Cloud computing is being labeled as a new Internet technology that provides cost-efficient and flexible infrastructure and applications to the business. However, there seems to be a gap between the technical possibilities and the practical usage of cloud services.

This article describes real cloud computing project case studies, which show that moving to the cloud is an important strategic decision for IT managers. The existing IT strategy must be reconsidered, and possible cloud computing scenarios must be deviated.

Current cloud projects are still characterized as being in the testing phase and are mostly performed for IT services that are considered to be uncomplicated. Even these projects show that challenges persist in the area of data security and compliance.

**Starting Points**

Different definitions and models of cloud computing exist and are often used as starting points for evaluations. **Figure 1** was developed by the US National Institute of Standards and Technology (NIST) and provides an overview of typical characteristics, service models and deployment models.

The characteristics section summarizes relations and differences to existing IT services. The service models section refers to software, platform and infrastructure decisions based on functional requirements and sourcing strategies. The deployment models section covers access rights and responsibilities. A typical choice is the private cloud that runs solely for one organization and can be organized and managed either by the organization itself or by a third party. Additionally, the cloud can be located in

---

**Figure 1—NIST Visual Model of Cloud Computing**

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Service Models</th>
<th>Deployment Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broad Network Access</td>
<td>Infrastructure as a Service (IaaS)</td>
<td>Private</td>
</tr>
<tr>
<td>Rapid Elasticity</td>
<td>Platform as a Service (PaaS)</td>
<td>Community</td>
</tr>
<tr>
<td>Resource Pooling</td>
<td>Software as a Service (SaaS)</td>
<td>Public</td>
</tr>
<tr>
<td>Measured Service</td>
<td></td>
<td>Hybrid</td>
</tr>
<tr>
<td>On-demand Self-service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

the organization’s own data center (on-premises) or in that of a different institution (off-premises).

Frameworks such as those provided by NIST, the European Network and Information Security Agency (ENISA)\(^1\), \(^2\) or the German Federal Office for Information Security (BSI)\(^3\) provide a high-level overview, which should always be considered during the strategic planning of the usage of cloud services. However, those frameworks cannot replace detailed individual risk assessments and analysis of legal and compliance requirements.

### DATA SECURITY AND LEGAL ASPECTS

The majority of discussions about requirements specifications in cloud computing projects refer to data security and legal aspects. Data security especially requires a clear and well-defined specification of both cloud customer and cloud provider responsibilities. In general, the level of control and responsibilities varies depending on the provided cloud service model. For example, in the case of Infrastructure as a Service (IaaS), a cloud customer’s responsibilities usually cover the security platform configuration and maintenance, log collection, and security monitoring. Service models like Software as a Service (SaaS) and Platform as a Service (PaaS) typically include those activities at the provider side.

Internal and external data security requirements must be considered, depending on the classification of information stored, transferred or processed. Standards such as ISO 27001 usually lead to organizational and technical changes, whereas specific requirements such as the Payment Card Industry Data Security Standard (PCI DSS) for credit card data define very detailed requirements, which can lead to more time- and cost-consuming efforts.

Different national and international data protection laws define important requirements, which can lead to confusing legal situations for clouds, especially in international organizations. Questions such as where the cloud host is based, who has access to which data and how to react in case of possible security incidents are at the top of the agenda. Solutions can often be found in very detailed definitions of controls and responsibilities, user access rights, locations of service providers, contracts and service level agreements (SLAs).

### STRATEGIC CONSIDERATIONS

Strategic alignment between business and IT has become a key success factor to maximize value. To develop and implement an appropriate IT strategy, different technologies need to be identified, evaluated and—once acquired—integrated with IT and business processes. The implementation decision for cloud computing must follow a structured approach that considers pros and cons and includes a comparison of the total cost of ownership.

Cloud computing is an important part of modern strategic sourcing initiatives. In the case of outsourcing, the nature, risk and benefits of cloud computing require strong SLAs in place to manage the interface among organizations, processes and responsibilities to ensure control and accountability.

The described considerations can be summarized in a cloud computing strategy as part of the overall IT strategy to define the used service and deployment models, integration in processes and infrastructure, as well as the corresponding operational and legal parameters.

