GUIDELINES
Areas and problems to consider within information security and digital preservation during procurement and use of cloud services

Cloud Sweden
Powered by Dataföreningen

English version 1.1.1 - 2011-01-17

This paper is licensed under Creative Commons Share Alike 3.0
http://creativecommons.org/licenses/by/3.0/
## Change and Approval lists

### Change list

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06-Jun-2010</td>
<td>John Lindström, Lulea University of Technology Contributions from Ulf Berglund, Karl Mårten Karlsson och Erik Borglund</td>
<td>0.1</td>
<td>First version for review by the Security&amp;Legal subgroup</td>
</tr>
<tr>
<td>14-Jun-2010</td>
<td>John Lindström, Lulea University of Technology</td>
<td>0.2</td>
<td>Additions after review by management team</td>
</tr>
<tr>
<td>28-Jun-2010</td>
<td>John Lindström, Lulea University of Technology</td>
<td>0.3</td>
<td>Minor additions before internal review</td>
</tr>
<tr>
<td>5-Jun-2010</td>
<td>John Lindström, Lulea University of Technology Contributions from Lars G Magnusson and Karin Ahlin.</td>
<td>0.4</td>
<td>Smaller changes and additions after internal review during the Summer of 2010</td>
</tr>
<tr>
<td>14-Sep-2010</td>
<td>John Lindström, Lulea University of Technology</td>
<td>1.0</td>
<td>Final review with adm. additions by Inger Gran</td>
</tr>
<tr>
<td>6-Dec-2010</td>
<td>John Lindström, Lulea University of Technology Contributions from Erik Borglund, Lars G Magnusson, Karl-Mårten Karlsson, Lars Perhard Inger Gran, Dataföreningen John Lindström, Lars Perhard, Cecilia Magnusson Sjöberg, Gail Watt</td>
<td>1.1</td>
<td>Updates and addition of linkage towards business value</td>
</tr>
<tr>
<td>17-Jan-2011</td>
<td>John Lindström, Lulea University of Technology</td>
<td>1.1.1</td>
<td>Translation to English. Minor additions/edits</td>
</tr>
</tbody>
</table>

### Reviewers and Approval

<table>
<thead>
<tr>
<th>Namn</th>
<th>Approved version</th>
<th>Organization</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management team</td>
<td></td>
<td>Cloud Sweden</td>
<td>11-Jun-2010</td>
</tr>
<tr>
<td>QA-team</td>
<td></td>
<td>Cloud Sweden</td>
<td></td>
</tr>
<tr>
<td>Approx. 70 members of Cloud Sweden</td>
<td>0.4 - preliminary</td>
<td>Cloud Sweden</td>
<td>27-Aug-2010</td>
</tr>
<tr>
<td>Security subgroup and other members of Cloud Sweden</td>
<td>1.1</td>
<td>Cloud Sweden</td>
<td>3-Dec-2010</td>
</tr>
</tbody>
</table>
List of contents

1 Introduction ............................................................................................................................................. 1

2 Areas and problems within information security and digital preservation to consider ......................3
  2.1 Sources ....................................................................................................................................................... 9
  2.2 Questions, Issues or suggestions for improvement .................................................................................... 9

Word list and abbreviations used

SaaS Software as a Service
IaaS Infrastructure as a Service
PaaS Platform 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
Preservation “Preservation” is a shorter way of writing digital preservation

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.
INTRODUCTION

This document concerns aspects of information security and digital preservation regarding cloud services. Previously, for instance the word e-services was used to delimit this area. During the last years, the service content has expanded to not only comprise mainly software but to also include infrastructure and platforms. These 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.

When cloud services are starting to gain interest 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 and preservation in the cloud compared to methods used previously? The problem and challenge involve a number of issues, e.g. it is partly new, 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 process” and “preservation process” 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 now need to be considered.

- What security and preservation problems or areas need an organization consider? There is no exact template, as all organizations differ in their business processes. However, below are a number of problems and areas, 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 and preservation (regulations, laws or business requirements), but these usually differ depending on whether it is a small business or a public corporation or compared to 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. An organization’s top management also has responsibility for questions related to preservation. 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]). 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 and preservation 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 as well as adequate routines for preservation.

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.

Factors with impact on preservation in a cloud service are, for example, how long the stored information will be used, and how it may be used in the future as well as how fast stored information can need be made accessible for use. Required are an analysis and a plan.

This document is intended to be positioned in between the most simple and advanced publicly accessible documents concerning security for cloud services. Further examined are also preservation issues. The table in section 2 has its areas and problems linked to possible business value creation. In the table, the column “Business Value” includes what can be the result of thorough planning and well considered actions pertaining to the area or problem in question. Concerning business value for an organization, it 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. The two mentioned metrics require that an organization is able to produce a large volume of numbers for costs, or deduce to and from where the cash flows involved should be assigned. Finding these costs and cash flows can be difficult, as many of the business values are qualitative rather than quantitative. The different business values used have been gathered from the work within Cloud Sweden, business literature and research. As an attempt to simplify the linkage of security and preservation towards business value, different types of business values have been grouped into four main categories: improved organizational performance/profitability (PERFORMANCE), improved competitive advantage (COMPETITIVENESS), creative synergy (SYNERGY), respectively improved management ability (MANAGEMENT). Currently, this version of the document has a focus on improved management ability. Below, there are one or more examples of different business values for each main 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.

