Advisera

Report

Compliance and information security - How are they related?

2019

Table of content

Introduction

With the worldwide increase in the quantity and strictness of laws and regulations that impact information security, organizations should be more concerned about the balance they put on how they handle security risks, and how the security controls they implemented are compliant with such legal requirements. But how prepared are they for this scenario?

With this idea in mind, Advisera carried out the survey "Compliance and information security - How are they related?" from June 12 to 18, 2019, with 605 respondents. Survey respondents came from countries on five continents, from various industries, mostly from smaller and medium-size companies, acting mostly in IT and security positions. The poll was anonymous. The goal of the survey was to research the connection between security and compliance, and find out the following:

- whether companies prefer the focus on compliance or on security
- typical security methods used to cover compliance requirements;
- what kind of compliance their clients typically ask for; and
- why data breaches usually happen

We believe that the details contained in this report can help organizations assess their own state of handling compliance and information security. The main findings of this survey are:

Key finding 1)

Most respondents see security and compliance as being very tightly related.

Key finding 2)

The main difference between security and compliance seems to be the goal of satisfying the auditors/third parties, which is more important for compliance, while not so relevant for security.

Key finding 3)

The respondents place human factors and organizational factors as more important than technical safeguards as the cause of breaches.

Key finding 4)

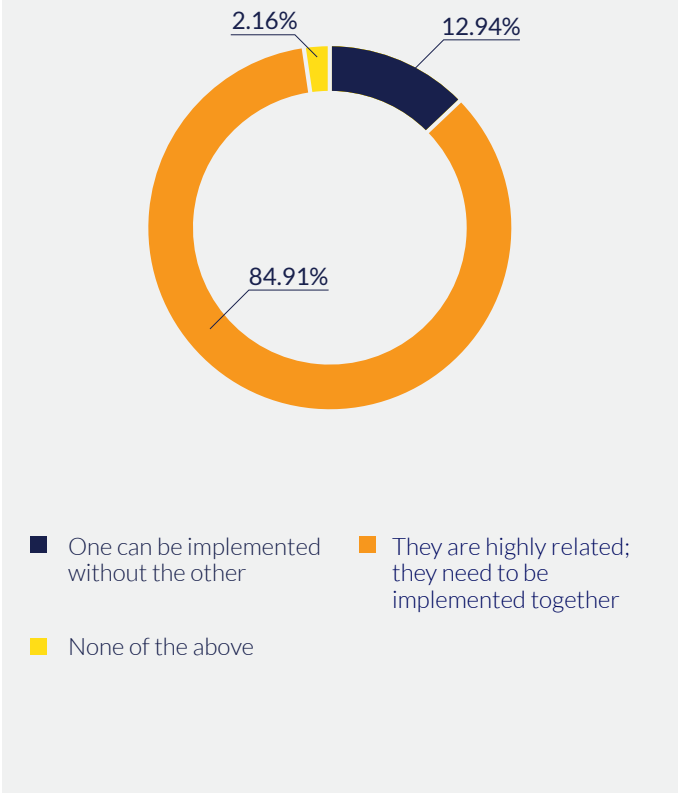
Being compliant with laws and regulations is not a guarantee against data breaches.

On the following pages, you will find more detailed information on these findings, as well as about other questions we considered in this survey. You will also find recommendations for improving compliance and information security in the form of articles and other useful materials.

For more information about any of the contents of this report, please contact Advisera support team.

1) How tightly are security and compliance related?

How much are security and compliance related?



Finding

Nearly 85% of respondents consider security and compliance to be highly related and feel that they need to be implemented together.

Advisera insight

This perception of respondents can be supported by the fact that most security managers take into account laws, regulations, and other legal requirements (e.g., contracts and service agreements) when implementing security.

2) Activities relevant for both compliance and information security

What are the common activities that need to be done both because of compliance and because of information security?

Finding

Surprisingly, there are a couple activities that seem to be less common for both compliance and information security. These include satisfying the auditors/third parties, using a framework for setting up a system, monitoring suppliers, setting KPIs and measuring their achievement, and reporting to the top management.

Advisera insight

Some potential reasons for organizations not using a common framework for both security and compliance may be:

1) lack of knowledge about available frameworks;
2) lack of understanding on how to integrate different frameworks;
3) separated teams without an integrated approach.

By not using a common framework for both security and compliance, an organization may have redundancy on common activities (e.g., identification of requirements, measurement, and management review), which leads to inefficiency, using more resources and effort than necessary.

