AL PROJECT SECURITY GMBH

Why should you trust ISO 27001?

A survey into the state of trust between customers and service providers

Disclaimer

This survey relies on publicly available information that any interested party of the mentioned service providers may request and validate independently. Additional information by the service providers may be available when signing a Non-Disclosure Agreement (NDA). Such information is not used in this survey as it may violate an existing NDA. Information used for this survey may have changed between the initial analysis and the publication of the survey as every management system requires processes for continual improvement. Mentioning a certain service provider in this survey must not be understood as a recommendation for or against choosing a business relationship with the service provider. We tried to contact various service providers to verify our understanding, but in some cases, this may not have been successful, and this survey might draw inaccurate or outdated conclusions.

The information this survey looks at are only “the tip of the iceberg” since it covers parts of the mandatory documentation and processes of the management system. For example, a missing information security policy is a major nonconformity, but the service provider may still provide technically sound and secure services. The conclusion of such a situation is, that it is more difficult for customers to establish trust to the service providers.

AL PROJECT SECURITY GMBH

Table of contents

Introduction

Service providers and customers are working more closely together than ever, and supplier relationships have evolved into partnerships. Trust and specifically trust in information security are the foundation of every partnership. ISO/IEC 27001:2013 is the international standard to assure proper management of information security. Whenever ISO 27001 is mentioned it shall be understood as ISO/IEC 27001:2013.

This ISO 27001 survey documents that in many cases the claim "We are certified to ISO 27001" by service providers is insufficient to create a trust relationship as it is often misinterpreted or not even validated or challenged by customers. We are examining three theses regarding the meaningfulness of an ISO 27001 certification, identify common misinterpretations and provide recommendations that every organization should follow.

This survey assumes basic familiarity with the ISO 27001 standard and reading the standard is recommended.

Motivation

Why is this survey meaningful? There are basically two factors that must be understood by organizations (service providers and customers) relying on an ISO 27001 certification.

1. Understand the degrees of freedom of an ISO 27001 implementation for a service provider and
2. How the ISO 27001 certification process works and what it means

A good example is the automobile industry that created the *Trusted Information Security Assessment Exchange (TISAX)* to overcome these challenges. While the TISAX approach is not in scope of this survey it shows that the ISO 27001 certification requires clarification and some industries choose to narrow the scope to have less degrees of freedom.

ALPS – AL Project Security GmbH is focused on training, implementing and auditing Information Security Management Systems (ISMS). In our daily work we are assessing service providers on behalf of our customers and those providers are often certified according to ISO 27001. More than expected, assessments lead to nonconformities that should have been identified during ISO 27001 certification audits.

We started asking ourselves: **"Are those nonconformities individual issues or is there a general problem with ISO 27001 certifications?"**.

The approach of this survey is to request, collect and analyze information from a variety of ISO 27001 certified service providers from different sectors. An in-depth assessment of each service provider will not be possible, but we will assess a sufficient number of service providers regarding a specific subset of mandatory ISO 27001 documents.

The objective for this survey is to clarify: **Which possibilities does a company as a customer have to validate and assess an ISO 27001 certified service provider?**

General Information about ISO 27001

Understand the degrees of freedom of an ISO 27001 implementation.

Organizations can choose the scope of their ISO 27001 implementation to be limited to a specific scope that can include any number of:

- business processes
- products or services
- sites
- departments
- or any combination of the mentioned above

Example: An organization can choose to certify the development of a software tool in Australia and exclude any activities that are related to the operation of the tool in Great Britain. Our experience shows that most customers expect a certification to cover the whole scope of services at all sites. An ISO certificate does not ensure that the whole company is in scope of the certification.

How is the ISO 27001 certification structure organized?

The certification process for ISO 27001 is the same around the world and builds on trust through international contracts and treaties.

The root of trust is the *International Accreditation Forum* (IAF). Its rules and policies are applied by national accreditation bodies. Those national institutions grant accreditation to national certification bodies whose task is to grant certificates to individual organizations.

