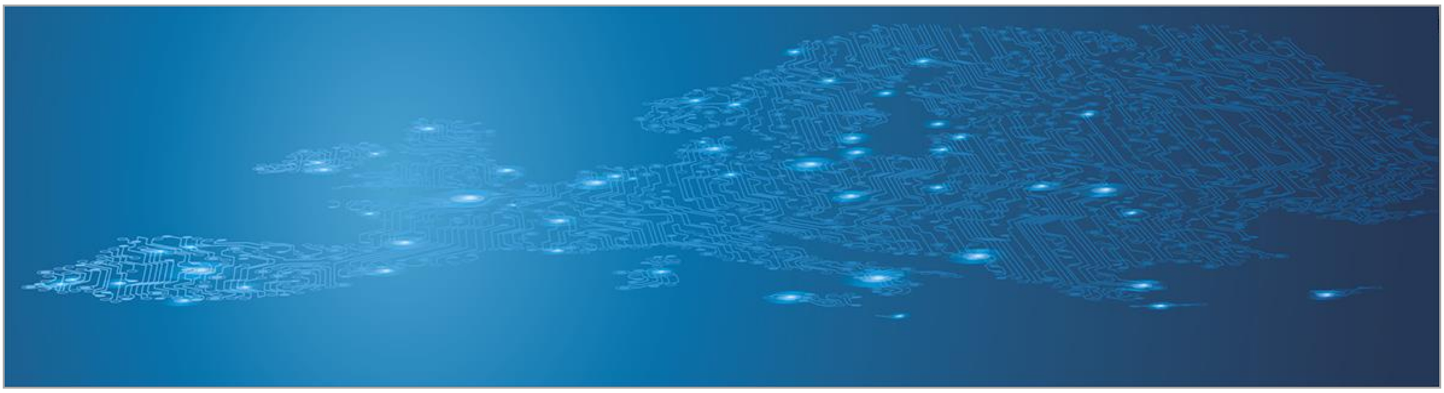


Cloud Security Guide for SMEs

Cloud computing security risks and opportunities for SMEs

April 2015

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. M.A.C. Dekker, Dimitra Liveri

Contact

For contacting the authors please use cloud.security@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

Acknowledgements

Thanks to Antti Vaha- Sipila and Janne Jarvinen from F-Secure Corporation for their help with this document.

Many thanks also to the experts of the ENISA Cloud Security and Resilience expert group who provided useful comments and feedback. Listing them in no particular order: Frank van Dam (Ministry of Economic Affairs, NL), Arjan de Jong (Ministry of the Interior and Kingdom Relations, NL), Tuija Kuusisto (Ministry of Finance, FI), Jesper Laursen (Agency for Digitisation, DK), Steve Agius (MCA, MT), Vangelis Floros (GRNET, GR), Aleida Alcaide (SEAP, ES), Tobias Höllwarth (EuroCloud), Aljosa Pasic (Atos), Roxana Banica (RO), Fritz Bollmann (BSI, DE), Marko Ambroz (MJPA,SI), Boggio Andrea (HP Enterprise Security), Tjabbe Bos (DG CONNECT, EC), Daniele Catteddu (CSA), Peter Dickman (Google, UK), Paul Costelloe (EuroCIO), Olivier Perrault (Orange, FR), Paul Davies (Verizon, UK), Raj Samani (McAfee), Jan Neutze (Microsoft, BE), Antonio Ramos (Leet Security), Jens Jensen (STFC, UK), Brian Honan (BH Counsulting, IE)

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-122-9, doi 10.2824/508412

Executive summary

Small and medium size enterprises (SMEs) are an important driver for innovation and growth in the EU. SMEs also stand to gain the most from cloud computing, because it is complicated and costly for them to set-up and run ICT in the traditional way. SMEs do not always understand all the information security risks and opportunities of cloud computing. This document aims to provide guidance for small and medium size enterprises (SMEs) about the network information security of cloud computing. It is important that SMEs do not only look at the network and information security risks of cloud computing but also at the opportunities to improve their network and information security. This document contains 3 main parts:

- First, we highlight **11 security opportunities,** explaining why certain features of cloud computing could present an opportunity for SMEs. We make a brief comparison also with traditional IT deployments.
- Secondly, we list **11 security risks** SMEs should take into account when adopting cloud computing. We compare also the risks with typical traditional IT deployments.
- Thirdly, we provide a list of **the 12 most important security questions** SMEs could use to understand better what are the security aspects of a cloud service when procuring a cloud service or when assessing different options in the market. The security questions address both the risks and the opportunities.

In an annex the SME can find empty forms to use for assessing risks, assessing opportunities and collecting relevant information about the security aspects of a cloud service: a **security cheat sheet**.

Risks and opportunities can be very different for different SMEs. A lot depends on the type of cloud service, the kind of data and processes involved, and other. Still to provide some practical examples we elaborate two specific scenarios where an SME is a cloud customer:

- ConsultLess, a 20 people consultancy firm, which wants to implement email and document management as a SaaS cloud service.
- EasyAgriSelling, a 10 people technology startup, which wants to run their webshop platform (for farmers to create e-shops to sell their produce) on top of a IaaS/PaaS cloud service.

Although not the focus of this document we address the issue of legal compliance briefly. We touch upon the main concepts of EU personal data protection legislation and we provide some pointers to relevant information.

This guide for SMEs updates the 2009 ENISA Cloud Computing Risk Assessment for SMEs and the 2009 ENISA Assurance Framework. We have deliberately consolidated the risks and reduced the number of security questions to make it more suitable for SMEs, with limited time and resources to go into a lot of details. It is important to stress that this guideline should not be seen as a replacement for the SME’s own risk assessment. Security measures should be appropriate to the risks; not always gold-plated solutions are necessary.

Since 2009 the cloud computing market has changed significantly. There are now many SMEs, enterprises and government organizations who use some form of cloud computing. Cloud computing has now become the backbone of the EU’s digital economy. Cloud services offered by providers are more mature, there is more choice, there is more information for customers and customers are more aware of the possibilities and limitations of cloud computing.

At the same time a number of issues have remained problematic, such as personal data protection legislation and the impact of foreign jurisdiction. In 2012, the European Commission issued the EU cloud strategy aiming to address a number of these issues. The strategy is an important initiative and the first results are currently being delivered.

Table of Contents

1 Introduction

This guide aims to help SMEs understand the network and information security risks and opportunities they should take into account when using cloud computing. This guide contains a list of 11 security opportunities for network and information security (see Section 3) and a list of 11 network and information security risks SMEs (see Section 4). These lists of opportunities and risks can be used directly by SMEs when they procure cloud services. For two specific fictitious scenarios we rate the risks and opportunities: An SME using SaaS for email and documents (see Annex B) and an SME using IaaS/PaaS for running a webshop platform (see Annex C). This guide also contains a list of security questions SMEs can use to understand the main features of the cloud service most relevant for network and informations security (see Section 5). Annex D contains empty forms for use during procurement. Although not the focus of the this guide, we address legal compliance and provide some pointers to information about personal data protection legislation in Annex A.

Scope

Network and information security

This document focusses on network and information security risks and opportunities; not other issues like legal compliance, legislation, contractual issues. In the annexes we briefly address personal data protection legislation, just to point to some relevant concepts and information.

Cloud relevant

This document focuses on the risks and opportunities which are *relevant* for an SME to consider. These opportunities and risks are not specific for cloud computing but may pertain to other types of ICT.

Cloud customers

We focus on SMEs in the role of customers of cloud services, not on providers.

Target audience

This guide is aimed at micro, small and medium-sized enterprises (SMEs)[1]. SMEs often have few IT or information security experts and it is infeasible for SMEs to negotiate with providers about custom features or custom contracts. SMEs typically buy standardized (off the shelf) services under fixed (boilerplate) contracts and SLAs. This document will be useful also for other small organisations, like government agencies.

Methodology

This guide has been created in close collaboration with the ENISA Cloud Security and Resilience expert group (public sector, private sector and industry association), based on the 2009 ENISA risk assessment guide. The risks and opportunities have been extensively cross checked and reviewed by subject matter experts.

Disclaimer about examples

In this document we sometimes give examples of past incidents. It is not our intention to single out specific services or specific providers for praise or criticism.

[1] http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm

Policy Context: the European Cloud Strategy

In 2012, the European Commission (EC) published its cloud computing strategy[2], called "Unleashing the potential of cloud computing in Europe”. The EU cloud strategy is designed to support the uptale of cloud computing across the EU. It centres around three key actions:

1. Standardization and certification of cloud services.
2. Safe and fair contract terms and SLAs, and a
3. Setting up a European cloud partnership to promote cloud computing adoption in the EU.

The EU Cloud strategy and the vision produced by the European Cloud Partnership both stress the importance of facilitating the adoption of cloud computing by SMEs, because they stand to gain most from cloud computing and they are an important driver for innovation and growth in the EU.

The ex-vice president of the EU’s Digital Agenda, Miss Kroes, said explicitly: *“These issues [blocking adoption of cloud computing] are particularly troublesome for smaller companies, which stand to benefit the most from the Cloud, but do not have a lot of spending power, nor resources for individual negotiations with Cloud suppliers”*.

ENISA has supported several actions under the EU cloud strategy: ENISA participated in the working group on cloud standardisation led by ETSI[3]. ENISA works with the EC and industry to create a list of cloud certification schemes[4]. ENISA also works in a working group which aims to clarify and harmonize Cloud SLAs[5].

Earlier drafts of this document have been developed as part of the activities of the European Cloud Partnership, by F-Secure Corporation (http://www.f-secure.com).

Past ENISA work

Since 2009 ENISA has engaged with the cloud industry and potential cloud customers and published a series of reports on cloud computing. Generally speaking ENISA supports the uptake of cloud computing because of the many opportunities the technology offers to improve network and information security. These are particularly relevant for SMEs which do not always have the resources and/or skills to implement state-of-the-art network and information security. Explaining the security opportunities (and the risks) of cloud computing is therefore an important objective for ENISA.

This document is based on previous ENISA work. In particular it updates two previous documents:

- The 2009 ENISA Cloud computing risk assessment, which lists opportunities and risks when adopting cloud computing[6].
- The 2009 ENISA Assurance framework for cloud computing, which provides a list of questions for SMEs to ask when procuring cloud services[7].

We have consolidated the risks and reduced the number of security questions in the 2009 publications to make it more suitable for SMEs, with limited time and resources to go into a lot of details.

[2] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
[3] http://ec.europa.eu/digital-agenda/en/news/standards-cloud-neelie-kroess-blog
[4] http://ec.europa.eu/commission_2010-2014/kroes/en/content/making-cloud-more-transparent-boost-secure-trustworthy-services
[5] https://www.huntonprivacyblog.com/2014/07/articles/european-commission-issues-cloud-service-level-agreement-standardization-guidelines/
[6] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
[7] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

2 Cloud Computing Basics

In this section the three basic types of cloud services are introduced and the different division of security tasks is explained.

