CENTRE FOR CYBER SECURITY

AGENCY FOR DIGITAL GOVERNMENT

Guide

Cyber security in supplier relationships

Protect your organization when outsourcing IT operations in the entire process – from start to finish.

Contents

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Tel: + 45 3332 5580
Email: cfcs@cfcs.dk

AGENCY FOR DIGITAL GOVERNMENT

Landgreven 4
1301 Købenavn K
Tel: + 45 3392 5200
Email: digst@digst.dk

Frontpage illustration: Iaroslav Neliubov/Shutterstock
2nd edition June 2023.

Introduction

Many public authorities and private companies opt to outsource all or parts of their IT operations to external suppliers. On the one hand, outsourcing can be a sensible decision, from a business point of view, in order to enable the organization to focus on its core business activities, ensure availability of specialized skills required to run the IT operations, free up resources for other purposes, etc. On the other hand, outsourcing also comes with significant risks that can impact adversely on the organization’s cyber and information security. For this reason, supplier management is a key element for any outsourcing organization to achieve an effective cyber defence.

Foreign states and cyber criminals often attack their victims through the supply chain by compromising suppliers and using them as stepping stones to compromise their intended target. Consequently, outsourcing organizations need to set relevant security requirements for their suppliers and conduct continuous audits to ensure supplier compliance throughout the contract period.

The cyber threat against the supply chain

For more information on the cyber threat against the supply chain, read the CFCS’ threat assessments ”Cyber-attacks against suppliers” and ”The cyber threat against IT service providers” (CFCS 2019 and 2020).

In addition, outsourcing often leaves the organization with little or no control of the outsourced IT operations. Even after outsourcing selected IT systems to an external supplier, the organization remains responsible for protecting their own systems and information, a task that supplier management can help accomplish.

This guide provides steps for organizations that plan to outsource their IT operations on how to manage cyber and information security in client-supplier relationships. The guide provides recommendations on how organizations can manage their cyber and information security risks during the various phases of an outsourcing process. Other aspects of the organization’s cooperation with the supplier such as procurement, tender and contract management are not included in this guide.

Cyber and information security considerations should be a core component of an organization’s supplier management system and be part of all phases of the outsourcing process. In addition, the organization’s approach to supplier management should always be based on a case-by-case assessment of the risks involved in cooperating with an individual supplier and procuring their services. As all organizations work under certain resource limitations, they should take a risk-based approach by focusing on their most critical IT systems. In addition, public authorities may be subject to legal requirements related to outsourcing of, for instance, IT systems that are critical to society.

The guide is mainly intended for state authorities that either outsource or plan to outsource their IT operations to one or more suppliers, including but not limited to major IT procurements. However, the guide is also applicable to non-state public authorities and private companies that have decided to outsource. The main intended audience of the guide is staff responsible for supplier management. Parts of the guide are also intended for the organizational executives managing the strategic outsourcing decisions.

General recommendations

Below is a set of overall recommendations on how to manage cyber and information security in relation to IT outsourcing. The recommendations are numbered to reflect the progressing phases of an outsourcing process. Each phase is dealt with individually in the separate sections below. As certain business areas, sectors or industries may come with particular risks, standards or security requirements that are not covered by the guide, the below recommendations are not exhaustive.

Phase	Recommendation
1. Planning	1.1 Document internal and external conditions related to the planned outsourcing that may impact the organization's cyber and information security.
	1.2 Identify the organization's business processes, focusing on the underlying IT infrastructure, including data streams and mutual dependencies.
	1.3 Conduct a risk assessment, focusing on particular risks pertaining to the planned outsourcing that may impact the organization's cyber and information security.
	1.4 Formulate a separate policy on the organization's management of cyber and information security in client-supplier relationships.
	1.5 Establish an internal organization to effectively manage supplier relationships with well-defined roles, adequate resources and competencies, documented processes and the necessary IT support.
2. Security requirements	2.1 Set relevant requirements for the supplier's cyber and information security based on a risk assessment.
	2.2 Set requirements for the supplier's cyber and information security, focusing on the desired effect rather than on specific solution models.
	2.3 Consider the need for external guidance and assistance, including involvement of the CFCS, when setting supplier security requirements.
3. Supplier selection	3.1 Select a supplier based on relevant criteria and an in-depth assessment of the supplier's overall ability to meet security and other requirements.
4. Contract	4.1 Establish a clear division of roles and responsibilities with the supplier in relation to the management of cyber and information security in the client-supplier relationship.
	4.2 Establish a cooperation framework and a formalized process for handling the dialogue with the supplier, including day-to-day communication as well as communication in the event of security incidents and emergency situations.
5. Supplier management	5.1 Document the organization's need for supplier management.
	5.2 Establish a dedicated role responsible for the organization's supplier management to ensure supplier compliance with contractual security requirements.
	5.3 Perform regular audits of supplier compliance with contractual security requirements as required and on the basis of a risk assessment.
	5.4 Conduct continuous risk assessments that includes input from the supplier and any sub-suppliers.
	5.5 Handle any security incidents and significant changes at the client, the supplier or in their surroundings that may impact security during the contract period.
6. Termination	6.1 Maintain the cyber and information security level during the termination of the client-supplier relationship.

Reading guide

Several aspects of the client-supplier relationship have the potential to impact the client's cyber and information security. This guide focuses on aspects of cyber and information security in client-supplier relationships related to IT outsourcing.

The guide is primarily intended for those responsible for the daily management of an organization's suppliers. The introduction and the section on the planning phase are also intended for organization executives that hold overall responsibility for the client's cyber and information security and thus need strong awareness of their roles and responsibilities related to outsourcing.

The guide is structured to reflect the phases of an outsourcing process. Each phase contains specific considerations related to cyber and information security that need to be addressed in the setting of the client-supplier relationship. The guide is thus applicable regardless of where the organization finds itself in a specific outsourcing process. For example, the guide can be used when starting a new outsourcing process as well as when managing a supplier based on a pre-existing contract.

Outsourcing of IT operations

For the purposes of this guide, outsourcing of IT operations is defined as a business practice in which an organization hires a third party to manage all or some of its IT operations. Outsourcing may include IT systems, applications, IT infrastructure and IT services with the supplier handling the day-to-day IT operations and, possibly, tasks such as maintenance, support and development. If these tasks are handled by multiple suppliers, the organization should monitor the security level of each supplier. As a rule, the everyday procurement of IT equipment and products is not covered by the definition, unless it represents a major IT acquisition that also includes the outsourcing of operational tasks.

For the purposes of this guide, the outsourcing organization will be referred to as "the client", while the organization handling the IT operations for the client will be referred to as "the supplier". To keep things simple, these terms are used consistently throughout the guide, though the roles of client and supplier are also termed "contracting party" and "tenderer" respectively in certain parts of the tender process that may precede the outsourcing.

The figure below illustrates the typical distribution of tasks and responsibilities in client-supplier relationships when outsourcing IT operations. Even after outsourcing the daily operation of IT systems, the client remains responsible for protecting their own IT systems and information. It is thus important that the client conducts regular reviews of the supplier's performance and security during the entire contract period.

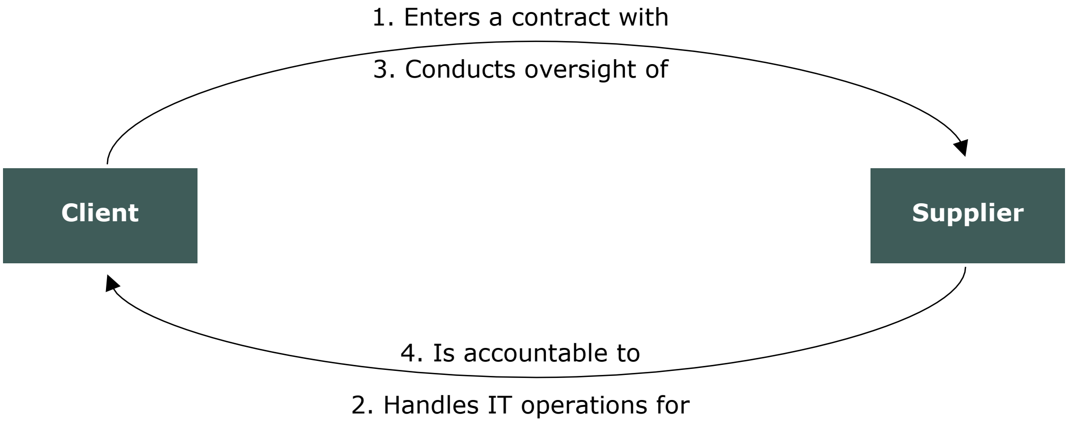


Figure 1. *Distribution of tasks and responsibilities in a client-supplier relationship.*

As the guide takes a general approach to management of cyber and information security related to outsourcing of IT, the recommendations also apply to the use of cloud service providers. For specific recommendations on how to manage cloud service providers, see ”Vejledning i anvendelse af cloudservices” (the CFCS and the Danish Agency for Digital Government 2020). Available in Danish only.

