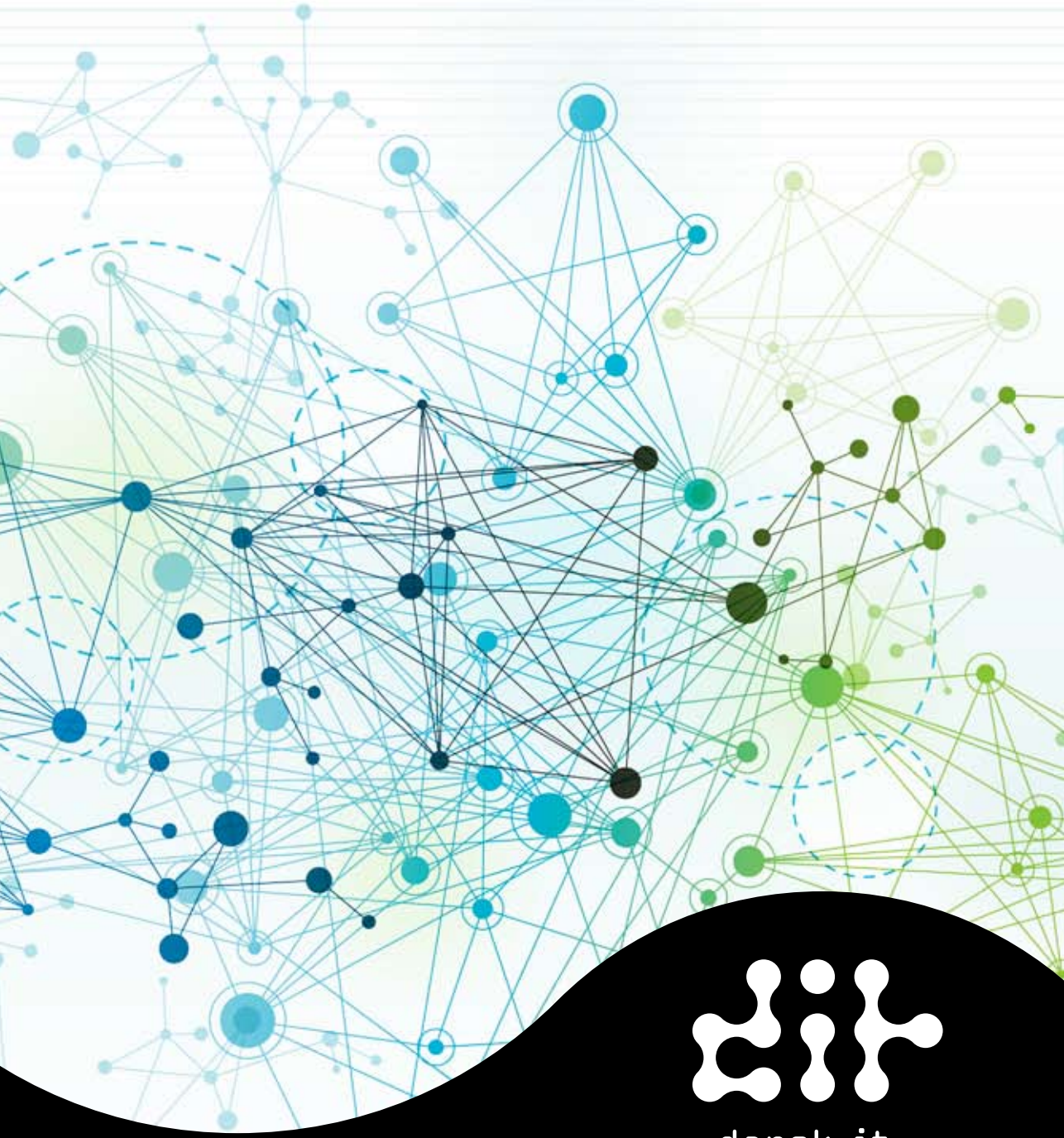
Security of IT outsourcing

Quick guide



dansk·it

Quick guide:
Security of IT outsourcing

1. edition

Release: November 2012

Authors:
Danish IT Society's Group of IT Security Managers

Layout:
Danish IT Society

Bredgade 25a
DK 1260 København K
Tlf: +45 3311 1560
dit@dit.dk
www.dit.dk

Quick guide

Security of IT outsourcing

Made by
Danish IT Society's Group of IT Security Managers

dansk•it

Content

Foreword 5
- Purpose 5
- Structure 6
- Definition of outsourcing and offshoring 6

Items of the guide as checklist 7
- Preparation 7
- Phases of co-operation 9
- End of co-operation 10

Elaboration of items from the checklist 11
- What kind of outsourcing 11
- Business case 12
- Establishment of scope 13
- Outsourcing versus offshoring 14
- Maturity 15
- Requirements to the provider's infrastructure 16
- Definition of SLA 17
- Risk analysis 18
- Assessment of the regulative and legal demands 19
- Provider assessment (CSR) 21
- Agreement on control/audit 22
- Decision of exit strategy 23
- Establishment og contract - up to and including the signing 24
- Establishment of organisation 25
- Roles and responsibility 27
- Handling remaining internal resources/competences 28
- Ongoing control of deliveries/are we getting what we bought 29
- Handling incidents 29
- Business Continuity 30
- Ongoing changes - Change Management 32
- Emergency tests 33
- Security tests 33
- Implementation of audits/follow-up of audit reports 35
- Execution of exit strategy 36

Lessons Learned / Common Pitfalls 37

Foreword

This guide is intended for the IT security aspects of IT outsourcing and does not deal with the commercial angle of outsourcing as it is assumed that the decision on outsourcing has been considered. Furthermore, the elements of audit, law, and CSR are briefly mentioned.

The Group of IT Security Managers has chosen to write this quick guide because they have experienced that security and other risk factors are often being overlooked or thought of in a phase where the company has already made the decision – maybe even signed the contract. Lack of focus on the security and other risk factors described in this guide will often entail an increase in the costs compared to the original business case when these factors later will be included.