One can distinguish among three different types of cloud services, each involving different types of assets:

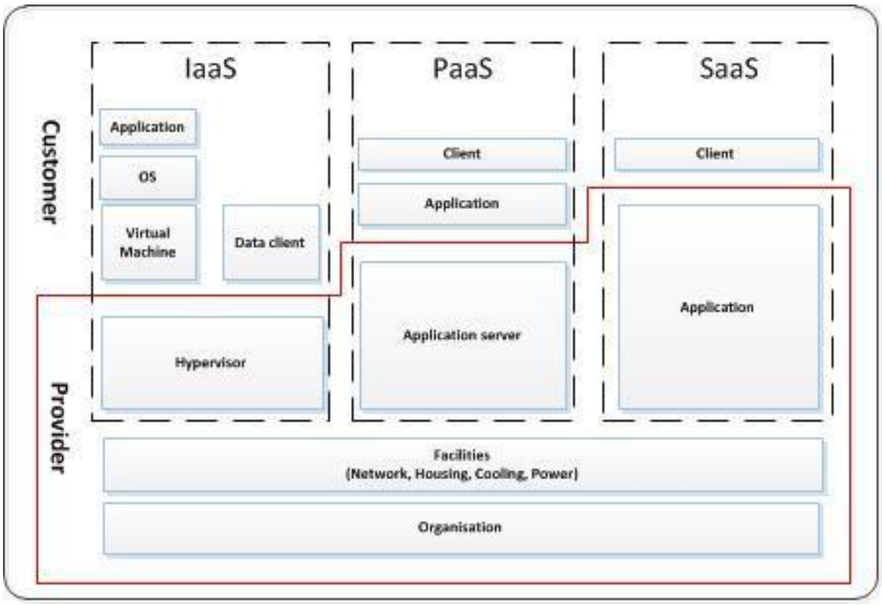


Figure 1: Asset in cloud computing

We go over the diagram from left to right:

- **Infrastructure as a Service**: In IaaS the provider delivers computing resources (virtual hardware), accessible online. The software providing access to the resources is called the hypervisor. Generally speaking there are two types of resources: processing power (including network resources), and (block) storage (memory resources). Examples include Amazon's Elastic Compute Cloud, Google's Compute Engine, Amazon Simple Storage Service, Dropbox, Rackspace, etc. Note that object storage services (e.g. Dropbox) are often considered a SaaS.
- **Platform as a Service:** In PaaS, the provider delivers a platform, or more precisely, application servers, for customers to run applications on. PaaS providers sometimes provide a software development tool for the platform. Examples of applications running on these platforms are scripts (PHP, Python, e.g.) or byte code (Java servlets, C#). Examples include Google App engine, Microsoft Azure, Amazon Elastic Beanstalk, etc.
- **Software as a Service:** In SaaS, the provider delivers full-fledged software or applications, via the internet. Applications range from email servers, document editors, customer relationship management systems, and so on. SaaS services can often be accessed with a browser or a web services client. Note that it is not uncommon for SaaS providers to run their applications on an IaaS or PaaS from another provider. An example is the video streaming site Netflix (SaaS) which runs on Amazon AWS computing services (PaaS/IaaS).
- **Facilities** denote the physical structures and supplies such as networks, cooling, power, etc.
- **Organisation** denotes the human resources, the policies and procedures for maintaining the facilities and supporting the delivery of the services.

In cloud computing delivery of ICT resources is, to some extent, outsourced to the cloud provider. Also some of the security tasks (such as monitoring, patching, incident response) are outsourced. Depending on the type of cloud service some tasks remain under the responsibility of the customer, while other tasks remain under the responsibility of the provider. Division of responsibilities can some times be a major source of problems as it was based on assumptions and poorly documented, leading to overlaps and gaps. This however seem to become extinct since SLAs have become more sophisticated documents and specify this information. For example, in IaaS/PaaS the customers run their own code on top of the cloud service, and often remain responsible for this (application) software. In SaaS, on the other hand, the application software is usually[8] under control of the provider. In the diagram below we illustrate how the division of certain security tasks can be different for different cloud services (IaaS, PaaS, SaaS).

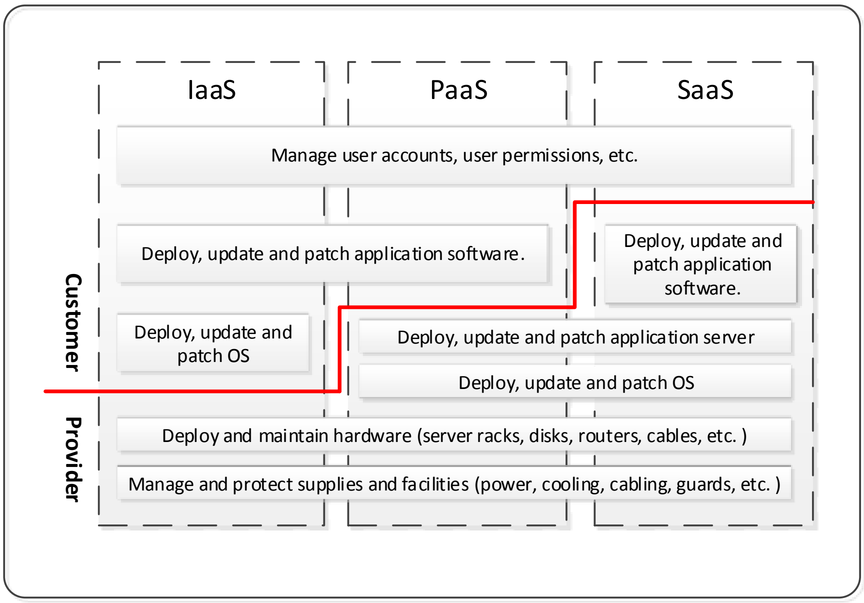

IaaS
PaaS
SaaS
Manage user accounts, user permissions, etc.
Deploy, update and patch application software.
Deploy, update and patch application software.
Deploy, update and patch OS
Deploy, update and patch application server
Deploy, update and patch OS
Customer
Provider
Deploy and maintain hardware (server racks, disks, routers, cables, etc.)
Manage and protect supplies and facilities (power, cooling, cabling, guards, etc.)

Figure 2: Outsourcing of tasks is different for different types of services

Note that this diagram is for illustration and does not provide an exhaustive list of security processes at the providers side or the customers side. In specific settings there may be specific agreements about the outsourcing of security tasks. An IaaS provider, for example, might have a service for patching the Operating System (OS) of customers. Sometimes such services are offered by a third-party (and this is also known as SECurity-As-A-Service). See the next section about opportunities. See also the annex for examples of security tasks in two fictitious scenarios.

In practice for SMEs, it is important to carefully assess which security tasks are outsourced to the provider and which security tasks remain under their own responsibility. It is not uncommon for SMEs to be confused about their responsibilities concerning security, for example, who makes backups of data or software, which type of failover/redundancy is offered by the provider and what needs to be done still by the customer.

[8] Barring cases where customers have some liberty to run additional software, on top-of-the service, like third-party apps, add-ons, or self-created code.

3 Network and information security opportunities

Cloud computing can be used by SMEs for a range of different applications (email, corporate website, CRM, CMS, internal payroll processing, archiving of internal corporate documents, etc). For SMEs cloud computing can offer many business advantages: Cloud services are typically "pay as you go", which may be an attractive cost structure for an SME, avoiding an upfront investment in hardware, software and IT experts. The overall costs when implementing are often lower than the cost when going with traditional IT solutions. Online collaboration is often easier in the cloud case as access is warranted to users from various physical locations, and various end-user devices etc.

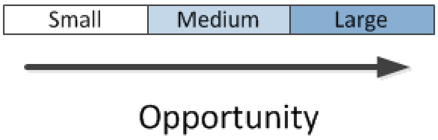
There are also opportunities for network and information security. Generally speaking large cloud computing providers can offer advanced security measures, while spreading the associated costs across several customers. In some cases this means that fundamental security settings might be 'shared' between costumers and might not be customisable but it also translates to a number of specific security opportunities. Below we highlight 11 specific opportunities for the network and information security of SMEs:

Network and information security opportunities
O1: Geographic spread
O2: Elasticity
O3: Standard formats and interfaces
O4: Physical security
O5: Incident response around-the-clock
O6: Software development
O7: Patching and updating
O8: Backups
O9: Server-side storage
O10: Security-as-a-service and security add-ons
O11: Certification and compliance

The rest of this section goes over each opportunity, explaining briefly why this could present an opportunity for an SME. For each opportunity a comparison with traditional IT deployments exists and points the reader to the relevant security questions in Section 6, which can be used in a procurement process.

As every SME is different, not all of these security opportunities are important to the same degree for all customers. Note that this report does not provide a rating or a ranking of the opportunities. In annex two specific (fictitious) scenarios, are examined and rating of the opportunities takes place using the following scale:

- **Small opportunity:** Customer could exploit this opportunity, but benefits would be limited.
- **Medium opportunity:** Customer should exploit this opportunity, because benefits would be significant.
- **Large opportunity:** Customer must exploit this opportunity, as there would be crucial benefits.



O1: Geographic spread

Cloud computing datacentres are often spread out across different geographic regions, nationally or globally. Geographic spread can provide resiliency against regional issues and local disasters such as storms, earthquakes, or cable cuts. It can also be used to mitigate certain Denial of Service (DoS) attacks, allowing customers to get access at other locations. Geographic spread can help reduce network latency, because the services are provided from sites closer to the customer. This could improve the overall availability and performance of the service.

***Cloud versus traditional IT:** In traditional IT deployments an SME would have to set up an additional remote site, sometimes even doubling the costs for IT facilities.*

It should be stressed here that not all cloud services come with geographic spread, and that sometimes it is available but needs to be first configured/requested by the customer specifically. Depending on the settings this might involve extra costs, because data synchronization across two remote sites requires network bandwidth, computing power and storage.

See security question SQ 3 (in Section 6).

O2: Elasticity

Cloud computing providers can use large data centres with large amounts of spare resources, to be able to respond to rapid changes in resource usage, peak usage, and Denial of Service (DDoS) attacks.

It should be noted here that not all cloud services offer the same kind of elasticity. There may be limits on resource consumption set by the provider or the customer. In some settings elasticity may need to be configured/requested specifically by the customer, and may increase costs.

See SQ11.

***Cloud versus traditional IT:** In traditional IT deployments a SME would need to invest in spare resources to accommodate peak usage, yielding high costs and inefficiency (because these resources would be unused most of the time).*

O3: Standard formats and interfaces

The idea of cloud computing is to offer one service to many customers at once. This means that in practice cloud services are often compliant with industry-wide standards. For example, most PaaS providers offer standard PHP application servers and many SaaS providers implement standard interfaces based on standards like XML and JSON (JavaScript Object Notation). This means that cloud services can be more easily integrated with other services, or ported to other platforms. This is a security opportunity because it facilitates backup, failover, and integration with existing security tools the customer may use, for example monitoring tools.

Cloud versus traditional IT: *In traditional IT deployments SMEs often use non-standard custom configurations and proprietary protocols, because of a lack of expertise and the (sometimes) higher costs of implementing standards.*

It should be noted here that while most cloud providers use standard interfaces and data formats, this is not always the case. Customers should ask which standards are used.

See SQ 10, SQ 11.

O4: Physical security

In case the business model of the SME includes shared resources requirements then physical security is indeed an opportunity when using cloud. Resource concentration makes physical security relatively cheap. If the costs of physical security measures, such as perimeter protection, 24/7 guards, alarm systems, camera surveillance, automated fire extinguishers etc., can be shared with many customers then the cost per customer is low. In practice this means that cloud providers can offer state-of-the-art physical security measures which drastically reduce the risk of physical theft of servers, disks and equipment, fires, floods, etc.

Compared with traditional IT: *In traditional IT deployments even a standard security measure like a guard on premise 24/7, would be too costly for an SME.*

See SQ 1, SQ 3, SQ 6.

O5: Incident response around-the-clock

Security incidents can happen at any time of the day or night. To ensure continuity most cloud providers continuously monitor their services around-the-clock and have response capabilities standing by to react to failures or attacks. Having personnel ready 24/7 is costly, but in cloud computing these security measures become affordable for customers because the costs are shared with many customers.