In many cases, Danish public authorities are legally obligated to carry out a competitive tender before outsourcing their IT operations. If so, the authorities are responsible for complying with the rules of the Danish Tender Act. Any such obligations are not described in this guide.

However, in connection with public IT procurements, Danish public authorities often use framework agreements through Statens og Kommunernes Indkøbsservice (SKI) or Statens Indkøb (SI). This may create some confusion as to who is responsible for ensuring supplier compliance with the framework agreement and the supply contract. Appendix 1 outlines the division of responsibilities between the parties in relation to supplier management when Danish public authorities use framework agreements through SKI or SI.

The supply chain is only as strong as its weakest link

The client and their supplier(s) are often part of a longer chain of client-supplier relationships that may also include sub-suppliers. This is commonly known as a supply chain. Supply chains often span multiple entities, with clients often using more than one supplier and suppliers often having multiple clients.

Suppliers often use sub-suppliers in their deliveries, which may ultimately impact the client’s cyber and information security. It is thus essential that the client is informed of any sub-suppliers used by their suppliers. Appendix 2 outlines a number of issues and considerations related to the supply chain of which the client should be aware.

Phases in an IT outsourcing process

Every IT outsourcing process follows a cycle that can be divided into a number of phases. This guide is structured after the six phases shown below. Cyber and information security considerations should be addressed in each of the phases – from the initial planning phase to the termination of the client-supplier relationship. The CFCS' recommendations for the individual phases are dealt with in more detail in the sections below.

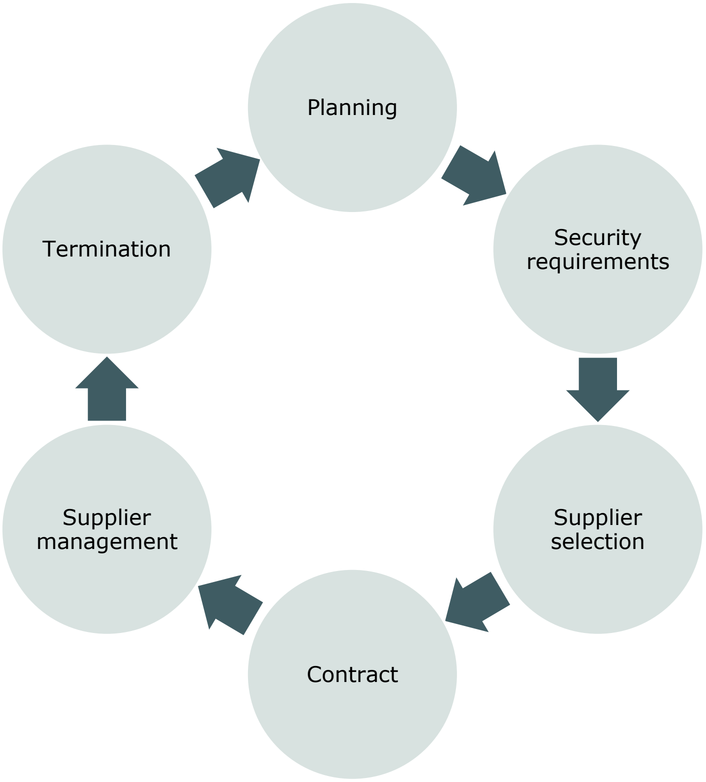


Figure 2. *Phases of an outsourcing process.*

In relation to outsourcing, Danish public authorities are not always free to choose a supplier, as some authorities are obligated by law to use specific suppliers – often other public authorities. By way of example, the IT operations of many state authorities are outsourced to the Danish Agency for Governmental IT Services by Royal Decree. As a rule, the recommendations of this guide apply regardless of whether the public authority has been free to select its own supplier or is obligated to use a specific supplier. However, a number of special conditions apply when outsourcing to the Agency for Governmental IT Services that impact the authority's management of cyber and information security in the client-supplier relationship (see appendix 3).

1. Planning

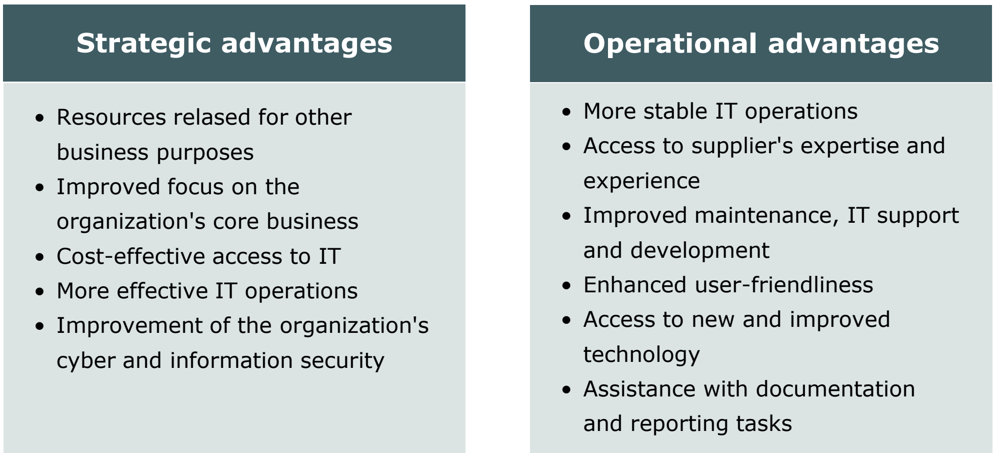
Planning
Security requirements
Supplier selection
Contract
Supplier management
Termination

1.1 Document internal and external conditions relevant to outsourcing

When a client plans to outsource all or parts of their IT operations, there are a number of cyber and information security considerations that the organization’s executives should include in their outsourcing preparations. Such considerations can be documented in an outsourcing plan or a similar strategy, as they are part of the organization’s general cyber and information security management. Organization executives should consider relevant internal factors (such as security requirements, risk appetite and organizational structure) as well as external factors (including legal requirements and other contractual commitments). These factors are outlined below.

In the planning phase, one of the first things for the client to consider is the criticality of the IT systems that are planned to be outsourced. The criticality of the IT systems to the client’s business plays a vital part when the client is to set security requirements for the supplier and determine steps to subsequently ensure supplier compliance with these requirements. Guidance on how to assess the criticality of an organization’s IT assets can be found in the publication ”Vejledning til model for porteføljestyring af statslige it-systemer” (The Danish Agency for Digital Government 2021). Available only in Danish.

The client should also consider their business needs when deciding to outsource IT operations. The client should carry out an analysis to identify their business needs and describe the business objective(s) behind the planned outsourcing, taking into account all relevant stakeholders within the organization. Outsourcing can entail strategic as well as operational advantages that the client should take into consideration, some of which are illustrated in the figure below:



Strategic advantages

- Resources relased for other business purposes
- Improved focus on the organization's core business
- Cost-effective access to IT
- More effective IT operations
- Improvement of the organization's cyber and information security

Operational advantages

- More stable IT operations
- Access to supplier's expertise and experience
- Improved maintenance, IT support and development
- Enhanced user-friendliness
- Access to new and improved technology
- Assistance with documentation and reporting tasks

Figure 3. *Potential advantages of IT outsourcing.*

Outsourcing often involves the client having to relinquish direct control of the IT operations that are outsourced to the supplier. Before making the final decision on outsourcing, organization executives should thus consider whether there are parts of the organizational IT operations that cannot be outsourced. Because of the risks related to outsourcing, the client may, for instance, wish to to keep full control over business-critical IT systems or particularly sensitive information. The willingness to relinquish control is often proportional to the client’s risk appetite.

When assessing the importance of the organization’s IT systems, organization executives should also consider whether the outsourcing arrangement involves critical IT infrastructure or IT systems that are critical to society. If so, the client should consider the need to implement additional security measures within the organization and impose further cyber and information security requirements on the supplier.

Definition of critical IT infrastructure
The data and digital elements necessary for maintaining or restoring vital societal functions.

Definition of vital societal functions
The activities, goods and services needed for the general functioning of society.

Definition of IT systems critical to society
IT systems where major disruptions result in significant challenges for society as a whole. The unavailability and unstable operation of IT systems can have significant consequences for society and for the maintenance of processes critical to society.