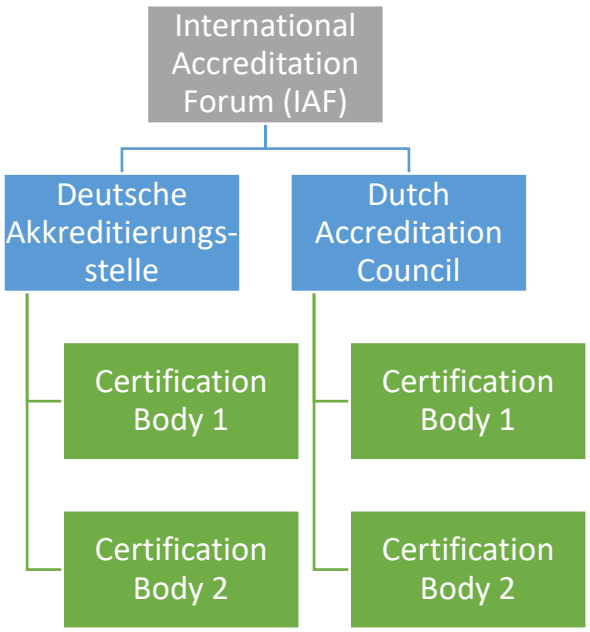

Figure 1: Example Certification Body Hierarchy

Theses

<u>Thesis 1:</u> The contact between customer and information security department is important

There must be a direct contact between the customer and the information security department of the service provider to exchange information about the certification scope to ensure that the certification covers the services procured by the customer. The responding personnel must be trained to answer requests correctly or involve additional personnel.

Note that the questions are listed in our checklist in the Annex.

<u>Thesis 2:</u> An ISO 27001 certification ensures that all 27001 requirements are implemented

The certificate can be related to a user product, process or service. The scope document lists the relevant services in scope and the information security policy explains which level of security the customer can expect.

Service providers should be aware of their duties that go along with the certification. The following documents should be available to interested parties:

- the ISO 27001 certificate
- Information Security policy
- Statement of Applicability (SoA) – not obligatory
- last audit report – not obligatory

Examples for interested parties are:

- (potential) customers
- service providers
- employees
- authorities

There is no requirement in ISO 27001 that requires the statement of applicability and the audit report to be shared with interested parties. We requested these documents since they are referred to on the certificate. As such, we consider these two documents as a part of the certificate. There are service providers that make these documents available in their compliance center without the customer requesting it.

<u>Thesis 3:</u> A certification body can be trusted. Therefore, customers can trust an ISO 27001 certificate

The service provider and certification body provide information that enhances the trust in the certification body.

A validation of the certificate shows that there is a trust chain (see figure 2 below) from the individual certificate of the service provider to the certification body, accreditation body and International Accreditation Forum (IAF).

Figure 2: Certification Chain of Trust

Methodology of the Survey

The methodology used for this survey covers both service providers as well as certification bodies.

The methodology used in this survey is based on our experience and knowledge of Information Security Management Systems.

Service Providers

We followed the same steps for each service provider:

1. **Select well known service providers** that have gained an ISO 27001 certification. Some of those service providers were already delivering services to our company while others have been asked to provide information about their ISO 27001 certification without an existing business relationship.
2. Request general ISO 27001 related information. This information **MUST** exist for any ISO 27001 certified organization and there are requirements to make this information available to interested parties. The following documents were requested by the service providers:
    a. The ISO 27001 **certificate (if not publicly available on the website)**
    b. The **scope** document as required by section 4.3 of ISO 27001:2013
    c. The **information security policy** as required by section 5.2 of ISO 27001:2013
    d. The latest valid **SoA** as required by section 6.1.3 d) of ISO 27001:2013 (customers can request it, but it must not be provided)
    e. The last **audit report** provided by the certification body (customers can request it, but it must not be provided).
3. Verify, analyze and assess the received documents regarding the three theses.
4. Clarify questions and validate our understanding of information security with the service provider.

It is important to understand that **we limited our clarification effort to only one call or e-mail** for each service provider as we want to assess the current state of the service providers and not train them on how such requests should be handled.

Assessed branches of service providers and number of employees are distributed among the following:

- Cloud Services: 4600 to 200.000
- Hosting: 200 to 10.000
- Telecommunication: 850 to 100.000
- Insurance: 1000 to 20.000
- Health Care: 200 to 500
- Tax Service: 15 to 7000
- Financial Service: 1500 to 3500
- Others: 15 to 500.000

Certification Bodies

The survey relies on certification bodies accredited by national authorities such as the *Deutsche Akkreditierungsstelle GmbH* (DAkkS). A certification body is a service provider to the customer that wants to be certified. As such, the customer must ensure that the certification body holds a valid accreditation by a relevant national authority (see figure 1).

