

Aspects to consider within information security during procurement and use of cloud services

Version: 2.00
Release date: 4-Mar-2014

*This paper is licensed under Create Common Share Alike 3.0
<http://creativecommons.org/licenses/by/3.0/>*

Preface

This document is partly based on the authors' previous work [i-iii] made under the Creative Common Share Alike 3.0. Further, the legal part is partly based on [iv-vi]. If using this document, please reference it properly. The objective with this document is to provide guidance on information security aspects to organizations looking into procurement of cloud services, as well as to organizations already using cloud services. Further, legal aspects of cloud security and compliance frameworks are addressed too.

Finally, if you have any ideas for improvement – please do not hesitate to e-mail the contact person for the last version of the document listed below.

Version history

Version	Contributors	Released
1.00, first version	John Lindström and Dan Harnesk (LTU) et al.	19-Apr-2013
2.00, second version. Legal aspects added	<p>Project leaders/Editors: John Lindström and Dan Harnesk (LTU)</p> <p>Contributors: Eva Ekelund, Karl-Mårten Karlsson (Actea Consulting AB), Lars G Magnusson, Lars Perhard (W&P Advokatbyrå KB), Ulf Berglund (U&I Security AB)</p> <p>Primary contact: john.lindstrom@ltu.se</p>	4-Mar-2014

Contents

1. Introduction	3
2. Some legal aspects on cloud security.....	5
3. Aspects to consider within information security during procurement and use of cloud services	8
4. Creating a compliance framework for cloud computing – what to address in such a framework?	12
5. Sources.....	13

Word list and abbreviations used

IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
SECaaS	Security as a Service
XaaS	X as a service – used as a collective term to denote “anything” or “everything” as a service
CIO	Chief Information Officer – corresponds to a senior management role responsible for IT- and information issues within an organization
CISO	Chief Information Security Officer – corresponds to a senior management role responsible for information security issues within an organization
Security	When the term “security” or “information security” is used, it encompasses security
Information security	for IT, information systems and information

Before you read this document...please read:

This document has been written for use mainly within Sweden, and although most of the aspects discussed are of a general nature, readers should have this fact in mind while reading.

These guidelines should not be construed as technical or legal advice on any specific facts or circumstances. The content is not exhaustive and is intended for limited general informational purposes only. The authors make no representations as to accuracy, completeness, actuality, suitability, or validity of any information and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis with no warranties, and confers no rights. Readers should consult appropriate technical, accounting or legal consultants concerning any specific question or the relevance of the subjects discussed herein to particular factual circumstances.

1. Introduction

This document concerns aspects of information security, including related legal and compliance matters, regarding cloud services. These cloud services are often referred to as SaaS, IaaS and PaaS and can of course be combined, or only partly be used, together with an organization's private IT environment. Additional recently introduced abbreviations are for instance SECaaS and XaaS. As the interest for cloud services start to gain momentum among stakeholders in an organization, and a procurement process is about to start (or if cloud service already has been procured), there are two questions to consider:

- **What is the problem and challenge with security in the cloud compared to methods or practices used previously?** The problem and challenge involve a number of issues, e.g. it is partly new, and that competences and personnel not existing in all organizations are required. The sourcing of personnel and specific competences may need to be examined. Many organizations will also probably need to make changes in their own security and risk management processes, update the legal/regulatory and compliance frameworks used, because there will not be the same transparency and possibilities to investigate, impact or follow up on issues. Many organizations are not familiar with procuring cloud services and the various legal issues which need to be considered.
- **What security aspects need an organization consider?** There is no exact template, as all organizations differ in their business processes. One example is if personal data is stored, processed or communicated within a cloud service, it may require additional actions regarding, e.g., clarification of responsibilities, agreements for export of personal data, and appointing a Personal Data Officer. However, this document comprises a number of aspects which we consider are of importance. Any organization should firstly consider what and where there can be problems before this document is used, not become too influenced by it and overlook important factors when the contents in this document are used and "ticked off".