These factors shall therefore be identified in an early analysis phase and be a part of the basis of calculation of a realistic business case.

The information security and the risk of the elements secrecy, integrity and access are the focal point in the guide.

Purpose

The purpose of this guide is to give a quick overview of the most significant risk factors you should take into consideration already in the analysis phase and thus a simple instrument to estimate these factors. At the same time the guide is a contributing instrument to get a description of a business case so "oops" will not occur later on.

The writers of this guide are the Group of IT Security Managers and consist of app. 35 security managers or IT security managers from big companies in Denmark, and the items of the guide are based on the members' compound experiences. Regarding the legal considerations the group has gotten help from Bettina Drejer Clausen, Compliance Officer in Tryg. The audit angles are described with help from IT auditors.

Structure

The guide contains a number of items which reflect the phases of an outsourcing situation.

- Preparation
- Phases of co-operation
- End of co-operation

It is described in a few lines what each item covers. This may be considered as the checklist which can be used independently. In its nature the guide is not exhaustive but it should arouse the reader's attention who may be concentrated on the separate element if needed.

The separate items are described more detailed later in the guide but again it must be emphasised that there are no detailed answers to everything. The reader's own concentration on the separate risk elements is required.

Definition of outsourcing and offshoring

There are different definitions of outsourcing. We have chosen to stick to a simple interpretation. In its simplicity outsourcing means to transfer handling of a task / part of a task to another company. It does not comprise buying of goods or services.

Offshoring is in principle the same as outsourcing but the definition means that the tasks are transferred to a company in another country.

We hope that this brief guide can be a help to raise the security when a company intends to outsource.

On behalf of the Group of IT Security Managers,
Tom Engly, Head of Group Security, Tryg Forsikring A/S.

Items of the guide as a checklist

Preparation

☐ **What kind of outsourcing** *(uddybning side 11)*
Outsourcing means basically letting other persons carry out a task. This means that IT sourcing as a concept covers a host of different services.

☐ **Business case** *(uddybning side 12)*
All larger changes in a company should be decided on the basis of a positive business case. Decision on outsourcing is no exception.

☐ **Establishment of scope** *(uddybning side 13)*
In addition to getting the business case sorted out the most important thing by outsourcing is to determine / establish the scope.

☐ **Outsourcing versus offshoring** *(uddybning side 14)*
In stead of outsourcing, offshoring with own resources may be an alternative. But even though the business case can look quite attractive there might be a lot of pitfalls.

☐ **Maturity** *(uddybning side 15)*
In order to obtain the optimum outsourcing / offshoring it is important that the company has a sufficient level of maturity.

☐ **Requirements to the provider's infrastructure** *(uddybning side 16)*
Design, construction, and maintenance of the provider's infrastructure are essential with regard to security of separation between the customers of the provider.

☐ **Definition of SLA** *(uddybning side 17)*
Through a SLA – Service Level Agreement – the company must make specific, measurable, and precise demands to the delivery giving by the provider.

☐ **Risk analysis** *(uddybning side 18)*
A sourcing provider is basically exposed to the same risks as an in-house IT function. The company must thus make sure that these risks are met according to the needs and risk appetite of the company.

☐ **Assessment of the regulative and legal demands** *(uddybning side 19)*
In connection with outsourcing a series of legal circumstances exists of which you must take a stand. These circumstances must be described in a written agreement between the parties with involvement from legal adviser, if necessary.

☐ **Provider assessment (CSR)** *(uddybning side 21)*
One of the important milestones of an outsourcing project is to choose provider. But which provider should you choose in a competitive market where both price and the services offered are largely comparable.

☐ **Agreement on control /audit** *(uddybning side 22)*
Consider how you can secure that the agreement is observed or how the company auditor gets conviction that the control environment works in an adequate way at the outsourced provider.

☐ **Decision of exit strategy** *(uddybning side 23)*
Consider how you through an exit strategy or exit plan can secure the company data in a situation where you shall leave your outsourcing provider or where the co-operation in another way has ceased.

☐ **Establishment of contract – up to and including the signing**
(uddybning side 24)
It is important to pay attention to the preceding identification of needs in the process regarding establishment of the scope in order to secure a procedure where the parties have sufficient clarity of what to deliver and thus the relevant conditions.

☐ **Establishment of organisation** *(uddybning side 25)*
The success of an outsourcing project depends to a great extent on establishing the "right" organisation for the project. However, the "right" organisation is not necessarily the same through all the phases of the project.

☐ **Roles and responsibility** *(uddybning side 27)*
The investment of establishing the remaining organisation which shall function after the outsourcing will be repaid manifold once the outsourcing is in operation.

☐ **Handling remaining internal resources / competences** *(uddybning side 28)*
Navigation of an IT organisation in the middle of an outsourcing process demands great attention. The end objective of the company is to secure that the right competences in handling the remaining tasks exist.

Phases of co-operation

☐ **Ongoing control of deliveries / are we getting what we bought** *(uddybning side 29)*
At the signing of the contract the company should decide on an adequate level for control of the deliveries.

☐ **Handling incidents** *(uddybning side 29)*
When incidents occur it is important that they are handled as agreed upon in the contract, possibly in the appurtenant SLA – Service Level Agreement.

☐ **Business Continuity** *(uddybning side 30)*
Business continuity is a discipline which based on prioritisation of business processes and business services shall secure the continuation of the business in case of serious incidents or catastrophes.

☐ **Ongoing changes – Change Management** *(uddybning side 32)*
Agreements of outsourcing may often last for several years and in this period both the commercial conditions and technical possibilities will probably develop. Therefore, in an outsourcing contract, you have to take possible needs for changes into account.

☐ **Emergency tests** *(uddybning side 33)*
Test of the established IT emergency with the outsourcing partner and the division of the responsibility for the specific areas shall be described.

☐ **Security tests** *(uddybning side 33)*
Security tests may be a part of self-regulation of the outsourced service and possibility for using this must be included as a part of the basic contract.

