27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

How to Budget an ISO 27001 Implementation Project

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Introduction

Over the years, ISO 27001, the leading global framework for implementation of Information Security Management Systems (ISMS), has established itself as an appropriate organizational supporting tool to ensure that information is being protected, with optimized costs, and delivers its intended results.

But, these benefits of management systems come at a cost, in terms of time, man-hours, and organizational resources, and the better your organization know about these costs (their sources, values, and when they will be needed), the better the chances of achieving a successful implementation and effective operation with minimal costs.

This paper's goal is to present some aspects that an organization should consider when preparing an ISO 27001 implementation project budget, to help identify the implementation approach best suited, considering resource availability, and three implementation options known as "On your own," "Hiring a consultant," and "Do it yourself with external support" (for more information, see: 3 strategic options to implement any ISO standard.

1. Benefits of using budgeting practices in an ISO 27001 implementation project

In an ISO 27001 implementation project, there are two main types of costs where the ability to forecast expenses can be useful:

- The **initial costs**, related to ISMS implementation, where budgeting practices can help plan and control the project's progress, by identifying risks and opportunities related to project expenses before they occur, so they can be properly treated and maximize the chances of project success.
- The **regular costs**, related to ISMS operation, where budgeting practices applied to the project can support the organizational budgeting process, by developing a forecast of the operational and maintenance costs of the ISMS after implementation / certification, so the new process can be better integrated into the business.

2. Impact of the steps of an ISO 27001 implementation project in budget planning

In general, these are the steps that an organization should take to implement an ISO 27001 ISMS, and their influence on the project budget:

#	Project step	Influence on the budget	Estimated % of overall cost
1	Obtain management support	Paramount component to get the funds to start the project Critical to ensure funds availability for the project activities during organizational changes and priorities changes	5%
2	Establish a project structure	Minimization of losses and maximization of savings by the forecasting and treating of project's costs, risks, and opportunities	

#	Project step	Influence on the budget	Estimated % of overall cost
3	Define the ISMS scope	The larger the scope, the greater the budget needs, in all aspects (e.g., staff, organizational resources, money, etc.).	15%
4	Implement basic documentation for management system and risk management	Mandatory documents required by the standard are few; however, the organization may define as many documents as it deems necessary and the greater the number or complexity of these documents, the greater the costs to develop them.	
5	Perform risk assessment and risk treatment and develop mandatory documents	The larger the scope, the more costs will have to be allocated related to staff (outside the implementation team) who must be involved (e.g., processes owners, key users, suppliers, etc.).	
6	Implement all required controls	At the beginning of the project, this is the most uncertain cost you will have, because information that is more reliable comes only with risk assessment; however, implementation frequently involves acquisition of new technologies or services that must be accounted for in the budget.	50%
7	Perform training and awareness	The more people in the scope, the more costs will be required for training and awareness. A diversity of areas in the scope (e.g., production, marketing, HR, etc.) also demands a greater variety of competencies to be mastered by the instructors for effectiveness.	
8	Operate, monitor, and evaluate the ISMS	Project costs are associated with the monitoring, by the project team, of activities performed by users within the ISMS scope. Additionally, this "first" cycle will validate the project's forecast for the ISMS operational and maintenance costs.	30%
9	Improve the ISMS	Costs related to required corrective actions and approved opportunities for improvement identified in the ISMS's first running cycle should be considered with more care if the organization intends to get certified.	
10	Certify the ISMS	Costs related to certification will vary according to the size and scope of the ISMS, and the chosen certification body.	

For more detailed information, see these articles: Four key benefits of ISO 27001 implementation, ISO 27001 implementation checklist, and List of mandatory documents required by ISO 27001 (2013 revision).

3. Types of costs in an ISO 27001 implementation project

From the previous section, it is possible to identify the following cost sources that should be considered when planning or evaluating a project budget:

Personnel costs: Costs related to work of internal people involved with the project (full-time or occasionally), considering the number of required working hours and hourly rates.

Material costs: Costs related to equipment, tools, facilities, documents, software, and similar needed to perform the work, considering leasing, renting, and purchasing conditions and item price.

Supplier costs: Costs related to the organization's regular contractors (e.g., IT equipment suppliers, transport services, and others that already work with the organization before the project begins) that will be involved in the project, considering number of required working hours and contractual situation.

Service costs: Costs related to external trainings, consulting, and certification services required to support the project, considering the benefits of getting external assistance, price of service, and frequency of use. Note that some of these costs may become permanent (e.g., certification services and specific trainings on risk management and legal issues).

Risks costs: Costs related to the implementation of controls to prevent or minimize project losses regarding the realization of risks, like a project team member leaving the project or organization, loss of a laptop, rework on a deliverable, delays in activities, etc.

Depending on the implementation solution adopted, some cost sources may become saving sources, by reducing the budget needs, as will be shown in the next section.

For more detailed information, see this article: How to address main concerns with ISO 27001 implementation.

4. Implementation options impacts in budget planning

The possible alternatives an organization has to implement a project, as stated at the beginning of this paper, are:

- On your own: you use only the knowledge and the capacity of your own employees.
- Hiring a consultant: you hire an expert from outside who has experience with the implementation of the standard.
- Do it yourself with external support: your employees are doing the implementation, but they get resources (e.g., document templates, checklists, etc.) and support (e.g., orientation on specific issues) from an external party.