Most organizations have a number of requirements regarding security (originating from regulations, laws or business requirements), and these usually differ depending on whether the organization is a small business, a public corporation, a public authority/government agency, or municipality. In most cases, the top management of an organization has a responsibility to investigate risks related to IT, as well as to take action to mitigate possible risks in a responsible manner. A hinder related to cloud services is that an organization, in most cases, does not have the same possibilities to control, impact or influence, and that an increased transparency is required from providers (see [1, 3, 7]). There is a need to build trust in between the parties. From a legal standpoint, work tasks with related responsibility to maintain the levels of security can be, to a certain degree, delegated to providers by a contractual agreement. For example, regarding a public corporation, its board and president (top management) are always ultimately responsible to the shareholders. In general, there is a legal obligation to continuously investigate risks and maintain an adequate level of security.

Among the factors affecting the security requirements for a cloud service, importance of the information processed is as well how it needs to be protected (confidentiality, integrity, secure backup etc.), and what availability that is required. To facilitate the assessment of the availability level required, organizations need to analyze their business processes on a high level and also map out which IT resources and information systems etc. that are used in the processes. Following, an assessment of which business processes that are critical, i.e. that always need to be operational or operate at a very high level of availability, should be conducted. It is easier to "cloud source" the support for parts or whole business processes that are not critical. A security audit of a cloud service requires significant time and resources. Thus, an organization ought to be more thorough while auditing cloud services used in critical business processes compared to for non-critical business processes. A security audit should not only be made initially, but be made continuously as long as the cloud service is used. The security audit should always use your own policies related to the

area. Input to the audit requirements are, for example, changes in business and business environment requirements. Consequently, it is a good idea to start with a business process which is non-critical nor processes any confidential information, to learn and get experience before addressing critical business processes where demands are higher. Required are an analysis and a plan.

In addition to listing and highlighting issues and problems, we link what business value can be created upon appropriate planning, management and actions pertaining to those issues or problems.

Concerning business value for an organization, business value can be interpreted very differently, depending on type of organization, its mission and stakeholders. Preferably, the business value should be measured in straight figures like total-cost-of-ownership (TCO), where the cost for having a solution run by the organization is compared to using a cloud service, return-on-investment (ROI) or the like. However, finding these costs and cash flows can be difficult, as many of the business values are qualitative rather than quantitative. We suggest, as part of any cloud services business case, that the business value generated from information security and related topics are described and highlighted – in order to show that not only costs are generated but also business value. Examples of business value categories, found in business literature and research, applicable for a cloud service context are: improved organizational performance/profitability (PERFORMANCE), improved competitive advantage (COMPETITIVENESS), creative synergy (SYNERGY), respectively improved management ability (MANAGEMENT). Below, there are one or more examples of different business values for each category:

- **PERFORMANCE** – productivity increase, more efficient processes, lower costs, increased profitability, higher return on capital or investment, increased sales, more mobile workforce.
- **COMPETITIVENESS** – facilitator for new products or services, improved adaptability/changeability and scalability (i.e. pay for usage), increased ability to attract or get resources that are difficult to imitate/rare/valuable/non-substitutable and make these productive and create competitive advantage, more content customers and employees, shorter time to markets for products/services, lower cost barrier, ability to reach new markets, lowered risk.
- **SYNERGY** – improve the relation between information systems/IT and organization/strategy/structures/management processes to create synergies among strategies/organization/processes/technology/humans and further increase the effect from technology to reach higher profitability.
- **MANAGEMENT** – management gets better understanding of available resources/customers etc. that may lead to better sourcing of resources and improved product/service design, management and organization are better prepared to manage a crisis, increased trustworthiness/reliability from customers and the own organization, organization is able to manage business/legal requirements.

This document has a focus on improved management ability. Recommended is that you, besides using this document, further read and use the documents listed in the reference section.

2. Some legal aspects on cloud security

This section aims to address some crucial legal aspects on cloud security that a potential organization should consider before deciding to migrate its IT-operations to the cloud.

Inside or outside the [fire]walls

In the legal analysis, it is first necessary to investigate whether any legal obstacles to the use of cloud services exist. This analysis should be conducted from the viewpoint of any jurisdiction where the intended cloud services shall be produced, used, stored, or where from any other viewpoint the services in question will gravitate. In practice, e.g., from a Swedish perspective as in many other jurisdictions, there are few direct legal challenges. However, sometimes requirements set forth in legislation may be difficult to fulfil using cloud services due to their particular features in relation to traditional IT services produced within the “four [fire]walls” of the using entity’s own facilities.