We recommend that you, besides using this document, also read and use the other documents in the reference list.
2 AREAS AND PROBLEMS WITHIN INFORMATION SECURITY AND DIGITAL PRESERVATION TO CONSIDER

This document is not a complete collection of areas or problems that need to be considered. The intention is to provide a basic structure for the work regarding security and preservation 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 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 areas and problems, and work downwards to the operative level.

Swedish public authorities/government agencies must consider legal issues prior to employing cloud computing solutions. There are number of legal concerns that ought to be addressed proactively.

In practice, it is difficult to let one single official be in charge of the legal issues. Legal issues – depending on application, of course – require knowledge within the areas of rights of access to public documents, archival rules, personal data processing, application of administrative procedure rules, procurement etc. Therefore it is recommended that cloud computing applications within the public sector be governed by what may be referred to as a strategy or policy for legal system management.

To briefly illustrate the kind of legal framework governing cloud computing, attention to the fact that Swedish public authorities have an obligation to ensure that they are organized in a way that makes it possible: (i) to provide anyone with public documents, (ii) to satisfy the administration of adjudication and other administrative functions, and (iii) to also meet the legal requirements for research. Hence, the authority/agency shall insure that there is compliance to the Swedish Archives Act and thereby the constitutional right of access to public documents according to Chapter 2 of the Freedom of the Press Act.

Furthermore, public authorities, as well as private entities, shall insure that personal data is correctly processed and managed according to the Personal Data Act and related legislation etc. The overall aim of this Act is to protect the right to privacy.
<table>
<thead>
<tr>
<th>Level</th>
<th>Area/Problem</th>
<th>Who has most interest</th>
<th>Business Value</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Complianceⁱ with legal requirements and regulations. Which are fulfilled, and which need to be fulfilled?</td>
<td>Top management</td>
<td>MANAGEMENT</td>
<td>Partly [1], [4]</td>
</tr>
<tr>
<td>S</td>
<td>Compliance with the own security policy. Anything that renders problems? Is there a need to change the own security policy?</td>
<td>Top management</td>
<td>MANAGEMENT</td>
<td>[1, 3, 4, 6]</td>
</tr>
<tr>
<td>S</td>
<td>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?</td>
<td>Top management</td>
<td>MANAGEMENT</td>
<td>Partly [1], [3, 4]</td>
</tr>
<tr>
<td>S</td>
<td>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?</td>
<td>Top management</td>
<td>MANAGEMENT</td>
<td>[3]</td>
</tr>
<tr>
<td>S</td>
<td>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?</td>
<td>Top management, procurement function</td>
<td>MANAGEMENT</td>
<td>Partly [1], [3, 4]</td>
</tr>
<tr>
<td>S</td>
<td>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?</td>
<td>Top management, procurement function</td>
<td>MANAGEMENT</td>
<td></td>
</tr>
</tbody>
</table>

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

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?

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?

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?

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?
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

MANAGEMENT Partly [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

MANAGEMENT Partly [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

MANAGEMENT Partly [1, 4]

T 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?

Architect, procurement function

Performance SYNERGI

[1], partly [2, 3]

T 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)?

Procurement function

Competetive-NESS

[1, 3, 4]

T 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?

CISO

Performance COMPETETIVE-NESS

Partly [1, 3, 4]
<table>
<thead>
<tr>
<th>T</th>
<th>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?</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>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?</td>
</tr>
<tr>
<td>T</td>
<td>Dynamics of the cloud service. How quickly can additional resources or performance always be provided, and for how long? What is our need regarding dynamics?</td>
</tr>
<tr>
<td>O</td>
<td>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?</td>
</tr>
<tr>
<td>O</td>
<td>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?</td>
</tr>
<tr>
<td>O</td>
<td>Does the cloud service have a standardized open interface to MSS (managed security services) providers for its customers? Do we need or want this?</td>
</tr>
</tbody>
</table>

| CISO | PERFORMANCE [2], partly [3, 4] | COMPETITIVENESS SYNERGY |
| CIO/CISO | MANAGEMENT [1], [2, 3, 4] | COMPETITIVENESS |
| CIO | PERFORMANCE [3] | COMPETITIVENESS |
| Buyer | MANAGEMENT [1], [3] | |
| Buyer, CISO | PERFORMANCE Partly [2], [4] | |
| Buyer, CISO | PERFORMANCE [3] | SYNERGY |
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?

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)?

O  How often are penetration tests and different attacks applied towards the cloud service? Examples are attacks towards password sources and authentication mechanisms, password- and key cracking, availability (DDOS/EDOS) etc.?

O  Can any user add links, applications or other source code to the cloud service? If needed, can this be controlled by authorization? Logging?

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?
2.1 Sources


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).

Digital preservation [relating to public authorities] – Swedish Freedom of the Press Act and Swedish Archives Act

2.2 Questions, issues or suggestions for improvement

If you think there are questions or have ideas on how to improve this document, please feel free to contact any of the persons listed below:

- Information security: John Lindström - john.lindstrom@ltu.se
- Information security: Ulf Berglund – 2ube@glocalnet.net
- Information security: Karl Mårten Karlsson – karlmarten.karlsson@gmail.com
- Digital preservation: Erik Borglund – erik.borglund@miun.se
- Legal matters: Lars Perhard - lars.perhard@weplaw.se