☐ **Implementation of audits / follow-up of audit reports** *(uddybning side 35)*
Make sure that the report agreed has been received and that its quality is adequate in order to be able to base management follow-up as well as audit follow-up.

End of co-operation

☐ **Execution of exit strategy** *(uddybning side 36)*
Consider how you through an exit strategy or exit plan secure the company data in a situation where you shall leave your outsourcing provider or where the co-operation has ended in another way.

Elaboration of items from the checklist

Preparation

What kind of outsourcing

IT outsourcing exists in many forms, from outsourcing of IT operation through outsourcing of software development to today's cloud computing. And even though there will be some common features every form will have distinctive characteristics – an own set of risks to which you must relate.

The traditional form of outsourcing – outsourcing of IT operation – includes a range of scenarios which is different from the division of responsibility between company and provider. At full outsourcing the ownership of both data centre, equipment, software and operating staff lies with the provider, and seen with the company eyes the service is pure service. But many other forms may exist, e.g. operation of the company platform at the provider data centre etc. A traditional outsourcing is often directly connected with the services delivered and the equipment from which the services are delivered, and the company in question. And you will be able to trace the company data to a certain physical unit.

Cloud computing is a modern concept of outsourcing and includes services on several levels of abstraction. Common for cloud solutions is that it is virtual services and that they often support many customers at a time. There is thus no connection between physical equipment and the services delivered, and data can not be traced to certain physical units.

Supplementary information:

Cloud Security Alliance:
"Security Guidance for Critical Areas of Focus in Cloud Computing v. 3.0"

ENISA:
"Cloud Computing, Benefits, Risks and Recommendations for Information Security"

Business case

As basis for decision the business case describes the businesslike benefits which an outsourcing project will produce. These benefits may be of financial character and other, e.g. quality, agility etc. In order to make a fair comparison all benefits are quantified typically into finances. The business case is as basis a “living” document that should be updated if the outlined conditions are changed.

The business case should include a time schedule and plan of action for the project, a resource scheme, an outline of the project economy, a strategy for crop of benefits, a plan of organisation of the project, and an assessment of relevant risks.

As foundation for the business case an exact scope for the project is defined. For the sake of the comparison it is necessary to know the present condition for this scope in details. It includes the financial conditions (investment needs, running costs, staff charges), the more qualitative conditions (SLA, accessibility, support etc.) and the security requirements (compliance, confidence, integrity). This list will be the base line for the business case.

Outsourcing contracts are normally signed for a longer period. The business case should reflect the whole period and include conceivable conditions at resignation from the contract.

Supplementary information:

ISACA:
”The Business Case Guide: Using Val IT 2.0”

OGC:
”Managing Successful Projects with PRINCE2”

Establishment of scope

In connection with the establishment of the scope it is important to consider the background for the company's wish to outsource. Here are the typically motives:

- Makes the company able to focus on the core business
- Can reduce the investments of the company
- Can reduce the company's risk
- Makes the company more flexible against changes
- Can contribute to give the company international experience and network

The outsourcing may thus be a proactive strategic decision of being more cost effective or the decision may be influenced by external circumstances as for example the access to qualified labour. In any case the company must realise that the decision of outsourcing requires management resources and a whole different organisation compared to keeping the IT operation, IT support or IT development in-house.

When the scope is being established you should analyse the following:

- How much will you really save by outsourcing?
- What are the costs in time and money by implementing the process?
- Are lower IT costs the most critical for the company and its customers?
- Which processes will pay off to keep in-house?
- Are there other circumstances than price / costs that really have greater importance?

Supplementary information:

Erran Carmel, Paul Tjia:
"Offshoring Information Technology to a Global Workforce"
ISBN: 978-0-521-84355-3

Outsourcing versus offshoring

In connection with the preparation of the business case especially companies which today have their own production facilities in Eastern Europe or Asia will experience that offshoring of IT tasks (making use of own people) actually will give a more positive business case compared to outsourcing the tasks to an external provider.

However, you should pay attention to the fact that there are a number of risks which can easily be overlooked when the business case is made but these risks must be handled.

You may experience that for example the cultural difference implies that you must calculate with a much larger management overheads than you are used to as the handling of the tasks requires continuous follow-up. Therefore you may expect that you must invest both extra time and resources in a co-operation like that.

You must also pay attention to the qualities of language in the area to which you offshore. What is the use that the labour is much cheaper if it is more or less impossible to communicate with the employees? Here it may be an advantage to establish offshore in an area, e.g. in or not far from a big city, where you will find better English skills. But on the other hand – this will make the time rate higher.

Finally, it is important to notice that offshoring typically requires that a Danish employee is posted for a shorter or longer period of time in order to be labour coach. Depending on family circumstances this expense may be very high as you might pay for international school for the children, lost monthly earnings for the spouse etc.

Supplementary information:

Erran Carmel, Paul Tjia:
"Offshoring Information Technology to a Global Workforce"
ISBN: 978-0-521-84355-3

Maturity

Unfortunately, many companies have too late understood that it takes a very high processing level of maturity to be able to establish a proper outsourcing / offshoring.

The result of this is that they must scrub the project entirely or at least have to recapitulate and get the process maturity raised before the project can continue. The project will thus be delayed and it will also become much more expensive than expected.

As mentioned above under “Establishment of scope” the outsourcing / offshoring do not typically apply to the company’s core competences, but on the contrary tasks / areas where you might be in less control of the matter and where the maturity of the process thus is lower.

This is of course especially a problem with offshoring where you just relocate present tasks to a low paid area. Here you will only obtain the same “quality” to lower costs.

On the other hand, by outsourcing one of the incentives by using an external provider might be getting access to qualified labour and / or processes so you do not have to construct the skills yourself. Still, it is necessary that the company’s process maturity is on an adequate level as it will not help that the tasks outsourced are running most optimum with an external provider if the internal processes related to these are not optimum /mature.

