPLOYEES	42
3.5 DEALING WITH CUSTOMERS	43
3.6 DEALING WITH SKEPTICS.....	45
3.7 BRIDGING THE GAP BETWEEN IT AND THE BUSINESS.....	46
4. GETTING READY FOR YOUR PROJECT	48
4.1 IMPLEMENTATION OPTIONS	49
4.2 PROJECT MANAGER, PROJECT MANAGEMENT TEAM AND THE SPONSOR.....	50
4.3 HOW TO CHOOSE A CONSULTANT.....	52
4.4 STEPS IN ISO 22301 IMPLEMENTATION & PDCA CYCLE.....	54
4.5 INTEGRATING WITH ISO 27001 AND/OR ISO 9001.....	55
4.6 HOW LONG DOES IT TAKE?	58
4.7 USING TOOLS AND TEMPLATES	59
4.8 HOW DETAILED THE DOCUMENTATION SHOULD BE.....	60
4.9 BUDGETING BUSINESS CONTINUITY	61

5.	SETTING UP THE FRAMEWORK FOR MANAGING BUSINESS CONTINUITY.....	65
5.1	UNDERSTAND WHAT YOUR ORGANIZATION DOES (CLAUSE 4.1).....	66
5.2	PROCEDURE FOR DOCUMENT CONTROL (CLAUSE 7.5).....	67
5.3	IDENTIFYING INTERESTED PARTIES AND THEIR REQUIREMENTS (CLAUSE 4.2)	70
5.4	SETTING THE SCOPE OF YOUR BCMS (CLAUSE 4.3)	72
5.5	WRITING THE BUSINESS CONTINUITY POLICY (CLAUSE 5.3).....	75
5.6	SETTING THE BCMS OBJECTIVES (CLAUSE 6.2).....	78
5.7	AWARENESS & TRAINING (CLAUSES 7.2 AND 7.3).....	81
6.	IMPLEMENTING THE CORE BUSINESS CONTINUITY ELEMENTS	86
6.1	HOW TO DEFINE THE ACTIVITIES/UNITS	87
6.2	DEVELOPING THE RISK MANAGEMENT METHODOLOGY (CLAUSES 8.2.1 AND 8.2.3).....	92
6.3	PERFORMING RISK ASSESSMENT (CLAUSES 6.1 AND 8.2.3).....	98
6.4	PERFORMING RISK TREATMENT/MITIGATION (CLAUSES 6.1 AND 8.3.3).....	103
6.5	DEVELOPING THE BUSINESS IMPACT ANALYSIS METHODOLOGY (CLAUSES 8.2.1 AND 8.2.2)	108
6.6	PERFORMING THE BUSINESS IMPACT ANALYSIS (CLAUSE 8.2.2).....	116
6.7	DEVELOPING THE BUSINESS CONTINUITY STRATEGY (CLAUSE 8.3).....	124
6.8	DISRUPTION SCENARIOS (CLAUSE 8.5).....	134
6.9	BUSINESS CONTINUITY PLAN (CLAUSE 8.4).....	138
6.10	CRISIS MANAGEMENT AND COMMUNICATION (CLAUSES 7.4 AND 8.4.3)	145
6.11	INCIDENT RESPONSE PLAN (CLAUSE 8.4.2).....	152
6.12	RECOVERY PLANS (CLAUSE 8.4.4)	158
6.13	SPECIFICS FOR DISASTER RECOVERY PLANS (CLAUSE 8.4.4).....	166
6.14	RESTORATION PLAN (CLAUSE 8.4.5).....	169
7.	MAKING SURE EVERYTHING WILL WORK	172
7.1	EXERCISING AND TESTING (CLAUSE 8.5).....	173
7.2	MAINTENANCE OF THE PLANS (CLAUSE 9.1.2).....	177
7.3	POST-INCIDENT REVIEW (CLAUSE 9.1.2)	179
7.4	MONITORING AND MEASUREMENT (CLAUSE 9.1.1).....	182
7.5	INTERNAL AUDIT (CLAUSE 9.2).....	185
7.6	MANAGEMENT REVIEW (CLAUSE 9.3).....	189
7.7	CORRECTIVE ACTIONS AND IMPROVEMENTS (CLAUSE 10).....	191
8.	GETTING READY FOR THE CERTIFICATION	195
8.1	SHOULD YOU GO FOR THE CERTIFICATION IN THE FIRST PLACE?	195
8.2	HOW TO PERFORM THE FINAL CHECK	197
8.3	CHOOSING THE CERTIFICATION BODY.....	199
8.4	STAGES IN THE CERTIFICATION AND HOW TO PREPARE	201
8.5	HUMAN PERSPECTIVE OF THE CERTIFICATION AUDIT	204
8.6	ARGUING WITH A CERTIFICATION AUDITOR	206
8.7	DEALING WITH MAJOR NONCONFORMITIES	208

9. AT THE END.....	209
APPENDIX A – DIAGRAM OF ISO 22301 IMPLEMENTATION PROCESS.....	210
APPENDIX B – CHECKLIST OF ISO 22301 MANDATORY DOCUMENTATION.....	212
APPENDIX C – ISO 22301 VS. BS 25999-2: AN INFOGRAPHIC	224
APPENDIX D – LIST OF RELATED BUSINESS CONTINUITY STANDARDS AND FRAMEWORKS	229
APPENDIX E – NFPA 1600 VS. ISO 22301.....	231
GLOSSARY.....	236
BIBLIOGRAPHY	240
INDEX	242
RESOURCES.....	247