Cloud versus traditional IT: *In traditional IT deployments, an SME would have to invest a lot to have a 24/7 incident response capability.*

Note that cloud providers do not always monitor and respond to all types of security incidents which could affect a cloud service or a cloud customer. Customers should check which kind of security incidents are monitored and responded to, and what kind of response actions will be undertaken by the provider, to understand what remains to be done by the customer.

See SQ 1, SQ 2, SQ 3.

O6: Secure software development

Cloud versus traditional IT: In traditional IT deployments, if off-the-shelf software cannot be used, then an SME would need to invest significant resources in a secure software development.

Secure software development is not easy and requires a lot of time and investment in people, tools, and processes. Even building a simple website is rife with security pitfalls. A secure software development pipeline (unit tests, continuous integration, penetration and security tests, load tests, and most importantly, skilled and trained software programmers) is not easy to set-up and maintain. To build custom software, securely, is expensive, and outsourcing software coding is not always cheap or easy either.

Because of their scale, cloud providers can afford to invest in secure software development, spreading these high costs across many customers. Customers may lose some flexibility in terms of customization, but they reduce the risk of software vulnerabilities in code they developed.

Note that not all cloud software is developed securely. Some providers may have bad development practices. Other providers may use third-party software (proprietary or open source), over which they have limited control. Customers should assess which software is developed by the provider and how the provider ensures secure software development.

See SQ 1, SQ 7, SQ 8.

O7: Patching and updating

Timely patching and updating of software is crucial for security as attackers need only a small window to attack and exploit a discovered vulnerability. Particularly when standard, off-the-shelf software is used, cyber criminals pay particular attention to provider patches and often try to reverse engineer a patch in order to exploit the underlying vulnerability; and this can happen in a matter of hours. In fact, many cyber-attacks exploit the fact that organisations are slow to update and patch systems. Due to their scale, and because they deliver the same software to all customers, cloud providers can automate patching and updating to a high degree. They can set up procedures and tools which automatically[9] deploy timely patches and updates, reducing the window in which systems can be exploited by attackers.

Cloud versus traditional IT: In traditional IT deployments, SMEs often need to dedicate a lot of time and resources to patch and update their software. Even then they are often late. The fact that traditional IT deployments are often not industry-standard further complicates updating/patching because of incompatibility issues.

Note that not all the software relevant to the customer is always patched and updated by the provider. Particularly in IaaS and PaaS, the customer runs its own software on top of the cloud infrastructure and the customer usually remains responsible for patching and updating it. Customers should ask who patches and updates the relevant software in their setting.

See SQ 7, SQ 8, SQ 9.

[9] Note that in some settings automated patching and updating might break functionality, especially when customers are using services or APIs in a non-standard way, or when customers run their code on top of a cloud services, like in IaaS/PaaS. Of course this is also an issue in traditional IT deployments, and often the reason for delays in patching and updating.

O8: Backups

For an SME, making backups, across a range of applications and devices, and restoring them when needed, can be difficult and time-consuming. Cloud providers can implement tools to automate creation and testing of backupsand offer advanced backup restore solutions, allowing customers to roll-back mistakes and errors quickly. Additionally, in many cloud usage scenarios software applications are implemented as online (client-server) applications (as opposed to running stand-alone on clients). This reduces the amount of data that is on the end-user device, simplifying backups.

Cloud versus traditional IT: *In a traditional IT deployment, an SME need to dedicate time and resources to backups leading to high costs.*

Backups in the cloud (between cloud data centres) require both storage and network bandwidth and in some settings cloud providers do not provide backups automatically of all data, for free. Customers should assess which backups are made by the provider and if they need to implement or request additional back-up mechanisms.

See SQ 3.

O9: Server-side storage

In many settings, SMEs have a range of mobile (and less mobile) end-user devices which are relatively vulnerable to theft, loss, physical damage, etc. These threats can easily have a big impact on the assets of an SME. Especially when dealing with mobile devices, it is not always easy to keep timely backups of data (due to connectivity andbandwidth issues), nor to cryptographically protect the device components, from physical access to device storage (i.e. after loss or theft), nor to control access to devices with strong authentication etc. Cloud computing can mitigate some of these risks. Using cloud services SMEs can reduce the amount of data on the end-user devices. For example, using cloud-based email, SMEs can reduce the amount of corporate data on end-user devices, meaning that less data is at stake when something goes wrong with end-user devices.

Cloud versus traditional IT: *Often in traditional IT there is a significant amount of data on end-user devices, which further complicates back-ups.*

Customers should assess which data is stored server-side, and client-side.

See SQ 8.

O10: Security-as-a-service and security add-ons

As discussed in the previous section, some security tasks remain with the customer, particularly in the case of IaaS and PaaS. In cloud computing it is often more easy to outsource some of these security tasks to third-parties or the provider (if it offers such services). For example, an SME running custom software on an IaaS platform, could get a third-party to patch its OS regularly detect and respond to security incidents by isolating and replacing infected hosts instantly. Such security-as-a-service would be much harder to implement in a traditional IT deployment, typically requiring physical access to the premises.

Cloud versus traditional IT: *In traditional IT deployments it is often harder for an SME to use security-as-a-service because often in such settings access to the SME's premises would be needed, or at the very least a high-bandwidth connection.*

There are cloud providers who provide a range of additional security services (such as patching software), sometimes partnering with specialized (third-party) firms, enabling customers to procure additional security services in an easy way.

See SQ 2.

O11: Certification and compliance

In cloud computing one cloud service is offered to many customers at once. Certification, by independent auditors, against network and information security standards (like ISO27001 certification[10]), could be used by customers to fulfil their own compliance obligation. An auditor, when assessing compliance of an SME, would not have to check all the assets underlying the cloud services, by using existing compliance certificates for the cloud services they use.

Cloud versus traditional IT: *In traditional IT deployments, an auditor would have to cover all the ICT assets and check compliance to standards or policies from scratch, yielding high costs for SMEs.*

Note that there may be standards or compliance processes which are not cloud-ready. For example there may be settings where auditors need physical access to ICT assets, which (in a cloud computing scenario) might be impossible or infeasible because cloud providers may not always allow all sorts of audits of and visits to their datacentres[11].

Use SQ 1.

Understanding opportunities with security questions

For each opportunity we point the reader to relevant security questions in Section 6, which can be used in a procurement process, to understand if and how opportunities can be used.

Network and information security opportunities	Relevant security questions
O1: Geographic spread	SQ 3
O2: Elasticity	SQ 11
O3: Standard formats and interfaces	SQ 10, SQ 11
O4: Physical security	SQ 1, SQ 3, SQ 5, SQ 6
O5: Incident response around-the-clock	SQ 1, SQ 2, SQ 3
O6: Software development	SQ 1, SQ 7, SQ 8
O7: Patching and updating	SQ 7, SQ 8, SQ 9
O8: Backups	SQ 3
O9: Server-side storage	SQ 8

[10] As one of the actions under the EU cloud strategy, an expert working group (C-SIG), together with the EC and ENISA developed an overview of, for potential cloud computing customers, relevant certification schemes, which can be found at https://resilience.enisa.europa.eu/cloud-computing-certification.

[11] For reasons of security or logistics.

O10: Security-as-a-service and security add-ons	SQ 2
O11: Certification and compliance	SQ 1

4 Network and information security risks

In this section we look at 11 important security risks which should be taken into account by SMEs:

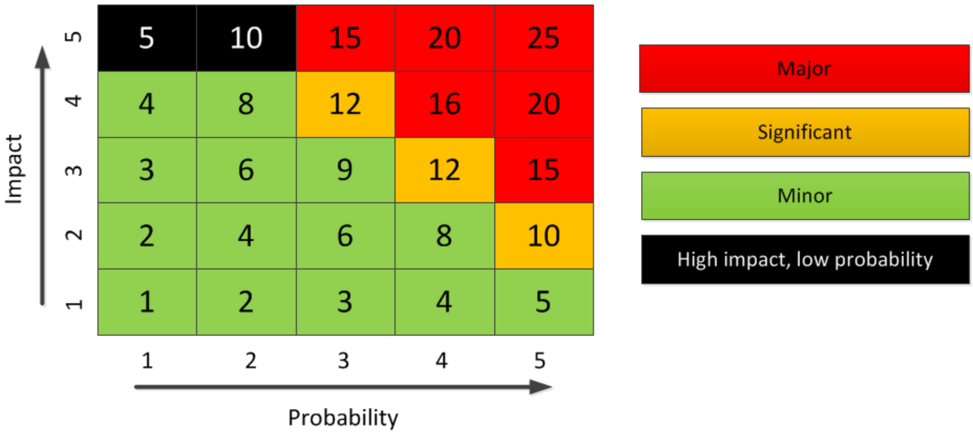
Network and information security risks
R1: Software security vulnerabilities
R2: Network attacks
R3: Social engineering attacks
R4: Management GUI and API compromise
R5: Device theft/loss
R6: Physical hazards
R7: Overloads
R8: Unexpected costs
R9: Vendor lock-in
R10: Administrative or legal outages
R11: Foreign jurisdiction issues

For each risk we refer the reader to relevant security questions (section 5) to answer during procurement of a cloud service. These questions should help customers understand if certain risks need to be addressed.

In this section the risks are are *not* ranked or rated, because risks depend on the specific setting (the type of SME, the type of cloud service, the data or processes involved, and other).

In annex two (fictitious) scenarios are analysed, rating the risks using the product of likelihood and the impact of a threat (following the ISO 27005 [12] standard on risk management). The scale used is depicted in the figure below, and ranges from 1 to 5: very low (1), low (2), medium (3), high (4), very high (5).

Black is used to indicate threats which are rare but could have high impact. These risks (also called "black swans") should be handled with care because the organisation often has little hands-on experience in dealing with these incidents.



Impact					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Probability	1	2	3	4	5

[12] http://www.iso27001security.com/html/27005.html

R1: Software security vulnerabilities

Software vulnerabilities in cloud software could have a major impact on customers. For example if an SME uses a SaaS email service, which is vulnerable to SQL injection, then this vulnerability could lead to a breach of confidentiality of the customer's emails, severely damaging the SME's reputation.

It is important to understand who is responsible for which software component. In the case of SaaS, all the responsibility for preventing software vulnerabilities is with the provider. In IaaS/PaaS, however, the customer is responsible for the software it runs on top of IaaS/PaaS, barring any special arrangements[13].

Remark on isolation failures[14]: Certain types of software vulnerabilities could lead to one customer getting access to another customer's data, either directly or via a side-channel: these vulnearbilities are called isolation failures[15]. In non-cloud settings, isolation failures are less of an issue since there is no co-tenancy.

***Cloud versus traditional IT:** Cloud service providers (using economies of scale) can implement advanced processes to develop, deploy and maintain software, which reduces the likelihood of software vulnerabilities. In traditional IT deployments it is expensive for an SME to set up state-of-the-art processes for software development and maintenance.*

Especially if sensitive data is involved, it is important to ask the right questions regarding software security. Some well-known SaaS providers are among the largest companies in the world, and they boost a great track record and advanced security measures. But this does not imply that all SaaS providers always do a great job at software security. One complicating factor is that cloud software vulnerabilities become more attractive to attackers/hackers to exploit, because this would allow them to attack many customers at once.

See security question SQ 7 (in Section 6).

> *Example: In 2011 a large SaaS provider deployed new software, which had unknown for the time vulnerabilities causing an isolation failure that was effectively allowing users to log into accounts using any password. The bug was alive for approximately 4 hours16.*

R2: Network attacks

Cloud computing services are consumed and managed via internet connections. This means that customers need to be aware of the risk of network attacks, like spoofing websites, sniffing/eavesdropping network traffic, Denial-of-Service attacks, man-in-the-middle attacks, pharming, wiretapping, etc., on the normal end-user interfaces, as well management/administrator interfaces, application programming interfaces (APIs), webservices.