Such obstacles are often related to specific security requirements for a given activity or for a particular type of information. However, more common is that general legal requirements for security, e.g., confidentiality, security in the processing of personal data¹, or stock exchange requirements need to be converted to requirements set out when choosing a cloud service provider or to security requirements in the contract for cloud services. With an increased flow of business secrets that are sent and placed outside corporate firewalls, the encryption of data must also be considered.

Information security

Security issues from a technical perspective often go hand in hand with the legal issues as all aspects of security should be addressed in a cloud sourcing agreement. A migration of services to the cloud places special demands on the systematic work of information security, not only on the supplier but also on the customer. Deficiencies regarding information security that already exist at the customer’s end before any decision is taken to use cloud services will not automatically be corrected through migration. In most cases, it will instead become more complex to address the shortcomings when the services are placed in a cloud environment. However, used in the correct way, cloud services can in most cases provide an adequate level of security.

Due diligence

A general observation is of course, that a customer should not rely entirely on a well-designed contract, but should also investigate the status and history of a supplier. This can, for example, involve obtaining references or carrying out a more or less comprehensive survey of the supplier’s operations and status, from a legal, financial and technical perspective (due diligence), where the customer may for example have access to the supplier’s documentation, routines and processes in order to determine the supplier’s ability to meet the customer’s requirements. These aspects are particularly important as cloud services in most cases are delivered by players in the international arena.

International aspects

Cloud services are often performed across borders and in different parts of the world simultaneously. Thus, it is not sufficient simply to find out where data is stored, but also where it is processed in the case that cloud services are used for the processing of data, since providers often try to optimise their computing power when processing data. This means that information can be transferred for the purposes of processing, and then returned and stored in processed form at the agreed storage site. The consequence is that a customer -

¹ The EC Directive on data protection requires that all member states have rules that provide an equivalent protection for personal data and privacy, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT> EU as well as Sweden as a member state can be considered to have a high standard concerning the protection of personal data. The EC-directive has been implemented in Sweden and here you can find the Act in English: <http://www.government.se/content/1/c6/01/55/42/b451922d.pdf>

regardless of what the contract says - may be exposed to other countries' legal systems. These technical aspects are important in determining how, for example, personal data protection issues are solved. Moreover, data stored within a particular country can, for example, be subject to publishing laws or the equivalent, or forcibly made available to authorities such as police or intelligence agencies. Such circumstances should also be considered before cloud services are used.

Risk analysis

Before a decision on transition to the cloud is taken, the customer must analyse the applicable risks and requirements in the given situation. It is essential that the customer converts the results of the analysis to precautionary measures and communicates these to the provider. Cloud Security Alliance [7] has identified a number of primary threats to deal with in connection with a migration to the cloud elaborating on many of the risks.

Personal Data legislation

An example of a legal framework that applies for every use of services is personal data legislation. Users of cloud services need to be aware of the responsibilities arising from the provisions of the [Swedish] Data Protection Act². This means, amongst other things, that the Act's rules on when processing of personal data is permitted must be taken into account, that the Act's security requirements must be met and that there must be a [written] contract between the parties that regulates the cloud service provider's processing of personal data. In order for personal data to be included in a cloud service whereby data may be stored (or processed) outside the EEA (i.e. EU and EFTA countries), specific legal requirements apply. Anyone who wants to use a cloud service for storing personal data must therefore either ensure that storage occurs only within the EEA or actively ensure that storage meet the requirements for transfer to a third country.

As mentioned above cloud services are often carried out across borders and in different parts of the world. From the perspective of personal data legislation, however, the transfer for the purposes of processing, the processing itself and the returning of the processed data are all processing of personal data. The contract should clearly state where the customer's data may be processed (for example determined to a region, country/countries or data centres) and that this processing is traceable. Where systems' administrative work may be carried out should also be covered in the contract.