External conditions to be taken into consideration by organization executives in the planning phase may include commitments in pre-existing contracts with other suppliers or special rules and regulations pertaining to outsourcing of IT. Legal requirements, other regulations and contractual commitments may narrow the pool of outsourceable IT systems and the geographical location of admissible suppliers, or may dictate how certain information should be processed and protected. For instance, depending on the planned outsourcing, there may be requirements related to the protection of classified information and personal data as well as location requirement rules and export controls that the client should consider. Under the rules of the Danish Act on Screening of Foreign Direct Investments, outsourcing of critical infrastructure may also be subject to permission by the Danish Business Authority.

Document internal and external factors related to the planned outsourcing that may impact the organization’s cyber and information security.

1.2 Map the organization’s business processes, IT infrastructure and data

If a client decides to outsource an IT system without having prepared a full overview of the organization’s business processes, IT infrastructure and data streams, new vulnerabilities could arise, bringing with them new cyber and information security risks that could have been foreseen and prevented.

Before making the decision to outsource, the client should thus look into all aspects of the IT infrastructure composition and data stream flows, as well as mutual dependencies and interfaces between the different IT systems within the organization. This will make it easier for the client to select which segments of the IT infrastructure and layers of the technology stack to outsource and to describe them in adequate detail to the supplier. If such a mapping has been carried out on an earlier occasion, it must be updated in order to provide an accurate picture of the client’s business processes and the underlying IT infrastructure.

Identify the organization’s business processes, focusing on the underlying IT infrastructure, including data streams and mutual dependencies.

1.3 Conduct a risk assessment and decide on risk mitigation measures

During the planning phase, the client should conduct a risk assessment, focusing on the particular risks related to the planned outsourcing that may impact the confidentiality, integrity and availability of the client’s information. This is an important step, as outsourcing of IT can introduce new cyber and information security risks for the client, thus changing their organization’s risk landscape. In addition, the risk assessment enables the client to subsequently identify relevant security requirements for the supplier in order to mitigate specific risks related to the planned outsourcing.

The risk assessment of the planned outsourcing can be incorporated into the organization’s general risk management framework and should be conducted based on a documented process and method. For inspiration on how to conduct risk assessments, see ISO/IEC 27005 or ”Vejledning til risikostyring inden for Informationssikkerhed” (The Danish Agency for Digital Government 2020a). Available in Danish only.

Below is a list of outsourcing considerations that can be relevant to include in the client’s risk assessment. The list is not exhaustive and only includes some of the risks that should factor into the client’s overall decision to outsource IT services:

- Major changes at the supplier end can impact the supply of services, such as the supplier relocating to another country, changing sub-suppliers or being taken over by another company.
- As the client leaves some of their risk management in the hands of the supplier, the client should ensure that the supplier makes continuous contributions to the client’s risk assessment, for instance by sharing knowledge on relevant threats and vulnerabilities.

- Lack of alignment between the client's security requirements and the supplier's risk appetite and security level can result in inadequate risk management. Conversely, outsourcing could potentially improve the client's security if the supplier's organization is more mature in terms of cyber and information security.
- The threats of cyber crime, cyber espionage and destructive cyber attacks, as outsourcing can increase the client's attack surface for hackers. Such risks include supply chain attacks in which hackers try to compromise the client by exploiting vulnerabilities at the supplier end or at the supplier's other clients.
- Supplier and sub-supplier employees over whom the client has no managerial powers can gain physical and logical access to client assets.
- The supplier can gain insight into the client's organization, business processes, security measures, internal procedures, etc.
- The supplier's willingness to provide the required documentation and the client's scope for supplier management can be limited.
- Any non-compliance with legal requirements or relevant regulations on the part of the client or the supplier can result in risks for the client.
- The potential impact of a security incident depends on the business criticality of the outsourced IT systems and the sensitivity of the client's information.
- Challenges related to the termination of the client-supplier relationship and continuation of client IT operations, including verification that client data has in fact been deleted by the supplier as agreed.
- Potential risks related to outsourcing that can carry unintended consequences for the client's other supplier relationships. This is particularly relevant in connection with multi-sourcing – an outsourcing approach in which IT operations and services are contracted to multiple suppliers at the same time.

Once the client has identified the relevant risks related to the planned outsourcing, they should prepare a plan on how to treat these risks in the client-supplier relationship, reducing them to a level acceptable to the client. One way is to impose relevant security requirements on the supplier in the contract and the associated appendices (see section 2 on security requirements). All risk mitigation measures should be documented in a risk treatment plan. Some of the client's risk mitigation measures will often be transferred to the supplier, though some will remain with the client. Before reaching a final decision on which tasks to outsource, the client should thus consider the division of responsibility between themselves and the supplier.

Conduct a risk assessment, focusing on particular risks pertaining to the planned outsourcing that may impact the organization's cyber and information security.

Multi-sourcing places greater demands on the client’s risk and supplier management

Many organizations opt to contract their IT operations to multiple suppliers rather than keeping their entire IT portfolio with one single supplier. Motivations include financial advantages, flexibility and access to more specialised services. On the downside, multi-sourcing increases the complexity of the client’s IT infrastructure, just as their attack surface is increased. Multi-sourcing thus places greater demands on the client’s risk and supplier management processes, a factor that should enter into the overall decision to multi-source.

If an organization is planning to multi-source, organization executives should formulate an outsourcing strategy and establish a standardized process and life cycle on how to handle the cooperation with the suppliers, with security being a key element throughout the entire process.

1.4 Develop a policy on cyber security in client-supplier relationships

The client should also develop a separate policy on the organization’s management of cyber and information security in client-supplier relationships based on the client’s risk assessment, and general cyber and information security policy. The purpose of this policy is to set the overall framework for the organization’s management of cyber and information security related to outsourcing of IT operations.

The policy should define the organization’s strategic goals and overall requirements for the management of cyber and information security in client-supplier relationships, including the general processes, procedures and guidelines that must be implemented by both parties. In addition, the policy should outline the division of tasks and responsibilities between relevant roles in the client’s organization that deal with supplier management, and cyber and information security management (see section 1.5 and appendix 4). In this way, the policy helps ensure that the client has established an organization that is ready to manage cyber and information security in client-supplier relationships.

Develop a separate policy on the organization’s management of cyber and information security in client-supplier relationships.

1.5 Establish an internal organization to manage suppliers effectively

Outsourcing IT operations to a supplier with strong cyber security capabilities can reduce a client's cyber security risks, compared to keeping the services in-house. In any case, managing cyber and information security in a client-supplier relationship is a continuous cross-organizational task. Organization executives should thus ensure that a fitting supplier management organization is set up inside the organization. Supplier management is an area that requires well-defined roles within the organization and sufficient resources in terms of legal expertise, financing, IT, security, etc. The organization's supplier management often includes a number of different roles and functions such as:

- Organization executives
- Information security coordinator/IT security manager
- Contract manager
- Legal function
- IT manager
- Data and system owner
- Data Protection Officer (DPO)

Appendix 4 provides an example of how tasks and responsibilities can be divided between the above-mentioned roles within management of cyber and information security in connection with outsourcing. Depending on the client's size and organization, one employee may take on more than one role at the same time.

Effective supplier management requires organization executives setting the right priorities as well as cooperation across the organization.

In the planning phase, organization executives should also make a decision as to which cyber and information security responsibilities and competencies to keep in-house and which ones to outsource to the supplier. For example, the client may decide to outsource a number of technical security tasks as this will provide access to supplier expertise and optimize the use of internal resources. Outsourcing specific tasks to a supplier with specialist competencies may thus prove advantageous for the client. However, the client should always keep in mind that managing security in a client-supplier relationship requires skills and experience, and that responsibility for the protection of organization IT systems and information remains with the client even after the outsourcing.

In connection with outsourcing, organization executives should thus ensure that the organization retains relevant in-house security competencies to manage its suppliers. Organization executives should also ensure that the organization has documented processes and relevant IT support in place to enable supplier management.

Establish an internal organization to effectively manage supplier relationships with well-defined roles, adequate resources and competencies, documented processes and the necessary IT support.

2. Security requirements

Planning
Security requirements
Supplier selection
Contract
Supplier management
Termination

2.1 Set relevant cyber and information security requirements for the supplier
Imposing relevant requirements on potential suppliers is of key importance, as it provides the client with a strong basis for selecting the right supplier and also creates a good starting point for subsequent supplier management. Supplier cyber and information security requirements can help reduce risks to a level that is acceptable to the client and ensure an adequate level of security related to service supply. Supplier security requirements should be supplemented with requirements regarding monitoring and follow-ups to ensure supplier security compliance for the duration of the contract.