Supplementary information:

Erran Carmel, Paul Tjia:
”Offshoring Information Technology to a Global Workforce”
ISBN: 978-0-521-84355-3

Requirements to the provider's infrastructure

By outsourcing your own infrastructure becomes a part of a bigger infrastructure. This means a number of new risks of different kinds, e.g. a virus in another part of the provider's network may spread to your own network, or your data may be leaked, for example by using shared services. The design of the operational provider's network is thus important for the security in your own network.

Requirements to the infrastructure can roughly be divided into three areas:

1. Demands on separation between other customers and the provider's own administrative network.
2. Demands on possibility to keep own environment strategy and internal segmentation.
3. Demands on possibility for proactive controls in connection with using shared services.

Re 1
It must be secured that the provider's administrative network is adequately secured and separated from their customers' network. An important component is the jumphost from which the provider handles the different customers' network. Here it must be demanded that only a select few has administrative access to the actual host and that the customers do not have access.

Re 2
Internally the infrastructure must support your own demands on an environment strategy, e.g. that the production and non-production and internally and externally exposed areas must be separated. Another focus should be the transverse systems that have access to all other systems (antivirus, backup etc.). These services should be placed correctly in service-in / service-out net. At the same time systems handling internally and externally exposed systems should be separated.

Re 3
Finally there should be demands on separate risk management focus in connection with the provider's shared-services. These pose a potential source of data leakage and virus spreading. Possibly found weaknesses should be handled – mainly by implementation of proactive controls. The solution to above mentioned could be implementing own control of design and implementation of the provider's controls. This you can implement by yourself or get a third party to assess – either as a part of the general audits or as a separate analysis of selected areas.

Definition of SLA

Make sure that the SLA is a part of the basic contract and which the provider with his signature has approved as the demands stipulated to the delivery. Afterwards it is difficult to stipulate demands on the delivery in a SLA when the contract is approved and signed by the parties. The SLA can be drawn up as a part of the contract or as an appendix. If the last-mentioned is the case it must be written into the contract as a part of the provider's responsibility. The consequence of violation of the SLA must be documented either in the contract or in the SLA.

There can easily be demands to the provider which depend on services or compliance with certain conditions from the company before the provider can comply with his demands. For example, it is no use to demand that the provider shall alert at incidents if the company does not have a person who can receive and act on the alarms.

In the SLA all specific demands on the provider's service can be stipulated, e.g. uptime, planned downtime, security, response time, response time at incidents, alarm call, etc. It is important that you realise what you as a company demand from the service that you buy. This also tells about the provider's maturity and capability to deliver if he for example will not or cannot deliver 99.5% but only 94% uptime, and only support between 9 to 5 if you need support 24/7.

As a company it is in the SLA you stipulate possible demands on backup and

access to your data which is necessary if the co-operation ends (as mentioned in “Exit strategy”).

Make sure that the demands in the SLA are specific, precise and measurable. Calculate what it really means in time and costs. What does for example 95% uptime against 99.999% uptime mean? Are planned maintenance windows included or excluded? What is the provider’s price? Support 24/7 is more expensive than support 9 to 5 Monday to Friday. A cost / benefit analysis is here advisable so you do not pay for a service that you do not need.

Risk analysis

All companies are exposed to risks that can harm the cost-effectiveness of their company or even the existence of the company. Risk analysis is an organised discipline that makes the company able to assess and deal with these risks – maybe share the risk with others, e.g. through insurance or on a stated accept a risk.

The overall risk analysis will thus set the framework of the level of risks that the company is willing to accept. And it is within this framework that the business processes must be supported by IT – whether IT is handled internally or has been outsourced.

However, in an outsourced environment the company is no longer in direct control of the IT function. The aim here is to secure that the sourcing-provider implements the necessary arrangements, procedures and controls in order to secure the company’s needs. And here standards and “best practices” will be useful. Certifications according to acknowledged standards like ISO 20000 and ISO 27001 make it probable that the provider has reasonable operation and security processes in place. Implementation of “best practice” operation procedures, e.g. ITIL, gives transparency and measurability. And a strong governance model like COBIT secures that the interfaces between provider and customer will work efficiently. Finally, the external assessments like for example the independent ISAE 3402 or SSAE16 certificates and the security scanning will make it probable that the provider meets the company’s requirements.

But if all this shall be of some value it is important that the company knows the environment inside out that is being outsourced. A risk assessment shall be completed before the outsourcing, data shall be classified, and possible compliance requirements shall be identified. This baseline forms the basis of the requirements for the sourcing-provider and for the controls which shall show the provider's performance.

Supplementary information:

IT Governance Institute:
"Control Objectives for Information and Related Technology" (COBIT)

ISACA:
"The Risk IT Framework"

Cloud Security Alliance:
"Security Guidance for Critical Areas of Focus in Cloud Computing v. 3.0"

ENISA:
"Cloud Computing, Benefits, Risks and Recommendations for Information Security"

Assessment of the regulative and legal demands

When a company outsources services which so far have been taking care of by the company itself it may give rise to legal issues which on the whole require involvement of legal expertise.

If personal data is a part of the outsourcing the agreement of outsourcing must include a special agreement of processing personal data. You can take inspiration to the formulation of this agreement from the website of The Danish Data Protection Agency. The Danish Data Protection Agency has special rules of approval if you outsource to providers in countries outside EU / EEA. If you outsource to third countries a special EU standard contract may be used.

The former National IT and Telecom Agency has published a guide on "Cloud computing and the legal framework" which may be relevant to read if cloud computing is a part of the solution.

You must also pay attention to the fact that employees occupied with the activities that now are being outsourced may be protected by rules in the act on transfer of business and have the right to follow the outsourced activity. The contract with the outsourcing partner should address this situation.

By outsourcing rules in the Bookkeeping Act and Act on Annual Accounts may furthermore be relevant – including rules on where to keep the data if the outsourcing partner's server is placed outside Denmark.

By outsourcing you must make up your mind how interest in hardware, software, and data should be in the duration of the agreement and at the end of the agreement.