The contract should, as a minimum, include the provisions that according to the Personal Data Act should be found in a *contract* with a party who processes data on behalf of the customer; also ensure control over where and by whom personal data is processed. For example, the customer must consider, including provisions that the provider shall assist the customer in questions concerning obligations under the Personal Data Act, that consent should always be obtained from the customer in the case of the use of a subcontractor or if personal data shall be transferred to a third country (i.e. countries outside the EEA), that the provider shall bear the costs and risks relating to agreements with subcontractors and that the provider will reimburse the customer for any damage caused to the customer due to the supplier or subcontractor failing to meet obligations arising from the contract.

If the contract allows the cloud service provider in practice, directly or indirectly through subcontractors, to process the customer's personal data outside the EEA, the contract must include regulation of the legal basis for this. There are several ways in which the customer can ensure that requirements for the transfer of personal data to a third country are met. The customer can, for example, conclude a separate standard contract (a 'model clause contract') with the provider that regulates the transfer of personal data. Here it is also important to consider what kind of data is being transferred in the particular case, how long the processing will last and what kind of data protection rules exist in the country where the processing wishes to be carried out.

² <http://www.datainspektionen.se/in-english/>

Confidentiality

In some cases, legal requirements set explicit demands that certain information shall be given confidentiality protection. One example is the framework of the [Swedish] Official Secrets Act (2009:400). Confidentiality requirements need to be addressed in the contract with the provider of cloud services. The contract should state that the customer's data is not allowed to be disclosed to third parties or to be used by the provider for purposes other than the provision of services. The provider should ensure that access to the customer's data is limited to those persons within the organization who need access to the data in order to perform their duties.

It should also be regulated how and in what way the provider can monitor and collect information about how and to what extent the customer uses the service (such as frequency, changes in volume and bandwidth usage etc.). If the provider is given such a possibility, this should be strictly regulated and in addition state which parties (companies, authorities etc.) the provider is able to share such information with.

Particularly sensitive data shall be protected by encryption when transferring to and from the service provider. It should also be considered whether the data should be protected by encryption when in "rest". Furthermore, it shall be ensured that the service meets the applicable regulations on export control, particularly in cases where the service is delivered from the USA.

The contract should also include a requirement for the provider to store the customer's data separate from other customers' data.

Service levels

Depending on whether the service is wholly or partly standardized, it may be necessary to contract on customized service levels. If the provider states a percentage for availability, this shall be converted into absolute numbers in order to get a precise estimate of, for example, how many minutes per month a service can be down without incurring liability for the provider. Almost any cloud services contract shall contain elaborated stipulations on service levels. The Swedish Standard Institute (SIS) has recently presented a standard on service level agreements (SLA). The most important legal aspect on SLA, apart from the contractual aspects, is the possible sanction. Penalty payments are often given as a sanction when service levels are not met. In case of delays in the customer's connection or service failures, the customer should be compensated.

A fundamental requirement from the customer on the provider should be that work with information security (see next section) is conducted in accordance with established standards within the field – and that adequate security measures exist. The structure and level of each security measure should be determined by the result of the customer's analysis of risks and requirements.

Further, it is necessary to consider who shall be responsible for loss of data (for example due to technical failures, theft of data or intrusion) and how this term is defined in the particular case. It is important that the contract clarifies precisely what is considered to be included in such a loss, and which party shall bear responsibility for precautionary measures such as resets and back-ups. The customer should therefore critically review the contract regarding if data loss is considered to be indirect harm, and as such exempt from the responsibility of the provider.

3. Aspects to consider within information security during procurement and use of cloud services

This section does not comprise a complete collection of aspects that need to be considered. The intention is to provide a basic structure for the work regarding security to enhance and continue to build upon. Hopefully this basic structure will enable organizations to save time, resources and money. The sources used are explicitly marked as references. However, the authors' own experiences or research have been added into the text without any explicit references.

The aspects are tagged with a level, which corresponds to the level where the aspect should be addressed. The levels used are strategic (s), tactical (t) and operative (o). By *strategic* we mean top management level consideration and decision that affect a whole organization with a long time frame (i.e. years). By *tactical* we mean the management responsibility for functions or processes and decisions that affect people's work with a medium time frame (i.e. months). Finally, by *operative* we mean department or group level where the decisions impact on the daily business with a short time frame (i.e. weeks or days). Suggested is to start with the strategic level aspects, and work downwards to the operative level.