In addition to integrating the cloud computing strategy with the IT strategy, organizational IT governance aspects should be considered. IT not only enables new services and business processes, but also business units may increasingly use IT and the cloud without involving the IT department. This can lead to miscommunication between business and IT.\(^4\)

### PROJECT CASE STUDY: CLOUD COMPUTING STRATEGY

The following project case study illustrates the successful integration of cloud computing within the IT strategy. The basis for the project was an organizationwide strategic initiative covering all business departments and IT. Within this initiative, the existing old IT strategy was analyzed, updated and integrated with the other business strategies to ensure proper business IT alignment and to increase IT awareness.

As a starting point of the IT strategy development project, benchmarking tools were deployed to analyze the current
state of the organization against industry and revenue peers. In addition, interviews with key players were performed to collect business views and requirements and to get an understanding of the perception of the IT department within the organization. Based on the results and the collected information, future targets were defined and used to develop ways to achieve them.

A top-down model was applied to break down general strategic approaches, step by step, into specific actions. Figure 2 shows that the generic mission and values were first broken down into vision and strategic positions. This included sourcing and cloud computing decisions. After that, strategic cornerstones and objectives were specified. Finally, concrete projects, including cloud computing projects, were integrated in the strategic programs and initiatives.

Short-term actions, such as the identification of potential cloud service providers, were performed to start the implementation of the new strategy. For the long term, the Six Disciplines approach was adopted to ensure ongoing verification and updating of the IT strategy, including corresponding cloud computing decisions. Figure 3 provides an overview of the Six Disciplines cycle.

This ongoing process with an annual step-back phase ensures that the IT strategy, programs and projects follow the right direction. Regular evaluation includes cloud services and cloud computing projects, and leads to changes and updates where needed.

Since cloud computing is a fairly new field of providing IT services, the strategic decision that resulted from this project was to start using the cloud with relatively small applications in private cloud environments.

**PROJECT CASES: EMAIL AND BACKUP CLOUDS**

Cloud computing is a heavily increasing area of providing IT services. However, the described challenges and strategic considerations still lead to misconception within IT and business departments. Therefore, IT services considered to be uncomplicated are often outsourced into a cloud as a test for future projects.

However, the following two project case studies of an email and backup implementation project illustrate the relevance of data security and legal aspects for cloud computing—indeed from the technical complexity of the service. Both examples show that in addition to strategic considerations, risk management and compliance can be the most challenging aspects for current cloud computing projects. Figure 4 provides a short overview as an introduction.

Within the first project, an email service was outsourced to a cloud provider. At the beginning, a risk and opportunity
evaluation was performed. Cost reduction, functionality and flexibility emerged as the drivers of the project. However, legal aspects that had to be resolved first were identified.

The project was performed by an international organization with more than 100 entities worldwide. A lawyer was engaged to identify important compliance requirements that were relevant in this context. One of the main challenges of the project was the different data security and labor laws worldwide. Out of these considerations, the decision for a cloud service provider was driven by the location of the legal entity and the location of the data center.

To minimize security and compliance risk, a private cloud managed and hosted by a German provider within Germany was chosen. The provided services and the related SLAs were analyzed and changed as required. An audit clause was included to allow verification of controls onsite.

The second project case study illustrates security concerns related to the use of cloud services for backup management. As a part of the IT strategy, the decision to replace backup tapes with an automated SaaS cloud backup solution was taken after consideration of the management benefits and business continuity aspects.

Due to the growth of sales and services in the past years, the old tape backup solution became difficult to manage. Limited personal resources and physical space made the manual backup process less reliable and cost-inefficient.

As in the first project case described, the security and legal concerns were identified as the most challenging part of the usage of the cloud. The analysis of legal requirements led to the decision to use a private cloud provided by a Swiss hosting company to ensure an acceptable data security level.

**CONCLUSION**

Cloud computing is not just another IT trend, it is also a new and flexible way of delivering IT services. The decision to move data or applications into the cloud must be well considered by IT management to ensure reasonable and secure usage of cloud services. It is important to consider cloud computing as an integrated part of the IT strategy. The described project case studies show that security and compliance requirements were identified as currently challenging aspects in practice. As a result, cloud providers are evaluated not only by their service levels and costs, but also by their location. The usage of SaaS cloud services is currently common practice in order to carefully approach this new way for IT services, as well as to gain experience for further outsourcing initiatives into the cloud.

**ENDNOTES**

4 Protiviti, *IT Governance Insights Germany—Sustainable Competitive Advantage Through IT Governance*, November 2011
5 Six Disciplines, [www.sixdisciplines.com](http://www.sixdisciplines.com)