We followed two steps to verify the trustworthiness of certification bodies:

1. **Select certification bodies** that have gained an ISO 27001 accreditation.
2. **Verify the accreditation on the website of the accreditation body.**

The following certification bodies are part of this survey, because they have issued certificates for service providers:

- BSI Assurance UK Limited, London, United Kingdom
- Datenschutz Cert GmbH, Bremen, Germany
- DEKRA Certifications GmbH, Stuttgart, Germany
- DQS GmbH, Frankfurt am Main, Germany
- Ernst & Young CertifyPoint, Amsterdam, The Netherlands
- Fox Certification, Stuttgart, Germany
- KPMG Cert GmbH, Köln, Germany
- PüG Prüf- und Überwachungsgesellschaft mbH, Gäufelden, Germany
- PricewaterhouseCoopers Certification B.V., Amsterdam, The Netherlands
- Schellmann& Company, Tampa, USA
- The Standards Institution of Israel, Tel Aviv, Israel
- TÜV Nord Cert GmbH, Essen, Germany
- TÜV Rheinland Cert, Köln, Germany
- TÜV SÜD Management Service GmbH, München, Germany

Survey Results

The survey provides evidence to validate or invalidate a thesis. We approached each topic based on the quantity of replies as well as the quality of the provided information. For each thesis we present the relevant evidence and provide a conclusion.

Theses 1: The contact between customer and information security department is important

Evidence 1: No contact person visible

56% of the queried service providers provided a dedicated contact point for information security inquiries. The other 44% had to be contacted through other channels such as general information helpdesk, sales contacts or the data protection department. The main contact channel was by e-mail – and the contact form often lead to an e-mail response from the service provider.

The main response came back by e-mail while some service providers immediately called us to better understand our request. A total of 25% did not respond to our request at all. There were two exotic responses by written letters which came back weeks after the initial request.

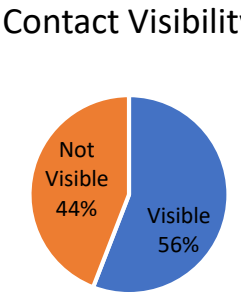

Figure 3: Contact Visibility and Used Contact Channels

Evidence 2: Lack of knowledge

Using the non-information security channels often leads to a dead end or the delivery of incorrect or incomplete information. There were several occasions where the information security requests were answered by personnel from the data protection office. Information that must be provided (see thesis 2) was not provided because of a lack of knowledge from the data protection personnel.

The second situation we frequently encountered was that sales personnel informed us that we first must procure the service to be entitled to receive information about information security. For some service providers we did not get the requested information even though there is an active business relationship.

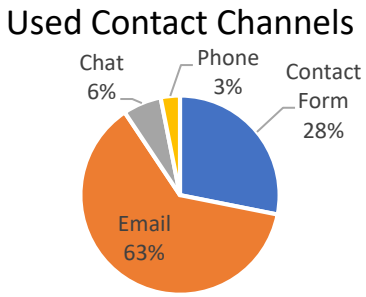

Figure 4: Used Contact Channels

Evidence 3: Responsiveness

The responsiveness of service providers was very different – we experienced anything between immediate feedback on the same day and weeks of silence with a late response four weeks later or no response at all.

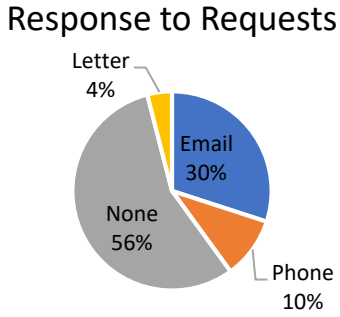

Figure 5: Response to requests

Conclusion Thesis 1

Our survey shows that the *General Data Protection Regulation (GDPR)* ensures that most service providers have a dedicated contact for all data privacy requests but does not have the same for information security requests.

The data protection contact persons or departments may be capable and trained to deal with requests related to the GDPR but do not know how to deal correctly with information security requests as required by ISO 27001. There seems to be a lack of internal communication between information security and data protection.