LIST OF FIGURES

Figure 1: Relationship between business continuity and information security	24
Figure 2: Words to avoid and words to use when presenting business continuity.....	40
Figure 3: Overlapping of documentation between ISO 22301, ISO 27001 and ISO 900156	
Figure 4: Overlapping of processes between ISO 22301, ISO 27001 and ISO 9001	57
Figure 5: Relationship between core business continuity elements.....	86
Figure 6: Steps in risk management	92
Figure 7: Example of risk assessment table.....	103
Figure 8: Example of risk treatment table	107
Figure 9: Example of BIA Questionnaire – determining the Maximum Acceptable Outage.....	122
Figure 10: Example of BIA Questionnaire – determining the Maximum Data Loss/RPO	123
Figure 11: Example of determining the RTO based on activity dependencies.....	132
Figure 12: Example of a disruption scenario	137
Figure 13: Timeline of incident response, recovery, restoration and crisis management.	139
Figure 14: High-level structure of Business continuity plan	143
Figure 15: Elements that are to be included in the Business continuity plan, Incident response plan, recovery plans, and restoration plans	144
Figure 16: Example of a communication responsibilities matrix.....	152
Figure 17: Example of an Incident response procedure for a bomb threat.....	158
Figure 18: Structure of recovery plans – main recovery steps to be included.....	164
Figure 19: Example of a Maintenance and review plan.....	178

PREFACE

Why did I write this book? It is true that there are other books and tutorials on ISO 22301, but the more I communicate with both beginners and experienced business continuity practitioners, the more I found it necessary to write a book that has a lot of practical examples and is written in easy-to-read language, avoiding all those hard-to-understand phrases.

What you'll find in *Becoming Resilient* is a summary of requirements and best practices, not only from ISO 22301, but also from at least a dozen other business continuity and information security standards and frameworks.

But what I think you'll like the most about this book is that I give practical answers to real-life situations when implementing business continuity. These bits of advice came not only from reading the standards, but primarily from my interaction with many people engaged in building resilience in their companies – I was lucky enough to be in a position to deliver many in-person courses and online webinars, answer thousands of questions through forums, deliver many consulting jobs, and speak at a number of conferences.

Therefore, you could consider this book to be a comprehensive summary of all the concepts, advice, examples, questions and answers, fitted into the framework of ISO 22301.

1

INTRODUCTION

1.1 Why business continuity?

Meet Jack. Since his early childhood, Jack has spent most of his free time on computers; he dreamed of becoming a programmer once he grew up. His dream came true – during his last year in university he came up with an idea for a groundbreaking software that will help banks serve their clients better. After graduating, he borrowed some money, invited two of his friends to work for him, and started developing the business. After one year he became profitable, and after three years he already had 25% of the market share and a nice team of 10 people.

Only a couple of days after he made a big investment into new equipment and development tools, he came one morning to his office, only to find the door smashed – since they were the only company in the building, the thieves had enough time to take all the valuables from the office, including computers. All this wouldn't be so bad if they had a backup; they surely did make the backup, but because of the banking regulations they couldn't store their backup in the cloud, so they backed up all the data on disks which they archived next to the servers – these disks were also stolen.

He went bankrupt – all the code they were developing for years was lost, as well as all the client data. Since he asked his parents to pledge their property as collateral for his bank loan, they were forced to sell their family house. Jack was never able to get into business again.

Moral: it doesn't take a tsunami to destroy your business, let alone hackers – it can be a much more prosaic reason like described above. But most of all, it is the "It is not going to happen to me" syndrome that kills companies and destroys lives.

1.2 Why is planning important?

Meet Pamela. She was more prudent than Jack, and made sure her marketing company kept her backup in two different locations. Not only that, her company went a step further and developed a mini disaster recovery site where they installed all the spare servers that could be used in case their main servers (i.e. primary location) became unavailable.

On a nice sunny day a fire broke out, spreading so rapidly so that it wasn't possible to save any of the computers or the documentation. Pamela was thinking rapidly – "Luckily, no one was hurt, and we do have everything we need at a disaster recovery location." So she ordered everyone to go to this secondary location; but there, chaos ensued. Everyone started to panic, and no one knew what to do or what to start with: IT guys were not sure which system they should recover first; key account managers didn't know which clients to call and what to tell them; office administrators

knew that part of the paper documentation was missing, but weren't sure how to recover it. No one knew how quickly they needed to respond to their customers. As if that wasn't enough, they couldn't recover one of the servers because it turned out that the only person who knew the root password to that server happened to be on a vacation in South America, unreachable by cell phone.

The result: Pamela's company managed to recover their operations, but it took a full week. By then, 80% of their clients had left them.

Moral: technology is an important element of business continuity, but certainly not sufficient; something else needs to exist: knowledge of the business needs, a clear course of action on what needs to be done, and people who know how to react.

If I may use a military parallel here, business continuity is for a company what an army is for a country – it may cost a lot, not many people see its purpose, it takes a lot of training to maintain it, it is (hopefully) used very rarely, but when it is used it saves the country.