The client should define security requirements for the supplier based on a risk assessment conducted ahead of the outsourcing, a risk treatment plan and a policy on the organization's management of cyber and information security in client-supplier relationships (see section 1 on the planning phase). The client should carefully consider all cyber and information security aspects, including but not limited to organizational, behavioural, physical and technical security measures. In addition, the security requirements should cover detective controls as well as preventive, and corrective security measures.

The client should also take steps to ensure that security requirements align with the sensitivity of the information and the business criticality of the outsourced IT systems. If the outsourced systems are critical to society or part of critical IT infrastructure, the requirements on the supplier's cyber and information security should be stricter than in the case of less vital systems. In addition, the client should consider whether requirements related to the confidentiality, integrity and availability of information are equally important or whether they should be given different priorities.

When preparing security requirements, the client should use best practice and international standards for cyber and information security such as ISO/IEC 27001 and 27002 or similar standards as their benchmark. The client should prepare a requirements specification to clearly outline all security requirements, enabling the supplier to familiarize themselves with client security expectations ahead of the bidding process. In order to facilitate good security management practices, clients are advised to detail all security requirements in a separate security requirements specification. Where relevant, the general requirements specification should contain clear references to items listed in the security requirements specification.

Place "SMART" security requirements on the supplier

It is important to set well-defined security requirements that are suited to evaluate solutions from potential suppliers. In addition, the requirements should be suited for control and follow-ups throughout the duration of the contract. Appendix 5 provides a guide to assist the client in specifying better security requirements using the SMART principle under which requirements, as far as possible, should be: Specific, Measurable, Achievable, Relevant, and Time-bound.

The client should ensure that the supplier requirements cover the following areas of cyber and information security as well as supplier management:

Cyber and information security areas	Supplier management areas
• Relevant legal and regulatory requirements. • The supplier’s risk management process and information security management system based on ISO 27001 or similar international standards. • Division of roles and responsibilities between client and supplier (see section 4). • The need to establish a data processing agreement (DPA) with the supplier. • Training of relevant supplier and sub-supplier staff with access to client assets. • Security clearance needs of relevant supplier and sub-supplier staff with access to client assets. • A non-disclosure agreement (NDA) that includes any sub-suppliers. • Management of cyber and information security in the transition phase, for instance from one supplier to another. • Security tests and vulnerability scans by the client, supplier, or a third party. • The supplier’s control over access to client assets, including the supplier’s ability to support the client’s information classification system. • Plans for incident response, business continuity and disaster recovery, including regular testing of these plans. • The supplier’s obligation to notify the client of any circumstances or events that may impact security in the supply of services, including security incidents. • Secure communication between the parties, including, for instance, use of TLS and DMARC. For more recommendations see the CFCS’ guides at cfcs.dk.	• Supplier reporting, including forms and content of reporting as well as structure and frequency of status meetings between the parties. • Client rights to oversee supplier compliance with the contract and applicable regulation. • Supplier’s use of any sub-suppliers (see appendix 2). • Supplier’s obligation to appoint key personnel to manage supplier compliance responsibilities. • The establishment of a cooperation framework by the supplier (see section 4). • Supplier obligation to cooperate with the client’s other suppliers. • Client’s scope for involving third parties to provide support in connection with the supply and during termination of the contract, including technical or legal assistance. • Supplier obligation to provide accurate, adequate and up-to-date documentation on the fulfilment of the supply. • The parties’ procedures for handling changes in terms of continuously adjusting cyber and information security measures throughout the contract period (see section 4). • Terms that take into account any sale, changes in ownership or cessation of the supplier’s business. • Supplier obligation to remedy any errors and deficiencies in the supply. • Supplier obligation to implement additional or corrective security measures to to ensure compliance with security requirements. • Protocols for the handling of disputes. • Consequences related to the supplier’s failure to comply with security requirements that could result in penalty and the client’s right to immediate termination of the contract. • Provisions on the termination of the client-supplier relationship (see section 6).

Inspiration on how to specify security requirements can be found at the homepage of the Danish Agency for Digital Government (en.digst.dk) that offers a range of tools and templates that can help the client make relevant security requirements in contracts, including the K04 Standard contract for IT operations, a library of clauses and a catalogue of requirements (The Danish Agency for Digital Government 2016; 2017; 2020b). In addition, sikkerdigital.dk has a catalogue of contract specifications for IT systems critical to society and an appendix with additions to the operationalization of the catalogue (The Danish Agency for Digital Government 2022a; 2022b). Available only in Danish.

Set relevant requirements for the supplier's cyber and information security based on a risk assessment.

2.2 Set requirements for supplier security focusing on the desired effect

When setting requirements for the supplier's cyber and information security, the client should also carefully consider the level of details in their requirements. Generally, the client should set up security requirements that express desired effect rather than specifying in detail how the supplier should meet these requirements. As the supplier knows their own staff, internal procedures and IT infrastructure, they are often much better equipped to design and implement security measures within their own organization than the client would be. Suppliers may have alternative and perhaps better ways of solving a given task, just as specific and detailed requirements on technical security measures may become outdated during the course of the contract period due to technological developments.

If the supplier can document their ability to achieve the desired effect of the security requirement, this will often be preferable to sticking to fixed ideas on how the requirement should be met. Sometimes, however, the client may need to place very specific and detailed security requirements on the supplier, for instance in terms of technical security measures due to applicable regulation or specific client security needs, etc.

Catalogue of requirements

The client can prepare a catalogue of general security requirements that can be incorporated into all supplier contracts regardless of the nature of the services supplied. The requirements should be formulated as generically as possible to be relevant in all contractual contexts and to be adaptable to the specific service supplied. This will help ensure a benchmark security level for all client suppliers.

If the client uses an information classification system, a catalogue of security requirements should be prepared for each classification level, enabling the client to transfer security requirements from the relevant catalogue to the contract. This helps ensure that the security level reflects the information classification level.

If the client has to carry out a public tender as part of the outsourcing process, a number of special conditions apply that should be take into consideration. The public tendering rules contain requirements regarding the tender process and the design of the tender documents. The client should thus always seek legal assistance in the tender process.

When preparing tender documents, the client should consider setting certain security requirements as minimum requirements that must be met before tenderers can be taken into consideration as potential suppliers. Alternatively, the client may choose to present security requirements as award criteria, giving tenderers a better chance of competing on security if the contract is awarded based on the best balance between price and quality, including security. Any minimum requirements, however, are not part of the evaluation of tender submissions.

If certain security requirements are deemed mandatory, it may be expedient to specify them as minimum requirements. If, however, a tender contains a lot of minimum requirements, this could deter potential suppliers from bidding for the contract, just as suppliers risk having their bids rejected on grounds of non-compliance due to failure to meet the minimum requirements. Furthermore, the client is precluded from making subsequent adjustments to the minimum requirements. The client should thus carefully consider which requirements to include as minimum requirements. In addition, the tender documents should clearly state whether the requirements are to be considered minimum or general requirements.

Set requirements for the supplier's cyber and information security, focusing on the desired effect rather than on specific solution models.

2.3 Consider the need for guidance from the CFCS and other external parties

Even though clients have the best knowledge of their own business, the underlying IT infrastructure and internal security measures, they do not always hold the competencies required to identify all relevant security requirements and other terms relevant to the contract. Consequently, clients should consider whether it would be relevant to seek guidance from external parties, such as legal, IT or technical security assistance.

Authorities should seek advice from the CFCS when setting security requirements for suppliers in connection with outsourcing of critical IT infrastructure or IT systems that are critical to society.

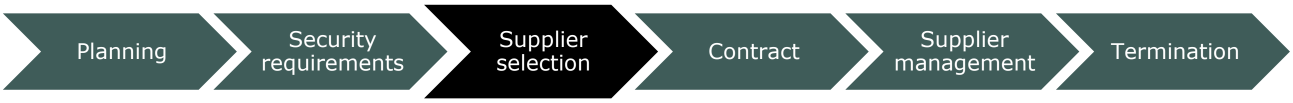
Consider the need for external guidance and assistance, including involvement of the CFCS, when setting supplier security requirements.

Catalogue of contract specifications for IT systems critical to society

For Danish state authorities responsible for the outsourcing of IT systems critical to society, a new catalogue of contract specifications applies that is to be incorporated into future contracts based on the comply or explain principle. The catalogue comprises four themes: 1) IT operations, 2) security, 3) personal data and 4) control. The catalogue can be found at sikkerdigital.dk (Danish Agency for Digital Government 2022a). Available in Danish only.

Each state authority must ensure that the provisions of the catalogue become part of future supplier contracts when outsourcing IT systems that are critical to society. The authority must also consider the need to tighten the provisions or to add further requirements based on a risk assessment of the IT system to be outsourced. It is up to the individual authority to decide whether the planned outsourcing includes an IT system critical to society. This decision can be based on the definition and supporting questions in ”Vejledning til model for porteføljestyring af statslige it-projekter” (Agency for Digital Government 2021). Available in Danish only.