See SQ 8.

***Cloud versus traditional IT:** In traditional IT, key systems like servers are typically managed locally, on-premise, which reduces the risk of network attacks on administrative interfaces. Many organisations provide online access to services, so a number of these network attacks are also a risk in traditional IT.*

[13] The different assets supporting cloud services are explained in Section 2.

[14] This type of failure (Isolation failure) was separately mentioned in ENISA's 2009 risk assessment.

[15] An example of an isolation failure is described at: http://nakedsecurity.sophos.com/2011/06/21/dropbox-lets-anyone-log-in-as-anyone/

[16] http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/

Example: DDoS attacks on one customer of a large (SaaS) reverse proxy and DNS service, had a severe impact on the internet connections for many other users, affecting their use of cloud services. [17]

R3: Social engineering attacks

In cloud computing, some administrative processes, like issuing user credentials, do not happen face-to-face between colleagues, but online via emails and websites. This increases the risk of social engineering attacks, in which an attacker fakes communication or information so it appears to come from a trusted source, like the cloud provider, etc. For example an attacker might try to impersonate a customer and initiate a "credential recovery" process, which eventually allows the attacker to access the customer's account, and access or delete all the customer data. Or, vice versa, attackers might try to impersonate the provider and in this way obtain the customer's credentials (aka phishing).

Attackers may target normal users, or users with high-privilege roles, such as software developers, system administrators, managers, both on the cloud provider's and the customer's side.

SMEs should take into account the risk of social engineering, such as phishing/spear-phishing, spoofing, etc. and assess the potential impact on the data and processes.

***Cloud versus traditional IT:** Social engineering is an issue also in traditional IT deployments. In a way social engineering is technology-agnostic. However, it must be said that in traditional IT a number of critical processes (like credential recovery, etc) are often carried out face-to-face. So customer should take extra care, particularly to prevent attacks on administrator's interfaces.*

See SQ 8

Example: Famously a journalist from Wired (a technology magazine) wrote about his ordeal when, an attacker, using a social engineering attack, managed to access his (SaaS) email account. Using the email account, the attacker hacked also other accounts of the victim and wiped data from his devices.[18]

R4: Management interface compromise

Most cloud services offer the customer a management interface, which give administrators access to a a large number of assets; in the case of SaaS, all the user accounts of the SMEs employees for example, or in the case of IaaS/PaaS, all the different virtual machines and applications of the SME. Sometimes the cloud service. If an attacker can get access to this interface then damage can be big for an SME.

Customers should verify that providers offer secure interfaces with good authentication and authorization mechanisms, particularly for high-privilege role like administrators. Additionally, customers should take into account the security of PCs and browsers used by administrators and high-privilege roles, because if attackers get control of

***Cloud versus traditional IT:** In traditional IT interfaces are often only accessible from the local company network and from local workstations, which provides some protection against phishing and spoofing.*

[17] http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/
[18] http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/

those, then they could by-pass some protection measures taken by the provider

See SQ7, SQ 8, SQ 9.

> *Example: A company, offering code backup and code repositories (as a SaaS) for software developers, stopped its operations permanently when an attacker had deleted virtual machines, storage volumes and backup data via the cloud management interface [19].*

R5: Device theft or loss

One of the defining characteristics of cloud computing, and key advantages, is accessibility from both fixed and mobile devices, PCs, tablets, smartphones, and so on. This introduces also some new risks. Mobile devices are relatively vulnerable to theft and loss. Theft and loss could mean data and/or authentication credentials on the devices could get stolen by attackers.

A complicating factor, for SMEs, is the trend bring-your-own-device (BYOD), which means that employees use different types of devices, not fully under control of the SME's IT experts. Features like screenlock, disk and storage media encryption, and many more may work differently on different types of devices.

> ***Cloud versus traditional IT:*** *In traditional ICT deployments the impact of device theft/loss is typically higher, because there is more code and data on end-user devices. At the same time mobile devices are less common in traditional IT settings.*

Cloud customers should assess which data and authentication credentials are stored on end-user devices, and ensure that device theft/loss is mitigated, by using backups, encryption, data minimization, etc.

See SQ 3, SQ 8

R6: Physical hazards

Natural disasters like floods, earthquakes, or fires, can affect the customer's ICT asset, or the data centres and infrastructure of a cloud provider. In cloud computing, customers might be affected by natural disasters occurring far away from their own premises.

Note that IaaS/PaaS customers might need to specify if and which data centres will be used as failover.

SMEs should have a business continuity strategy which addresses the risk of physical hazards. As part of this strategy, customers should ask which measures are in place to protect the cloud service from physical hazards. Customers might need to consider backing up their data regularly, in a standard format, to be able to migrate to another datacenter or another provider when needed.

> ***Cloud versus traditional IT:*** *Cloud providers can invest in state-of-the-art perimeter defence, because the associated costs are spread across many customers. In cloud computing natural disasters are often mitigated by using multiple geographically spread datacentres.*

See SQ 1, SQ 2, SQ 3, SQ 5, SQ 10.

[19] http://www.networkcomputing.com/cloud-infrastructure/code-spaces-a-lesson-in-cloud-backup/a/d-id/1279116

> *Example: Thousands of customers of two major cloud providers were affected by a lightning struck in the Dublin region in summer 2011. The outage lasted 2 days[20].*

> *Example: A large scale electrical storm caused an outage in a large cloud provider affecting the datacentre facilities. The outcome was that 3 major public services were out for more than 8 hours affecting thousand customers that didn't have access and, in some cases, lost data.[21]*

R7: Overloads

Sharing infrastructure offers great cost-savings and economies of scale - allowing customers to get more value for less costs. Logical isolation ensures that tenants cannot access each other's data, but cloud tenants still use the same physical infrastructure, so customers may be affected by peaks in resource usage by other tenants or DoS attacks on other tenants.

Cloud customers should ask if and how their cloud service handles peaks in demand or increased usage. Cloud customers should also check the service level agreements (SLA) which should guarantee availability of their service (or penalty fees or refunds in the case of outages).

***Cloud versus traditional IT:** In cloud computing overloads are often mitigated by providing customers with elasticity, using spare resources, while in traditional IT it is often much more expensive for customers to have large amount of spare resources.*

See SQ 3, SQ 11.

> *Example: A cloud provider suffered an outage that seemed managable in the beginning, but lasted longer than expected. During the outage, there was a large number of reboot requests from customers, which caused a bottleneck, and caused outages for customers[22].*

R8: Unexpected costs

Cloud computing is often pay-as-you-go, which means costs are not always fixed. This also means that costs could unexpectedly become very high. For example, customer may get a high bill because one of their websites becomes very popular, because employees upload and store a lot of data, or because attackers mount a DoS attack, consuming all the resources. One could argue the risk of unexpected costs is not purely an information security risk (but rather a business risk) but we nevertheless discuss it here briefly, because unexpected costs could quickly lead to financial issues which could result in an outage.

Customers should check how their service scales with increased usage and what are the associated costs.

***Cloud versus traditional IT:** In traditional IT costs are often fixed, although it should be said they are usually higher than in cloud computing, especially for smaller organisations.*

See SQ 11.

[20] http://www.theregister.co.uk/2011/08/08/bpos_amazon_power_outages/

[21] https://aws.amazon.com/message/67457/

[22] http://www.eweek.com/c/a/Cloud-Computing/Amazon-Cloud-Outage-Caused-by-Storms-Worsened-by-Software-Glitches-280060/

> *Example: An engineering team in an SME forgot to shut down a cluster of 250 servers over a weekend — a $23,000 mistake since the servers were idle during that period. A marketing group decided to run analysis on data collected in the cloud on their local servers — after downloading 10 TBs of data, they racked up $1000 dollars in unexpected data transfer fees[23].*

R9: Vendor lock-in

Vendor lock-in (also called customer lock-in) is a situation where it is hard for the customer to migrate to another cloud provider. For SMEs vendor lock-in can become a financial issue but it can also become a security risk, for example when circumstances force a customer to migrate to another provider, for example in case of a legal conflict, issues about billing, major outages, etc. If the customer does not use standard data formats and interfaces, then migration may become difficult and/or time-consuming.

Cloud versus traditional IT: *Cloud computing is often more standard than legacy IT (using standard XML/HTML interfaces, standard data formats, standard VM images, etc), which reduces vendor lock-in.*

Customers should have a business continuity strategy, which includes migration/exit plans for moving data and/or processes to another provider. As part of this strategy, customers should consider backing up their data regularly, in a standard format, to be able to migrate when needed, and test regularly if migration works.

See SQ 10.

> *Example: A cloud storage pioneer, closed its doors and left over 1,000 customers with only two weeks to save their data that was hosted on the cloud storage provider[24].*

R10: Administrative or legal aspects

Administrative and/or legal conflicts (even if no technology breaks or gets hacked) could have an impact on the availability of a cloud service. For example when a provider goes bankrupt and creditors could threaten to confiscate assets belonging to the supplier, then backups may become unavailable, before customers can migrate out. Service may also be interrupted when the cloud provider gets a legal court-order to cease operations, for example because of legal proceedings against the provider or against one of their customers/tenants. Cloud customers could also end up in an administrative dispute about billing for example.

Cloud versus traditional IT: *In traditional IT there is often is less dependence on third-parties, hence administrative or legal issues usually have less impact.*

The obligations of the provider are described in the contract the two parties counter sign; the contract should address SLA issues, jurisdiction, liability, indemnity etc. The contract need to be negotiated carefully and fully understood especially by SMEs. Customers should assess the risk of outages caused by administrative or legal issues and assess whether security measures need to be taken to mitigate this risk.

See SQ 4.

[23] http://formtek.com/blog/cloud-computing-companies-worry-about-unexpected-costs-and-fees/
[24] http://www.infoworld.com/article/2612299/cloud-storage/cloud-storage-provider-nirvanix-is-closing-its-doors.html

> *Example: A cloud provider went bankrupt without giving notice to their customers, leaving them on the spot with their data non reachable. In the aftermath, no data was lost thanks to the quick response of other vendors to support the customers' needs.*[25]

R11: Foreign law issues

Cloud services sometimes involves the use of cloud providers or datacenters abroad, which means that to a certain extent foreign jurisdictions may have an impact on the security and privacy of the cloud service. For example, violations of the law by the other customers (co-tenants) may lead to services being ordered shut (for example as part of a criminal prosecution), without taking proper care of the other customers. It has been argued by legal experts that even if the physical location of supporting equipment or datacenters are not in a foreign country there could still be an impact[26].

Cloud versus traditional IT: *In traditional IT data and processes remain on-premises, so foreign jurisdictions are hardly an issue.*

Cloud computing customers should ask which foreign jurisdictions may play a role and if there are incompatibilities with their own national legislation.

See SQ 12.

> *Example: a European governmental body (for similar reasons) restricted their employees from using widely used cloud services to share documents and exchange emails*[27]*.*

Understanding risks with security questions

For each risk we point the reader to relevant security questions in Section 6, which can be used in a procurement process, to understand if and how risks can be mitigated.

Network and information security risks	Relevant security questions
R1: Software security vulnerabilities	SQ7
R2: Network attacks	SQ8
R3: Social engineering attacks	SQ8
R4: Management GUI and API compromise	SQ7, SQ8, SQ9
R5: Device theft/loss	SQ3, SQ8
R6: Physical hazards	SQ1, SQ2, SQ3, SQ5, SQ6, SQ10
R7: Overloads	SQ3, SQ11
R8: Unexpected costs	SQ11

[25] http://gcn.com/Articles/2013/09/26/avoid-cloud-shutdown.aspx?Page=2

[26] IVIR has issued an analysis in which it argues that the US FISA legislation makes the use of cloud services from US providers by Dutch educational organisations unconstitutional, regardless of the physical location of datacenters.