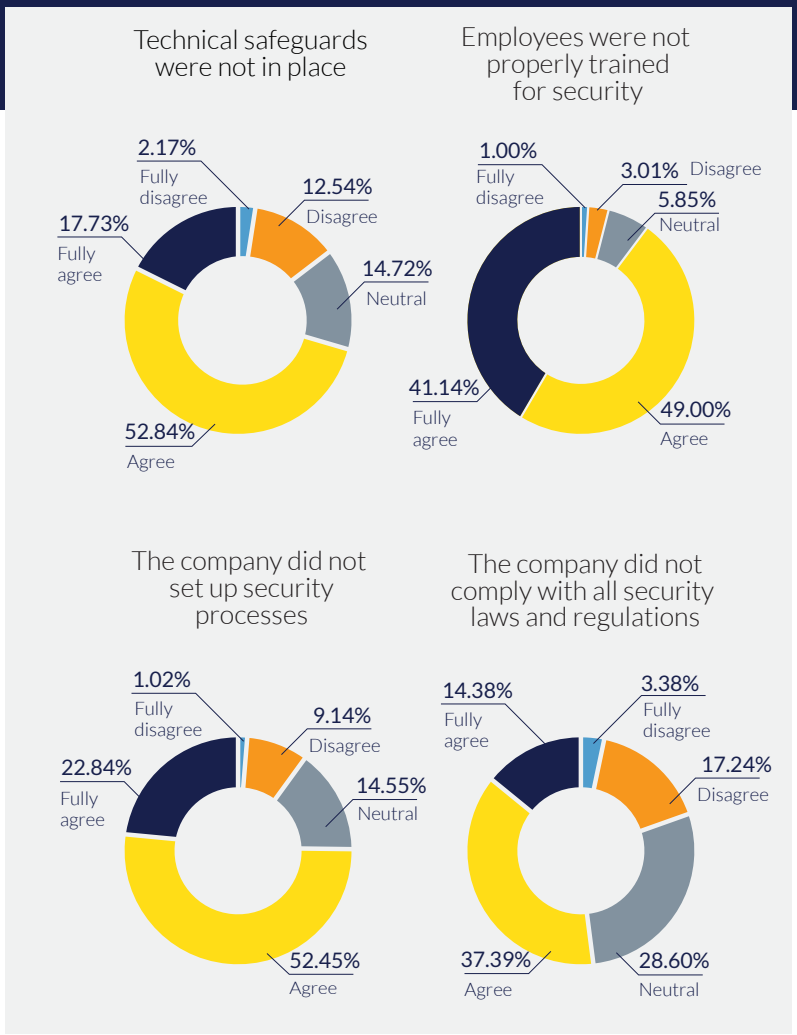
For example, by not considering both security and compliance requirements that satisfy auditors and third parties (e.g., customers and regulators), an organization may finish with many more KPIs than necessary, instead of using fewer KPIs that are useful for both issues.

Additionally, by performing joint monitoring of suppliers, as well as joint reporting to management, an organization can provide to top management a wider view of compliance and security, allowing for the identification of situations that could be missed if seen separately, and improving the overall effectiveness of information security and compliance.

For further information about the importance of KPIs and their monitoring, see these articles based on ISO 27001, which is the main ISO standard for information security management that has been adopted worldwide:
Key performance indicators for an ISO 27001 ISMS and
How to perform monitoring and measurement in ISO 27001

3) Causes of data breaches

In your opinion, why do data breaches usually happen?



Finding

Employees who have not been properly trained are considered by respondents to be the main cause of data breaches, followed by a lack of security processes and technical safeguards. Failure to comply with security laws and regulations is seen as the least frequent cause of data breaches.