Below is a list of security aspects to consider:

<u>Level</u>	<u>Aspect</u>	<u>Who has most interest</u>	<u>Source</u>
S	Compliance with applicable legal requirements and regulations. Which are fulfilled, and which need to be fulfilled?	Top management	[1, 4]
S	Compliance with the own security policy. Anything that renders problems? Is there a need to change the own security policy?	Top management	[1, 3, 4, 6]
S	Fulfillment of requirements from standards, certifications, "best practices" etc. (i.e. compliance). Which requirements should/must we fulfill and - which does the provider fulfill? How can we demonstrate this at a (re)certification?	Top management	[1, 3, 4]
S	Audit and evidence collection. How can audits be conducted, and how can potential evidence needed be collected? Is there a common audit for all customers together?	Top management	[3]
S	Risk management – transparency at provider. Is it possible to maintain a continuous high qualitative risk management/mitigation? Are there audits made by independent third parties after a standard model with publicly known criteria or metrics? Are the audit protocols for a number of previous years available?	Top management, procurement function	[1, 3, 4]
S	Insurance. Does the provider have an insurance which covers damages or costs that can arise due to data breach, mistakes or other causes? Does insurance cover what the identified risks can cause?	Top management, procurement function	

S	Information issues. Will our organization have ensured access to our own information during a certain period of time from a notified point in time, even if the cloud service is shut down for any reason, or during a contractual dispute? Ownership of information – always owned by our own organization no matter what? Will the information be kept partitioned at storage and processing (possible to recreate if one or more partitions fail), and is it due to the partitioning more difficult to recreate information at a breach? Is the information stored or processed globally, or at appointed data centers? The last issue is of importance if there is sensitive personal information which is affected by, for example, the EU Data Protection Directive, and Safe Harbor/Patriot Act in the USA etc.	Top management	[1, 3, 4]
S	Long term digital preservation and storage. How do we want this to be set up and operate? Who has responsibility for migration and emulation etc. of the formats stored? Does the provider manage all this, or is more knowledge and competence needed?	Top management, CIO	
S	In case of a potential change of cloud service. Is it possible to port (or directly use) the information and its meta-data in new environments and other providers' cloud services?	Top management, CIO, architect	[3, 4]
S	Business continuity planning – to extend the own or synchronize with the provider's. Is it easy, or does it comprise a large effort? How often to practice?	Top management, resp. for business continuity planning	[1, 3, 4]
S/T	How far does the provider's responsibility stretch and where does the own responsibility end (does the provider responsibility end at the hypervisor, i.e. the virtualization/physical- and environmental security, or does it stretch shorter/longer)? What applies for security checks of infrastructure, operating systems, data/information, applications etc.? Is the virtualization shared with other customers, or is all separated per customer? How do we want it?	Top management, procurement function	[3, 4]
S/T	Disaster recovery planning on cloud service/system level – how is it set up? Are our own services/systems integrated with the provider's?	Top management, IT and Information systems departments	[1]
S/O	Disaster recovery – how is the provider's process devised? Is there a need to integrate with our own process, or is it enough that the provider's process looks OK? How often to test?	Top management, IT and Information systems departments, operation/support	[3, 4]
S/O	Incident response – how is the provider's process set up, and how can the own process be integrated with the provider's process? How often to test?	Top management, IT and Information systems departments, operations/support	[1, 4]