Regarding financial business outsourcing essential activity areas the Danish FSA makes special demands on the content of the agreement, including that the Danish FSA must have access to the provider's premises etc.

Supplementary information:

Danish Data Protection Agency: www.datatilsynet.dk/english/

Danish FSA: www.finanstilsynet.dk/?SC_lang=en

The National IT and Telecom Agency: http://en.itst.dk

Provider assessment (CSR)

In short perspective the price is almost always in focus. Many outsourcing projects have as a highly prioritised purpose to save money – often made probable in a financial business case. Another important circumstance is the technical solution. But what about the longer horizon?

Today companies are increasingly measured by other parameters than the price and quality of the service. Values like social responsibility, sustainable production, decent working conditions for the employees etc. are suddenly also important and prioritised just as highly. And these demands on social responsibility are made, even though the company has its own production or uses sub-provider. Therefore you should take as your starting point how your company is profiled in the CSR area (Corporate Social Responsibility) and bring these values into play towards potential sub-providers.

The CSR score has an increasing importance in most of the companies – both to the company's image and certainly also to the bottom line. Therefore the principles of UN Global Compact should be an important part of the considerations in the business case and be weighted adequately in connection with the choice of sourcing provider.

Supplementary information:

Ministry of Foreign Affairs of Denmark and UN:
"Global Compact: Små og mellemstore virksomheder på vej til global ansvarlighed"

ISBN: 978-87-7087-174-7 (trykt)
ISBN: 978-87-7087-175-4 (elektronisk)

(UN initiative stating ten general principles for company work with social responsibility.
These are arranged within the main fields: Human rights, employee rights, environment, and anti-corruption.)

Agreement on control / audit

When outsourced a part of the company's activities occurs outside the company's direct self-regulation. Therefore it is important to consider how the management secures that the control environment in the company to which you outsource works adequately. This can be done in several different ways or as a combination of these, e.g.

1. You make self-regulation with the outsourcing provider's compliance with the contractual basis.
2. You obtain a statement of assurance showing that the contractual basis is followed during the period of statement.

The demand on extent of the control can be derived from legislation which is known from financial companies.

The company management should start a dialogue with the company's auditor as soon as possibly in the process. If you are dealing with essential activities or activities which can have influence on the accounts the auditors must consider their audit strategy accordingly. This means that the auditors shall either make their audit at the provider (as a starting point this should be an option in the agreement), or from a firm of auditors they shall receive a statement regarding the compliance of the contractual basis. (It is important that the audits which are essential and on which the company's auditors base their audit are included in the contractual basis.)

The company's auditors consider typically in correlation with their audit if they can use the statement in their audit, including if giving audit is regarded as independent and has adequately professional skills etc. It is an advantage to discuss choice of auditor already in connection with the signing of the agreement. The statements mentioned will typically be the same. Thus the use between the company's management and the auditors can be coordinated.

There are different types of statements but international auditing standards are used in the field. This makes the reporting more transparent to the receiver and the submitting party. Together with the company's auditors you should consider which standard statement you shall use.

There are several levels of the depth of the statement which shall be determined before the agreement is signed including statement if the controls are present and adequate (correctly designed) and if they are implemented and operates efficiently during the period of statement. Typically an auditor wants a statement of assurance covering tests of design, implementation and efficiency.

Note that the word “audit” in a contract often is interpreted as only auditors can make an audit. It should appear specifically if you as an IT security department also want to make audits.

Supplementary information:

The Danish FSA:
”Bekendtgørelse om outsourcing af væsentlige aktivitetsområder”

ISACA:
”G4 Outsourcing of IS Activities to Other Organisations”

IAA:
”GTAG 7 - Information Technology Outsourcing”

Decision of exit strategy

In connection with the preparations of outsourcing a risk and consequence assessment must be made. Among other things this assesses where there is critical data for the company which now is assigned to the outsourcing provider to process but where there is a request or demand that the company controls the processing.

On this basis it must be assessed if the company can tolerate data loss and possibly how much data loss the company can accept, e.g. 24 hours of data loss, and whether the company is able to restore the lost data from for

example input material.

In the contract it must be documented who the owner of the data is which the provider processes on behalf of the company, and that the provider at the end of the co-operation shall be of assistance to hand over the data.

Through the SLA (Service Level Agreement) in the contract you should sign a backup agreement with the provider so that the company itself can make a regular online backup or ask the provider to send a backup with agreed period. Remember to get the data in a format that makes the company able to recreate data. All according to risk, the company should test if system and / or data can be recreated from the backup.

Furthermore alternatives should be conceived and if possibly verified as to how you optimally move your outsourced activities to another provider or in worst case insource again.

Establishment of contract – up to and including the signing

The establishment of the contract should start with a preliminary clarification of needs and possibly a tender process. Specification requirements, specific conditions and time schedule for the tender should be included in the tender documents and also contract conditions to which the outsourcing provider must relate. There are special rules for public procurement. Later the provider will typically give a proposition with reservation of outage of due diligence especially regarding staff conditions.

Outsourcing has the specific features that you enter into a long-term agreement with a provider about some services that in all probability will change over a period of time and which are of such nature that it will often be difficult to transfer the agreement to another provider at short notice. Among other things this means that the contract shall regulate how changes in the service shall be handled regarding governance and how the price structure will be influenced by changes in service and changes in other external conditions including possibility of benchmarking.

The service itself should be described thoroughly in a SLA with specific stipulated objectives of for example uptime / downtime, efficiency, penalty and bonus structure, requirements of reporting, and other requirements to the provider, e.g. documentation, alert etc. Other conditions that should be regulated may be guarantees, violation, force majeure, rights, client confidentiality, and the issues mentioned under the item "Assessment of the regulative and legal demands". Cancellation including return of the service or transfer of the service to third party should also be regulated thoroughly. Here the provider should be committed to participate. By transferring to third party you may risk that employees shall follow from the provider to the third party.

Outsourcing agreements can among other things be difficult and resource demanding to cancel and therefore it is important with a description of conflict resolution process which can escalate from involvement of steering committees to appointment of technical specialist, possible dispute settlement and arbitral award conditions.