Advisera insight

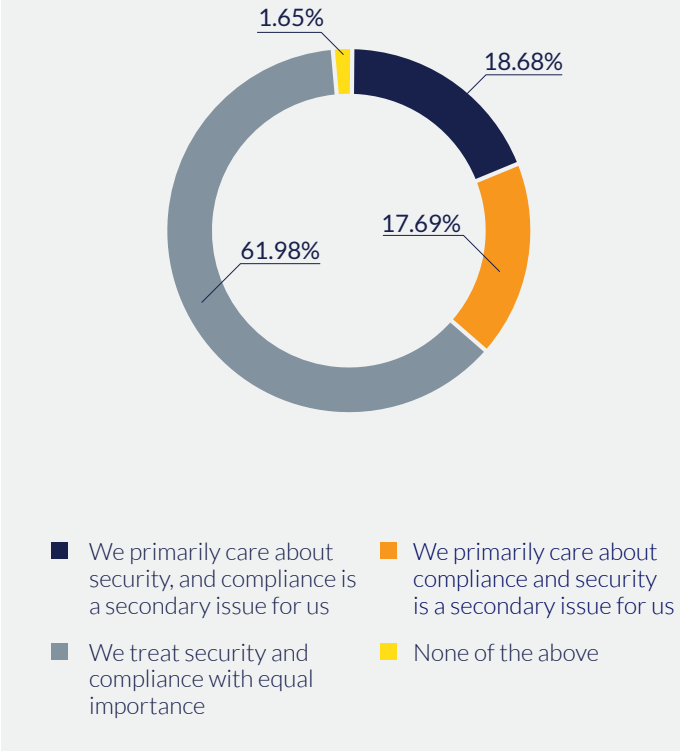
Social engineering and exploitation of technical vulnerabilities are among the main weapons used by attackers to compromise an organization's data, and their chance of success is increased by the lack of training (not only of common users, but also of technical staff), and also by not adopting robust processes and technologies.

Regarding laws and regulations, because in most cases they cannot cover all possible situations, simply fulfilling their requirements is not a guarantee that an organization will be safe, so organizations should also rely on risk management approaches.

For further information see the article 8 security practices to use in your employee training and awareness program

4) Which is more important: Security or compliance?

> Does your company typically place more emphasis on security or on compliance?



Finding

Almost 62% of the respondents believe that security and compliance must be treated with equal importance.

Advisera insight

We can point to at least two reasons that contribute to this result:

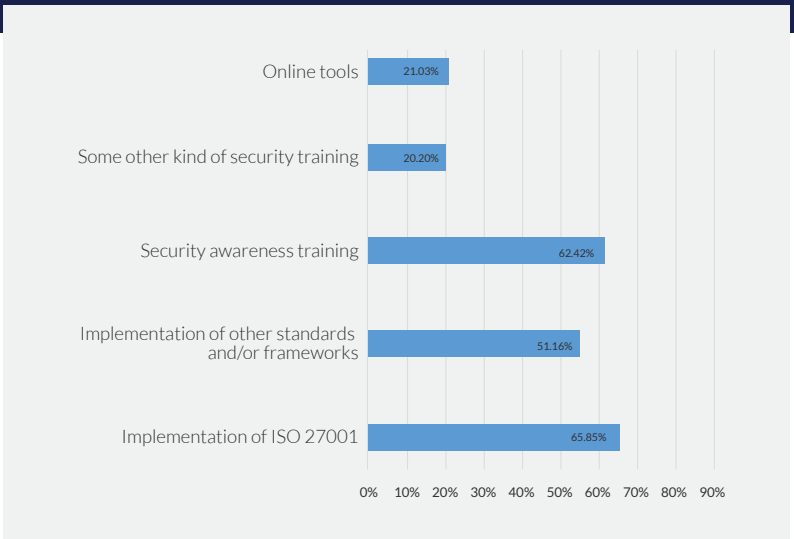
Organizations need to fulfill customers' requirements, who also consider both compliance and security equally important to their business (see question 6 below), so they expect the same commitment from their suppliers.

Although covering different issues (i.e., complying with various requirements, and protection against security threats), both compliance and security aim for the same ultimate goals:
1) minimization of incidents;
2) minimization of negative impacts of incidents;
3) maximization of opportunities (e.g., getting new customers who value both compliance and security);
4) achievement of business goals (e.g., revenue increase, better governance, etc.)

For further information see the article Should information security focus on asset protection, compliance, or corporate governance?

5) Methods for managing information security and compliance

Which methods do you use when managing information security and compliance in your company?



Finding

ISO 27001 and security awareness training are the methods of choice when managing information security and compliance.

