TRUST IN THE CLOUD

WHITE PAPER

ONLINE TRUST COALITIE

02-2021 White paper

CONTENTS

WHITE PAPER

Introduction

At the initiative of the Ministry of Economic Affairs and Climate, the Online Trust Coalition (OTC) was set up, uniting more than twenty organisations from government, industry and science. OTC's purpose, as set out in the September 2020 manifesto, is to explore, develop and make available more unambiguous, more efficient and accessible methods that let cloud service providers demonstrate that their services are reliable and secure and support the validation process of the users or customers of a cloud service (whether direct or indirect – hereinafter simply referred to as "purchasers").

The OTC focuses on the way in which trust is offered, requested, supplied and substantiated, rather than on the measures to control information security or continuity of services and data.

In this white paper, the OTC describes a number of actions that contribute to demonstrating the reliability and security of cloud services. This helps to increase trust in the cloud. These actions are aimed at all stakeholders, based on the conviction that a reliable and secure cloud is a joint responsibility. The intention is that the actions included in this white paper will be adopted, in the conviction that this approach will let the Netherlands play a leading role in this field that will then be adopted in the rest of Europe.

Reading guide

The white paper is structured as follows. First, the nature of the problem of trust in cloud services is introduced. The approach in this white paper centres on a distinction between trust, reliability and assurance. Each of these concepts is related to a number of shortcomings. In the final section, six actions have been formulated for addressing these shortcomings.

1. Trust in cloud services

It is impossible to imagine life today without the cloud. The cloud plays an important role in our daily activities, in companies, in digital innovations and in addressing the major social issues that society is facing.

What is the cloud?

The OTC uses the following definition for cloud services:

"Cloud services are an aggregate of IT resources, processes and organisational structures that facilitate remote access to physical or virtual IT resources through a network, so that the use of these resources is scalable and flexible with "self-service" delivery and on-demand administration."

In simpler terms: instead of having your own computer centre with your own computers, peripherals, software and administrators who keep things running, you use computer centres, computers, peripherals and software administered by others. These resources can be used when you need them, in the form of services ("as a Service"). Access to those computer centres etc. is usually via the Internet; sometimes you do not even know where those computer centres etc. are physically located.

Continuous growth and specialisation mean that cloud services are in practice almost always a combination of other cloud services from various providers. A big advantage of the cloud is scalability. You pay for what you use. If you need more capacity (temporarily), you can get it without structural investments. Another advantage is that you can always access your data and applications as long as there is access to a network (usually the internet), so you can continue to do your work wherever you are and with whatever device you are using (PC, laptop, tablet, mobile phone). In addition, cloud service providers make things a lot easier: they ensure, for example, that the service availability is kept at the optimum and that your data is safe. Making life easier is one of the reasons why using cloud services has become so popular.

The issue of trust in the cloud

However, there are also drawbacks. Because you are outsourcing the management of your IT to third parties, you become dependent on them. You do not always know where your data is physically located and who has access to it. This raises a number of issues, such as:

- What happens to my data and applications if something happens to the provider? Will I be able to continue to work? Will my data still be accessible?
- Who can look at my data besides me? The provider promises me that I am the only one who can access my data, but is that true? What legislation applies to the privacy and protection of my data? Can authorities demand access to my data from the provider?
- Can the provider change my software without my approval?
- If I want to switch providers, will my old provider cooperate and transfer my data? Will I still have access to old data?
- Does the service I purchase comply with the laws and regulations that apply to me? Can I demonstrate this at all times?

- How safe am I when it comes to cyberattacks?
- What should or can I do, as a customer, to achieve the promised safety and reliability?
- What about responsibilities and liability if providers fail to deliver on their promises?

This list is far from complete. The questions are fairly generic and play a role in most cloud services.

Cloud services behave differently with regard to responsibility, liability, direction and control than traditional outsourcing. In traditional outsourcing relations, there is always a party with (ultimate) responsibility. This party determines the risks and control measures and implements the measures. That works well. The responsible party sets requirements for contractors lower down the chain. Control over outsourcing is traditionally top-down, by a single responsible party.