1.3 What business continuity is not

There are many myths about business continuity management, and without clearing up these fallacies it would be very difficult to understand what business continuity is all about:

Business continuity is a job for IT guys. Very often the perception of business continuity is that it is enough to make a

backup, a few plans on how to restore your main servers, and – if you’re a bit more ambitious – to build an alternative data center at a remote location. This normally is called *disaster recovery*, and while all that is quite often necessary (and should be a part of business continuity management), it is by no means enough. In case of a disruption you need not only your information systems operational, but also your people to work with these machines. After all, people are the ones who make things happen, not the computers – otherwise, your company would already consist only of computers, with no human beings employed.

Business continuity equals business continuity plans. “It is enough to write detailed plans, and this is how you will be able to counteract all the tsunamis, hurricanes, thefts and hackers.” Really? And how would you know which of your systems, and which of your processes you should recover firsts? And how quickly do you need to recover certain processes or systems? (Your plan will differ very much if you have to recover within four hours as opposed to four days.) Where would you continue your operations if your main site was unavailable? Which IT systems, which employees, which information would you need at this alternative site? Without having very clear answers to all of these questions *before* you start writing your plans, your plans will be unusable. Therefore, you need to analyze your needs and make some strategic decisions, but you also need a system to pull all these things together.

Business continuity is a one-time job. “We’ll implement this ISO 22301, and we’ll be fine – after we’re done, we’ll move on to something else.” But what will happen if you implement some new

products or some new information systems? What if one of your employees leaves the company and you had written the phone number of this employee in the business continuity plan? Obviously, without maintaining the plans they will become useless very quickly. But even worse: do you really expect these plans to work perfectly since they have never been tried in a realistic situation? I must admit that with all my experience I never managed to write a perfect business continuity plan right at the start, because this is simply impossible; the only way to get around it is to test how those plans would perform in some realistic situations – this is why exercising and testing are important. What I’m trying to say is that once your ISO 22301 implementation project is finished, this doesn’t mean that you can forget about your business continuity – the care and maintenance of your business continuity should become a part of your day-to-day operations, and you should have at least one person who will coordinate the business continuity activities.

1.4 ISO 22301 puts it all together

What I like about ISO 22301 is that it has this comprehensive, and at the same time, balanced approach to building up a business continuity management system (BCMS) – it not only gives a perfect balance between the IT and business sides of the organization, it also requires the direct involvement of top management in the business continuity implementation, ensuring that business continuity not only has all the required resources, but that it also supports the strategic objectives of the company.

ISO 22301 explains how to structure the business continuity plans, but also all the other business continuity elements – business continuity policy, risk assessment, business impact analysis, business continuity strategy, exercising and testing, etc. It gives you the tools to permanently review the whole system and improve it whenever it is possible; it provides you with a system on how to train your employees and make them aware of the importance of business continuity; it includes the requirements on how to plan the resources, including financial resources.

As I will explain later on in greater detail, it gives a perfect implementation path – it is written in such a sequential way that you just have to follow the structure of the standard to implement your BCMS in the most logical way.

Finally, it provides a management framework on how to evaluate whether business continuity has achieved some business value – by setting objectives and measuring whether these objectives are fulfilled. You may be surprised, but I like this part very much – this is because if the management sees concrete benefits in business continuity, it is the best way to ensure the long and successful life of business continuity in your company.

1.5 Who should read this book?

This book is written for beginners in this field – I structured this book in such a way that someone with no prior experience or knowledge about business continuity can quickly understand what it is all about, and how to implement the whole project. So

if you are an IT administrator, information security professional, quality manager, or a project manager with a task to implement ISO 22301 in your company, this book is perfect for you.

However, I think this book will be quite useful for consultants, also – being a consultant myself I have tried to present in this book the most logical way to implement a Business Continuity Management System, so by carefully reading this book you will gain the know-how for your future consulting engagements.

Finally, I think this book can be a kind of a checklist for experienced business continuity practitioners – I’m saying this because I’ve had many such experienced professionals in my ISO 22301 courses, and although they didn’t learn anything especially new, they were thankful for getting a comprehensive and structured view of how business continuity should be implemented. And this is exactly how this book is written.

1.6 How to read this book

I’ve tried to make this book as easy as possible to read and to use in practice:

- When certain sections of this book are related to a particular clause in the standard, then the standard clause is written in the title of that section.
- Since Chapters 5, 6 and 7 describe the implementation of particular clauses of the standard, each section has these elements:

- **Purpose** – describes briefly why such a clause exists and how it can be used for your BCMS
 - **Inputs** – which inputs you need to have in order to implement the requirement
 - **Options** – which options you should consider when implementing the requirement
 - **Decisions** – which decisions you need to make to move forward
 - **Documentation** – describes how to document the requirements of ISO 22301
 - **Documentation tip** – briefly summarizes the documents you need for each requirement
- You'll find lots of useful information in the appendices – glossary, implementation diagram, checklist of mandatory documentation, etc.

1.7 What this book is not

This book is focused on processes, project management, documentation, etc.; however, it is not focused on technology. This book won't explain which kind of backup systems you need to purchase, which communication technology you should use, or which kind of servers to install at a disaster recovery site. However, this book will give you a methodology on how to get all the inputs so that you can make relevant technology decisions – how to

determine which critical data you have and how often it needs to be backed up, what amount of data you need to communicate and to whom, how distant your alternative site should be, and how quickly you need to restore your IT and communication systems.