3. Supplier selection



3.1 Select a supplier based on the right selection criteria
Supplier selection can have a significant impact on the quality and security of the IT operations delivered. It is thus important for the client to base the selection of supplier on relevant criteria and an in-depth investigation of the supplier's overall ability to fulfil the client's security needs and other service delivery requirements. This will help ensure that the supplier is able to provide an adequate level of cyber and information security for the duration of the contract and upon contract termination.

When selecting a supplier, the client should take into account a number of considerations regarding potential suppliers, some of which are exemplified below:

- The supplier's ability to deliver the IT services requested.
- The supplier's ability to meet the client's security requirements.
- The supplier's geographical location.
- The supplier's acceptance of potential transition obligations if the IT operations have previously been outsourced to another supplier.
- The supplier's willingness to cooperate and contribute to audits.
- The supplier's acceptance of the terms of termination, including the obligation to maintain cyber and information security throughout the termination period (see section 6).
- The supplier's financial position and ownership structure.
- The supplier's use of sub-suppliers.
- The supplier's integrity and any previous material breaches of public contracts.
- Client and supplier equality in terms of size and mutual dependency.
- The risk of supplier lock-in because the future costs of switching to a new supplier could be too great to facilitate a move due to the dependence of the client on the services provided by the supplier.

The list is not exhaustive as there may be special conditions related to the specific supply of services that the client also needs to consider during the supplier selection process. Some of the above-mentioned considerations are elaborated below.

The client's financial position is often a significant factor in supplier selection. The client often has to strike a balance between price and quality, including security, when selecting a supplier. As regards security, the client should consider whether there is a good balance between the security level offered by the supplier and the overall price of the contract. Some suppliers may be willing to cut corners on security in order to offer a lower price. It may thus be advisable for the client to ask potential suppliers to specify the price of security in the tender and contract. This gives the supplier a stronger financial incentive to actually meet the agreed security requirements. If the planned outsourcing includes critical IT infrastructure, the client should attach greater importance to security in the trade-off between price and quality when evaluating potential suppliers.

The client should also consider whether the relative size and dependency between the parties could impact on the client’s scope for managing the supplier during the contract period. If the client is small relative to the supplier, the client will generally find it more difficult to set specific security requirements and subsequently manage the supplier than if the opposite were the case. Conversely, if the supplier is small, the client has to pay special attention to the risk of bankruptcy and changes in the supplier's ownership structure during the contract period. When selecting a supplier, the client should thus consider the pros and cons in relation to supplier size and dependency.

The client may consider which scenario described in the figure below best characterizes their client-supplier relationship. Please note that the figure provides a simplified overview of potential pros and cons which cannot necessarily be directly applied to a specific client-supplier relationship.

		Client	
		Small	***Large***
Supplier	***Small***	**Scenario 1:** The client is one in a small pool of clients. **Pros:** • The client is prioritized • Good opportunity to make specific requirements and manage the supplier **Cons:** • Risk of supplier bankruptcy or change of ownership • Limited selection of IT services • Limited number of documented supplier processes and procedures in place	**Scenario 2:** The client is strategically important to the supplier. **Pros:** • The client has high priority • Rich opportunity to make specific requirements and manage the supplier **Cons:** • Risk of supplier bankruptcy or change of ownership • Limited selection of IT services • Limited number of documented supplier processes and procedures in place
	Large	**Scenario 3:** The client is not important to the supplier. **Pros:** • Freedom of choice within a large selection of standard IT services • The supplier has more documented processes and procedures in place **Cons:** • The client has low priority • Difficult to make specific requirements and manage the supplier • Risk of supplier lock-in	**Scenario 4:** The client is one among many other clients. **Pros:** • Freedom of choice within a large selection of standard IT services • The supplier has more documented processes and procedures in place • The client is given higher priority than smaller clients **Cons:** • Difficult to make specific requirements and manage the supplier • Risk of supplier lock-in

Figure 4. *Potential pros and cons connected with supplier selection.*

In addition, the client should consider the supplier's geographical location, as conditions outside the client's home country may impact the client's cyber and information security. In some parts of the world, factors such as local legislation, public authorities' access to data, crime rates, cultural differences, political conditions, natural disasters and geopolitical tensions may affect security in the supply of IT services. For instance, there may be legal issues to consider when outsourcing IT operations to suppliers in some countries. Consequently, the client should ensure that the legal regulations under which the supplier operates are not at odds with the client's requirements. For that reason, the client should always seek legal assistance during supplier selection.

Danish public authorities should also be aware that their supplier selection process often has to comply with public tendering rules. Thus, authorities should make sure that the tender documentation, as far as possible, contains relevant requirements and terms to mitigate the above-mentioned risks related to supplier selection in accordance with public tendering rules.

Select a supplier based on relevant criteria and an in-depth assessment of the supplier's overall ability to meet security and other requirements.

4. The contract

Planning
Security requirements
Supplier selection
Contract
Supplier management
Termination

4.1 Establish a clear division of roles and responsibilities

Once a supplier has been selected or designated, a contract between the parties will be prepared. The contract should ensure that the parties know their respective roles and responsibilities related to cyber and information security management during the contract period. It is important that the contract details their tasks and obligations to remove any doubts as to the division of responsibilities between the parties.

The contract should clearly state the client's cyber and information security expectations to the supplier. The contract should include security requirements to ensure their enforceability on a par with any other requirements in the contract. If the client has carried out a public tender, the contract should include the same security requirements as those included in the tender documents as well as any adjustments made in response to the supplier's tender.

The contract should also include provisions to ensure supplier compliance with the security requirements during the contract period. The provisions of the contract should cover the supplier's documentation and reporting obligations as well as the right of the client to – either by themselves or by use of a third party – verify supplier compliance with the contract. The supplier should also be obligated to allocate sufficient resources to ensure compliance with controlling and reporting requirements, including time for planning of meetings, preparation of documentation and follow-ups.

The client's right to oversee the supplier should include all aspects of the supplier's compliance with the contract, including those related to the supplier's use of any sub-suppliers. Supplier management can be performed in different ways (see examples under section 5 on supplier management). In addition, the supplier should be obligated to assist the client in the supplier management process by giving the client physical and logical access to supplier facilities, IT systems and data as required, and by delivering all relevant documentation, etc.

Client and supplier employees responsible for drawing up the contract are not always given operational responsibility once the cooperation starts. When the contract is complete, those responsible for contract implementation from both client and supplier side should gather for a kick-off meeting to set out further details and discuss any contract ambiguities. Alignment of expectations may contribute to ensure agreement as to the parties' respective roles and responsibilities and to prevent any misunderstandings and disputes during the contract period.

Establish a clear division of roles and responsibilities with the supplier in relation to the management of cyber and information security in the client-supplier relationship.

4.2 Establish a framework of cooperation with the supplier

The contract should establish a framework for cooperation, and a formalized process for communication between the client and the supplier. This process should specify procedures for handling the day-to-day dialogue between the parties, mechanisms to solve potential disputes, and communication paths in case of security incidents or emergency situations.

The client and supplier should establish a framework that anchors cooperation between the parties in one or more forums, thereby ensuring continuity in the dialogue. Theseshould be established based on the client's needs and an on assessment of relevant factors such as the criticality of the outsourced IT systems, the overall contract value, and the strategic importance of the supply of IT services to the client's business (see section 5 on supplier management).

The framework could, for example, be comprised of a steering group and one or more underlying working groups that are either temporary or permanent. Relevant representatives from both parties – for example representatives at the operational or managerial level – should meet regularly in these forums to discuss status of the supplier's delivery of services, including progress, current issues and suggestions for changes related to the contract. The contract should describe the composition and areas of responsibility of each cooperation forum, including meeting frequency and agenda, with security being a permanent agenda item.

The contract should enable both parties to adjust the level of security in the client-supplier relationship as needed during the contract period.

In addition, the client should consider which options should be available for the parties to adjust cyber and information security measures during the contract period when relevant. Circumstances may change at both the client and supplier end that introduce new risks, just as the overall threat landscape is constantly evolving. Consequently, the contract should enable the parties to adjust the security level to reflect the changing threat landscape, for example by allowing the client to impose additional security requirements on the supplier. However, the contract should ensure that any adjustments made by the supplier are subject to client approval, ultimately giving the client control of the security level associated with the supply of services.

Establish a framework for cooperation and a formalized process for handling the dialogue with the supplier, including day-to-day -as well as crisis communication in case of security incidents or emergency situations.