[27] http://www.dechert.com/files/Publication/59c8f721-ba27-4397-99a1-72f6b554820e/Presentation/PublicationAttachment/655d6df2-b7ec-4f8c-917f-58efd20fb862/Cloud_Computing_02_12.pdf

R9: Vendor lock-in	SQ10
R10: Administrative or legal outages	SQ4
R11: Foreign jurisdiction issues	SQ12

5 Security questions

In this section we address the risks (see Section 5) and opportunities (see Section 4) with a list of 12 security questions. Customers can use these questions to get the most relevant information about the security of their cloud service, and to understand if more needs to be done to use certain opportunities or to mitigate certain risks. The table below shows the main topics and how they relate to the opportunities and risks:

Security questions	Related opportunities	Related risks
SQ1: Organizational security, governance and risk management	O4, O5, O6, O11	R6
SQ2. Responsibilities and liabilities	O5, O10	R6
SQ3. Contingencies and backups	O1, O4, O5, O8	R5, R6, R7
SQ4. Legal and administrative issues	-	R10
SQ5. Human resources security	O4	R6
SQ6. Access Control	O4, O9	R6
SQ7. Software security	O6, O7	R1, R4
SQ8. User, management and application programming interfaces	O6, O7, O9	R3, R4, R5
SQ9. Monitoring and logging	O7	R4
SQ10. Interoperability and portability	O3	R6, R9
SQ11. Scaling, sizing and costs	O2	R7, R8
SQ12. Compliance with national/international legislation	-	R11

For each question, an indication of the kind of information customers might need to get an answer is included. It should be stressed that not all providers will respond to customer question-forms about one particular service they may offer. A defining characteristic of cloud computing is that one provider offers the same service to many customers, so answering questionnaires for all customers may be infeasible and/or too costly. Customers may find some of the answers on the websites of providers or in other material (for example via cloud certification schemes[28]).

For each question below examples of possible supporting evidence or guarantees are included, which could back up or support claims made by the provider. Typically supporting evidence or guarantees may be clauses in a contract or SLAs, audit reports from third parties[29], self-assessments by the provider, a track record of past performance, statements from past customers etc.

Annex D includes empty question forms for use during procurement.

SQ1: Organizational security, governance and risk management

Before procuring a cloud service from a provider the customer should have an idea about the quality and effectiveness of the organizational structure and risk management processes at the provider. It is

[28] ENISA, EC, together with industry, has developed a list of certification schemes relevant for cloud customers: https://resilience.enisa.europa.eu/cloud-computing-certification

[29] At the same time formal compliance certification and audits by 3rd parties carry a cost and are not always the most appropriate or the only way to provide evidence.

also important for the customer to know which parts of the provider's organization will be dealing with security incidents, how key roles can be carried out by the customer, how to find security-relevant information, security advisories, information about outages.

Question	Possible answers
1. How does the cloud provider manage network and information security risks related to the cloud service?	- *General policy and approach to managing security risks.* - *Contact point for security incidents.* - *Presentation of critical dependencies of the Cloud Service Provider on third parties.* - *Compliance with best practice or industry standard on governance or risk management.*
(Supporting evidence/guarantees)	- *Audit reports by independent auditors.* - *Certification against information security risk management standards (for example ISO 27001), including scope statement.* - *Self-assessment against an industry standard or best practice.* -

SQ2. Security responsibilities

It is important to apportion responsibilities for security tasks and responsibilities/liabilities for security incidents. As explained in Section 2, the division of security tasks, and the division of responsibilities/liabilities for incidents is different for different types of cloud services.

Question	Possible answers
2. Which security tasks are carried out by the provider, which type of security incidents are mitigated by the provider (and which tasks and incidents remain under the responsibility of the customer)?	- *Assets under control of the provider.* - *Key security tasks carried out by the provider (patching, updating, etc).* - *Examples of incidents under the responsibility of the provider.* - *Tasks and responsibilities under the responsibility of the customer.*
(Supporting evidence/guarantees)	- *Relevant security tasks mentioned in contract or SLA,* - *Incident classification and response/recovery time objectives,* - *Liability clauses in contracts or SLA i.e. financial compensation*

SQ3. Contingencies and backups

An earthquake, a power cut or a thunder storm could affect facilities, supplies, an entire datacentre or power or network cables. For customers it is important to understand how the cloud service is resilient in the face of disasters and how data is backed up.

Question	Possible answers
3. How does the cloud service sustain disasters affecting datacentres or connections and which data is backed up where?	- *Physical security policy/ measures (backup power, fire extinguishers, etc.),* - *Network redundancy, geographic spread, availability zones, access control,* - *Backups and failover mechanisms,* - *Disaster recovery plans.*
(Supporting evidence/guarantees)	- *Relevant clauses included in contract and SLA,* - *Recovery time objectives.*

SQ4. Legal, regulatory and administrative issues

Legal, regulatory and administrative issues can cause outages (for example, issues about contracts, billing, legal procedures against co-tenants). Customers should understand how the security of their data and processes is guaranteed in the event of legal issues or administrative disputes.

Question	Possible answers
4. How is security of the cloud service guaranteed when there are legal issues or administrative disputes?	- *Service continuity in case of legal issues, administrative disputes, bankruptcy, confiscation by law enforcement, etc.* - *Guaranteed data export.*
(Supporting evidence/guarantees)	- *Contract and SLA relevant clauses about access to data.* - *Disclaimers addressing legal issues or administrative disputes, guaranteeing access to customer data and backups.*

SQ5. Personnel security

Personnel at the provider could have an impact on security of services or data processing. Customers should ask how the provider ensures that personnel works securely.

Question	Possible answers
5. How does the provider ensure that personnel works securely?	- *Training/certification for key roles.* - *Recruitment policies.* - *Penetration tests/social engineering testing.* - *Compliance to ISMS standard or best practice (SQ1).* - *Security vetting procedures for highly sensitive posts (handling sensitive data)*

(Supporting evidence/guarantees)	- *Certification or self-assessment against ISMS standard or practice (see SQ1).*

SQ6. Access Control

Data and processes of customers should be protected from unauthorized access. Customers should ask how access control is implemented to protect their data and processes.

Questions	Possible answers
6. How is customer data or processes protected from unauthorized physical and logical access?	- *Physical access control protection measures.* - *Logical access control protection (roles, permissions, privilege minimization, privilege segregation).* - *Authentication mechanisms used.* - *Compliance to ISMS standard or best practice (SQ1).*
(Supporting evidence/guarantees)	- *Certification or self-assessment against ISMS standard or practice (see SQ1).*

SQ7. Software security

Software vulnerabilities could have a big impact on the customer’s data or processes. Customers should ask which measures are in place to make sure software underpinning the cloud service is kept secure and which software is not under control of the provider, and should be kept secure by the customer.

Question	Possible answers
6. How does provider ensure software security and which software remains customers responsibility?	- *Secure software development method.* - *Vulnerability management process (contact points for vulnerabilities, time to report etc.),* - *Training for developers,* - *Patch and update procedures.* - *Standards or best practices used (such as ISO 27034).*
(Supporting evidence/guarantees)	- *Information about past vulnerabilities of relevant software.* - *Vulnerability scan reports.* - *Third-party audits of software,* - *Measures of software security activities e.g. BSIMM or OpenSAMM.*

SQ8. User, management and application programming interfaces

Cloud services are typically accessible via online web-based user interfaces and APIs. These interfaces should be protected from unauthorized access, particularly the management interfaces for administrators and high-privilege roles should be protected carefully because via these interfaces attackers could gain access to a large number of customer data and processes.

Questions	Possible answers
SQ8. How is access to the GUI's and API's protected, and are their additional measures for administrators/high privilege roles (under the customer's side)?	- *Authentication methods at GUIs and APIs,* - *Protection measures for administrator interfaces.* - *Authentication for administration interface,* - *IP restrictions, administrator roles and privileges.*
(Supporting evidence/guarantees)	- *Technical description of interfaces and protection methods.*

SQ9. Monitoring and logging

Customers should be able to monitor the performance and security of the service, via alerts, periodic reports, dashboards. Customers should also be able to analyse issues by analysing transaction logs, either via automatic interface or upon request, for example in the case of an incident.

Questions	Possible answers
9. How can the customer monitor the service, which logs are kept, and how can they be accessed for example when the customer needs to analyse an incident?	- *Dashboard with access to performance monitoring.* - *Transactions logs, performance logs.* - *Alerts and triggers for notification.*
(Supporting evidence/guarantees)	- *Relevant clause of the SLA on retrieval of transaction logs.*

SQ10. Interoperability and portability

Interoperability makes it easier for customers to integrate a cloud service with other, existing, solutions, and portability makes it easier for customers to migrate to a new provider (if needed in an exit scenario, for example). Customers should ask which standards are used for data and interfaces (and maybe one step further to hardware and devices), or if export functions and backup data uses standard formats.

Questions	Possible answers
10. Which standards make the cloud service portable and interoperable?	- *Interface standards and data formats for GUIs, APIs, export, applications and code, virtual machines, etc.*
(Supporting evidence/guarantees)	- *Relevant clauses in contract or SLA,* - *Audit reports, certifications, self-assessment report indicating compliance.*

SQ11. Scaling, sizing and costs

Cloud services often provide elasticity in terms of resource usage, on the basis of a pay-as-you-go payment model. Customers should clarify how peak usage or increased usage is dealt with, and how the additional costs are handled.

Questions	Possible answers
11. How is increase of usage or peaks handled, and what are the corresponding costs?	- *Examples of elasticity scenarios, cost calculation, and so on* - *Cost alerts and billing limitations.*
(Supporting evidence/guarantees)	- *Relevant clauses in contract or SLA,* - *Performance track record.*

SQ12. Compliance with national/foreign legislation

Cloud computing changes the way IT resources are delivered and there may be compliance issues with national legislation. In cloud computing customers sometimes work with providers and/or datacenters across borders, so also foreign legislation might be relevant to take into account. Customers ask which jurisdiction is relevant to take into account and which legislation applies to their cloud service (national, international etc).

Note that often personal data protection legislation is applicable (see Annex A).

Questions	Possible answers
12. Which national legislation applies?	- *Relevant national legislation (including national bodies that have jurisdiction to impose provisions).* - *Relevant foreign jurisdiction and applicable foreign legislation.* - *Location of datacentres.* - *Applicable personal data protection legislation.*
(Supporting evidence/guarantees)	- *References and links to legislation*

6 Conclusions and Outlook

In this document we highlight 11 important security risks and 11 important security opportunities SMEs should take into account when procuring a cloud service. We also provide a list of 12 security questions SMEs can use to understand the security features of cloud services in the market.

Since 2009 the market has evolved: Providers offer products which are more mature, they offer more information about security, customers understand cloud computing better, and know better what are the risks and opportunities of cloud computing. Also policy makers have taken action. In 2012 the European Commission issued an EU Cloud strategy aimed at removing remaining barriers to a wider uptake of cloud computing. Also national governments in the EU are adopting policies (such as cloud-first policies) to improve the use of cloud computing in the private and public sector.

At the same time work still needs to be done to ensure a single digital market in the EU. Cloud computing exasperates the differences between different countries and different jurisdictions. Some of these issues may be addressed by technological solutions (such as encryption), but not all.

ENISA believes security should be a driver for cloud computing, and that, when organization need better network and information security, then cloud computing (in different forms) becomes an opportunity to meet those requirements (sharing resources, sharing costs, sharing expertise).