Advisera insight

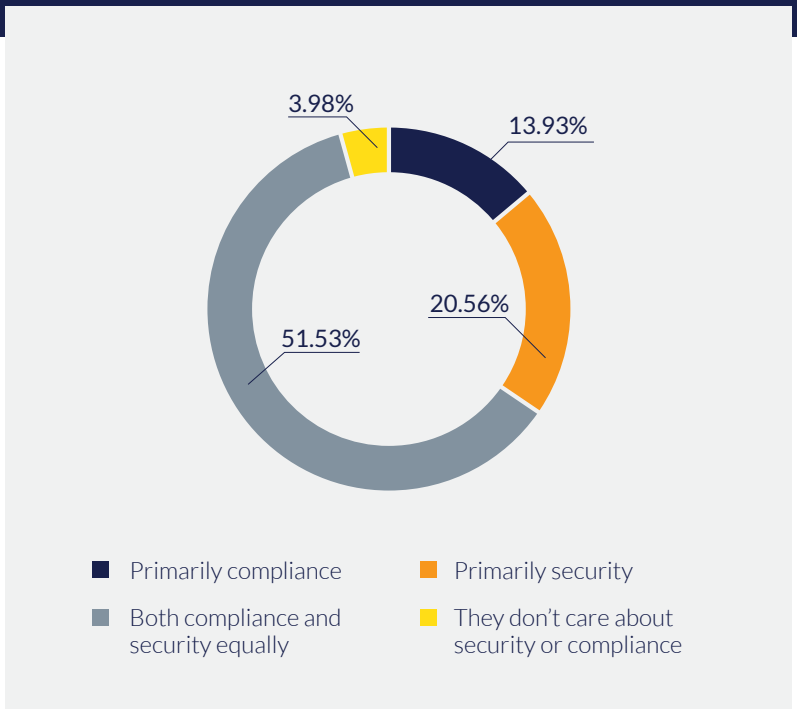
First, it is important to note that this specific result is probably biased due the fact that respondents are all subscribed to the 27001Academy website and, as such, they already recognize that the adoption of ISO 27001 offers to organizations a globally recognized and proven way to protect information security considering not only business needs, but also third-party expectations, like those of governments, regulators, and customers.

Even though there is a general market trend that focuses on IT security, companies are becoming aware that technological controls are expensive and slow to implement if the employees do not understand why such technology is needed, or how to use it. This is the reason why security awareness and training are gaining recognition as an important tool for cybersecurity management.

For further information see this helpful material: 25 free videos for a security awareness program

6) How do customers view compliance and information security?

What do your clients/customers primarily require from you?



Finding

Almost 62% of the respondents answerted that their clients/customers require compliance and information security equally.

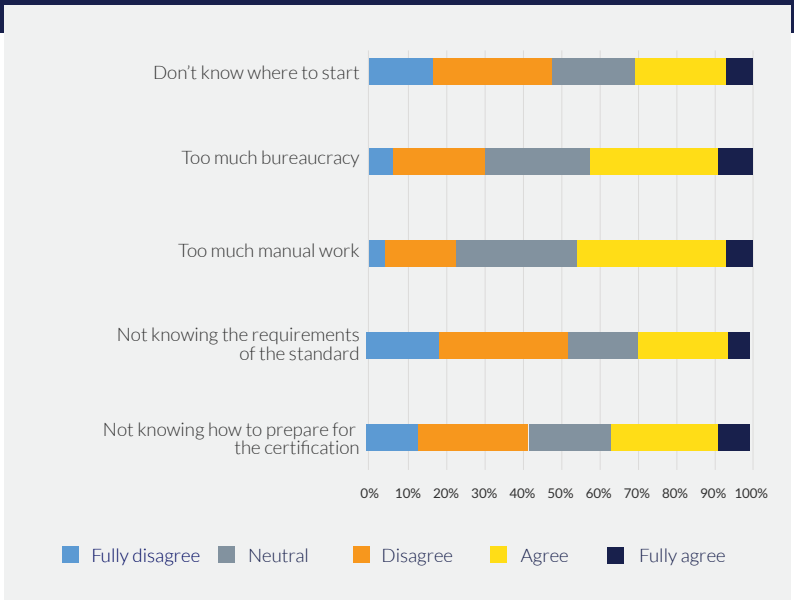
Advisera insight

This finding is interesting, because it supports a trend of transferring security requirements from customers to their suppliers, who now must be as concerned about data from their customers as they are about their own data.

For further information, see this ISO 27001 article, because this standard provides guidance for the evaluation of suppliers' security practices: 6-step process for handling supplier security according to ISO 27001

7) Main challenges with ISO 27001 compliance

When thinking about compliance with ISO 27001, what do you see as the biggest challenge?



Finding

Manual work and bureaucracy are seen by the respondents as the main challenges when thinking about compliance with ISO 27001.

Advisera insight

The implementation of ISO 27001 is often viewed as being much more complex than it really is. The number of documents and records required to be compliant with the standard is not as big as most people think, so bureaucracy can be kept to a minimum.