Cloud services, on the other hand, are generic - that is the essence of the cloud business model. Individual purchasers of a cloud service do not decide on functionality, risks and the associated regimes: that is the cloud service providers' job. Service providers decide on the basis of their own generic risk models, choosing their control regimes and frameworks of standards. Although cloud service providers do this with a keen eye on the intended users, they do not differentiate between measures for individual purchasers.

The consequence of the cloud business model is that the purchasers of cloud services only have limited influence on how the provider organises its service. All they can do is assess whether the provider's generic regime suits the intended use. As a result, the purchaser has to trust that the information presented by the cloud provider about the risks and control measures is available, understandable, accessible and correct. In addition, the purchaser has to trust that the measures are sufficiently effective in practice. After all, if there are gaps or inaccuracies in these measures, it is the purchaser rather than the cloud provider who is the one held directly accountable by the end users, shareholders and supervisory bodies, even though the purchaser has no means of intervening directly if problems arise.

This tension between the business model of cloud services and the needs of the various stakeholders (purchaser, end users, shareholders and supervisory bodies) is intensifying all the time because of public attention to data protection and resilience of online services. The reliability of the cloud is thereby also becoming society's responsibility.

Finally, providers play an important role in the reliability and security of cloud services. This does not change the fact that purchasers also have a responsibility. For example, purchasers must verify whether the cloud service is suitable for the purpose for which they will use it. In summary: society's increasing dependence on the cloud reinforces the tension between the cloud's business model (offering many parties the same service, at small margins) and trust: the need for assurance that a service meets the requirements of users and society.

The participants in the Online Trust Coalition have noted that it is not easy for purchasers to set requirements and to get answers to their questions. The provider does not have sufficient options to give simple answers to those questions and generate trust: provide assurance of reliability.

In the following sections, we will discuss the question of what trust and reliability are.

The nature of trust in cloud services

As explained in the previous sections, using cloud services means we have in practice outsourced the management of our information systems on the grand scale. We process our data in places that we do not know the physical locations of and without knowing who can access them. We share the IT infrastructure with potentially millions of others. Our personal data is processed and stored by parties that we are sometimes not aware of. We do this, trusting that all parties involved adhere to laws and regulations and undertake to abide by specific agreements. Without that trust, the use of cloud services in our digital society would not be as extensive as it is today. Trust is therefore crucial for the use of cloud services, both now and in the future. It is therefore important for cloud service providers to be able to demonstrate that their services can be trusted. It is important for users that they can easily obtain that evidence and that it is understandable.

To help the consumers and providers of a cloud service establish mutual trust, we have made a distinction in this white paper between trust, reliability and assurance.

The goal of this white paper is to build up trust in cloud services.

*A consumer will **trust** a cloud service if they can assume with sufficient certainty that the cloud service is reliable.*[1]

But how do you gain trust in cloud services? The basis for trust is a reliable service: a service that lives up to promises and agreements and complies with laws and regulations. This trust is strengthened when certainty is given, i.e. assurance is provided. An important aspect of providing assurance is communication.

1 **Trust** is "hoping with certainty". https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/VERTROUWEN. Consulted 10.11.2020

2. Reliability

Using cloud services means we are entrusting them with the processing of our personal, medical, financial and business data and intellectual property, expecting that they will act responsibly.

Cloud services are essential for our daily functioning and for digital innovations. Cloud services can only play this vital role in society if they are secure, reliable and comply with laws and regulations.

Generic or specific?

At first glance, every situation seems to be one of a kind, and no two companies are the same. However, a closer look shows that there are generic requirements or criteria relating to the reliability of basically every cloud service. These are, for example, accuracy, completeness, confidentiality, timeliness and security. For specific application areas and users, additional requirements or criteria can be formulated for demonstrating the suitability of the cloud service for those specific application areas or target groups. If providers proactively prove a cloud service is suitable, purchasers of a service do not need to set any requirements (or maybe just a few).