This book won't give you finished templates for all your policies, procedures and plans; however, this book will explain to you how to structure every document required by ISO 22301, which options you have for writing such documents, who should be involved in writing and decision making related to each document, where to find the inputs, etc.

This book is not a copy of the ISO 22301 standard – don't expect that by reading this book you won't have to read the standard. This book is intended to explain to you how to interpret the standard, and how to implement every element of the standard; however, this book is not a replacement for ISO 22301 itself.

So, please don't make the mistake of starting an implementation of a standard without actually reading it – I think you'll find the ISO 22301 standard and this book to be the perfect combination for your future work. You can purchase the standard at the **ISO official website**.



So, what is this ISO 22301 all about?

6.6 Performing the business impact analysis (clause 8.2.2)

Here's how to apply the BIA methodology in practice.

Purpose. The purpose of business impact analysis is to determine the Maximum Acceptable Outage/Recovery Time Objective, Maximum Data Loss/Recovery Point Objective, required resources and other important information that will help you determine the strategy for each of your activities.

Options. The options for performing the business impact analysis are basically the same as the options for performing the risk assessment, so I'll repeat them in this section.

Since this step in the project is also time consuming and complex, you can decide whether it will be performed by the Business continuity coordinator, or by some hired expert (e.g., a consultant) – for the sake of simplicity, I will mention only the Business continuity coordinator in this section. In any case, this person has to develop the BIA Questionnaires for collecting the information (or configure the tool, if it is used), organize interviews or workshops, compile all the data and produce the report (or include the results in the Strategy if no separate report is produced).

If you only send the methodology and BIA Questionnaires to the responsible persons in each activity and tell them to fill them in, the results you get will probably be unusable. The reason this will happen is that people find it very difficult to understand what business impact analysis is all about, even though you have written your methodology well.

Therefore, if you want your BIA to succeed, you basically have two options:

a) Perform business impact analysis through interviews

– this means that the Business continuity coordinator will interview the responsible person(s) from each activity, where he will explain the purpose of BIA first, and make sure that every assessment made by the responsible person makes sense and is not biased.

b) Perform workshops with responsible persons first

– in such workshops, the Business continuity coordinator explains to all responsible persons the purpose of BIA, and through several real-life examples, shows how to perform the analysis.

Of course, conducting interviews will probably yield better results; however, this option is much more time consuming for the Business continuity coordinator.

Inputs. The main input for the business impact analysis process naturally is the BIA Methodology, and you also need a list of your business continuity activities (see section 6.1).

All the information must be given by, and assessments made by, the responsible persons from each activity. While doing that, they must use the worst-case scenario criteria: what would have happened in a huge storm, not some average storm; a breakdown of your whole IT infrastructure, not just some insignificant server; loss of data from your main server, not from one laptop only; your CEO and main system administrator are missing, not only some

lower-level employees; and all of this happens when you have a short deadline to deliver an important product to your most important customer.

If your respondents tell you “This is never going to happen to us!” – just tell them to read a couple of news stories from the crime section. Besides, business continuity is here to prepare you for bad times, not for good times.

Here are a few tips for collecting the required information from the responsible persons from each activity:

- **Impact assessment** – they have to consider the business damage that will happen if their operations are halted, in light of particular questions that are asked. For example, for the question “How will your clients react to a disruption?” – for a disruption that lasts 2 to 4 hours, you should receive assessment (1) on a scale 1 to 4 if there would be no client reaction whatsoever; assessment (2) if clients would start calling you, but nothing significant would happen in that time frame; if after an 8-hour disruption some clients would start leaving your company, then this would mean an assessment of (3); if after 48 hours the majority of clients would leave your company, this would mean an assessment of (4). See also Figure 9 for an example.
- **Assessment of RPO/Maximum Data Loss** – you have to ask your respondents to list all their databases, applications and files, but also all services (e.g. email), etc., and for each of them separately to state the acceptable limit up to which you can afford to lose the data. Usually, this limit is displayed

in number of hours, but sometimes it can also be in number of transactions or records. The main criteria while doing the analysis must be the damage of any potential data loss to the company – in terms of money or other impacts like legal, reputation, etc. Also, while doing such analysis it is important not to be distracted by the fact that you already have the backup; the question is – if your existing backup fails, how much data can you really afford to lose? See also Figure 10.

- **Minimum Business Continuity Objectives (MBCO)** – you should specify the minimum acceptable level of capacity required immediately after the recovery for a particular activity, taking your peak hours or days into account. For example, December is typically the busiest month in banks for most activities, so you should specify the minimum number of transactions or customers you would have to process if a disruption occurred on the busiest day of December.
- **Required resources** – taking into account the MBCO (number of transactions, customers, products, etc.), you should identify how many people and other resources you need for the recovery. Resources like laptops, furniture, mobile phones, offices, etc. usually depend on the number of people; capacity of resources like software and telecom links depend on number of users or number of transactions that need to be processed; data as a resource needs to be described in terms of how many and which records you need – for example, all the records created in the past six months (for, e.g., a database), or only the current documents (for,

e.g., contracts that are signed with partners and clients); external services are described in terms of transactions, products or whatever it is they provide to you; financial resources are expressed, well, in money (in your local currency or the currency your company normally uses).