5. Supplier management

Planning
Security requirements
Supplier selection
Contract
Supplier management
Termination

5.1 Document the organization’s supplier management needs

Not all suppliers require the same supplier management focus in terms of time and resources. The scope and frequency of the client’s supplier management efforts should reflect the criticality of the supplier’s delivery of IT services to the client’s business and rest on an assessment of related cyber and information security risks. This assessment should be documented and updated regularly depending on the specific contract and potential changes in the overall risk landscape.

If the client has multiple suppliers, they should be ranked according to business criticality. The client should conduct a more thorough and frequent control of their most important suppliers based on a risk assessment. The client can draw up a prioritized list of suppliers by preparing a risk assessment based on relevant factors such as:

- The sensitivity and volume of the client’s information related to the delivery.
- Whether the delivery includes the client’s business critical IT systems or processes.
- Whether the delivery includes critical IT infrastructure or IT systems critical to society.
- Whether the delivery is standardized or specialized.
- The geographic location of the data (with the client or with the supplier, domestic or abroad).
- The nature of the delivery, including the supplier’s operational responsibility and access rights to client data (access to read and/or write data).
- The overall contract value.
- The number of errors and deficiencies in the delivery as well as security incidents at the supplier end.
- The supplier’s willingness to cooperate with the client and the client’s other suppliers.

The client can use the above mentioned factors to prepare a supplier management plan and prioritize resources by focusing on the organization’s critical suppliers, ensuring that its supplier management practice is risk-based and thereby yields the highest value.

Document the organization’s need for supplier management.

Risks related to inadequate supplier management

Inadequate supplier management can lead to:

- Subpar risk management on the part of the supplier.
- Increasing number of errors, delays and deficiencies in delivery.
- Non-compliance with the contract by the supplier.
- Failure to enforce the contract by the client.
- The supplier deprioritizing client needs in favour of other clients.
- Increasing supplier dependence.

5.2 Establish a role responsible for supplier management related to security

As cyber and information security is an integral part of the client's supplier management practice, the client should establish a dedicated role to manage supplier compliance with the security requirements listed in the contract (see appendix 4). It is important that the role has sufficient supplier management and security competencies to conduct controls and assess supplier compliance. As supplier management is a cross-functional discipline that requires legal, financial, IT and security skills, the role should involve relevant staff from other organizational departments and functions as needed.

In addition, the client should ensure that the supplier designates a similar role within the supplier organization to manage cyber and information security in the client-supplier relationship. This role should be the client's point of contact for cyber and information security issues, including the client's supplier management practice and in case of security incidents during the contract period.

Establish a dedicated role responsible for the organization's supplier management to ensure supplier compliance with the contractual security requirements.

5.3 Manage the supplier's compliance with security requirements as required

Once the contract has been signed by the parties and cooperation has commenced, the client should regularly control the supplier's compliance with the security requirements set out in the contract as required. Supplier management enables the client to enforce the contract and thus helps to ensure that the supplier delivers the agreed services and meets their obligations during the contract period.

The client should always manage the supplier by actively using the contract entered between the parties. The client can, for example, use a risk assessment to identify which security requirements to focus on when verifying supplier compliance with the contract. If the supplier fails to meet the security requirements, it is important that the client immediately follows up and enforces the contract. It is the client's responsibility to point out the supplier's non-compliance and ensure that the supplier subsequently adopts the necessary security measures and rectifies any errors and deficiencies in accordance with the contract. The client should also ensure that their supplier management activities and results are documented for the sake of any enforcement of the contract.

Examples of supplier management activities

Supplier management can be conducted in multiple ways and include different forms of documentation and reporting. The supplier's documentation of their compliance may consist of reports, statements, risk assessments and other relevant information security management system (ISMS) documents. In addition, supplier management may include a number of activities such as:

- Status meetings between the client and supplier (regular meetings or ad hoc).
- Written reporting to the client (regular reporting or upon request).
- Supplier inspection (announced or unannounced visits).
- Internal audits or reviews by the supplier.
- External audits or reviews by the client or an independent third party.
- Disaster recovery tests with the client as participant or observer.
- Security testing (also known as penetration testing).

The supplier's reporting and the client's supplier management practices should be conducted as specified in the contract. Both parties are thus required to set aside the necessary time and resources for preparation, documentation and follow-up. Security should be a permanent item on the agenda at status meetings between the client and supplier. In addition, minutes should be taken at key meetings and subsequently approved by both parties.

In addition, the client should consider the need to include a third party in their supplier management efforts. Under certain circumstances, authorities and companies can seek advice from the Danish Agency for Digital Government or the Centre for Cyber Security on management, including help to identify relevant security requirements in existing contracts and to manage supplier compliance with these requirements.

Perform regular audits of supplier compliance with contractual security requirements as required and on the basis of a risk assessment.

5.4 Conduct continuous risk assessments with input from suppliers

The client should conduct risk assessments continuously to determine whether the security level in the client-supplier relationship needs to be adjusted to reflect changes in the risk landscape. The risk assessment should be updated once a year as a minimum as well as in case of any significant security incidents, significant changes (see section 5.5.) and on the basis of supplier audit. After updating the risk assessment, the parties should make plans regarding mitigation of newly identified or adjusted risks – and document these plans. The client should follow up on the implementation of the agreed risk treatment plans.

The client should ensure sufficient supplier involvement during the risk assessments. With regards to cooperation with a supplier, the client should have a clear understanding of each party's role and input in relation to risk management. The client should assess the potential business impact of any compromise of confidentiality, integrity or availability of the client's information. Based on the risk assessment, the client should determine how to treat (i.e. accept, mitigate, transfer or avoid) the identified risks depending on the organization's defined risk appetite and subsequently prioritise resources to effectively mitigate unacceptable risks.

The supplier should contribute to the risk assessment of the client's business by conducting risk assessments of the supply of services, considering relevant input from potential sub-suppliers in the supply chain (see appendix 2). The supplier can often help identify relevant risks and qualify their likelihood and technical consequences, since the supplier has a detailed knowledge of their own security measures and IT infrastructure used to support the delivery of services. Consequently, the client should ensure that the supplier contributes with valuable information on relevant threats and vulnerabilities to the client's risk assessment.

Conduct continuous risk assessments with input from the supplier and any sub-suppliers.

5.5 Follow-up on any significant changes and security incidents

During the contract period, unexpected or planned changes may occur with or within the client and/or supplier organization, or in their surroundings that affect the cyber and information security related to the delivery of services. Consequently, it is important that both parties contribute to maintaining security levels in the client-supplier relationship. As part of their cyber and information security management efforts, the parties should continuously assess, document and handle any significant changes occurring during the contract period. The client should ensure that the supplier follows up on any changes in a timely manner by making the required adjustments and implementing additional security measures in accordance with the contract.

Changes may occur to the parties' organizations, business processes and IT infrastructure during the contract period. The client should pay special attention to circumstances at the supplier end that might affect the security in the delivery of services such as changes to the supplier's business strategy, financial position and use of sub-suppliers. With regards to their surroundings, the client should pay special attention to technological developments, changes in the threat landscape and changes to regulation under which the parties operate.

In addition, the client should ensure that the supplier addresses any security incidents that arise during the contract period as stipulated under the agreement. It might also be necessary to revise the contract as a result of any changes during the contract period. Consequently, the client should review the contract once a year as a minimum to ensure that it still meets their security requirements.

Handle any security incidents and significant changes at the client, the supplier or in their surroundings that may impact security during the contract period.

6. Termination

Planning

Security requirements

Supplier selection

Contract

Supplier management

Termination

6.1 Maintain the negotiated security level throughout the contract termination process

The client’s cyber and information security must be maintained during contract termination and the winding down of the client-supplier relationship, regardless of whether IT operations are transferred to another supplier or returned to the client (insourcing).

When entering the contract with the supplier, the client should ensure that the termination provisions, as a minimum, include:

- The supplier’s continued obligations and service-level agreements (SLA) during the termination process if the contract is terminated prematurely by mutual agreement or as a result of disputes between the parties.
- The client’s cyber and information security requirements while the supply of services is transferred to another supplier or returned to the client.
- A complete list of which client assets, including backup, stored by the supplier that are to be returned to the client, transferred to a new supplier or destroyed.
- Procedures ensuring that client assets are returned to the client, transferred to a new supplier or disposed of as specified in the contract.
- The parties’ continued confidentiality agreement post contract termination.
- The supplier’s obligation to contribute to a smooth transition and continuation of IT operations if the contract is to be re-tendered, transferred to a new supplier, or if the client decides to insource, including requirements for the supplier’s documentation, transfer of knowledge and cooperation during the transition period.