We look forward to helping SMEs in the EU as well as other customers, like government agencies, to adopt cloud computing in a secure way and make full use of its opportunities.

Annex A: Legal compliance

Cloud computing changes radically the way ICT resources are delivered and consumed. Customers should assess which cloud computing services are compatible with applicable legislation. Depending on the setting a range of laws could apply: for example legislation on the protection of personal data (DP), legislation on sector-specific data like financial data or medical records, legislation for critical information systems, like energy, water supply or transport, legislation on the handling of state classified data, criminal law, administrative law etc.

Depending on the setting there may be different requirements, which could have an important bearing on the way cloud computing can be used by SMEs and which are security measures which must be taken by the customer. Legal compliance is *not* only about personal data protection legislation.

We give some examples of different types of legal requirements which could have an impact:

- **On-site audits** – Legislation might require the customer to facilitate on-site audits of ICT systems. Cloud providers might not always be able to subject to all sorts of on-site audits.
- **Physical separation** –Legislation might require the use of physically separated systems for certain functions. Cloud providers might not offer physically separated systems.
- **Outsourcing** – Legislation might allow outsourcing to third-parties only under certain conditions, for example, if customers are notified.
- **National borders** – Legislation might prohibit transfer/ processing of data outside the country's border. Cloud providers might operate abroad or use data-centres abroad.
- **Certified products** – Legislation might require use of specific (tested/certified) hardware for certain (for example, cryptographic) operations. Cloud providers might be using different hardware and/or products.

Legislation is different from sector to sector, from country to country, and compliance depends on the type of service, how the service is implemented technically, the type of processes or data involved etc.

Generally speaking customers should take into account first their national legislation and secondly, when needed, foreign legislation in the provider's country and/or other countries involved with the service, for example countries hosting datacenters or subsidiaries. It should be noted that legislation is constantly changing and the need to keep up with it is something the customer should do or for the cloud provider to take up and notify clients.

One type of legislation which often has an impact on how SMEs can use cloud computing is national personal data protection legislation. In the rest of this section we provide the reader with some explanation of relevant concepts and pointers to relevant documents on *personal data protection legislation in the EU*, because many SMEs have questions about this type of legislation. Another type of legislation would be the specific regulatory law that could impact on top of national legislation; this could include inter alia finance, telecommunications, healthcare etc. While SMEs may not be directly regulated they may be legally required to comply with sector specific regulation if they are a supplier to that industry sector.

Note that ENISA does NOT aim to give legal recommendation or advice on legal matters: Applicable legislation might be complex so SMEs might need to use legal advice for their analysis. This report doesn't substitute any legal analysis provided by experts.

A.1 EU personal data protection legislation

SMEs often have concerns about compliance with personal data protection legislation[30]. Given the broad definition of personal data[31], in a lot of settings DP legislation plays a role. As with other legislation, data protection requirements differ from country to country, sector to sector. This complicates the use of cloud computing across borders and the development of a single market for online services; which is why the European Union made it one of its priorities (under the Digital agenda, the EU cloud strategy, and the Data protection reform initiative) to harmonize national DP legislation across the EU (see below).

A.1.1 Covered organisations and individuals

The goal of the EU's personal data protection legislation is to protect the privacy of EU citizens. The legislation affects cloud providers based in the EU, cloud customers based in the EU, and organisations offering cloud services directed at EU citizens.

The main EU-wide data-protection legislation is the Data Protection Directive 95/46/EC. It is currently being reformed into a new Data Protection Regulation[32].

A.1.2 Personal data and processing

Key definitions used in the EU personal data protection legislation are:

- *Personal Data* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[33].
- *Sensitive (personal) data* means personal data revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life.
- *Processing of personal data* (*processing*) means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

A.1.3 Roles: Data controllers and data processors

The EU personal data protection legislation distinguishes different roles:

- Data-controllers: The individual or organization who collects the personal data and who

[30] For instance, in Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take, 2012, p. 42-43, available at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf

[31] Business email addresses may be considered personal data and some (the European Court of Justice, e.g.) have argued that even IP addresses are personal data.

[32] http://ec.europa.eu/justice/data-protection/

[33] For the notion of personal data see also Article 29 Working Party Opinion 4/2007 on the concept of personal data and the recent Opinion 8/2012 providing further input on the data protection reform discussions, where the notion of personal data is further explained with regard to "identifiability" (legal term for the notion of being indirectly identified) in terms of singling out the individuals

controls how the data is subsequently used and processed.

- Data-processors: The individual or organization processing the personal data (which might include storage, computing, sharing, etc.).
- Data-subject: The citizen whose personal data is involved.

The EU legislation mostly targets data-controllers, and only indirectly targets data-processors (only when they process data on behalf of data-controllers).

A.1.4 Appropriate security measures and due-diligence

The requirement most relevant to network and information security is the obligation for the data-controller to ensure that appropriate security measures are in place to protect the security of the processing of personal data. This means that the data-controller should carry out a risk assessment about security measures as needed. Risk assessment, on network and information systems, is a central part of information security governance and information security risk management. For SMEs this means that they need to carry out a due-diligence on the setup of the cloud service and the security measures in place to protect the security of the processing of personal data (initially during procurement).

In this guide, in Section 3 (Risks) and Section 4 (Security questions), we provide SMEs a tool for assessing, if appropriate, security measures in place to protect security of the cloud service and the security of the processing of the customer data. Note that the national Data Protection Authority might have specific and detailed recommendation about which are “appropriate security measures.”

A.1.5 Security breach notification

In the Data Protection Reform provisions for breach notification obligations are included, for those security breaches which have an impact on personal data. In practice this would mean that SMEs, as data controllers, whenever personal data is involved, should be in a position to investigate breaches and communicate about them to data-subjects or authorities, in a timely manner. This is still under consultation and does comprise a formal requirement for the data controller. The security question SQ 12 in Section 4 addresses security breaches and security breach reports[34].

A.1.6 National guidance on data protection legislation

Many Data Protection Authorities across the EU have developed excellent information, in local languages, about compliance to the applicable personal data protection legislation in their country. We list some of the guidance below, in no particular order[35]:

- The UK data protection authority, ICO, issued guidance on cloud computing[36].
- The French data protection authority, CNIL, published recommendations for companies planning to use Cloud computing services[37]
- The Swedish DPA, Datainspektionen, issued guidance on use of cloud services and the Swedish personal data protection legislation[38]
- The Italian DPA, Garante per la protezione dei dati personali, issued a guide on personal data and cloud computing[39]

[34] More details can be found in the Art29 WP opinion 5/2012 on personal data breach reporting.

[35] This list is not exhaustive. Feel free to send us additions via email to cloud.security@enisa.europa.eu.

[36] http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

[37] http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-cnils-recommandations-for-companies-using-these-new-services/

[38] http://www.datainspektionen.se/in-english/cloud-services/

[39] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906143

- The Irish DPA, called Data Protection Commissioner, issued guidelines on cloud computing[40]
- The German DPA issued guidance on cloud, called Entschliessung und Orientierungshilfe Cloud Computing[41]

The Article 29 Working party, a forum of national DPAs across the EU, has issued several opinions about cloud computing and on the concept of processors and controllers:

- Opinion 5/2012 on Cloud Computing, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
- Opinion 1/2010 the definition of processor and controller, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

A.1.7 Personal data protection in the EU Cloud Strategy

The EU Cloud Strategy recognizes that personal data protection legislation across the EU is currently a barrier to the adoption of cloud computing. Under the cloud strategy the EC has worked jointly with industry on a code of conduct on personal data protection for cloud computing providers, to be submitted for approval by the Article 29 Working party. The code of conduct aims to make it easier for customers to be compliant with data protection legislation while using cloud computing. The progress of that work can be found at: https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

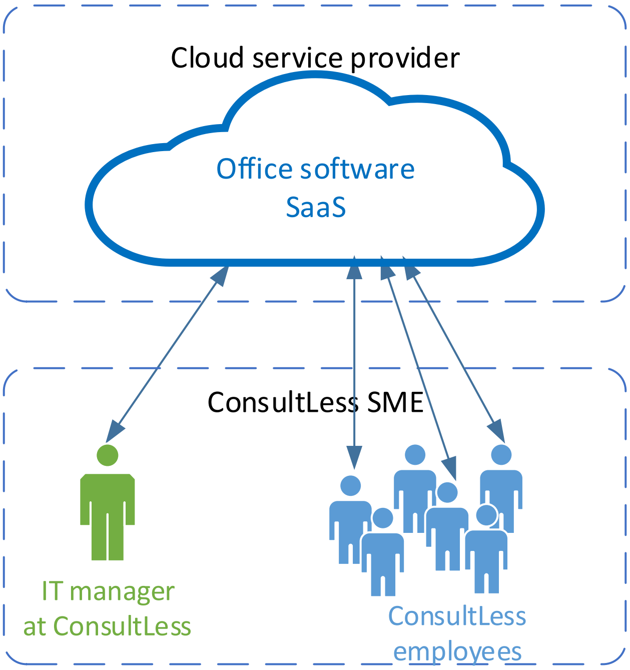
[40] http://www.dataprotection.ie/docs/03-07-12-Cloud-Computing/1221.htm

[41] https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Annex B: Example scenario: ConsultLess, SME using SaaS

B.1 Introduction

ConsultLess is a small consultancy firm in the EU that has 20 employees (mostly legal and management experts). One of the employees is partner and also the Chief Information Officer (CIO) of the firm. Occasionally the CIO pays consultants for IT advice or support. ConsultLess decides to procure office software as a service (SaaS) for use by its employees: the cloud service offers document storage/editing, email and calendar. This cloud service should replace an internal mail-server and office software installed on computers. The setup is depicted below.



B.1.1 Business drivers

For ConsultLess there are many reasons to use a SaaS cloud service are many: better collaborative features, lower hardware costs, lower management and maintenance costs. Compliance is a key issue - and the CIO of the firm (the only employee with specialized IT expertise) wants to understand which standard (boilerplate) services to choose, and also which issues remain to be addressed by specific mitigating measures, custom features, etc. Some (not all) of the data stored and processed is sensitive, and data leaks could have a severe impact on the reputation of the firm - and/or possibly even expose the firm to legal actions by affected customers (which will have great reputation impact for such a small firm).

B.1.2 Outsourcing information security tasks

In this fictitious scenario the security tasks which will be carried out by the cloud provider are:

- Managing of hardware and facilities, including physical security, power, cooling, etc.;
- Managing of server operating systems and the application server, including development, deployment, patching, updating, monitoring, checking logs, etc. For example, it is the responsibility of the provider to patch the server operating systems in time;

- Managing the application software, including development, patching, updating, monitoring, and checking logs, and so on. For example, it is the responsibility of the provider to fix software flaws in the office software;
- Managing updates of software and data.

The customer, ConsultLess, is merely responsible[42] for handing out accounts to its employees, revoking accounts when employees leave, resetting passwords, etc.

In this scenario most security tasks are outsourced to the provider. The customer, once the service has been procured and is up and running, will have few security tasks left to perform. It should be stressed that the responsibility for security cannot be "outsourced". If something goes wrong with the office software ConsultLess has procured, causing sensitive data about its clients to leak, then ConsultLess will in the first place be held responsible for the damages. For ConsultLess, hence, clarity about security tasks and responsibilities is a crucial consideration in the procurement process.

B.2 Opportunities and risks

B.2.1 Assessing the security opportunities

Let's look at the security opportunities for ConsultLess (SME uses SaaS).