- **Dependency on others** – basically, these are all other activities without which you wouldn't be able to perform a certain activity. These are usually divided like this:
 - 1) Dependency on other activities within your organization – for example, all of your activities will probably depend on the IT department/IT activity, whereas only some of your activities will depend on your legal department/legal activity.
 - 2) Dependency on suppliers and outsourcing partners – typically, all of your activities depend on electricity and telecommunication links (Internet, fixed lines and mobile phones), but many companies also depend on software development companies, hosting providers, cloud providers, accounting services, etc. Here you need to evaluate the business continuity capabilities of those third parties by studying the clauses in agreements you signed with them, inquire as to how they handled disruptions in the past, or perhaps audit them to get a deeper insight into their capabilities.

Decisions. As already mentioned, all the assessments must be done by the responsible persons from each activity – this is because they know their activities the best, so doing the assessment is not the job of the Business continuity coordinator. However, the

Business continuity coordinator is crucial for coordinating the whole effort, and for making sure that the criteria for assessing the impact are the same. For example, responsible persons from activities tend to overestimate the importance and the impact of their activities – so you might get an assessment, say from your accounting department, that if their activity is disrupted for two hours it would have a catastrophic impact (4). To counteract such an unreasonable assessment you should ask them the following question: “Do you really think that the company will go bankrupt if your department doesn’t work for two hours?” – after such a question, the assessment usually becomes reasonable.

Where the Business continuity coordinator must be actively involved is in making the decision about MAO and RPO – usually, he makes these decisions together with the responsible persons from activities, based on the results from BIA Questionnaires.

Here is an example of how the responses related to Maximum Acceptable Outage in the BIA Questionnaire for a particular activity might look:

	2 hours	4 hours	8 hours	24 hours	48 hours	1 week
Qualitative questions – assessment scale: (1) - marginal impact, (2) - acceptable impact, (3) - high impact, (4) - catastrophic impact						
1) How will your clients react to a disruption?	2	2	3	3	4	4
2) What will be the impact to other activities?	1	2	2	3	3	4

3) How will the disruption influence the loss of reputation?	1	2	2	3	4	4
4) How difficult will it be to catch up on the backlog of work?	1	1	2	2	3	3
Quantitative questions – in U.S. dollars						
5) How much will the legal and contractual penalties cost?	0	1,000	2,000	30,000	60,000	210,000
6) How much will repair expenses be?	0	0	5,000	20,000	25,000	40,000
7) How much revenue will we lose?	0	0	0	10,000	20,000	70,000

Figure 9: Example of BIA Questionnaire – determining the Maximum Acceptable Outage

The decision about MAO is basically made visually – by looking at this example (and assuming this is a small company with annual revenue of 1 million U.S. dollars and a profit of 150,000 U.S. dollars), higher impacts begin with 8 hours (question #1), whereas it is obvious that multiple high impacts will begin at 24 hours. Therefore, as the first step, some consideration should be given if clients’ reactions might be tolerated for a disruption longer than 8 hours (question #1) – if so, in the second step, MAO for this activity will be set somewhere between 8 hours and 24 hours. To determine the Recovery Time Objective (RTO) for this activity, the dependencies on other activities will have to be examined, as explained in section 6.7: Developing the Business continuity strategy (clause 8.3).

And here’s an example of how the responses to the BIA Questionnaire might look for Maximum Data Loss/RPO:

	2 hours	4 hours	8 hours	24 hours	48 hours	1 week
Assessment scale: (1) - marginal impact, (2) - acceptable impact, (3) - high impact, (4) - catastrophic impact						
Software #1	1	1	2	3	3	4
Software #2	2	2	3	4	4	4
Database XYZ	4	4	4	4	4	4
Paper-based document ZXY	1	1	1	2	2	3

Figure 10: Example of BIA Questionnaire – determining the Maximum Data Loss/RPO

The decision about Maximum Data Loss/RPO is also made visually – in this example, RPO for Software #1 should be 24 hours, for Software #2 it is 8 hours, for Database XYZ it’s less than 1 hour (probably zero), and for Paper-based document ZXY, about 1 week.

What does this mean in practice? This means that backup for Software #1 should be done at least every 24 hours, because you can afford to lose a maximum of 24 hours of data. For Software #2, the backup should be made at least every 8 hours, Database XYZ should be probably backed up in real time (e.g. synchronous or asynchronous replication – this is typical for transactional databases in banks), and Paper-based document ZXY should be copied or scanned at least within a week of its creation. All these conclusions should be documented in the Business continuity strategy or related Backup policy.

Documentation. Similar to risk assessment, if the organization doesn't use the tool, then the results are usually collected through Excel questionnaires – in this case, the Business continuity coordinator collects all these questionnaires; if the tool is used, then these are collected automatically.

No matter if the tool is used or not, the information that is collected during the BIA process must include all the elements previously mentioned in BIA Methodology.

If yours is a larger company, you should probably compile all these results in a Business impact analysis report; however, smaller companies will be just fine with summarizing all the results in the Business continuity strategy.



Documentation Tip (mandatory) *BIA Questionnaires* or information collected through a BIA tool. The results of the Business impact analysis must be summarized in the *Business continuity strategy*.

(non-mandatory) *Business impact analysis report* that compiles all the information collected through all the BIA questionnaires or a tool. Also, you could summarize the results of Recovery Point Objective/Maximum Data Loss in the *Backup Policy*.