In addition, the parties should prepare a plan on how to maintain the agreed security level during the termination phase, including security requirements if the client decides to insource or transfer the IT operations to a new supplier. The client can also establish a role in-house to oversee that the client-supplier relationship is dissolved in accordance with the agreed termination plan and that the dissolution is sufficiently documented before cooperation is officially concluded.

When terminating the contract with the supplier, the client should also ensure to promptly remove the supplier’s physical and logical access rights to the client’s assets, including client information, IT systems and facilities. The contract should clearly state which assets are to be returned to the client, disposed of or transferred to a new supplier. Similarly, the contract should contain procedures to ensure safe transfer or disposal of client assets in terms of format, completeness, verification, security, etc.

In addition, the parties can agree that the supplier continues to store some of the client's information post contract termination. For instance, the supplier may store relevant log files collected during the contract period to ensure that it remains possible to investigate potential IT security incidents at the supplier. If so, the client should consider what information the supplier should continue to store and for how long before it is deleted or securely returned to the client.

Maintain the cyber and information security level during the termination of the client-supplier relationship.

References

The Centre for Cyber Security and the Danish Agency for Digital Government (2020). *Vejledning i anvendelse af cloudservices.* https://digst.dk/data/vejledning-til-anvendelse-af-cloudservices/ (available in Danish only)

The Centre for Cyber Security (2017). *Investigation report: Outsourcing – hvem har ansvaret?.* https://www.cfcs.dk/da/cybertruslen/rapporter/arkiv/outsourcing---hvem-har-ansvaret/ (available in Danish only)

The Centre for Cyber Security (2019). *Threat assessment: Cyber attacks against suppliers.* https://www.cfcs.dk/en/cybertruslen/threat-assessments/supply-chain/

The Centre for Cyber Security (2020). *Threat assessment: The cyber threat against IT service providers.* https://www.cfcs.dk/en/cybertruslen/threat-assessments/it-service-providers/

The Danish Agency for Digital Government, Local Government Denmark (KL) and Danish Regions (2018). L*everandørstyring – en rejsefortælling om krav og opfølgning på sikkerhed.* https://www.sikkerdigital.dk/media/8785/leverandoerstyring-en-rejsefortaelling-om-krav-og-opfoelgning-paa-sikkerhed.pptx (available in Danish only)

The Danish Agency for Digital Government (2016). *Klausuler til informationssikkerhed.* https://digst.dk/Styring/Standardkontrakter/Klausuler-til-informationssikkerhed (available in Danish only)

The Danish Agency for Digital Government (2017). *Sådan stiller du krav til leverandører om informationssikkerhed – katalog.* https://digst.dk/styring/standardkontrakter/klausuler-til-informationssikkerhed/kravkatalog-til-leverandoerer/ (available in Danish only)

The Danish Agency for Digital Government (2020a). Vejledning til risikostyring inden for informationssikkerhed. https://sikkerdigital.dk/media/6835/vejledning_til_risikostyring-_nden_for_informationssikkerhed_2020.pdf (available in Danish only)

The Danish Agency for Digital Government (2020b). *K04 Standardkontrakt for it-drift.* https://digst.dk/styring/standardkontrakter/k04-standardkontrakt-for-it-drift/ (available in Danish only)

The Danish Agency for Digital Government (2021). *Vejledning til model for porteføljestyring af statslige it-systemer.* https://digst.dk/styring/systemstyring/dokumenter-vejledninger-og-vaerktoejer/ (available in Danish only)

The Danish Agency for Digital Government (2022a). *Katalog over kontraktbestemmelser for samfundskritiske it-systemer.* https://sikkerdigital.dk/Media/637819816667401542/Katalog%20over%20kontraktbestemmelser_2022_web.pdf (available in Danish only)

The Danish Agency for Digital Government (2022b). *Appendiks I: Tilføjelser til operationaliseringer af kontraktbestemmelser.* https://sikkerdigital.dk/Media/637819816660682223/Appendiks%20I%20-%202022.pdf (available in Danish only)

The Ministry of Finance (2017). *Vejledning om tilsynet med Statens It.* https://fm.dk/udgivelser/2017/december/vejledning-om-tilsynet-med-statens-it/ (available in Danish only)

ISO/IEC 27036-1:2014 Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements

Appendix 1: **Framework agreements**

Procurement of IT products and services through framework agreements
When procuring IT products and services, etc., Danish public authorities often use framework agreements through Staten og Kommunernes Indkøbsservice (SKI) or Statens Indkøb (SI). A framework agreement defines which products or services are to be provided under the agreement and sets out terms and conditions as well as price. Danish public authorities are either free or obliged to use these framework agreements when procuring IT.

The client remains responsible for ensuring supplier compliance with the delivery contract despite using a framework agreement from SKI or SI.

One of the advantages of framework agreements is that SKI or SI completes the tender on behalf of Danish public authorities. Based on a number of criteria, SKI or SI concludes framework agreements with one or more suppliers. When a framework agreement has several suppliers, the client may award the contract to a supplier either directly based on the price and possibly the quality of the supplier's tender or through a mini competition that enables the client to place additional requirements on the pre-qualified suppliers in the framework agreement. However, Danish public authorities may be obligated to use a framework agreement that has only one supplier. The figure below shows the division of tasks and responsibilities between SKI/SI, the public authority and the supplier when using framework agreements to procure IT.

SKI/SI	Client	Suppliers
• Concludes a framework agreement with one or more suppliers • Executes the tender on behalf of the client • Ensures supplier compliance with the framework agree-ment, including security •requirements •Handles the contract management of the framework agreement	• Selects a supplier from the framework agreement • Concludes a delivery agreement with the supplier based on the framework agreement • Ensures supplier compliance with the delivery agreement, including security requirements	• Solves the task on behalf of the client • Is accountable to both SKI/SI and the client as regards to compliance with the framework and delivery agreement respectively

Figure 5. *Division of tasks and responsibilities related to framework agreements.*

Although the client uses a framework agreement, the responsibility for awarding the contract to the right supplier from the framework agreement remains with the client. The client must also conclude a delivery agreement with the selected supplier based on the framework agreement. The client is solely responsible for ensuring supplier compliance with this delivery agreement, irrespective of whether using the framework agreement is mandatory or voluntary. In case of doubt, the client should seek advice with SKI/SI.

Appendix 2: **Remember the supply chain**

Keep track of sub-suppliers in the supply chain
Even when the client has chosen to outsource their IT operations to a specific supplier, the supplier will often use one or more sub-suppliers to deliver the services. The use of sub-suppliers limits the client's ability to control the supply of services and exposes the client to new cyber and information security risks. It is thus important that the client has an overview of the supply chain and considers any risks related to sub-suppliers.

When concluding the contract with the supplier, the client should consider the supplier's potential use of sub-suppliers. The contract should specify that the client reserves the right to approve any sub-suppliers and that the supplier is obligated to notify the client of any use hereof. In addition, all the client's cyber and information security requirements on the supplier should also apply to any sub-suppliers. It should thus be clear from the contract that the supplier is obligated to ensure that any security requirements and obligations set out in the contract also extend to sub-suppliers.

If the client has approved the transfer of parts of the contract to a sub-supplier, the supplier is responsible for controlling the partial delivery of services by the sub-supplier to the client. The client is thus advised to ensure that the contract assigns responsibility to the supplier for audit of compliance by any sub-suppliers with the security requirements and any other requirements set out in the original contract between the client and supplier. The contract should also state that the supplier must document completed sub-supplier inspections and audits, etc. The figure below shows the relationship between client, supplier and potential sub-suppliers in the supply chain.

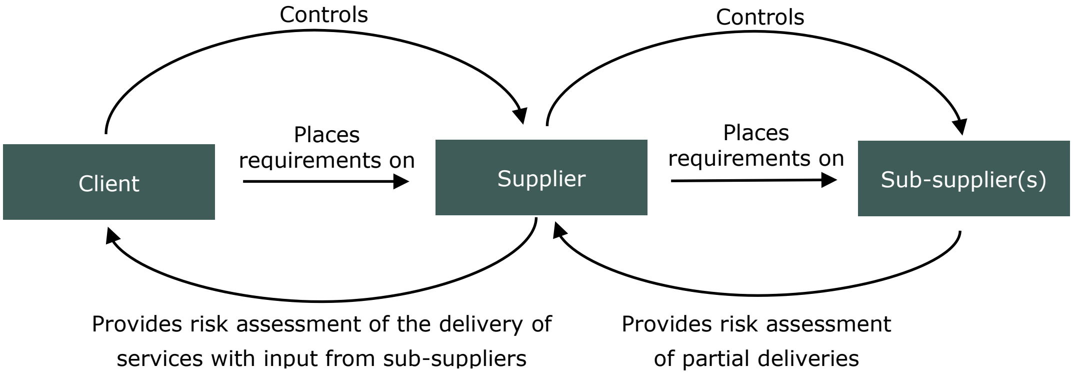

Controls
Controls
Places requirements on
Places requirements on
Client
Supplier
Sub-supplier(s)
Provides risk assessment of the delivery of services with input from sub-suppliers
Provides risk assessment of partial deliveries

Figure 6. *Relationship between client, supplier and sub-suppliers*

The client should ensure that the supplier manages their sub-suppliers sufficiently to ascertain their compliance with the security requirements set out in the contract between the client and supplier. In addition, the client should conduct a business-related risk assessment that includes suppliers and any sub-suppliers in the supply chain. The client should ensure that suppliers contribute to this business-related risk assessment with risk assessments of their supply of services that also include input from any sub-suppliers on relevant risks to the client's business.