T	<p>Identity and access management (IAM). How many such IAM-systems will our organization be involved in? Are there proprietary and/or different variants used by the potential providers? Some of these IAM-systems require additional knowledge, resources and separate control processes. Is it possible to find an interoperable solution that all or several providers can use in common? How many security levels are required? What users/roles will we need to have? Do we have a process to add/remove users and roles?</p>	Architect, procurement function	[1, 2, 3]
T	<p>Service integrity. Does the provider's development process concern security and personal integrity issues during the whole lifecycle of the cloud service? Does the delivery of the cloud service fulfill the contractual requirements on security (availability, monitoring/audit/logging, response times and support level)?</p>	Procurement function	[1, 3, 4]
T	<p>Security at end users (i.e. end point security). Do we need training and an awareness program to achieve a secure behavior (for example, towards social engineering, identity theft, phishing, viruses, malicious links etc.)? How should users (and administrators) securely connect to the cloud service – requirements? Is it possible to have "single sign-on" together with other cloud services/systems depending on how directory services, keys, key management and firewall policies look like? What does the own security policy require of the IT environment and users in general?</p>	CISO	[1, 3, 4]
T	<p>Security in the cloud service interfaces. How are the cloud service's security levels in the interfaces set up? Are the interfaces for instance securely developed, see [5], and are any APIs (Application Programming Interfaces) or other possibilities to connect within, around or to the cloud service secure and securely developed? Encryption levels and key generation/management? How and how often is all this tested?</p>	CISO	[2, 3, 4]
T	<p>Protection of information. Is the information always protected while being within the cloud service according to the requirement/classification in the security policy (encryption, integrity, backup and recovery etc.)? How is the information kept separated from other organizations' information? Levels of encryption and key management – how are these set up? Backup – method, safe and secure storage? How often is all this tested?</p>	CIO/CISO	[1, 2, 3, 4]
T	<p>Dynamics of the cloud service. How quickly can additional resources or performance <u>always</u> be provided, and for how long? What is our need regarding dynamics?</p>	CIO	[3]

- | | | | |
|---|---|-------------|--------|
| O | Physical security, background checks and logging of personnel at the provider etc. The requirements posed on the provider shall mirror the own business requirements on security. Are backups safe and secure? | Buyer | [1, 3] |
| O | Is the cloud service developed to prevent intrusion? In case of an intrusion, will the intruder get access to information stored in other data centers? What is monitored and logged? How is the monitoring function set up, and is it manned 24x7? | Buyer, CISO | [2, 4] |
| O | Does the cloud service have a standardized open interface to MSS (managed security services) providers for its customers? Do we need or want this? | Buyer, CISO | [3] |
| O | Patch management. How is patch management managed within the cloud service software, security solutions and supportive software like operating systems, device drivers, virtualization etc.? Is there a process for this and is it executed in a controlled manner? Are always new parameter settings changed by a patch reverted back to the prior settings if wanted? | Buyer, CISO | [2, 3] |
| O | Who have, and who should have access and be able to log in to the cloud service, supportive software, and the information stored in the cloud service? Do these really need to be able all that they can, or do they have too much access rights or authorization (goes for both employees at the provider and the own organization)? | Buyer, CISO | [2] |
| O | How often are penetration tests and different attacks applied towards the cloud service? What were the results of prior penetration tests? Examples are attacks towards password sources and authentication mechanisms, password- and key cracking, availability (DDOS/EDOS) etc.? | Buyer, CISO | [2, 3] |
| O | Can any user add links, applications or other source code to the cloud service? If needed, can this be controlled by authorization? Logging? | Buyer, CISO | [2] |
| O | Removal/deletion of data. If data should be removed/deleted on demand by us, how is this managed and how can we ensure that the data has really been removed/deleted? How long will it take? What goes for the backups? | Buyer, CISO | [3] |

4. Creating a compliance framework for cloud computing – what to address in such a framework?

A compliance framework for cloud computing should preferably be integrated into an organization's overall risk management and compliance set up. Compliance can be seen as a tool for top management to ensure that risks are managed and requirements from legal/regulatory bodies, customers, standards, certifications or best practices that should be honored are in fact honored. Further, if an organization has additional internal requirements that should be upheld, those can be added to a compliance framework as well to be followed up on and kept updated. There are a number of ways to set up an organization's overall risk management and compliance activities, but those will not be covered in this document.

The idea with this section is that an organization should get an idea on what "elements/controls" that a simplistic compliance framework for cloud computing can comprise. The elements/controls are aimed to be input for risk management departments, CIOs, CISOs, or other functions or roles responsible to honor requirements or to proactively monitor, manage and mitigate existing and emerging risks related to cloud services used by the organization in its operations. A further comprehensive set of elements/controls can be found in [7] (which maps to various international standards), and if used it should be adapted to your organization and the applicable Swedish conditions related to your business context.