6.7 Developing the Business continuity strategy (clause 8.3)

Purpose. Very often neglected, this is also a crucial part of your business continuity. Actually, this is where you will make decisions

BIBLIOGRAPHY

BS 25999-1:2006, *Business continuity management – Code of practice*

BS 25999-2:2007, *Business continuity management – Specification*

ISO 22301: 2012, *Societal security – Business continuity management systems – Requirements*

ISO 22313:2012, *Societal security – Business continuity management systems – Guidance*

ISO 9001:2008, *Quality management systems – Requirements*

ISO/IEC 27000:2009, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*

Kosutic, Dejan, *9 Steps to Cybersecurity*, Zagreb: EPPS Services Ltd, 2012

NFPA 1600, *Standard On Disaster/Emergency Management And Business Continuity Programs*

<http://blog.iso27001standard.com/> *ISO 27001 & ISO 22301 Blog*

INDEX

- 9/11 45, 226
- acceptable level of risk 95
- accounting department 43, 121
- activities 15, 21, 22, 23, 35, 48, 93, 94, 97, 99, 100, 101, 102, 104, 106, 108, 109, 110, 111, 112, 115, 116, 117, 118, 119, 120, 121, 122, 125, 126, 128, 130, 131, 132, 142, 144, 145, 147, 149, 151, 153, 154, 158, 159, 160, 161, 162, 163, 165, 166, 168, 169, 170, 174, 178, 180, 184, 186, 187, 188, 192, 198, 215, 217, 219, 231, 232, 233, 234
- alternative data center 105
- alternative location 42, 127, 129, 139, 141, 150, 163, 189, 192, 231
- alternative site 14, 19, 45, 126, 127, 128, 129, 163, 174
- ANAB 200
- Annex SL of ISO/IEC Directives 28
- Annualized Lost Expectancy (ALE) 41
- Annualized Rate of Occurrence (ARO) 41
- assets 93, 94, 100, 101, 113, 169, 171, 233
- awareness 212, 215
- awareness and training 30
- backup 11, 12, 14, 18, 23, 42, 45, 101, 105, 108, 109, 119, 123, 126, 131, 165, 166, 206, 232, 234
- Backup policy 123, 206
- Backup Policy 124
- Balanced Scorecard 183
- bank 108, 200
- banks 11, 53, 119, 123, 141, 163, 185, 195
- BCI Good Practice Guidelines 26
- benefits 16, 32, 36, 38, 39, 42, 44, 45
- British Standards Institution 20
- BS 25999 235
- BS 25999-1 26, 235
- BS 25999-2 20, 26, 27, 32, 36, 109, 223
- budget 105, 189
- Business continuity 235
- Business continuity coordinator 51, 99, 100, 101, 102, 106, 116, 117, 120, 121, 124, 131, 132, 140, 145, 147, 155, 159, 171, 176, 178, 179, 181, 183, 184, 190
- business continuity management system (BCMS) 15, 16, 17, 18, 22, 29, 48, 125, 175, 181, 183, 184, 189, 191, 192, 202, 211, 213, 214, 215, 217, 220, 231, 232
- Business continuity manager 51
- business continuity plan 14, 16, 22
- business continuity plans 25, 30, 31, 36, 44, 45, 46, 141, 173, 221
- Business continuity plans 15, 22, 23, 56, 57, 139, 140, 142, 143, 144, 145, 146, 150, 152, 153, 158, 159, 161, 166, 169, 170, 171, 178, 217, 218, 219, 232, 243
- Business continuity policy 16, 184, 185, 211, 213, 214
- business continuity project 25
- business continuity standards and frameworks 25
- business continuity strategy 16, 30, 45, 102, 106, 107, 108, 109, 110, 112, 113, 114, 122, 123, 124, 130, 142, 150, 161, 165, 192, 207, 213, 216, 217, 220, 229, 234
- business continuity tools 53
- business impact analysis 16, 22, 23, 30, 94, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 121, 122, 123, 124, 125, 140, 161, 172, 211, 213, 216, 217, 228, 229, 232, 233, 243
- Business impact analysis methodology 110, 113, 115, 116
- business risks 36