Accountability information

The purchasers of a cloud service have to trust the reliability of the cloud service. This is an important condition for using or adopting cloud services. In many cases, especially in private use, this trust is based on the provider's reputation, previous experience and commercial communications.

---

*A cloud service is **reliable** if it complies both with the agreements made between provider and customer, and with general and specific quality requirements for a cloud service, and if it is fit for compliance with relevant laws and regulations..*

Certainty that a cloud service is reliable (i.e. assurance about reliability) is required for other applications too, often professional ones. This also applies to aspects that have an explicit social interest and are therefore subject to supervision. This is the case, for example, with personal data protection. Assurance is now a relative concept. There is no such thing as absolute assurance about the reliability of cloud services. However, an assurance service can provide a certain degree of certainty. This is important if users have to account for the reliability of the cloud service they use. This is the case, for example, if an accountant or auditor makes inquiries about a cloud service when auditing the annual accounts. To provide assurance about the reliability, the provider gives accountability information. The information may be backed by confirmation from a third party such as a certification body that has issued a certificate or certification mark.

Liability

Liability is closely linked to assurance. What happens if the certainties offered turn out not to be so certain in practice? Who is liable for damage?

This issue often leads to a game of cat and mouse between providers and purchasers of cloud services (though this is certainly not unique to cloud services). The greater the disparity in power and size between parties, the easier it will be for the larger party to pass the consequences of non-compliance onto the smaller party. As to the privacy aspect, and therefore also information security and data availability, the legislator puts responsibility largely at the top of the chain: the purchaser of a service. Nevertheless, processors within the chain also bear responsibility.

The cloud industry does not yet have standardised or legal models for chain liability. There are also no standard models for the division of responsibilities yet. There is still little development in the field of insurance to cover damage during crises.

3. Assurance

Trust in a cloud service requires reliability first, as explained in the previous section. This section examines the second important aspect of trust: assurance, providing certainty about reliability. How can providers of cloud services provide certainty (assurance) that a cloud service actually meets the requirements (e.g. in terms of quality) of the purchaser, end user and legislator?

*There is **assurance** about the degree of reliability of a cloud service if the customer and other stakeholders are convinced that the measures guaranteeing reliability are effective according to the current state of the art.*

Four methods can be distinguished for obtaining assurance about the reliability: assurance, certification, self-declaration and investigation by the user. The end of the section gives an overview of the various ways in which assurance is given.

Assurance

One term that is very often used when it comes to providing certainty is the concept of “assurance” as used by accountants and IT auditors. There is a lot of confusion about the concept of assurance in daily life. Assurance is often conflated with “insurance”. In the context of cloud services, it is about offering certainty that a cloud service meets the set requirements. That a cloud service meets the specified requirements is determined by an independent third party with the right expertise, often referred to as “auditor”. The auditor carries out research (called an audit or conformity assessment) to determine that the requirements (in that case referred to as ‘criteria’) are met.

In the financial world, the concept of “assurance” is well known. Accountants and auditors who audit the financial statements or internal control processes of organisations use globally recognised assurance standards (International Standards on Assurance Engagements, ISAE). Assurance reports are then used to account for internal control over a period of time. Well-known types of assurance reports are ISAE 3000, ISAE 3402, SOC 1 and SOC 2. Many large cloud service providers have such reports. Assurance reports contain detailed information about the framework of standards used (the criteria), the method of testing and the findings. The reports are intended for a limited target group and may not be redistributed.

In everyday speech, the assurance audit is often referred to as ‘third-party assessment’.