Certification bodies do not seem to verify that there is a contact possibility and a process for dealing with information security requests from customers.

As a rule of thumb, we learned that there is either a response within a week after the request or no usable response at all. Responses that take longer than a week usually lead to requested information not being provided.

Thesis 2: An ISO 27001 certification ensures that all 27001 requirements are implemented

Evidence 1: Information Security policy is not provided

ISO 27001:2013 states in clause 5.2 e) that *the information security policy shall*

- ***be available as documented information***

and states in clause 5.2 g) that it shall

- ***be available to interested parties, as appropriate.***

As pictured below, only 6% of the contacted service providers provided an information security policy.

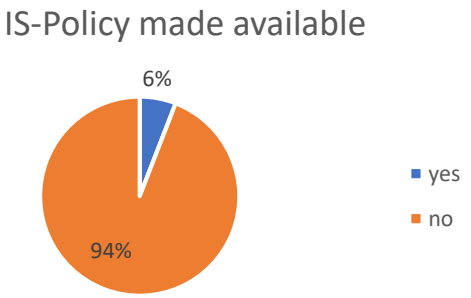

Figure 6: IS-Policy made available

Evidence 2: Statement of Applicability is not provided

ISO 27001:2013 states in clause 6.1.3 d) that the ***organization shall define and apply an information security risk treatment process to:***

- ***Produce a Statement of Applicability that (…)***

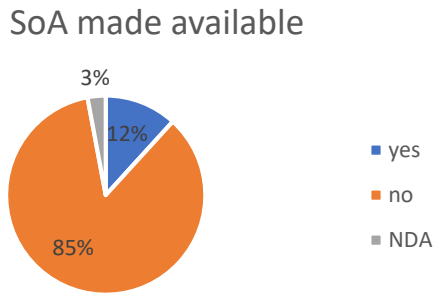

Figure 7: Statement of Applicability made available

The SoA was provided by 12% of the contacted service providers. When conducting a review of the SoA against 27001 requirements, only one of the four provided SoAs complied with all ISO 27001 requirements.

Conclusion Thesis 2

The certificate alone is insufficient without the information security policy. The main reason is that you cannot know which processes, services or products the service provider wants to secure or if this fits to your requirements. It is necessary to get the certificate AND the information security policy to determine that the requirements of your organization will be fulfilled. In most cases the information security policy was not provided to us. To our surprise we received the SoA document more often than the information security policy.

The quality of the provided documents is often not compliant with the ISO 27001 requirements. A common example for a nonconformity is the SoA document where there is no justification provided for excluding a control.

Example: The control A.6.2.2 "Teleworking"[1] is excluded from the certification and there is no justification recorded stating that "Employees do not have a permanent teleworking place, furnished by the company, at home".

A frequent nonconformity for the information security policy is the lack of security objectives which means to interconnect business and information security strategy. During our survey we only received two information security policies. One policy completely lacked the definition of security objectives while the other described a framework in which the security objectives are defined.

These examples of nonconformities do not mean that there is a security risk, but it shows that even simple nonconformities are not identified by service providers, internal audits or certification bodies.

[1] The control A.6.2.1 covers remote working from any location with a mobile device which is used by most organizations. Teleworking is a workplace, furnished by the organization, at the home of an employee.

Thesis 3: A certification body can be trusted. Therefore, customers can trust an ISO 27001 certificate

The service provider as well as the certification body can provide information that enhance the trust in the certification body.

Evidence 1: Validation Results

Each ISO 27001 certificate was validated by us using the checklist in the Annex of this survey. Each certificate could be successfully validated and thus we did not discover an invalid certificate.

In a single case a certification body website could not validate a certificate and claimed it was “unknown” to the certification body. We called the certification body and found out that they forgot to add the certificate to the system. One day later the certificate was available on the website and could be validated.

In another case the validation system of the certification body provided us with a copy of the certificate that had a different scope than the certificate provided by the service provider. We could not clarify which certificate is the valid one.

In several instances we received a certificate and additional document where the referenced documents of the certificate differ from the ones we received. For example, the certificate may reference SoA version 1.0 and the SoA we received was a newer revision 2.0.