Below are a number of elements/controls that can be part of a cloud computing compliance framework:

- Risk management – transparency at provider. Needed is to maintain a continuous high qualitative risk management/mitigation. Do we do the audits ourselves, or are the audits made by independent third parties after a standard model with publicly known criteria or metrics? Where are the audit protocols for a number of previous years available? [1, 3, 4]
- Risk management – internal. What risks should be tracked and how often should risk evaluations be conducted? Who is responsible and will manage the risk mitigation?
- Compliance³ with legal requirements and regulations. Which need to be fulfilled, which are and which remain to be fulfilled? [1, 4]
- Fulfillment of requirements from standards, certifications or "best practices" etc. Which requirements should/must we fulfill and - which does the provider fulfill? If there is a gap – how to manage that gap? How can we demonstrate this at a (re)certification? [1, 3, 4]
- Compliance with essential customer requirements. Which are the essential requirements (necessary to stay in business), and which are fulfilled or remain to be fulfilled?
- Compliance with the own security policy or policies. Anything that renders problems? Is there a need to change the own security policy? [1, 3, 4, 6]
- Business continuity planning – is the business continuity planning involving the provider and our own organization's related critical processes in line with the internal/external requirements (i.e. available within a decided timeframe in case of problems)? How often to practice crisis management, disaster recovery and incident response? [1, 3, 4]

³ It can be worth noting that not only the Swedish and EU legislation need to be considered, as planned and existing legislation in the USA can have an impact as well.

5. Sources

- [1] Microsoft (2010). Cloud Computing Security Considerations. www.microsoft.com
- [2] CSA – Cloud Security Alliance (2010). Top Threats to cloud computing v1.0. www.cloudsecurityalliance.org
- [3] ENISA (2009). Cloud Computing: Benefits, risks and recommendation for information security. www.enisa.eu
- [4] CSA – Cloud Security Alliance (2009). Security Guidance for critical areas of focus in cloud computing v2.1. www.cloudsecurityalliance.org
- [5] OWASP (2010). OWASP top ten project - www.owasp.org
- [6] Microsoft (2010). Information Security Management System for Microsoft Cloud Infrastructure - <http://www.globalfoundationservices.com/security/documents/InformationSecurityMangSysforMSCloudInfrastructure.pdf>
- [7] CSA – Cloud Security Alliance (2013). Cloud Controls Matrix v1.4 - <https://cloudsecurityalliance.org/research/ccm/>

Some further specific Swedish sources of information relating to the cloud (some of it not available in English):

- [i] Cloud Sweden (2011). Areas and problems to consider within information security and digital preservation during procurement and use of cloud services, v1.1.1, <http://natverk.dfs.se/node/21531#attachments>
- [ii] Cloud Sweden (2011). Legal issues when moving to the cloud – a checklist. <https://natverk.dfs.se/engelsk-oversattning-legal-issues-when-moving-cloud-checklist>
- [iii] There are a number of particular aspects to take into consideration before implementing cloud services in bodies and organizations within the public sector in Sweden, e.g., the principle of public access to official records - these are summed up in a document by Cloud Sweden: <http://cloudsweden.files.wordpress.com/2013/06/molnet-i-offentlig-sektor.pdf> (available only in Swedish).
- [iv] Edvardsson and Frydinger (2013). Legal – Molntjänster, Norstedts (only in Swedish)
- [v] IT&Telekomföretagen (2010). Cloud Computing, kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010 (in Swedish) <http://www.itotelekomforetagen.se/standardavtal/boken-om-cloud-computing>
- [vi] IT&Telekomföretagen (2010). IT&Telekomföretagens standardavtal Cloud Computing version 2010 also available in English, <http://www.itotelekomforetagen.se/standardavtal/boken-om-cloud-computing>

Personal information – Swedish Personal Data Act and the Personal Data Ordinance, and the Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), as indicated above cf. www.Datainspektionen.se which comprises useful information on personal data legislation and related security issues also in English.

Further documents of interest can found at CSA's main homepage at: <https://cloudsecurityalliance.org/>