- business strategy 36
- catalogues 100, 105, 228
- CEO 38, 39, 117, 147, 148, 151, 152, 157
- certificate 37, 52, 183, 195, 196, 197, 199, 202, 203, 208
- certification audit 33, 196, 202, 203, 204, 207
- certification auditor 33, 193, 195, 196, 198, 201, 202, 203, 205, 206, 207
- certification body 21, 32, 33, 196, 199, 200, 201, 202, 207, 208
- Chief Compliance Officer 39
- Chief Financial Officer 39
- Chief Financial Officer (CFO) 147, 149
- China 32
- Classification Policy 115
- clients 11, 12, 13, 36, 37, 53, 54, 96, 110, 111, 113, 118, 120, 121, 149, 151, 165, 177, 196
- client satisfaction 36
- Command centre 150
- commitment 29, 35, 42
- company strategy 38
- competences 57, 128, 211, 215
- compliance 36, 196
- confidentiality 49, 98, 115
- consequences 54, 94, 95, 97, 99, 101, 102, 107
- consultant 17, 27, 28, 39, 49, 50, 51, 52, 53, 54, 99, 116, 140, 159, 162, 186, 199, 209, 243
- consulting 10, 52, 53, 171, 204
- continual improvement 30
- controls 25
- core business continuity elements 30
- Corrective action form 56
- Corrective action procedure 181, 192, 193, 194
- corrective actions 30, 176, 181, 182, 188, 190, 191, 192, 193, 194, 198, 203, 208, 212, 222, 229
- cost 40
- cost cutting 36
- costs 106, 114
- crisis management 26, 27, 126, 139, 140, 142, 144, 145, 146, 147, 148, 149, 150, 151, 152, 156, 160, 224
- Crisis management team 126, 147, 150, 151, 156, 160
- Crisis manager 147, 150, 151, 152, 156, 157, 158, 160
- customers 13, 21, 35, 43, 53, 119, 126, 183
- data center 14, 42, 126, 131
- department head 106, 159
- department heads 140, 175, 190
- Department of Homeland Security 226
- disaster recovery 14, 23, 27
- disaster recovery location 105
- disaster recovery plan 141, 159, 166, 218, 232
- Disaster recovery plan (DRP) 142, 166, 232
- disaster recovery site 12, 18, 36, 126, 131, 231
- disruption 14, 37, 44, 103, 108, 110, 111, 112, 118, 119, 121, 122, 125, 126, 129, 130, 141, 160, 217, 233
- disruptive incident 21, 99
- disruptive incidents 92, 93, 139, 145, 169, 212, 219
- documentation review 201
- documentation templates 6
- documented information 211, 212, 216
- document management system 141
- DRII Professional Practices 26
- elevator speech 38
- emergency management 26
- Excel 96, 97, 102, 107, 112, 114, 124, 216
- executives 37, 139, 189, 191
- exercising and testing 15, 16, 27, 30, 57, 173, 174, 175, 176, 177, 183, 190, 192, 213, 220, 225, 228
- financial institutions 6, 32, 36, 111, 195
- financial resources 16
- financial risk 39, 104, 130
- fire-suppression system 94

- fire-suppression systems 40, 41, 104
- Foundation Course 34
- Gantt chart 52
- government agencies 6, 32, 139, 148, 150, 226
- health & safety 147, 154, 155
- Help desk 154
- human resources department 22, 147, 215, 231
- Hurricane Katrina 45
- implementation 16
- improvement 16
- Incident log 181, 182
- incident response 30, 139, 142, 144, 153, 154, 155, 158, 160, 180, 217
- Incident response plan 142, 143, 144, 145, 152, 153, 155, 156, 158, 159, 160, 178, 180, 218, 219
- India 32
- information and communication systems 23
- information security 24, 25
- Information security 235
- Information Security Management System (ISMS) 55
- Information security officer 51
- information security professional 17
- integrated audit 200
- integrated internal audit 187
- integrated management system 56
- interested parties 29, 144, 145, 151, 175, 211, 212, 214, 215, 218
- internal audit 30, 185, 186, 187, 188, 192, 198, 199, 212, 213, 221, 222
- internal auditor 33, 185, 186, 187, 188, 198
- Internal Auditor Course 33
- Internal audit program 56, 188, 213
- Internal audit report 56, 188, 222
- International Organization for Standardization (ISO) 20
- International Standardization Organization (ISO) 19
- Internet service provider 37
- interviews 49, 99, 100, 116, 117, 140
- Investment 40, 242
- IRCA 33
- ISO 26, 235, 236
- ISO 9001 21, 27, 28, 30, 31, 55, 56, 57, 186, 187, 189, 192, 193, 200, 216, 220, 222, 235
- ISO 14001 56, 216
- ISO 22301 236
- ISO 22313 27, 28, 228, 235
- ISO 27001 6, 27, 28, 29, 30, 31, 55, 56, 57, 93, 96, 97, 98, 102, 103, 105, 186, 187, 189, 196, 200, 212, 216, 217, 222, 242
- ISO 27002 27, 105
- IT administrator 17, 48
- IT and communication systems 19
- IT companies 111
- IT company 31, 53, 114
- IT department 22, 46, 51, 120, 147, 154, 159, 165, 166, 168, 175, 231
- IT infrastructure 104, 117, 127, 144, 158, 161, 167, 169
- IT systems 14, 47, 155
- key performance indicators (KPIs) 221
- laws and regulations 36, 96, 97, 113, 114, 171, 214, 233
- Lead Auditor Course 32, 33, 52
- Lead Implementer Course 33, 52
- legal and regulatory requirements 57
- legal department 106, 120
- likelihood 94, 95, 99, 101, 102, 103, 107
- line managers 35, 42
- List of key contacts 143, 150, 178
- List of legal, regulatory and other requirements 56, 211, 213
- loss/downtime 40
- main audit 201
- main site 14
- maintenance 15, 177