Evidence 2: Accredited Certification Bodies

During the survey we discovered **14 different certification bodies.** All of those are accredited with one of the following three accreditation bodies:

- *Deutsche Akkreditierungsstelle* (Dakks); https://www.dakks.de/
- *ANSI-ASQ National Accreditation Board* (ANAB); https://www.anab.org/
- *Dutch Accreditation Council* (RVA); https://www.rva.nl/en/

There was no certification body that is a “black sheep” without accreditation. All accreditation bodies are members of the IAF.

Note: You can see all certification bodies on the website of the accreditation body.

Conclusion Thesis 3

The conclusion for this part of the survey is: the trust chain works and thus ISO 27001 certificates can be trusted regarding the formal processes and treaties behind them.

The 14 certification bodies discovered during the survey show us, that there is a wide variety and competition of active certification bodies.

The validation of all individual certificates took more time than expected because every certification body uses a different system with different inputs, outputs and processes. Some certification bodies do

not provide a validation tool on their website and require manual interaction. There are no statistics how often the certificate validation services are used by customers.

We found out that all certification bodies mentioned in this survey are accredited by only three accreditation bodies. We expected more accreditation bodies – for example the UKs *National Accreditation Body* (UKAS). The *British Standards Institute* is not accredited by the UKAS but the ANAB.

Conclusion of the Survey

On the one hand, the survey found evidence that ISO 27001 is a good approach to define common ground between service providers and customers to establish a trust relationship. On the other hand, there are different issues regarding the validation of ISO 27001 certifications that surprised us.

Customers and service providers must establish a better understanding about the ISO 27001 certification process and challenge each other. In our opinion, there is also room for improvement for the certification bodies and national accreditation authorities. The following examples show good possibilities to improve the validation process of certificates.

Example 1: Compliance Center

There are several service providers that offer a compliance center where potential customers or existing customers can find information regarding certifications. Examples for these are SAP, Amazon Web Services or Microsoft Azure. The information served in these centers varies between service providers and most do not provide a possibility to request missing information. The information provided in the compliance centers often goes beyond the requirements of ISO 27001. In some cases, documents to be shared with customers according to ISO 27001 are not present.

Example 2: Certification Body Validation

When verifying certificates with certification bodies we used online services provided for example by TÜV Rheinland, TÜV Süd, DQS or the BSI. Some certification bodies do not offer these kinds of online services and thus certificates must be validated by phone or e-mail.

When validating individual certificates, we noticed that some information was not matching. For example:

- Difference in scope description on the certificate and online service result. Which scope is correct?
- Validation information was not helpful such as “certificate first issued 2014” – this information does not help us to determine if the certificate is still valid.

Glossary

Term	Definition
Accreditation Body	An accreditation body is an organization delegated to make decisions, on behalf of the higher education sector, about the status, legitimacy or appropriateness of an institution, or programme.
ANSI-ASQ National Accreditation Board (ANAB)	ANSI-ASQ National Accreditation Board (ANAB) is a US-based non-governmental standards organization known for providing ISO accreditation services to manufacturers, laboratories and other public and privately held organizations/ companies. ANAB is an underwriter for the International Accreditation Forum (IAF) and the International Laboratory Accreditation Cooperation (ILAC) providing documentations recognized by government agencies from a number of participating nations. The American National Standards Institute (ANSI) and the American Society for Quality (ASQ) jointly own ANAB.
Certification Body	An accredited registrar, also called an accredited certification body (CB), is an organization accredited by a recognized accrediting body for its competence to audit and issue certification confirming that an organization meets the requirements of a standard.
Deutsche Akkreditierungsstelle (DAkkS)	The Deutsche Akkreditierungsstelle (DAkkS) is the national accreditation body of the Federal Republic of Germany located in Berlin.
Dutch Accreditation Council	The Dutch Accreditation Council (RvA) is the only accreditation organization in the Netherlands working in the public field.
Information Security Management System (ISMS)	An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.
International Accreditation Forum (IAF)	The IAF is the world association of Conformity Assessment Accreditation Bodies and other bodies interested in conformity assessment in the fields of management systems, products, services, personnel and other similar programmes of conformity assessment. Its primary function is to develop a single worldwide program of conformity assessment which reduces risk for business and its customers by assuring them that accredited certificates may be relied upon. Accreditation assures users of the competence and impartiality of the body accredited.
Nonconformity	Non-fulfilment of a requirement of ISO 27001:2013
Non-Disclosure Agreement (NDA)	A non-disclosure agreement (NDA) is a legal contract between two or more parties that signifies a confidential relationship exists between them. The confidential relationship exists because the parties share information among themselves that should not be made available to any other parties outside of those involved, such as competitors or the public.
Trusted Information Security Assessment Exchange (TISAX)	TISAX enables mutual acceptance of Information Security Assessments in the automotive industry and provides a common assessment and exchange mechanism. Assessment results always remain under control of the assessed companies