ISO certification

Another way to provide assurance to users is by means of an ISO certificate. ISO is the International Organization for Standardization, which sets norms and standards for companies and organisations worldwide. In the Netherlands, the Netherlands Standardization Institute NEN manages the worldwide standards. ISO contains a very large number of standards for a very wide range of management systems, products, processes and services. There are currently more than 23,000 standards. That makes ISO quite confusing. The best known ISO standard is ISO 9001 quality management standard. However, there are also relevant standards for cloud services, such as ISO 27001, 27002, 27017 and 27018 (information security), ISO 27701 (privacy information management) and ISO 19086 (information technology, cloud computing and SLA framework). It should be noted that these standards only relate to the cloud provider’s management system and not to the cloud service itself.

ISO is a form of certification: a certificate is issued stating that a cloud service or service provider (depending on the type of certificate) complies with the relevant public or other standard. The user will not receive detailed information about the findings.

In everyday speech the ISO audit is often referred to as a 'third-party assessment'.

Self-assessment

Third-party assessment has advantages and disadvantages. The main advantage is that the independence and expertise of the auditor means that more confidence is can generally be derived from a certificate, for example. The main disadvantages are the generally high costs and long lead times. For simple and non-critical services in particular, providers often attempt to meet the demand for assurance through self-assessment. However, this only makes sense if the provider uses accepted methods to determine conformity and provides full transparency about the findings. A self-assessment will also have less value in legal proceedings than an assurance audit performed by third parties. After a self-assessment, the provider of cloud services declares that the services meet certain criteria, using a "Statement of Conformity".

Studies by users

Some laws, regulations and supervisors require users of cloud services in certain sectors to conduct their own investigations with their provider into the reliability of the services offered. An example of this is De Nederlandsche Bank. This can be a major burden for both the user and the provider, which is why banks generally work together and implement this requirement by means of a joint audit.

Choosing the appropriate method

The methods listed for obtaining assurance about the reliability of a service differ on a number of points:

1. **Who does the research:** an independent expert (assurance, ISO certification), the provider themselves (self-assessment) or the user? Given the complexity of cloud services, such studies often require the collaboration of investigators with various areas of expertise and knowledge. A clear picture of the composition and experience of the investigating team is therefore important if estimating the value of the research results is to be possible.

2. **What is being examined:** is it the organisation of the service provider that is being examined (ISO certification) or the service offered (assurance)? A service often requires involvement of various service providers and organisations.

3. What is the **framework of standards** (the criteria) against which the service provider or service has been assessed? Does that framework of standards include the wishes and requirements of the purchaser of the service or is there a generic framework of standards, or a framework of standards that the provider has drawn up itself? Does the framework of standards include legislation and regulations? Have general quality criteria been properly taken into account?

4. Is **the effectiveness (operation)** of the technical and organisational measures being investigated or merely the fact that they are present?

5. Do the **conclusions** of the research relate purely to the past or do they also make statements about the future?

6. Is there a report that shows the **risk considerations** of the provider in complying with the framework of standards (assurance) or is there an opinion (for example yes or no) about reliability (certification)?

One of the OTC's action points is that purchasers of cloud services must be given much more guidance about what assurances they can derive from the various conformity assessments.

A complicating factor is that purchasers of cloud services, as well as other stakeholders such as regulatory bodies, have difficulty giving a uniform definition of the evidence they need for saying whether the cloud service is sufficiently reliable. One of the OTC's proposed actions is harmonising the methods of providing assurance and offering guidance.

For private purchasers of cloud services, it is often sufficient to receive general information from the cloud service provider about reliability and the assurance it offers. Combined with publicly available information about the reputation of the provider, this is sufficient. Business users need information about the quality of the provider's processes and systems, detailed accountability information and third-party assurance such as a quality mark.

Professional purchasers often want specific information according to a method of their choice, requiring the provider to provide customised assurance. As a result, the provider's communication must also be customised, aimed at that one user with specific requirements regarding the reliability of the cloud service.

One of OTC's action points is that providers must be able to organise their reports and communication about reliability in a scalable way. This is in line with their core business: a single set-up that can then be provided to everyone. Standardisation offers a solution. Standards allow assurance to be offered in advance at various levels and communication can be set up accordingly. A provider then has a method for providing assurance that becomes just as standard as the provision of the cloud service itself. For the purchasers of a cloud service, obtaining assurance becomes just as easy as purchasing the cloud service.

