# 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

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

# 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 that 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 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