Regarding manual work, if you reduce documentation, you'll also reduce the effort to manually handle it and, in most cases, the standard allows you to adapt the documentation to your specific needs so that you do not need to add many more overhead activities.

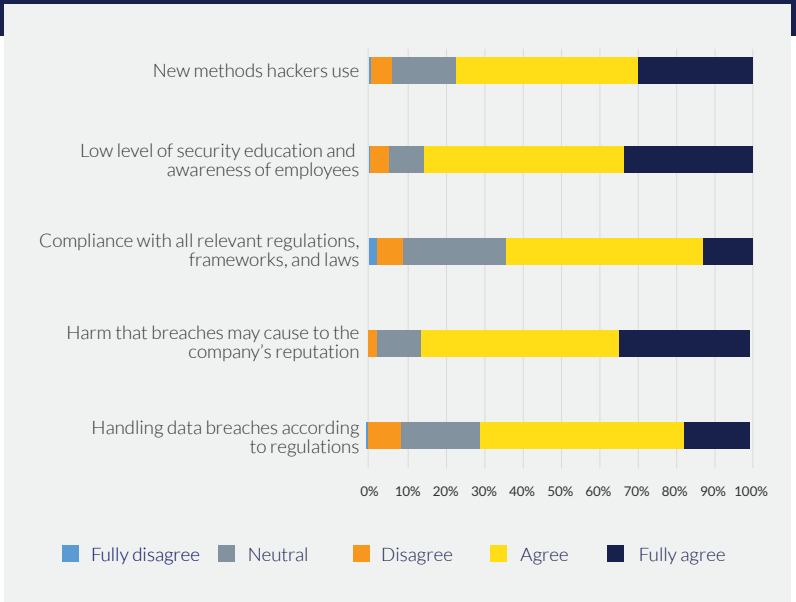
For further information see:

List of mandatory documents required by ISO 27001 (2013 revision)

5 ways to avoid overhead with ISO 27001 (and keep the costs down

8) Main concerns regarding information security and compliance

Which security and compliance issues concern you the most?



Finding

The organization's reputation and its employees' level of awareness and training are the main concerns of respondents regarding information security and compliance.

Advisera insight

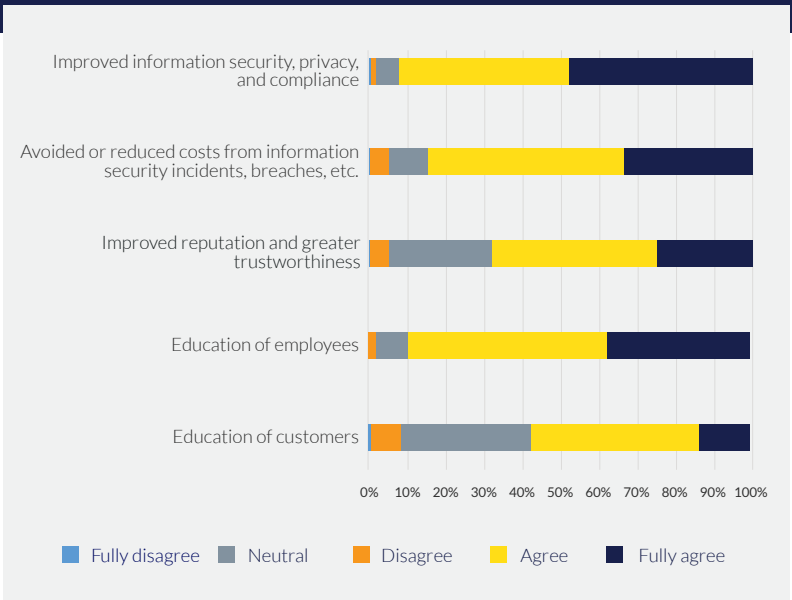
Reputation is something that takes years to build, and a lot of investment, and it can go away in a few seconds with just a single incident. And, because an incident is not a question of if, but when, organizations should think not only about preventive controls, but also on how to detect incidents at early stages, how to quickly react to minimize impact, including communication with affected parties, and how to resume normal operations as quickly as possible.

However, even the most well-designed controls and procedures can become useless if employees are not aware and educated about them. So, besides training on how to avoid the most common threats and attacks to compromise security, they also have to be trained on how to properly react in case of incidents.

For further information see the article: How to handle incidents according to ISO 27001 A.16

9) Benefits of security awareness and training

What do you see as the biggest benefits of security awareness training?