Establishment of organisation

An outsourcing project normally goes through a range of phases:

- An opening phase where the requirements are formulated and the provider is chosen
- A transition phase where services and possible staff are transferred
- An operational phase where the agreed services are delivered
- An exit phase where services are taken home or are moved to another provider

These phases are very different from each other and you should take this into account when each phase is organised.

The opening phase is a project phase where the commercial requirements shall be converted into a delivery agreement. Typically this will require participation of persons in charge of business with a deep understanding of the importance of IT for the business, persons in charge of IT, contract specialists,

lawyers, and possibly person in charge of personnel law. It is important that the security requirements are included in the delivery agreement.

The transition phase is a project phase, too, which shall secure that services are implemented according to what is agreed-upon and that possible staff is transferred. In this phase persons with project steering and solutions-oriented technical skills are required to a greater extent. Here it must be secured that the security is maintained in a period with big changes.

In the operational phase close governance of the agreement is required. The organisation must include both business and technical skills and contract specialists who can secure that the terms of contract are developed according to the needs of the business and that the agreed delivery in fact is delivered – also regarding the security.

Finally, the exit phase will be a project-oriented phase where stronger project steering and technical skills are required. Here the primary focus is on service continuity.

The phases of outsourcing project are thus different from each other and the success of the project depends on the organisation which must occur according to the tasks which must be solved by each phase.

Supplementary information:

ISACA - IT Governance Institute:
”Governance of Outsourcing”
ISBN: 1-933284-13-7

ISACA:
”Control Objectives for Information and Related Technology” (COBIT)

Roles and responsibility

It is important that the company itself analyses roles and how the responsibility shall be divided between itself and the company to which you outsource. The transition phase includes a range of definitions and decisions and if you as a company have a clear perception of the future roles and responsibility you will go through the transition much easier and with a better result. The following operation will also proceed more optimally.

In order to be able to define the future roles and responsibility you have to describe how things are before the outsourcing. This means to describe in details which services are provided and in which way. This description is the basis of the following processes you must go through.

Next step is to go back to the outsourcing strategy and the business case and take this as a starting point to develop the new organisation. The following is included in that process of development:

1. Select the relevant processes
2. Define the new organisational functions and size
3. Detailing of the processes that remain
4. Mapping of roles into functions
5. Establishment of RACI plan where you find connection between responsibility, communication and processes

Now the new organisation can be detailed and described.
Next a plan of communication can be implemented and established. It must be described exactly what kind of role IT Security shall play after an outsourcing. As we all know, the responsibility cannot be outsourced only the tasks – so IT Security will get a central role as controller.

Handling remaining internal resources / competences

Change management is the keyword in the processes that exist in the outsourcing task. Naturally, there will be much insecurity of the future that is unknown to the employees and to some extent to the management of the IT department.

The management has a special responsibility to secure a high level of communication to the employees. The communication shall be as open as possible and should include

1. Why outsourcing? What are the vision and the strategy behind the decision?
2. How shall it be done? Which project will be established?
3. What happens on the way? Which consequences will it result in for you as an employee?
4. How and how often will you as an employee get the ongoing information in the process?

When you have established the first designs of the remaining organisation it is important to write the job descriptions that shall be the permanent ones in the remaining organisation. These job descriptions are a good basis to get a dialogue of the future tasks started.

This, again, may lead to considerations with employees and management if it is the right position for the individual, if a competence boost is necessary or if you should follow the outsourcing company. The company has an obligation towards the outsourcing company that competence follows with the outsourcing in order to secure a complete documentation of the conveyance of systems / applications. These obligations must also be taken into account.

The risk of unhappy employees must be evaluated in this planning. It may be necessary to increase surveillance.

Phases of co-operation

Ongoing control of deliveries / are we getting what we bought

Based on the type of deliveries the company should decide what level of follow-up is needed.

The company can choose two overall strategies of follow-up which are based on the contract signed up with the provider:

1. The contract comprises the overall scope that in broad terms makes demands to the provider, e.g. that the provider shall comply with relevant parts of ISO 27001. Compliance of demands shall be documented as a certification of the provider or a statement of assurance about the internal control environment at the provider.

2. The contract can be specified into the individual controls which the provider must deliver according to the company's requirements, or demands may appear from the contract that the framework conditions of the control must be made in co-operation with the company at the beginning of the co-operation. The frame of control must include a description of the individual control, frequency of implementation and agreed reporting of the same.

Handling incidents

In the SLA it should be concretised how you as a company understand an incident and how you prioritise and classify incidents – from unimportant incidents to critical / unacceptable incidents.

For each category of incidents it must be agreed-upon in the SLA who with the provider contacts whom with the company, including how fast it can be done. There must be an updated and current emergency phone list with demands on emergency times when alarm call has been decided. Some times a mail as

notification can be adequate if you are dealing with an unimportant incident, as long as it is agreed-upon.

From the SLA it should also appear how long time the provider has to handle an incident including if it must be escalated to the Problem Management (ITIL). A penalty may be agreed-upon if an incident is not handled fast enough. Furthermore the incident can be so critical that you are dealing with violation of the contract.

If you have an agreement of periodic reporting and / or progress meetings, the handling of incidents must be dealt with as a fixed item in the report or on the agenda of the meeting.

Business Continuity

The purpose of business continuity – or business alert – is to secure continuation of business critical processes or services if a severe incident occurs that wholly or partly affects the way these are normally carried out. An example of such an incident is IT crash that affects the IT support of the critical business processes to such a degree that these must be carried out in a manual way or otherwise.

A possible process to draw up a business alert is:

1. To analyse and determine the critical business processes
2. To determine an overall strategy of alert
3. To establish the practical business alert
4. To put the alert to the test

In part 1 a so-called Business Impact Assessment (BIA) is implemented in order to expose the most business critical processes and services. Based on this exposure one or more strategies are selected to see how these processes can be carried on in case of severe incidents or catastrophes. In this connection the objectives of the business continuation should be determined, including a decision on RTO (Recovery Time Objective), i.e. how fast can the operation be continued.