Providing assurance at several levels thus becomes part of the cloud service. Providers can therefore include the costs in the fee they ask for a cloud service. The more assurance, the higher the fee. Every purchaser of a cloud service pays for the assurance is required. Arranging this collectively keeps the fee per user down.

The question of reliability and assurance of a cloud service cannot be answered without considering the responsibilities that purchases of cloud services and end users have when they use cloud services. This requires communication as well, and the recipient of the service may also have to have an independent investigation carried out to see whether they are taking that responsibility correctly; whether the technology and organisation are properly set up.

4. Practical case: a hospital

A hospital wants to store its patient data in the cloud. This is subject to strict security requirements. For example, NEN 7510 provides guidelines and principles for determining, setting and enforcing the measures that a healthcare organisation must take to protect the information system.

Many customers require cloud service providers to demonstrably comply with ISO 27001 and ISO 27002. Suppliers often already have various certifications such as NEN 7510.

However, in this case there are exceptional circumstances: the hospital is treating vulnerable groups and special individual cases.

The problem is that in the current situation, the hospital itself has to determine whether the provider's certifications are adequate in this particular situation. Detailed knowledge is required if you are to determine to what extent those certifications provide assurance about the overall reliability of the cloud service and about the effectiveness of the additional measures taken.

In this case, the hospital discovers that these requirements are not sufficiently covered by the generic quality requirements and laws and regulations for healthcare.

The hospital must then indicate to the provider what additional requirements are imposed on the cloud service. Any existing or potential provider must make an analysis and demonstrate how the service meets these additional requirements, and the hospital in turn must interpret this analysis and conclude whether the cloud service is compliant or not. In addition, there is the question of whether the additional measures taken by the provider are effective. The point here is that the hospital wants to know whether it can trust the cloud service concerned.

The OTC intends to develop support tools that help the user formulate requirements for the cloud service and analyse the accountability information supplied by the provider. The OTC also plans to develop security support tools so that providers can provide assurance to users.

5. Actions for reliable and secure cloud services

Cloud services do not stand alone. They consist of chains of services that are often offered by different providers. A provider of a SaaS service (software as a service, available in the cloud) will almost always use third-party hosting and platform services. A SaaS service is often supplemented with managed services (e.g. outsourcing of maintenance to SaaS solutions). These services must work well together in order to deliver a reliable and secure SaaS service in the end. To achieve this, the components of the cloud services must be largely standardised and harmonised. This also goes for the reliability requirements set for a cloud service and the evidence to be provided that the cloud service is reliable.

In this context, the OTC's aim is "to explore, develop and make available more unambiguous, more efficient and accessible methods by which providers of cloud services can demonstrate that their services are reliable and secure and support the validation process of the customers"[2].

The OTC wants to take action on the most important bottlenecks; the bottlenecks and associated actions are listed below.

Action point 1: comparability of certifications and frameworks of standards for reliability and for providing assurance

The sections on reliability and security show that a major bottleneck for the reliability of cloud services is the multitude of requirements that are imposed on e.g. information technology, cybersecurity and privacy. There is hardly any cooperation between parties on formulating these requirements, but a comparison of frameworks of standards from various certification schemes shows that the standards used overlap to a large extent.

The Online Trust Coalition therefore plans to conduct an analysis of existing certifications and frameworks of standards for reliable cloud services. We want to establish a generally applicable framework of standards so that standardisation and harmonisation of cloud services becomes possible. Standardised additions are then possible with additional requirements for specific applications in certain business sectors.

The intention is to build up the assurance levels for cloud services in a modular way so that assurance can be quickly and easily provided for each level using standardised modules. As a result, providers of cloud services no longer have to offer customised reliability and assurance statements for individual purchasers of their services. The reliability of cloud services then becomes transparent, allowing purchasers to make an informed decision about which cloud service to choose. An additional advantage is that this method involves lower costs.

