The Ideas Distillery

Cost Benefit Analysis Tool Guidance Document

For the ISO 27001 standard only

ABOUT THE ISO STANDARDS COST BENEFIT ANALYSIS

Could ISO certification benefit your business and help you achieve your wider goals? Yes, implementing a Standard, or indeed more than one, is certainly desirable. However, is this investment worthwhile?

We've developed this tool to help you to answer this exact question.

Is ISO Certification worth it? might be one of those million dollar questions but in reality it's more of a "work in, work out" answer. The benefits that are gained will vary greatly on the ISO Standard that you implement and the amount of effort you put into improving the management system.

Some of the benefits are not as obvious as they can be harder to quantify.

For example, when implementing ISO 27001 we would be looking at your processes and identifying streamlining opportunities, often reducing time and paperwork.

Unless you are doing time and motion studies then it will be hard to ascertain the cost benefits from these improvements.

You can estimate how much time and money you have saved and see the value from that perspective.

The more focus you place on process improvements the more benefit you will gain, the ISO 27001 standard is all about continual improvement.

The ISO 27001 Standard on the other hand could be easier to justify from a money perspective as you will need to monitor your information security.

The global average cost of a data breach has skyrocketed to £3.13 million (a 6.4% increase from 2017), according to Ponemon.

As the accepted global benchmark for the effective management of information assets, ISO 27001 enables organisations to avoid the potentially devastating financial losses caused by data breaches.

The Standard is also designed to ensure the selection of adequate and proportionate security controls that help to protect information in line with increasingly rigid regulatory requirements such as the EU General Data Protection Regulation (GDPR) and other associated laws.

HOW THIS GUIDE WORKS

Due to the nature of ISOs, it can be difficult to work out whether it's cost-effective - many of the costs fall into the 'it depends' category (it depends on your company size, sector, risks, etc) and the benefits will depend on many things so can only be estimated.

Accepting all this, we've tried to help you put together a rough-and-ready calculation to address the main areas of becoming ISO certified.

Some costs will be one-off - such as implementation costs from a company such as ours, and the certification costs if you decide to go down that route - and some will be ongoing, for example annual audit fees.

Some costs you might not have considered, such as your own staff's time (there will always be a need for some staff time allocation, even when using a full-service implementation option).

Similarly, however, there could be a raft of benefits that you hadn't considered either. It's these that only you can really estimate as you are the one who knows your business and what the potential could be.

On these occasions, we have provided some guidance from research which has been conducted, which you can use a guide to make an educated guess as to whether you can make similar gains.

The idea is, at the end of the process, you can see the overall costs and compare these with the overall benefits, in the context of both one-off and ongoing costs and benefits, and how ISOs might benefit you (or not) in the long term.

The following pages will give you a brief step-by-step guide about how to use the Cost Benefit Analysis spreadsheet.

Please note that there are two spreadsheets - one for ISO 9001, 14001 and 45001, and then a separate one for ISO 27001.

There is good reason for this - because of complex the nature of 27001 there are very different costs attached, both in terms of implementation but also in terms of certification, so it is easier to calculate the costs between these standards separately.

NON-RECURRING COSTS

These are the one-off costs that you'll incur to get your ISO system in place. So in this section you'll be looking at:

Implementation costs - this is where you'd use a company such as Ideas Distillery to help you to install your system. Refer to Tab A to see the size of company and put in the corresponding amount. *Please note that this is a base cost, and the actual cost will also depend on the complexity of your company, and whether you already have any system in place.*

Employee hours costs - you'll always need to put in some costs where employees will need to help with the implementation, whether it will be briefing a company such as ours to producing evidence. Work out the hourly rate of the employee who would be the most likely to be assigned to help with 27001 implementation (remember, it should be someone reasonably senior - there's no point handing it over to someone on work experience!), then to to Tab B and cross reference it with the size of business and judge whether you have a system in place at present. When you've got the amount, pop it into the spreadsheet.

Certification Body costs - IF you want to be certified - you don't HAVE to be certified (more of that in the next section), then go to Tab C and put in the figures against the size of your company. Remember, there may be additional elements of risk regarding what you do, this is only a judgement call and a Certification Body might not agree with you. However, it's all based on a rough average based on our experience and the pricing structure of CBs.