These strategies should include:

1. Security of the staff with sufficient knowledge
2. Use of possible, alternative locations
3. Technique / Technology strategy
4. Adequate access to information / data
5. Alternative provider / provider options

Depending on the strategy chosen it will later be possible to draw up a plan that secures that maximum acceptable downtime required by the company can be kept.

Outsourcing of IT delivery does not change the necessity of implementing the above mentioned. Furthermore, the BIA will be a pivotal exercise in connection with the design of the services that shall be bought from the provider because this will expose the criticality of the individual services. However, some of the aforementioned strategies will already be included in the services that will be bought from the provider. Test, audit and provider documentation will therefore be much more critical as the services represent an essential part of the support of the business alert. (Read more about test of alert later.)

Supplementary information:

British Standard:
"BS 25999"

Business Continuity Institute:
"Good Practice Guidelines"

Ongoing changes – Change Management

The needs of changes may fall within the scope of the signed agreement of outsourcing or be beyond the scope.

The governance structure implemented in connection with the agreement should be able to handle changes within the scope of the agreement, e.g. an increase of the capacity or the like on existing services. However, these requests of change can be of big importance to the total commitment and cause major extra costs. Here it may be a big advantage to base the process of change on standards and best practice, e.g. ISO 20000 / ITIL. In this way it can be secured that both company and provider have the same perception of the process and that the requests of change get the right managerial attention. The governance structure should also be able to handle changes in security conditions.

The requests of change beyond the scope of the agreement are in practice a start-up of a new outsourcing project. Such changes should therefore be object to a similar thorough businesslike assessment, both regarding solution and business case etc. The provider in question should also be assessed critically in correlation with the new assignment so that the optimal outcome of the investment is secured.

Change management is an important discipline and the organisational frame should be agreed upon in an outsourcing contract. If you use standards and best practice it helps to establish the process and to give a common understanding and terminology. This will secure a gradual operation. Changes far beyond the scope of the agreement should be handled separately.

Supplementary information:

Danish Standard:
"DS/ISO/IEC 20000"

OGC:
"ITIL®"

Emergency tests

It must be secured that the agreement of emergency is living up to the (overall) demands that appear from the IT security policy. Based on the decision on Recovery Time Objective, you must design a procedure for testing whether the provider in co-operation with the company is able to live up to the agreement of emergency. The following elements must be included in the agreement:

1. What to be tested (e.g. supply, network, backup, servers, etc.)
2. How to be tested (e.g. “desktop test”, restoring test, test of contact with relevant persons, etc.)
3. Which scenarios to be tested (e.g. disaster test, partly outage etc.)
4. Test frequency of the individual areas (In the areas which are to be tested it must appear how often they shall be tested, e.g. half-yearly, yearly, every other year, etc.)
5. Documentation of the emergency test including form, assessment and comparison with the objectives specified in the outsourcing agreement.
6. Liability arrangement
    - Who is the responsible for running the test?
    - Who has the task of running the test?
    - Who will provide documentation?
    - Who will provide the results and how?
7. Holding of emergency meetings, providing of test results and improvement measures

Security tests

The purpose of security tests is to test the level of security in the services provided by the outsourcing provider. Depending on the nature of the services provided, it should be considered how security tests can be used to assess whether the provider meets the demands agreed upon in the contract, or which are to be considered as being best practice in the field.

If the agreed service relates to for example development of application, it should be required that ongoing security tests are run illustrating whether the developed application has a sufficient security level to be put into production

at the time agreed upon.

In a similar manner security tests may be used to control the security level of an outsourced infrastructure. External security tests may be used to test how secure an external perimeter has been implemented, whereas internal security tests may be used to assess how good the provider's baseline for setting of security parameters is in general. These two types of security tests give an idea of the likelihood of circumvention of existing controls, and thus what any other compensating controls that should be made.

If you want to use a security test to identify weaknesses in applications or infrastructure it is essential that the overall rules for this have been agreed upon in connection with the signing of the contract. These rules should include: where, how, and when to run a security test, whom is responsible for the initiation of these, whom shall run the test, and how warning of the security test shall be giving, and who to pay.

Finally it must be agreed how possible finds from the security test shall be processed including whom to carry the burden of fixing the recovered weaknesses and a maximum time horizon for this.

Implementation of audits / follow-up of audit reports

If the audit department has chosen to do the audit itself at the provider, the audit of the company is done as a whole and will not be dealt with further in this guide.

If receipt of audit report has been chosen, the management and the audit department can go through the report in co-operation to check:

- if it is made by an independent and competent auditor. (There are special audit standards that secure that the audit report can be used and how.)
- if the extent is sufficient and according to agreement.
- if the conclusion regarding the control environment is adequate.
- if possible weaknesses with the outsourced company are established at compensatory controls or if further audit has to be done to establish the weaknesses reported.

The audit department will include the report in their total audit strategy and work for submission of the report on the annual report.

End of co-operation

Execution of exit strategy

Outsourcing of agreements is temporary. At expiry of the agreement or at violation the company or the provider can choose to terminate the co-operation. It is important that you as a company secure your data as soon as possible. Hopefully, it appears from the contract that you have obliged the provider to be of assistance with getting data out. An agreement of how it shall be done, e.g. through DVD or online, and in which format, may exist. It should be possible for the company to restore or transmit data to a new provider or to your own system.

It is important through the contract to secure that the provider deletes all the company's data when the data has been returned to the company, and when there is no contractual reason that data exists with the provider. This is in particular important if personal data has been processed.

If the provider has gone bankrupt and the bankruptcy trustee has closed down for access to the provider's systems there might be a risk that the company cannot gain access to its data and get a copy and later delete data on the provider's systems. Therefore, it is important that you as a company make a periodic and useful backup / security copy. The time between backups / security copies depend on how critical the data in question is for the company and how big a data loss you can sustain.