Finding

Respondents consider improved information security, privacy, compliance, and education of employees to be the biggest benefits of security awareness training.

Advisera insight

Employees who are aware and trained about information security can be of great value to help organizations with protecting information, especially given that, as of now, there is no technology available that is capable of properly evaluating and reacting to new or unstructured security threats.

Trained people are also more engaged on security and protection, because they have a clear understanding of their role in security and the damage an incident or lack of compliance can bring to the business and to their own lives.

For further information see the article: What are the benefits of security awareness training for organizations?

Conclusion

The purpose of this research was to provide an understanding of how organizations see the influence of both security and compliance on their business. The proposed questions targeted several issues, like the relationship between security and compliance, relevant activities, causes of data breaches, and main concerns.

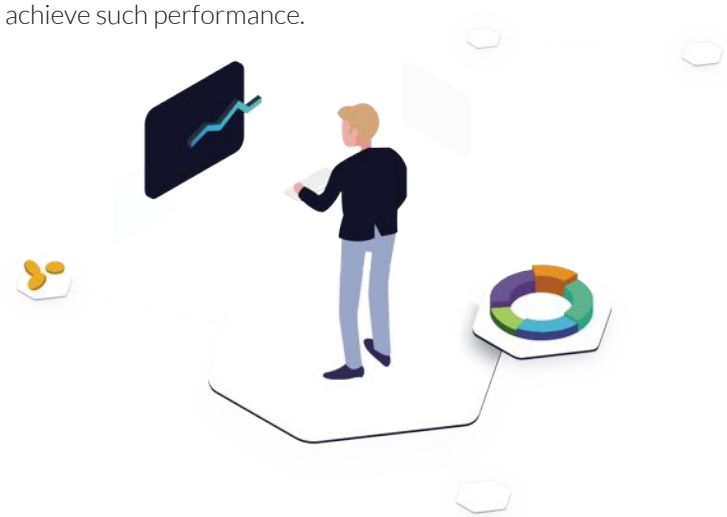
While, at first glance, responses indicate that organizations tend to address security and compliance issues in an integrated manner, largely due to demands from their own customers/clients, a more detailed analysis shows that this integration occurs only on operational activities, such as employees' training, document management, and application of security controls. Critical planning and control issues, such as KPI definition and reporting to top management, seem to be treated mostly in a separate manner.

The main disadvantage of this partial integration is a loss of efficiency. For example, separate planning and control may not consider optimization of resources used in common activities, or the use of complementary compliance and security controls for a wider and/or deeper level of protection, and today, any costs you can save while doing business can be critical to competitiveness.

One possible answer to this situation is the fact that companies focus on the implementation of single frameworks for management of security and compliance, and there does not seem to be a single framework that provides great detail on how to address both security and compliance issues. Organizations that implement multiple frameworks (like ISO 27001 with COBIT or COSO), may have a better understanding of the advantages of working on aspects that are related in the most integrated way possible.

For further information, see the article: How to integrate COSO, COBIT, and ISO 27001 frameworks

Finally, organizations have a clear understanding of employees' roles either as a cause of data breaches or as a source of increased security and compliance performance, while the awareness, training, and education activities are recognized as a main tool to achieve such performance.



References

27001Academy

About the authors

Rhand Leal has 14 years of experience in information security, and for 6 years he has continuously maintained **a** certified Information Security Management System based on ISO 27001.

Rhand holds an MBA in Business Management from Fundação Getúlio Vargas. Among his certifications are ISO 27001 Lead Auditor, ISO 9001 Lead Auditor, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), and others. He is a member of the ISACA Brasília Chapter.

Dejan Kosutic holds a number of certifications, including Certified Management Consultant, ISO 27001 Lead Auditor, ISO 9001 Lead Auditor, and Associate Business Continuity Professional.

Dejan leads the Advisera team in managing several websites that specialize in supporting ISO and IT professionals in their understanding and successful implementation of top international standards. Dejan earned his MBA from Henley Management College, and has extensive experience in investment, insurance, and banking. He is renowned for his expertise in international standards for business continuity and information security – ISO 22301 & ISO 27001 – and for authoring several related web tutorials, documentation toolkits, and books.

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12 , 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy
9100 Academy
13485 Academy
14001 Academy
16949 Academy
45001 Academy
20000 Academy
27001 Academy
EU GDPR Academy
Conformio
eTraining
AdviseraBooks

Advisera
Making certification simple.