Annex

Checklist to Verify ISO/IEC 27001:2013 Certification of Service Providers

There are many service providers who advertise their services with an ISO 27001 certificate. We raise the question*: "How will you ensure that the certification is justified and matches your requirements? "*

We want to show you our way to proof the most important preconditions of the certification to ISO/IEC 27001:2013.

Step 1: Check if a Certification Exists

You want to know if a service provider is certified according to ISO/IEC 27001:2013. You have the following options:

- Use a search engine (Google, Bing or similar)
- Search the website of the service provider
- Send a request directly to the service provider

Step 2: Requesting Additional Information

Now that you know that the service provider is certified according to ISO/IEC 27001:2013 the next question will be: *„What are the criteria to proof the trustworthiness of the certificate? ".*

	Question	Explanation
2.1	Which **service/process/product** of the service provider is certified?	Verify the **Scope** on the certificate and compare it to the services/processes / products you are procuring.
2.2	Is the certificate **available on the website** of the organization or do you have to send a request?	Some service providers such as Cloud service providers offer this information online.
2.3	Which **further information** should be requested?	Further requirements which should be available to interested parties are (ISO 27001:2013 chapters in brackets): • the **Scope of the ISMS** (4.3) • **Information security policy** (5.2) • the latest valid **Statement of Applicability** (SoA) (6.1.3d) (no obligation) • the last **audit report** (no obligation)
2.4	Is there a **dedicated department** for information security subjects? Is a **contact** (person) mentioned?	A specific contact makes it easier for you to retrieve the information. Sales or marketing personnel will not be able to answer your questions.

Step 3: Validating the Certificate

When you received the certificate, you can use the following questions to validate it:

	Question	Explanation
3.1	Is the **name of the company** correct?	The correct name of the company must be written on the certificate.
3.2	Is the **Scope** of the certification defined?	The scope must describe which service/process/product of the company has been certified.
3.3	Which **site** is in scope of the certification	Does the service provider provide its services to you from a site which is in scope of the certification?
3.4	Is the **Statement of Applicability (SoA)** with date and version available?	The SoA version requested in step 2.3 must match the one on the certificate.
3.5	Is the **certification body** named with address?	Ensure that the certification body is visible on the certificate.
3.6	Is the **accreditation body** named?	Check if the certifier is accredited by an accreditation agency.
3.7	Is the certification **valid** and how long?	Ensure that the certificate is not expired or will expire soon.
3.8	Is the **certification number** available?	Each certificate has a unique number which you can check on the certification body's website.
3.9	Is the certificate **signed** by the certification body?	Each certificate must be signed by the certification body representative.

If there are any questions, please feel free to contact us! – We are looking forward to your request!
Contact us at *info@alps-gmbh.de*

Your ALPS-Experts-Team

About ALPS GmbH

ALPS – AL Project Security GmbH (ALPS) is a consultancy based in Munich and provides implementation, auditing and training for management systems.

The detailed portfolio of ALPS includes the following services:

- **Training**
  - Training regarding „Auditing of management systems “
  - Training regarding „Implementation of management systems “
  - Security-Awareness Training

- **Implementation of Management Systems**
  - ISO 27001, ISO 22301, IEC 62443-4-1, ISO 13485

- **Audit**
  - Preparation and observation of internal or certification audits
  - Planning and execution of internal audits

- **Topic Specific Services**
  - Supervision of projects from the information security perspective
  - External ISMS Manager
  - External ISO (Information Security Officer)
  - Providing templates for all obligatory documents regarding ISO 27001

ALPS has experience in different industries including insurance, IT-Service, automotive and aviation. Our employees have at least 5 years of working experience and receive continual training and education.