Appendix 3: **Outsourcing to the Danish Agency for Governmental IT Services**

Considerations when outsourcing to the Agency for Governmental IT Services
The Agency for Governmental IT Services manages IT operations for many Danish governmental authorities that have transferred operational responsibility to the Agency by royal decree. The authorities can choose between a number of different operating models at system level describing the division of tasks and responsibilities between the authorities and the Agency based on the different layers in the technology stack. The authority should opt for the operating model whose division of tasks and responsibilities best suits the organization's business needs, security technical competencies and risk appetite.

For governmental authorities that have transferred responsibility for their IT infrastructure and operations to the Agency for Governmental IT Services, supervision of the Agency has been transferred to the Danish Ministry of Finance. The Department of the Ministry of Finance monitors the Agency's management of cyber and information security and shares its findings with the clients of the Agency. As a rule, this renders the authorities exempt from monitoring the Agency themselves. Instead, the authorities should focus on whether the Ministry of Finance's ongoing supervision and annual supervision reports highlight relevant risks or contain remarks concerning the Agency's level of security that may affect the security of the client's outsourced IT systems.

Depending on the choice of operating model, there may be parts of the technology stack that fall outside the scope of the Ministry of Finance's supervisory responsibility. If so, this supervisory responsibility will rest with the individual authority. The authority should thus make sure to supervise the Agency for Governmental IT Services in areas where supervisory responsibility rests with the authority itself and ensure that follow-ups are carried out as needed within these areas. The exact division of tasks and responsibilities between the Ministry of Finance and the authority as regards supervision of the Agency in the different operating models is described in the guide ”Vejledning om tilsynet med Statens It” (Ministry of Finance 2017). As the Ministry of Finance has assumed the supervisory responsibility for the Agency, the authority should also inform the Department of the Ministry of Finance if it finds the risk management performed by the Agency inadequate, or if disputes arise during the contract period between the Agency and the authority on specific conditions in the contract.

Even in the cases where governmental authorities are obligated to outsource their IT operations to the Agency for Governmental IT Services or another authority, the recommendations of this guide still apply. When outsourcing to the Agency, the authority should conduct a risk assessment of the IT system to be outsourced in order to determine whether the security measures described in the Agency's so-called product portfolio ensure an adequate security level or if additional security measures are required.

If the authority assesses that an IT system requires specific security measures that are not covered by the standard security level offered by the Agency for Governmental IT Services, the authority should make additional requirements on the Agency. Subsequently, the parties will decide the best way for the Agency to implement these security measures and document fulfilment of the client’s requirements. It is important that the authority is aware that any additional security requirements do not fall within the scope of the Ministry of Finance’s supervision; rather, the authority itself is responsible for ensuring the Agency’s compliance with these requirements. The authority should thus assess the need to follow up on the Agency’s fulfilment of these requirements and, as a minimum, request written reporting from the Agency as documentation.

Appendix 4: **Roles & responsibilities**

Roles and responsibilities within the organization related to outsourcing
The below table shows examples of relevant roles and responsibilities that should generally be included in the clients' management of cyber and information security in client-supplier relationships when outsourcing IT. In addition, a number of key support functions such as HR and Finance should also be included in the client's cooperation with the supplier. This list of tasks and responsibilities is not exhaustive.

Roles	Tasks and responsibilities
Organization executives	• Overall responsibility for the organization's cyber and information security management, including establishment of an Information Security Management System (ISMS) and for defining the organization's security level. • Responsibility for strategic decisions regarding outsourcing. • Responsibility for approving relevant organizational policies such as a policy on cyber and information security management in relation to outsourcing. • Responsibility for ensuring that the organization has the resources & skills required for managing suppliers as well as cyber and information security. • Responsibility for assessing the organization's need for external advice in preparing the contract and in the subsequent supplier management phase. • Responsibility for approving risk assessments and risk treatment plans.
Information security coordinator/IT security manager	• Daily responsibility for the organization's cyber and information security management, including cross-organizational coordination & communication. • Responsibility for ensuring consistency between the contract security requirements and the organization's cyber and information security policies, procedures and guidelines. • Responsibility for ensuring sufficient management of supplier compliance with security requirements. • Responsibility for ensuring the continuous preparation of risk assessments and risk treatment plans.
Contract manager	• Responsibility for contract management and enforcement in general. • Responsibility for updating the contract to reflect any changes. • Responsibility for ensuring that the supplier corrects or remediates any errors or deficiencies in the supply of services. • Responsibility for handling any disputes with the supplier and for escalating issues to organization executives if required.
Legal function	• Responsibility for ensuring compliance with procurement rules and other relevant legal and regulatory requirements related to outsourcing. • Responsibility for assisting with legal advice in relation to outsourcing, including reviewing security requirements and the contract as a whole.
System and data owners	• Responsibility for cyber and information security of IT systems and data when outsourcing, including supplier management. • Responsibility for classifying IT systems and data covered by the contract. • Responsibility for identifying relevant security requirements in the contract based on the client's security level and information classification system. • Responsibility for ensuring supplier compliance with contractual security requirements & for following up on any security incidents at the supplier end. • Responsibility for managing the supplier's access to client systems & data. • Responsibility for preparing risk assessments and risk treatment plans.
IT manager	• Responsibility for providing technical advice, including assistance to identify relevant security requirements in the contract.
Data Protection Officer (DPO)	• Responsibility for providing assistance related to the protection of personal information, including help in identifying relevant data protection requirements in the contract. • Responsibility for ensuring compliance with data protection rules. • Responsibility for assisting with the conclusion of a data processing agreement with the supplier & managing compliance during the contract period.

Appendix 5: **Set SMART security requirements**

Set SMART security requirements on the supplier

The client can define security requirements based on the SMART principle (Specific, Measurable, Action-oriented, Relevant, and Time-bound). The SMART criteria support the client's supplier selection evaluation process and subsequent supplier management process. The five criteria are adjusted to fit the context and exemplified below.

- **Specific: The requirements should be specific and formulated in a clear and precise manner, making it evident to the supplier how the requirements are to be fulfilled.**

Avoid general and non-specific terms such as *"The supplier must make backups of the system".* Instead formulate clear, precise and specific requirements, for instance by specifying the extent and frequency of the backup and the number of stored security copies online as well as offline.

- **Measurable: It should be possible to measure, document and evaluate supplier compliance.**

Avoid general requirements such as "The supplier must ensure adequate logging" that leave evaluation of supplier compliance to estimates, making them unsuited for follow-ups. Set specific and clear requirements, for example ones that can be easily documented and possibly answered in binary terms (yes/no), making it easy for both parties to assess compliance.

- **Achievable: The requirements should focus on the supplier's actions.**

Avoid long, complex and incoherent requirements that contain numerous sub-requirements and overlap with other requirements. Formulate short, consistent and achievable requirements starting with "The supplier must…". Divide any sub-requirements into separate requirements and avoid overlaps between requirements.

- **Relevant: The requirements should be adapted to the specific contract, be based on a risk assessment, and align with the client's information classification system and defined security level.**

Be careful not to copy and paste requirements from previous contracts as such requirements may be outdated and irrelevant in relation to the current contract. Set requirements based on a risk assessment, ensuring that they contribute to mitigating specific risks related to the planned outsourcing. In addition, make sure to adjust "standard requirements" taken from catalogues of requirements, frameworks or standards such as ISO, NIST, CIS and SANS. It is also recommended to include references to the specific security controls required to ensure compliance with requirements.

- **Time-bound: The requirements should specify frequencies or contain precise time designations for the supplier's activities, service goals, etc.**

Limit the use of imprecise time designations such as "repeatedly, periodically, regularly and frequently", as these terms are left to interpretation. Instead use specific time designations (for instance the number of minutes/hours/days) and frequencies (daily, weekly, monthly, quarterly, annually, etc.).