Certificate of Attestation costs - we provide a 'threshold' service whereby we implement a compliant management system to the requirements of ISO 27001, which is audited by a third party and where you get a certificate of conformance to the standards.

This means you can hold your company at the threshold of ISO compliance until such time as you take the decision to certify to UKAS via a Certification Body. So you can operate your business to 27001 standards, demonstrate your compliance, but don't have to go to the expense of UKAS accredited certification until you need to.

To show you at this Threshold, we can issue you with a certificate to attest that you are meeting the requirements of the standard and are ready to be certified when required.

RECURRING COSTS

These are the costs that you will have to meet every year in order to stay certified to your chosen standard(s).

Management System maintenance costs - these are the costs you would meet if employing the services of a company such as Ideas Distillery, as we would ensure that your management system would be in shape. Go to Tab D and put in the corresponding costs. Note that you don't have to take on a consultancy company in order to do this, you could choose to do it in-house. But you would need to bear in mind two things: you would have to incur some employee costs (see Tab B), and you would need to have a competent Internal Auditor, which means that at the very least you would need to get a relevant member of your trained with a suitable qualification. If you are the sort of person who wants to leave accounting to your accountant, and your company's legal affairs to a lawyer, then you'll probably want to leave this part to a professional company too!

Additional employee hours costs - even if you get a company in to maintain your system, you will undoubtedly need to allocate some staff time to help, although this should be minimal.

Certification Body costs - go back to Tab C to see what these are according to the size of your business.

It's important to recognise 27001 certification is not a single event, but rather an ongoing process that ensures your business complies with the requirements of the ISO 27001 standard.

The certification cycle is a three-year programme. After gaining your initial certification after a successful Stage Two audit, the following two years will see annual Surveillance Audits by the Certification Body.

During these, all the elements covered in the Stage Two audit are reassessed with a view to ensuring that all the original systems and processes are operating as specified and producing the correct outcomes.

Following these two years of Surveillance Audits, you will then get a Recertification Audit. Your ISO certificate is valid for three years after its initial issue.

So when you get to Year 4 on the spreadsheet, make sure you put in the recertification cost figure as this will be more expensive than a surveillance audit.

QUANTITATIVE BENEFITS - REVENUES

The objective of this section is to look at the potential increase in business that you would get by having ISO certification which you might get if you don't have it.

This section will be a guesstimate from you based on your knowledge of your business and the market it is in.

The first question asks roughly how many new customers you might get if you had ISO 27001. These customers might come to you for a number of reasons - for example, they might choose you over a competitor who isn't ISO certified.

Or it may mean that you can get on a suppliers list that you couldn't before. Or it could mean that doing so means you stand a better chance of winning a public sector tender, or a private sector contract, than you did before.

If you're looking to win tender business then it's undeniable that ISO certification is an important consideration when bidding for tenders with either central government[1] or local government[2].

Also, a British Standards Institute study found that 50.6% of businesses who get ISO certification attract new customers[3]

So try to be realistic - what would be the genuine increase in new customers that you think you might see with your chosen ISO, and what might a value on this be?

And with these new customers, what do you think your increased sales figures might look like? A Harvard Business School found that the adoption of ISO led to a 10% increase in sales[4]. Do you think that is about right, or would your figures be more or less?

[1] https://www.experian.co.uk/business-express/hub/wp-content/uploads/2018/03/The-Tendering-Process.pdf

[2] https://www.ukas.com/about/working-with-government/ukas-accreditation-a-tool-to-deliver-effective-local-authority-services/

[3] https://www.bsigroup.com/LocalFiles/en-GB/small-business/UK-SB-BSI-ISO-9001-Whitepaper-UK-EN.pdf

[4] https://pubsonline.informs.org/doi/pdf/10.1287/mnsc.1100.1159

COST SAVINGS (POTENTIAL)

Next we come on to the cost savings that you could realise from the introduction of ISO 27001.

Firstly, what do you think you might save by making yourself more efficient? The British Assessment Bureau has reported 76% of businesses saw improved efficiency[5]. What would be the effect year-on-year?

How about potential savings from improving the processes in your business? What would your estimation of these savings be? BSI found that 62.2% of businesses reported improvements in products or services after ISO certification[6].