- Maintenance and review plan 178, 179
major nonconformity 208
management framework 16
Management review 30, 57, 181, 184, 189, 190, 191, 198, 212, 222, 229
manufacturing 22, 128, 200, 231
market share 11, 36, 37
Maximum acceptable outage (MAO) 125
Maximum Acceptable Outage (MAO) 109, 110, 112, 116, 121, 122, 126, 132, 229, 233
Maximum data loss 115
Maximum Data Loss 22, 109, 112, 116, 118, 123, 124, 234
Maximum tolerable period of disruption (MTPD) 109
measurement 30, 57, 96, 182, 183, 184, 185, 190, 197, 203, 212, 213, 221, 229
measuring 16
meeting minutes 190, 222
minimum business continuity objective (MBCO) 23, 233
Minimum Business Continuity Objectives (MBCO) 23, 115, 119, 161, 162, 233
monitoring 30, 98, 114, 184, 185, 212, 213, 221
myths 13, 45
National Fire Protection Association (NFPA) 226, 242
National Preparedness Standard by the National Commission on Terrorist Attacks Upon the United States 26
natural disaster 21
NFPA 1600 26, 224, 226, 227, 228, 229, 230, 236
nonconformities 30, 185, 188, 191, 192, 193, 202, 204, 207, 208, 212, 222
nonconformity 193, 204, 205, 206, 207, 233
North America 32
objectives 16, 30, 55, 57, 175, 176, 182, 183, 184, 190, 191, 192, 211, 212, 214, 215, 217, 220
operational risk 25
outsourcing 115, 120, 125, 128, 130, 213, 216
physical security 154, 171
Plan-Do-Check-Act (PDCA) cycle 29, 54, 55, 56
Post-incident review 155, 179, 180, 181, 182, 212, 221
Preparation plan 107, 108, 151
prevention 40
primary location 12, 127, 139, 170, 206, 231
Procedure for corrective action 56, 213
Procedure for document control 56, 179, 221
Procedure for identification of requirements 213
Procedure for internal audit 56, 188, 221
profit 36, 37, 41, 122
project management 18, 25, 50, 52, 144
project manager 17, 47, 48, 50, 51
Project plan 50, 54
project team 50, 51, 52, 97, 106, 114
qualitative method 111, 114
Quality Management System (QMS) 56
quality manager 17
RABQSA 33
recertification audit 203
records 57, 119, 160, 179, 182, 192, 194, 198, 201, 202, 203, 211, 212, 213, 215, 218, 222
recovery plan 52, 142, 143, 158, 166, 169, 178, 180, 231
recovery plans 51, 139, 140, 142, 144, 145, 148, 159, 160, 161, 162, 164, 166, 167, 168, 177, 178, 217, 232
Recovery Point Objective (RPO) 22, 109, 110, 112, 116, 118, 121, 123, 124, 232, 234
Recovery Time Objective (RTO) 22, 109, 110, 115, 116, 122, 125, 130, 132, 139, 144, 158, 160, 161, 162, 166, 168, 177, 181, 215, 229, 232, 234
remote location 14
residual risk 96, 106, 107

resources 15, 16, 22, 23, 30, 46, 48, 101, 106, 113, 115, 116, 119, 125, 128, 131, 141, 142, 144, 147, 153, 158, 161, 163, 174, 190, 191, 215, 217, 231, 232

Restoration plan 142, 145, 169, 170, 171

return on investment 28

Return on investment (ROI) 40, 131

Return on security investment (ROI) 41

risk assessment 16, 30, 46, 56, 93, 95, 96, 97, 98, 99, 100, 101, 102, 103, 105, 107, 108, 110, 112, 113, 114, 115, 116, 124, 125, 140, 142, 153, 172, 175, 181, 211, 213, 217, 219, 227, 233, 234, 243

Risk assessment methodology 56, 98, 113, 114, 213

Risk assessment report 56, 102, 103, 217

risk assessment tool 96, 102, 103, 124

risk calculation 95, 97, 102

risk identification 93, 97, 100, 102

risk management 25, 92, 96, 97, 233, 234, 235

Risk Management Methodology 105

risk treatment (mitigation) 93, 94, 95, 96, 97, 98, 102, 103, 104, 105, 106, 107, 108, 217, 220, 232, 234

Risk treatment (mitigation) 213

safeguard 105, 232

safeguards 25, 40, 93, 96, 104, 105, 106, 107, 195

satellite phone 146

scale 37, 94, 95, 97, 102, 107, 110, 111, 112, 113, 114, 115, 118, 121, 123

scenarios 45, 149, 153, 176, 213, 219, 220

scope 29, 53, 162, 170, 175, 188, 191, 214, 215, 226

Security manager 155, 157

server room 126

shareholders 152

single point of failure (SPOF) 112, 131

sponsor 50, 51, 106

Stage 1 audit 201

Stage 2 audit 201, 202

stakeholders 21, 35, 142

strategic objectives 15

suppliers and partners 35, 36, 45, 46, 115, 120, 128, 129, 130, 174, 192, 198, 213, 216

surveillance visits 201, 202, 208

tax authorities 43

technical failure 21

telecom company 37

threat 40, 94, 97, 100, 101, 102, 103, 107, 155, 156, 157, 158, 227, 234

top management 15, 35, 38, 39, 42, 51, 97, 114, 131, 145, 155, 162, 171, 175, 176, 181, 184, 188, 189, 190, 192, 203, 214, 229

training 13, 32, 34, 49, 57, 101, 106, 128, 131, 151, 174, 212, 215

training & awareness 16

transportation 129, 141, 161, 162, 163, 218

UKAS 200

unacceptable risks 104, 105

United Kingdom 26, 32, 200

United States 26, 200

U.S. National Fire Protection Association 26

vulnerability 94, 97, 100, 101, 102, 103, 107, 227, 234

Western Europe 32

workshops 99, 100, 101, 116, 117, 140