Lessons Learned / Common Pitfalls

One of the common features that are in evidence among many members of the authorship is about consumption of resources internally in the company in order to build co-operation and relationship and make it operative. Many has also experienced that their own process maturity has been challenged in connection with the outsourcing. This has caused more non-expected challenges in the outsourcing procedure.

Below are listed specific challenges that companies have experienced:

- It is alpha and omega that the business has been informed on what they can expect of deliveries in connection to the outsourcing process. One of our objectives was more flexibility. However, we waited a good while before this became a reality but the business had expected this from day one.

- The provider had a high level of expertise within IT security. Too late we realised that this expertise was sold as a consultancy service. It was not a part of the delivery from the operating centre.

- The co-operation with the provider made great demands on our process maturity – not only on the outsourced processes but also on the remaining processes such as management and follow-up. We underestimated the resources we needed internally to make the co-operation work.

- The ultimate lever in the co-operation is escalation but it seldom makes a problem smaller. On the contrary, we have experienced that the co-operation gets some scratches which later on are difficult to wipe off.

- We have experienced cultural differences between the companies which are a big challenge – and they are not smaller in connection with conflicts.

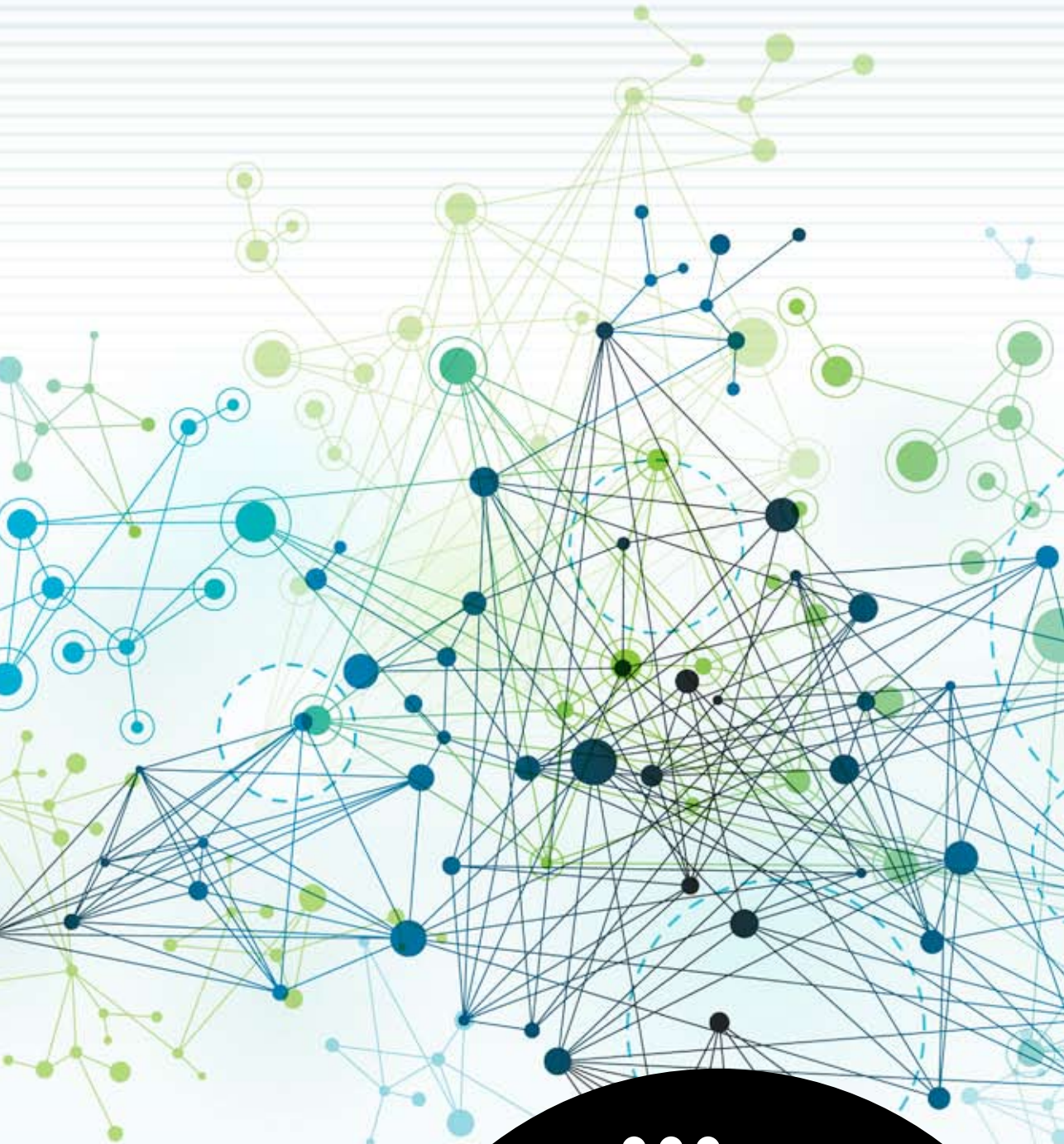
- We have experienced challenge with e.g. terminology: What does “Working Day” or “Severity” mean?

- You must not underestimate the challenges in connection with knowledge transfer to the new company – to top it all off maybe another country. We have learned that it is important to have transparent KPI on learning, knowledge level and use of new and trained employees, respectively. Furthermore, the KPI should be supported by awarding of prizes for good performance.

- You must be very careful with getting the agreement and the formulation of the right to inspect the compliance of agreed security demands including what and how (physical inspection etc.) It must be agreed how possible deviations found by the auditor or the IT security department shall be corrected and who must pay.

- You may experience that the missing knowledge that the provider has about the company compared to the company's own employees may cause longer or incorrect deliveries.

- The provider's employees will often be more specialised than the company's own employees. Their general knowledge of the whole environment may be less and may have importance for the delivery.



dansk·it

Bredgade 25 A I DK 1260 København K
Tlf: +45 3311 1560 I dit@dit.dk I www.dit.dk