All these options are basically a relative trade-off between cost (in money and human resources), time, risks, and opportunities:

Implementation option	Cost	Time	Risks	Opportunities
Do on your own	The cheapest alternative (you already have the HR resources).	Generally, takes the longest time (maybe there is no full-time team for the project or they have to learn "on the fly").	Errors and mistakes may prove more expensive than getting external assistance.	Increases staff commitment (they are developing and implementing the ISMS).
Hiring a consultant	The most expensive alternative (knowledge and experience are costly resources).	Generally, takes the shortest time (if you hire a good consultant).	Internal information is open to outsiders.	Knowledge transfer to staff (learn by seeing).
Do it yourself with external support	A compromise between "do on your own" and "hiring a consultant" (documents and knowledge provided by external support can save you time and effort in some activities).	Somewhere in between "do on your own" and "hiring a consultant" (if the project team has sufficient time to devote to the project).	Internal demands may overwhelm staff's capacity to work in the project, even with external support.	Better knowledge transfer to staff (learn by doing).

The important thing here is, if you realize savings in cost, this savings is being "paid" by increasing something else (time or risks).

5. Tips to improve budget planning

As you work on elaborating or evaluating a budget, the following questions, covering main cost types, should be considered for budget inputs:

Human resources

- Are there people in my team with project management background?
- Are there people in my team with experience in similar projects?
- Are there people in my team who can assume responsibility for the ISMS after implementation?
- How much time will be required for information security issues, during and after the project, and what will be demanded from the person responsible?
- Instead of a consultant for the project, should I hire a security professional to take care of the project and the following ISMS operation?

For more information about these issues, see:

- Who should be your project manager for ISO 27001/ISO 22301?
- What to look for when hiring a security professional
- What is the job of Chief Information Security Officer (CISO) in ISO 27001?

Material resources

- Can previous projects in my organization give insights into the development of ISMS documents (e.g., policies and procedures)?
- Can books, videos, and magazines about information security also provide good references to my project team and employees?

Note: You should at least consider buying the ISO 27001 standard.

Service resources

- Which information security trainings (e.g., risk assessment and treatment, secure development, etc.) my project team can perform if they have enough knowledge, and thereby save costs on external training?
- With proper training of my staff, could we contract external support only to deal with more complex information security issues, and thereby save costs on dealing with common issues by ourselves?

For more information about this issue, see:

- Do you really need a consultant for ISO 27001 / BS 25999 implementation?
- 5 criteria for choosing an ISO 22301 / ISO 27001 consultant

6. Verifying budget outline

When evaluating a budget, one of the most important things you have to do is to ensure the quality of the data used to prepare the budget. A budget is an estimate, and the less information you can find to support the budget, the more worried you should be.

However, there are levels of concern regarding what you know. In some cases, the lack of information is caused simply by the current project phase, for example, at the project's very beginning, or immediately after change requests. How can you estimate costs without a well-defined scope? How can you know how much ISMS implementation will cost without the information provided by risk assessment? How do you know how much a change request will cost without a scope analysis?

In this situation, instead of trying to come up with a precise value, you should consider in what range it might be, and you can use the following table to guide you:

Reliability level of the information used for budget planning	Range budget amount variation
You have only general industry statistics	-25% to +75%
You have data from similar projects / change requests	-30% to +50%
You have preliminary data about the project / change request	-20% to +30%
You have detailed data about the project / change request	-15% to +20%

For example, if you receive a budget value of $20,000 based only on industry statistics, you may expect that the final cost of the project will be between $15,000 and $35,000.

This information will not resolve you budget reliability problem, but at least it will give you some perception about what needs to be done to put the budget back on track.

7. Conclusion

All effort spent to meet a project deadline and users' needs may be useless if cost overruns exceed the added value. This situation makes a budget in a project a critical component to facilitate value creation and preservation.

By forcing the people involved to look ahead, plan, and coordinate efforts, the budget planning can help identify risks and opportunities that can be treated to keep the project under control. Nevertheless, even the best-planned budget will only be as good and as reliable as the information you consider.

The information presented in this paper, related to an ISO 27001 implementation project, can help an organization to better understand required investments and potential expenses, improving its capability to better allocate personal, technical, and other resources, greatly improving chances to be successful in such a project.

Check out ISO 27001 compliance software

To learn how to implement ISO 27001 in the most cost-efficient way when compared to other solutions, and to save your employees time, sign up for a 30-day free trial of Conformio, the leading ISO 27001 compliance software.

References

- 27001Academy
- PMI (2012), A Guide to the Project Management Body of Knowledge, 5th Ed
- http://www.pmdocuments.com/project-execution/

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting

Our offices:
Zavizanska 12, 10000 Zagreb, Croatia
Via Maggio 1 C, Lugano, CH-6900, Switzerland
275 Seventh Ave, 7th Floor, New York, 10001, U.S.

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
Switzerland: +41 41 588 0722

EXPLORE **ADVISERA**

EU GDPR Academy · 27001 Academy · 9001 Academy · 14001 Academy · 45001 Academy · 13485 Academy · 9100 Academy

16949 Academy · 17025 Academy · 20000 Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.