Action point 2: Guidance for purchasers of cloud services.

Purchasers of cloud services are outsourcing part of their IT and therefore becoming dependent on their provider. Users often do not know what requirements they should set and what requirements a cloud service meets (see the section on reliability). A clear example of this occurs with the termination of a cloud service. If an IT application is managed in-house, the application and the data processed and stored within it will generally still be available to the user after the lifecycle has ended. This is not a matter of course when a cloud service is terminated. Agreements will have to be made with the provider about the conditions under which data will remain available. Many providers have standard solutions for this. Another example of dependence occurs when one of the providers in the chain of cloud services stops providing services. The measures that the purchaser of a service has to take are fundamentally different from when the IT resources are under their own management. A final example of dependence is the cooperation required from the provider when switching to another

2 https://ecp.nl/wp-content/uploads/2020/09/Online-Trust-Coalitie-Manifest.pdf

cloud service. If a provider does not want to cooperate, there is a risk of a “vendor lock-in”.

The Online Trust Coalition will develop guidance for purchasers of cloud services, in consultation with providers, users and sector organisations, listing items that are important when choosing a cloud service and provider.

Action point 3: Rules for the cloud

It is important for potential purchasers of cloud services that providers promise that their services are reliable, that communication about reliability is correct and that providers cooperate in providing the desired degree of assurance about reliability. At the same time, providers should be able to expect that purchasers of services will use the service in a way that does not harm the provider’s efforts to ensure a reliable service. The previous sections highlighted the need for guidance – currently not available – on the interaction between the provider and purchaser of cloud services.

The Online Trust Coalition will work in consultation with providers, sector organisations and user representatives on developing “rules for the cloud”. This will explicitly link up with the code of conduct (Cloud Rule Book) for Gaia-X.

Action point 4: Monitoring

There is a great diversity of solutions providing assurance about the reliability of a cloud service. One characteristic of all these solutions is that they look back at the past. Moreover, they take the organisation and the internal management procedures surrounding technology into account, while hardly looking at technology itself.

A number of OTC participants will investigate possible innovative methods for demonstrating the reliability of cloud services. These could e.g. use technology for conducting assessments and audits, and real-time monitoring of the reliable operation of cloud services.

Action point 5: Standardization of accountability information

As concluded in the section on assurance, one of the main bottlenecks around the provision of assurance by the provider of a cloud service to the purchaser of the service is the lack of harmonised communication about the reliability of cloud services and the provision of assurance. Different forms of legislation and regulations require different forms of conformity investigations, accountability reports, certificates and the like. Each form has its own protocols and way of fleshing them out. It is very time-consuming and costly for providers – and especially for SMEs – to provide accountability through all these different forms. Harmonisation is therefore desirable.

The Online Trust Coalition wants to reduce the diversity in reporting forms on the reliability and security of cloud services to standardised accountability information for users and auditors of regulatory bodies. The standards for these reports are based on existing legislation and regulations and will be coordinated with regulatory bodies and other relevant stakeholders.

Action point 6: Gaia-X

Gaia-X is a Franco-German initiative that aims to establish a European cloud: a federated cloud in which providers work together, based on European laws and regulations and capable of competing with the large global cloud providers in terms of functionality. One of the main goals of Gaia-X is to regulate the governance of this federated European cloud. The Gaia-X Foundation was set up in Brussels. Parties can take part in this initiative to help define the governance of the future European cloud.

The Online Trust Coalition intends to participate in the Gaia-X Foundation, specifically in the working group that will arrange the “assurance” (i.e. reliability and security) of cloud services.

WHITE PAPER

IF YOU WANT TO CONTACT US OR RECEIVE MORE INFORMATION, SEND AN E-MAIL TO
info@onlinetrustcoalitie.nl
www.onlinetrustcoalitie.nl