OPPORTUNITY	RATING	REMARKS
O1. GEOGRAPHIC SPREAD	Medium	No need for making backups and bringing them to a remote site.
O2. ELASTICITY	Small	At Consultless usage of resources is quite stable. No peaks.
O3. STANDARD FORMATS AND INTERFACES	Medium	Consultless plan on keeping documents, communications long term in archives. Standard data formats are important.
O4. PHYSICAL SECURITY	Large	ConsultLess only secures laptops with disk encryption and pincodes, and does not need to handle physical security of servers, backup disks, etc.
O5.INCIDENT RESPONSE AROUND THE CLOCK	Small	Downtime overnight is not a major issue for ConsultLess.
O6. SECURE SOFTWARE DEVELOPMENT	Small	For ConsultLess the alternative would be off-the-shelf software, so secure software development is only a small opportunity in this setting.
O7. PATCHING AND UPDATING	Large	ConsultLess have only one IT manager, and patching and updating servers would take away a lot of time.
O8. BACKUPS	Large	ConsultLess has only one IT manager, and keeping backups would take up a lot of time.
O9: SERVER-SIDE STORAGE	Large	ConsultLess has employees which are mobile working from home and at clients. Server-side storage mitigates the risk of employees losing their devices.

[42] Refer to the Cloud model visual in section 2.

O10. SECURITY AS A SERVICE AND SECURITY ADD-ONS	Large	ConsultLess will use an add-on for scanning emails and documents for malware.
O11. CERTIFICATION AND COMPLIANCE	Large	ConsultLess can refer to certification of the provider making it much easier to fulfil their own compliance obligations.

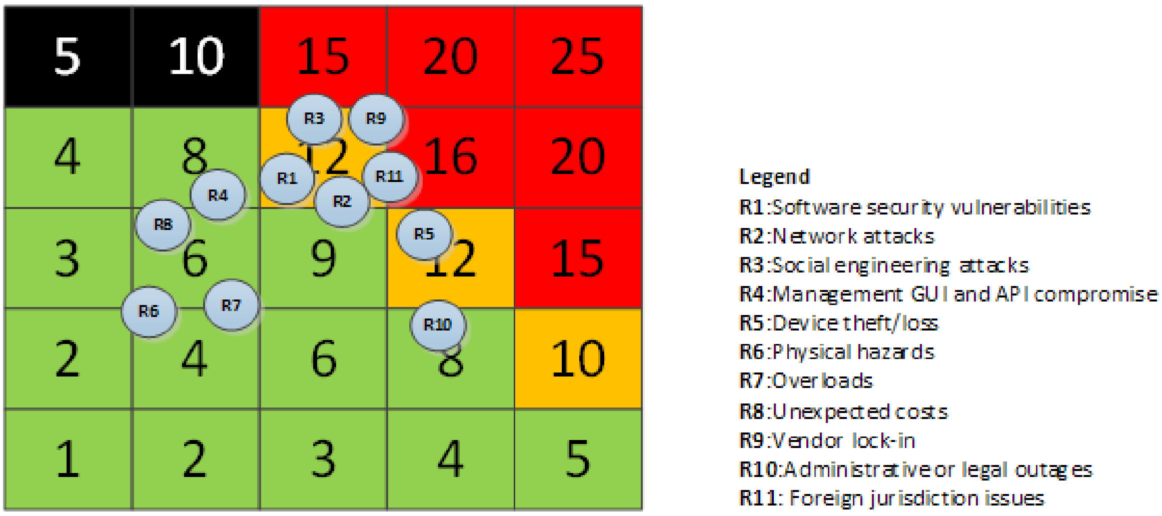
B.2.2 Assessing the security risks

Let's look at the different risks in more detail.

RISK TYPE	LIKELIHOOD	IMPACT	RISK	REMARKS
R1. SOFTWARE SECURITY VULNERABILITIES	Medium	High	Significant	ConsultLess uses the cloud service for sensitive data so the impact of vulnerabilities is high. ConsultLess will select a vendor with a good track record.
R2. NETWORK ATTACKS	Medium	High	Significant	ConsultLess has employees which are not tech-savvy, so it is possible that spoofing, sniffing and pharming attacks are successful. ConsultLess will secure its internal wifi network and raise awareness about insecure network connections, rogue hotspots, etc.
R3. SOCIAL ENGINEERING ATTACKS	Medium	High	Significant	ConsultLess has employees which are not tech-savvy, so it is possible that phishing attacks are successful. ConsultLess will raise awareness about fake emails asking for credentials etc.
R4. MANAGEMENT GUI AND API COMPROMISE	Low	High	Minor	For ConsultLess the main risk is the management portal. It will select a cloud service which has 2-factor authentication for the administrative user account. It will also set a policy which requires the administrative user to use a liveCD for administrative tasks.
R5. DEVICE THEFT/LOSS	Medium	High	Significant	ConsultLess uses the cloud service for sensitive data so device loss can be an issue.

				Using a cloud service mitigates some issue because less emails and documents are on user devices. ConsultLess will set a policy requiring employees to secure their devices from unauthorized access.
R6. PHYSICAL HAZARDS	Low	Medium	Minor	ConsultLess use the cloud service for its business data, which can not be lost. It will select a cloud provider with good physical security on its sites and backups to multiple sites to avoid data loss.
R7. OVERLOADS	Low	Medium	Minor	ConsultLess does not have high availability requirements. Outages are acceptable.
R8. UNEXPECTED COSTS	Low	Medium	Minor	ConsultLess does not expect dramatic usage patterns. It will select a cloud provider which warns about cost increases.
R9. VENDOR LOCK-IN	High	High	Significant	For ConsultLess this is a significant risk. ConsultLess will use the cloud service only for emails and documents stored in widely used data-formats to prevent lockin.
R10. ADMINISTRATIVE OR LEGAL OUTAGES	Medium	High	Minor	ConsultLess does not foresee major issues around administrative or legal disputes.
R11. FOREIGN JURISDICTION ISSUES	Medium	High	Significant	ConsultLess is not subject to any specific legal requirements about cross-border processing or data transfers.

The risks can be plotted in a matrix, showing what are key issues.



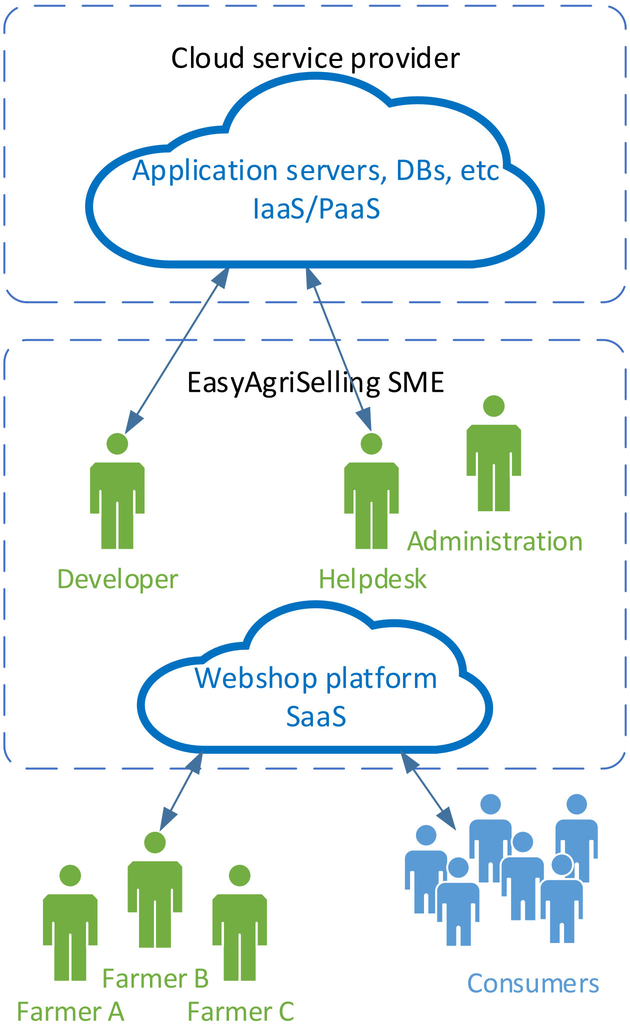
Legend
R1:Software security vulnerabilities
R2:Network attacks
R3:Social engineering attacks
R4:Management GUI and API compromise
R5:Device theft/loss
R6:Physical hazards
R7:Overloads
R8:Unexpected costs
R9:Vendor lock-in
R10:Administrative or legal outages
R11: Foreign jurisdiction issues

Figure 3: Risks for ConsultLess (SME using SaaS)

Annex C: Example scenario: EasyAgriSelling, SME using IaaS/PaaS

C.1 Introduction

EasyAgriSelling is a small tech start-up in the EU, which developed an online web shop software (as a service) for farmers who would like to start direct-selling their vegetables and other products. Their slogan is: “Selling your agricultural produce to consumers, made easy”. Farmers can set up an online shop in a few clicks - customizing their shop with a logo, colours and a description of their farm. EasyAgriSelling operates a pay-as-you-go model, charging no monthly fee, but only charging their customers when products are sold. EasyAgriSelling is a SaaS provider and they are a cloud services customer building services on a cloud provider who offers them IaaS and PaaS on which to build their product. In this document we are assessing risks and opportunities from both their roles as a service provider and as a service customer. The SaaS platform runs on top of the IaaS/PaaS platform. The setup is depicted below.



C.1.1 Business drivers

For EasyAgriSelling there are many reasons for using an IaaS/PaaS cloud service: IaaS/PaaS computing resources are elastic, so once their service takes off, they can easily scale up, without having to make an upfront investment. A start-up with limited capital, they need to make the right investments into building their product and responding to increasing demand. Cloud computing fits their long term plan. Moreover, employees at EasyAgriSelling are web design specialists, while running and maintaining the nuts and bolts of hardware and networks is not their competence. Key concerns are availability, security and privacy of the payment data and some of the personal data of consumers (home address, billing address etc.). EasyAgriSelling is responsible for the software security of the online web shop software, the web interfaces used by the farmers (customers of EasyAgriSelling) and the personal data and payment data of the consumers buying from the farmers.

C.1.2 Outsourcing information security tasks

EasyAgriSelling is a customer of an IaaS/PaaS service which it uses for running its web shop software for farmers.

In this setting the security tasks the IaaS/PaaS provider carries out are:

- Managing hardware and facilities, including physical security, power, cooling, etc.;
- Managing the server operating systems and the application server, including development, deployment, patching, updating, monitoring, checking logs, and so on. For example, it is the responsibility of the provider to patch the server operating systems in time.

EasyAgriSelling, the customer, remains responsible[43] for:

- Managing the application software, including development, patching, updating, monitoring, and checking logs, and so on. For example, it is the responsibility of EasyAgriSelling to fix software flaws in the deployed web shop software;
- Managing the accounts of the farmers using their web shop software, as well as the consumer accounts, including resetting passwords, troubleshooting issues with payments etc.;
- Managing backups of application software and data.

In this scenario some security tasks are outsourced to the provider, but many security tasks still have to be carried out by the customer (EasyAgriSelling). Security considerations in the procurement process really only regard security of the facilities, the operating system and the application servers which are under control of the provider.

C.2 Risks and opportunities

C.2.1 Assessing security opportunities

We look at the different opportunities for "EasyAgriSelling" in more detail in the table below:

OPPORTUNITY	RATING	EXPLANATION
O1. GEOGRAPHIC SPREAD	Medium	For EasyAgriSelling geographic spread means more resilience and it makes it easier to keep SLAs with the farmers.
O2. ELASTICITY	Large	For EasyAgriSelling elasticity means it is easier to keep SLAs with the farmers, even if one farmer has a peak in demand.
O3. STANDARD FORMATS AND INTERFACES	Medium	For EasyAgriSelling it is important to be able to have the cheapest cloud provider, so standard formats for code and virtual machines are important to be able to migrate if a better offer is found on the market.