Then how about making your company more productive (getting more out of the staff and equipment that you already have)? Ask yourself honestly, could you get more out of your business with a bit better organisation? What would you estimate the value of this to be? A study by the journal Production and Operations Management found a management system could increase productivity by up to 11%[7]. What would this mean year-on-year?

Then take a look at staff turnover. Having a better organised workforce with the morale brought by a proper management system will cut this down. The average cost of employee turnover, based on the average UK salary, is around £11,000 per person; a study the the Chartered Management Institute found that in a company introducing an ISO management system staff turnover fell from 44% to 1% over 10 years[8].

Finally, can you put a price on how much you would save by having less information security incidents each year? Statista puts the average cost of a cyber security breach in the United Kingdom is £1,410 across all businesses, however, this figure becomes greater as the size of a business increases[9].

[5] https://www.british-assessment.co.uk/services/iso-9001/

[6] https://www.bsigroup.com/LocalFiles/en-GB/small-business/UK-SB-BSI-ISO-9001-Whitepaper-UK-EN.pdf

[7] https://onlinelibrary.wiley.com/doi/abs/10.1111/poms.12000

[8] https://www.managers.org.uk/~/media/Files/PDF/Quality_Management_CQI_CMI_June2012.pdf

[9] https://www.statista.com/statistics/586788/average-cost-of-cyber-security-breaches-for-united-kingdom-uk-businesses/

OTHER BENEFITS

Finally, what are the other benefits that could come of getting ISO certification? These ones are a lot harder to quantify, but it's worth taking a look at them and trying to estimate an overall value, as some can actually be the key to the success of your business.

The first question asks you to estimate what value your business would get from having a consistency of service and performance. What kind of value could you put on this?

The next question asks you to place a value on having higher customer satisfaction levels. If you're in an industry where this is extremely important, what would be its estimated monetary value every year?

Next, if your company had better internal communication, which led to increased staff moral and better job satisfaction, what would be a year-on-year value to this?

Then there is the question of business image - if your company had the elevated image that comes with being ISO certified, could you put a price on this? BSI has found that 60.8% of ISO certified businesses reported an increase in trust in their business[10].

Finally, would having an improvement in your delivery times bring a big difference to your business? In monetary terms, what would this be?

[10] https://www.bsigroup.com/LocalFiles/en-GB/small-business/UK-SB-BSI-ISO-9001-Whitepaper-UK-EN.pdf

RESULTS AND CONCLUSION

After you've filled in all the costs and benefits, it's time to go to the final Tab on the spreadsheet - the Results Tab. This will have crunched all the numbers you've put in - all the costs at the top and all the benefits at the bottom, and will come out with either a Net Benefit or a Net Cost.

Depending on whether the figure is a positive or a minus will give you a solid indication of whether an ISO makes financial sense for your business.

The real value of this whole exercise is that it gives you a real indication of the costs AND the benefits. Obviously the benefits are not guaranteed, and it's your call as to how realistic and achievable they are - but taking a risk is what business is all about!

It's also worth reiterating that installing more than one standard from 9001, 14001 and/or 45001 doesn't mean that costs go up by a multiple (e.g. putting in two standards means costs double).

All of these standards operate to what's called 'Annex SL' - this means that there are many common elements between them all (for example, having to undertake a context analysis or a management review.

This means that if you're doing one standard, you don't need to replicate work for others. Therefore, a good rule of thumb is that costs go up only by around 50% per standard.

So, if you do one standard and the overall cost is, say, £5,000, then estimate on putting another £2,500 on top of this for two standards, then another £2,500 for another standard, so it would be £10,000 for all three.

You can also cut significant costs using our Threshold service if you want all of the benefits of a management system, but don't want to commit to what can be significant UKAS certification costs.

We really hope that this guide has been useful, and that it might form the start of an ISO journey for you - if it makes financial sense of course!

If you do, just remember that ISO Certification should be implemented in a practical way. This will ensure that Systems that are adopted improve the business and are not just a set of procedures that your employees will find hard to manage.

The Ideas Distillery

The Ideas Distillery
3B Westfield Road
Cardiff
CF14 1QQ

Tel: 029 2196 1066

Email: info@ideasdistillery.co.uk