[43] Refer to the cloud responsibilities model in section 2

O4. PHYSICAL SECURITY	Medium	For EasyAgriSelling it is important to outsource physical security of the datacentre to a cloud provider. “EasyAgriSelling” still needs to secure its employees’ end-user devices, but this is relatively easy.
O5. INCIDENT RESPONSE AROUND THE CLOCK	Large	For EasyAgriSelling 24/7 response means it is easier to keep SLAs with the farmers.
O6. SECURE SOFTWARE DEVELOPMENT	Small	For EasyAgriSelling the main issue is security of its own application software.
O7. PATCHING AND UPDATING	Medium	For EasyAgriSelling automated patching and updating of the underlying application servers and operating systems can be time-consuming.
O8. BACKUPS	Large	For EasyAgriSelling backing up to a remote site can be time-consuming, so it is very convenient to outsource this.
O9 SERVER-SIDE STORAGE	Small	N/A – EasyAgriSelling is using IaaS/PaaS.
O10. SECURITY AS A SERVICE AND SECURITY AD-ONS	Small	N/A – EasyAgriSelling just needs barebone virtual hardware.
O11. CERTIFICATION AND COMPLIANCE	Medium	It is very important for EasyAgriSelling to show compliance to industry standards. EasyAgriSelling will select a vendor with a certification so its own compliance obligation regard only the application software and the processes around managing the famers’ webshops .

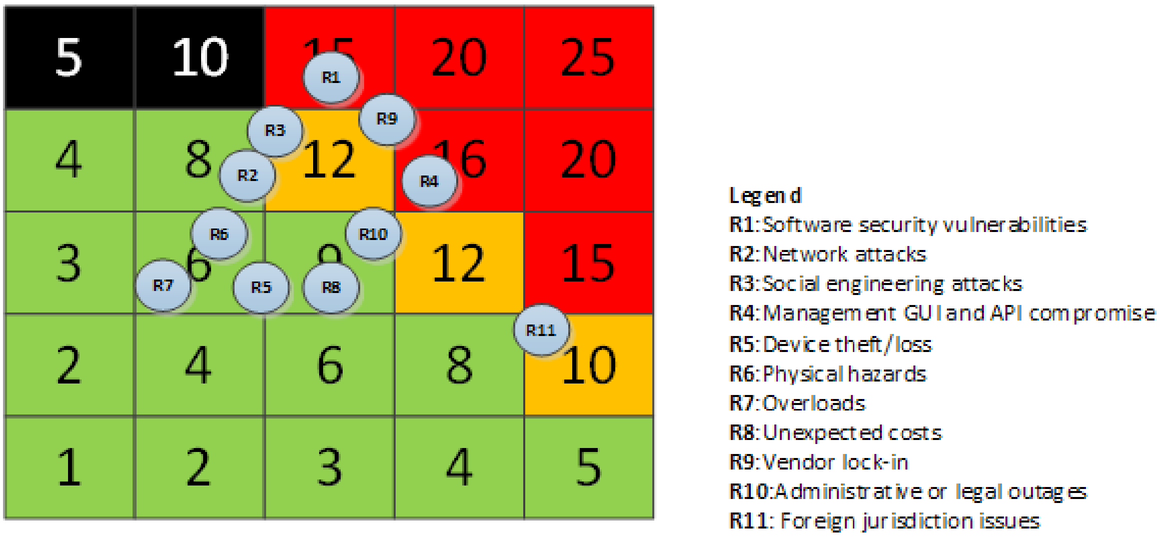
C.2.2 Assessing the risks

We look at the different risks in more details and rate them individually for this fictitious scenario:

RISK TYPE	LIKELIHOOD	IMPACT	RISK	REMARKS
R1. SOFTWARE SECURITY VULNERABILITIES	High	Very high	Major	For EasyAgriSelling software vulnerabilities are a big risk (because the payment and personal data of consumers is at stake). EasyAgriSelling will look closely at how the IaaS/PaaS is patched and updated.
R2. NETWORK ATTACKS	Medium	High	Significant	For EasyAgriSelling network attacks are not a major issue, because its employees are rather savvy when it comes to using the IaaS/PaaS.
R3. SOCIAL ENGINEERING ATTACKS	Medium	High	Significant	For EasyAgriSelling network attacks is an issue, because its employees have access to a lot of assets, and such attacks could ruin the SME. EasyAgriSelling will

				raise awareness on social engineering with staff.
R4. MANAGEMENT INTERFACE AND API COMPROMISE	Medium	Very high	Major	For EasyAgriSelling network attacks is an issue, because its employees have access to a lot of assets, and such attacks could ruin the SME. EasyAgriSelling will select a service which has two-factor authentication.
R5. DEVICE THEFT/LOSS	Low	Medium	Minor	For EasyAgriSelling this is a limited issue because most sensitive data (e.g. the payment data of consumers) is not on their employees' end-user devices.
R6. PHYSICAL HAZARDS	Low	Medium	Minor	For EasyAgriSelling physical hazards are an important risk,because it has SLAs to uphold with the farmers.
R7. OVERLOADS	Low	Medium	Minor	For EasyAgriSelling overloads are an important risk,because it has SLAs to uphold with the farmers.
R8. UNEXPECTED COSTS	Medium	Medium	Minor	For EasyAgriSelling this is not a major risks because increased costs are billed to farmers (pay-as-you-go) also.
R9. VENDOR LOCK IN	High	Very high	Major	For EasyAgriSelling it is important not to be tied to one provider, so it can always go to the cheapest cloud provider. EasyAgriSelling will select a provider which supports standard formats for code and virtual machines.
R10. ADMINISTRATIVE OR LEGAL OUTAGES	Medium	High	Minor	For EasyAgriSelling administrative and legal outages are an important risk, because it has SLAs to uphold with the farmers.
R11. FOREIGN JURISDICTION ISSUES	Medium	High	Significant	EasyAgriSelling works with farmers and consumers from several countries. The data and processes are about simple e-commerce and there are no specific legal requirements that could cause issues with foreign jurisdiction.

We show the different risks in a matrix (see below).



Legend
R1: Software security vulnerabilities
R2: Network attacks
R3: Social engineering attacks
R4: Management GUI and API compromise
R5: Device theft/loss
R6: Physical hazards
R7: Overloads
R8: Unexpected costs
R9: Vendor lock-in
R10: Administrative or legal outages
R11: Foreign jurisdiction issues

Figure 4: Risks for EasyAgriSelling (SME using IaaS/PaaS)

Annex D: Comparison with the 2009 cloud risk assessment risks

For the interested reader we show the relation with the risks in the 2009 ENISA cloud computing risk assessment:

- Risk 1 Lock-in: See R9 Vendor lock-in.
- Risk 2 Lack of control: Not in this guide.
- Risk 3 Compliance challenges: Certification against standards is addressed as an opportunity.
- Risk 4 Loss of business reputation due to co-tenant activities: Not in this guide.
- Risk 5 Cloud service termination: See R10 Adminstrative or legal outage.
- Risk 6 Cloud provider acquisition: Not in this guide.
- Risk 7 Supply chain failure: Not in this guide.
- Risk 8 Resource exhaustion: See R7 Overloads.
- Risk 9 Isolation failure: See R1 Software vulnerabilities.
- Risk 10 Cloud provider malicious insider: Not in this guide.
- Risk 11 Management interface compromise: See R4 Management interface compromise.
- Risk 12 Intercepting data in traffic: See R2 network attacks
- Risk 13 Data leakage on up/download: See R2 network attacks
- Risk 14 Insecure deletion of data: Not in this guide.
- Risk 15 Distributed denial of service attacks: See R2 Network attacks
- Risk 16 Economic denial of service: See R8 Unexpected costs.
- Risk 17 Loss of encryption keys: Not in this guide
- Risk 18 Undertaking malicious probes: Not in this guide.
- Risk 19 Compromise service engine: See R1 Software vulnerabilities.
- Risk 20 Conflicts between customer hardening and cloud environment: Not in this guide.
- Risk 21 Subpoena and legal risks: See R12 Foreign jurisdiction issues.
- Risk 22 Risk from changes of jurisdiction: See R11 Foreign jurisdiction issues.
- Risk 23 Data protection risks: See annex Legal compliance.
- Risk 24 Licensing risks: Not in this guide.
- Risk 25 Network breaks: See R6 Physical hazards.
- Risk 26 Network management: Not in this guide.
- Risk 27 Modifying network traffic: See R2 Network attacks.
- Risk 28 Privilege escalation: See R1 Software security vulnerabilities.
- Risk 29 Social engineering attacks: See R3 Social engineering attacks.
- Risk 30 Loss or compromise of logs: Not in this guide.
- Risk 31 Loss or compromise of security logs: Not in this guide.
- Risk 32 Backups lost: Not in this guide.
- Risk 33 Unauthorized access to premises: See R6 Physical hazards.
- Risk 34 Theft of computer equipment: See R6 Physical hazards.
- Risk 35 Natural disasters: See R6 Physical hazards.

Annex E: Procurement cheat sheets

In this annex we provide empty forms SMEs can use directly in their procurement.

E.1 Assessing security opportunities

OPPORTUNITY	RATING	EXPLANATION
O1. GEOGRAPHIC SPREAD		
O2. ELASTICITY		
O3. PORTABILITY		
O4. PHYSICAL SECURITY		
O5.INCIDENT RESPONSE AROUND-THE-CLOCK		
O6. SECURE SOFTWARE DEVELOPMENT		
O7. PATCHING AND UPDATING		
O8. BACKUPS		
O9 SERVER-SIDE STORAGE		
O10. SECURITY AS A SERVICE AND SECURITY ADD-ONS		
O11. CERTIFICATION AND COMPLIANCE		

E.2 Assessing security risks

RISK	LIKELIHOOD	IMPACT	REMARKS
R1. SOFTWARE SECURITY VULNERABILITIES			
R2. NETWORK ATTACKS			
R3. SOCIAL ENGINEERING ATTACKS			
R4. MANAGEMENT GUI AND API COMPROMISE			
R5. DEVICE THEFT/LOSS			
R6. PHYSICAL HAZARDS			
R7. OVERLOADS			
R8. UNEXPECTED COSTS			
R9. VENDOR LOCK-IN			
R10. ADMINISTRATIVE OR LEGAL OUTAGES			
R11. FOREIGN JURISDICTION ISSUES			

E.3 Security questions form

Question	Relevant information
1. How does the cloud provider manage network and information security risks?	
(Supporting evidence or guarantee?)	
2. Which security tasks are carried out by the provider, which type of security incidents are mitigated by the provider?	
(Supporting evidence or guarantee?)	
3. How does the cloud service sustain natural disasters affecting datacentres or connections?	
(Supporting evidence or guarantee?)	
4. How does the provider ensure that personnel works securely?	
(Supporting evidence or guarantee?)	
5. How is the physical and logical access to customer data or processes protected?	
(Supporting evidence or guarantee?)	
6. How do you ensure software security?	
(Supporting evidence or guarantee?)	

7. How does the provider ensure that personnel works securely?	
(Supporting evidence or guarantee?)	
8. How is the physical and logical access to customer data or processes protected?	
(Supporting evidence or guarantee?)	
9. How does the provider ensure that personnel works securely?	
(Supporting evidence or guarantee?)	
10. How is the physical and logical access to customer data or processes protected?	
(Supporting evidence or guarantee?)	
11. How is the physical and logical access to customer data or processes protected?	
(Supporting evidence or guarantee?)	
12. Which national legislation is applicable and which foreign jurisdictions are involved, for instance due to the physical location of datacentres or cables?	

TP-01-15-227-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

doi: 10.2824/508412

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu