Get in touch with your IT supplier

As a company manager who purchases IT solutions, you have the overall responsibility for ensuring that the solution you purchase is sufficiently secure and that it is used responsibly. However, it may not be your job to implement the necessary security measures, this being the responsibility of your IT supplier and the IT manager at your company.

Use this dialogue tool to see whether the supplier is sufficiently focused on IT security. You should talk to your IT supplier about all the points, but the requirements for security can of course vary depending on how critical and sensitive your company's data is.

The dialogue tool is primarily intended for communication with smaller IT suppliers, where it is important to check that they have security under control.

Send the questionnaire to your IT supplier and ask them to answer the questions. This will give you a clear idea of their security measures and you can then use the form as a way to start a relevant conversation about it. Based on the answers, you can see how the responsibilities are distributed. There are certain tasks that you, as a company manager, are responsible for when you buy IT solutions.

The questionnaire is clear and concise, and therefore only deals with the key points you need to be aware of. For further and more detailed information, refer to, e.g., the Centre for Cybersecurity guidance on information security in supplier relationships.[1]

It is always worth getting external assistance from an adviser if there is anything you are unsure about.

The questionnaire is not a checklist or a legal document such as a data processing agreement. The form can help you determine the points to include in a contract typically drawn up between a company and supplier of IT solutions.

1)https://www.cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

Overview of suppliers

When you have a new requirement, it is worth getting an overview of your existing suppliers to see if any of them can fulfil that requirement. This approach limits the number of suppliers involved while also ensuring that there is no functional overlap.

Risk assessment and your company's security needs

When you have to choose a new IT solution, carefully consider how big the risk is of using the solution in question. You should have an overview of which data the solution must be able to handle for your company and how important the data is to the business. You also need to decide what the technical and organisational consequences are of using the solution. This includes not only the IT supplier's security, but also the impact it will have on your business if something goes wrong. If the consequences of using the solution are considerable for the business, correspondingly high demands must be placed on the IT supplier. The dialogue about the supplier's security measures is an important part of the risk assessment process. For further information on how to assess risks, please refer to the guidance and template for risk assessment at sikkerdigital.dk.

The use of the IT supplier's solution can also place demands on you and your security policy. It is therefore important to clarify what responsibility you have in relation to the solution.

You can use the dialogue tool both when signing agreements with new IT suppliers and to regularly assess existing IT suppliers' security level.

On-premise solutions and cloud services

Traditionally, IT solutions have been something the company buys and runs on its own servers located at the company itself (also referred to as an on-premise solution). Today, many IT solutions are delivered as hosted solutions or cloud services, i.e., services that are processed on central servers that are either with the IT supplier itself or in large central data centres. The cloud service is often accessed via an ordinary web browser.

The requirements that must be placed on the IT supplier are different depending on whether it is a cloud service or an on-premise solution. With a cloud service, you transfer more of the responsibility for security to the IT supplier, i.e., responsibility for physical security, updating the solution and storing data. However, there will still be a number of things you yourself are responsible for.

When you have to assess the security of cloud services, it is important to prioritise the work. Large and widespread cloud services usually have a good grip on basic security. Here it makes the best sense to focus on your own responsibility. In the case of smaller IT suppliers of cloud services (e.g., providers of industry-specific solutions or hosting of their own solutions), on the other hand, there is often a need for a more in-depth dialogue about their security.

If your company runs the solution itself on its own or hosted servers, the IT manager should be able to answer most of the questions.

Understanding the answers from the IT supplier

Help to understand the answers from your IT supplier
The questionnaire itself is split into the following five main areas:

1. What does the IT supplier do to protect against unwanted access?
2. What does the IT supplier do to ensure availability and high uptime?
3. What does the IT supplier do to document their security?
4. What does the IT supplier do to protect personal data (GDPR)?
5. What is the distribution of responsibility between you as a customer and the IT supplier?

In the following, you will find a number of in-depth comments on the individual questions in the questionnaire. The comments are intended as an aid to understanding the responses from the IT supplier and indicate the responses that can be expected at an appropriate level of security. Remember that the overview is not a list of facts, but rather is intended as input for a conversation with the IT supplier.

1. What does the IT supplier do to protect against unwanted access?

1.A. In order for you to know where your data is stored, the IT supplier of cloud services must be able to state where the servers for their solution are located and whether they use subcontractors, the supplier's solution is processed, e.g., via a hosting or another cloud provider. The IT supplier must also be able to state how they ensure physical access to their data centre and servers.

If the IT supplier stores or transfers data outside the EU, you must pay particular attention to any transfer of personal data (GDPR).

The physical security should, among other things, include appropriate physical security measures against burglary (e.g., fencing, locked areas, video surveillance and logged access control).

1.B. The IT supplier of cloud services must be able to explain how your data is protected and which technical security measures they have established. This can involve many different things, including the use of malware protection (antivirus), firewall, network segmentation and encryption (both at storage and in transit).

The IT supplier of cloud services should at least have established a firewall solution, as well as adequate protection against malware, while the other measures must be seen in relation to how the solution works.

1.C. The IT supplier of cloud services is expected to continuously monitor the security of their solution and systems, i.e., keep an eye out for abnormal activity and that the solution is not compromised by hackers who steal data or compromise availability.

As a minimum, the IT supplier should collect log files from firewall, antimalware, servers and applications, as well as have a fixed procedure for ongoing review of log files for possible security incidents.

The supplier should also be able to explain the monitoring, including the use of tools for recording security incidents, e.g., use of Security Information and Event Management (SIEM), processes and staffing.

1.D. Vulnerabilities can lead to compromise of the solution and thus affect the security of your data. It is therefore important that the IT supplier continuously updates the solution with security fixes. An update must be completed shortly after the update has been made available. The IT supplier must also be able to explain how they handle enquiries about security problems.

The IT supplier should at least be able to explain when they update their systems. Regular security updates should be installed no later than one month after they are released, and the supplier should also have a process for rapid installation of critical security updates.

1.E. The IT supplier must be able to explain what initiatives they have taken to secure the solution against unwanted access. Unwanted access can occur for various reasons, e.g., by a hacker who has gained access to a user account.

The solution should include making use of an encrypted connection (e.g., https) and be protected against hacking of passwords, e.g., by locking the account after 10 incorrect login attempts, using multi-factor login or Single Sign-On (SSO).

2. What does the IT supplier do to ensure availability and high uptime?

2.A. The IT supplier should be able to explain whether they have provided a redundant solution. This is particularly important for solutions that contain business-critical data. A redundant solution ensures uptime in the event of a breakdown of hardware, network connections or the like.

The IT supplier can have many different levels of redundancy, e.g., more connections to the Internet, extra servers and the option to run the solution from different physical locations. The type of redundancy must make sense in relation to how important the solution is.

2. B. The IT supplier must inform you how, when and how quickly you can get help with critical problems. For cloud services, the guaranteed availability must be stated. This is usually stated in the form of a Service Level Agreement (SLA), which, i.e., indicates when a service is available and response times for errors and problems.

The IT supplier should be able to explain which SLA levels are offered and what these entail. It is usually possible to purchase a higher SLA level. You must assess what level your company needs in relation to the importance of the solution's uptime.

2. C. The IT provider of cloud services should have a plan for how the solution can be recreated if something goes wrong. It could be a hacker who has entered the system, a server that has broken down or something else entirely. It is too late to devise solutions once the damage has been done.

The supplier should have daily backup routines. It is important that the IT Supplier can explain how often backups are taken,
how the backup is stored and the processes they have in place to ensure quick recovery. The IT supplier must also have tested the backup to ensure that it is functional. The supplier must be able to explain how often their backup is tested and be able to state when it was last tested. These tests can, e.g., be monthly, however, a test must always be done when a major change to the solution has been carried out.

For on-premise solutions, your company must have its own routines and procedures in place. It is important to know how quickly the solution can be recreated after a crash.

2.D. In the event of an incident, e.g., ransomware, it is important to have a plan for how incidents are to be handled. The plan must be predefined so that there is no doubt about how the situation should be handled and who should be contacted if something goes wrong.

The IT supplier should at least have drawn up a contingency plan that contains as a minimum an escalation procedure, contact point and response time.

Your company should consider whether there is a need for similar internal procedures at your company.

3. How does the IT supplier work with security and how is it documented?

3.A. The supplier may refer to or be certified according to one or more standards or frameworks that exist for IT security. This can, e.g., be

- ISO 27001, which is an international ISO standard that you can be certified to when you have processes in place to manage your IT security.
  www.ds.dk/da/standardisering/ledelsesstandarder/informationssikkerhed

  www.iso.org/isoiec-27001-information-security.html

- ISAE 3402, which is an international audit statement standard, is primarily used for auditing the technical controls of IT service providers.
  en.wikipedia.org/wiki/ISAE_3402
  https://www.stil.dk/administration-og-infrastruktur/systemrevision-af-studieadministrative-systemer

- OWASP, which is a project with a number of recommendations and best practices, in particular for protecting web applications.
  www.owasp.org/

- STRIDE, which is a model for modelling threats to software solutions to ensure all potential vulnerabilities and threats are considered.
  en.wikipedia.org/wiki/STRIDE_(security)

- The NIST Cybersecurity Framework, which is a framework for the processes and competencies that must be in place to maintain a proper level of security.
  www.nist.gov/cyberframework

- The Centre for Internet Security (CIS) Top 20 Controls, which is a prioritised list of the 20 controls that most effectively counter cyber-attacks.
  www.cisecurity.org/controls/cis-controls-list/

There is a big difference between what the individual standards or frameworks cover and whether it is simply a best practice recommendation that is followed or whether the IT supplier has gone through an actual certification or audit process. It is your company's current security needs that determine whether a certification is relevant. If the company has large security requirements that include a lot of critical data, it makes sense for the IT supplier to have the appropriate certification. If the solution processes less critical data, the solution should still comply with the best practice from one of the above standards or frameworks.

3.B. The IT supplier should have their product or service security tested, and the results must be able to be presented. Depending on the solution, security tests can be carried out at different levels, e.g., penetration tests, third-party audit, code review or security review.

- Penetration testing is a form of legal hacking, where vulnerabilities in the solution are identified via the same methods that a criminal would use.

- Third-party audit means that an external certified auditor reviews the solution's IT controls for security holes.

- Code review includes reviewing the security controls in the solution (source code) and assessing whether the solution is secure.

- The security review can contain various elements, e.g., an assessment of the composition of the security products used and the protective capacity these provide.

The IT supplier should at least have security tests carried out when major changes are made to the solution. For cloud services, regular security tests should be carried out against the supplier's risk assessment.

3. C. The IT supplier should have considered security in the design and development of the solution. In continuation of this, the supplier should be able to present an overall (written) consideration of the security of the solution (risk assessment). There are various best practice tools that you can rely on, and the level of detail should depend on how business-critical the solution is and how sensitive information is processed. It can, for example, be "Security by design" and "Privacy by design", both of which are based on security being thought into the solution from the start.

The IT supplier should be able to explain their process and security considerations.

3. D. It is important that the IT supplier works systematically to remedy the security problems found during audit reviews, e.g., ISAE3402 which concerns general IT controls in relation to IT operations and hosting activities. It is also important that the IT supplier regularly considers how the security of the solution can be improved.

The IT supplier should be able to send updated security documentation at least once a year. This can be in the form of an annual auditor's statement or valid certification according to one of the standards mentioned.

4. What does the IT supplier do to protect personal data?

It is important that you know which personal data the supplier can come into contact with, as your company will usually always be the data controller. The type or extent of personal data can have an impact on which security requirements your company must meet.

The EU General Data Protection Regulation (GDPR) sets out a wide range of requirements for both the company's own and the IT supplier's processing of personal data, i.e., requirements for risk assessment in relation to data, appropriate security measures and entering into a data processing agreement. A data processing agreement is a legal document that ensures that the IT supplier does not process personal data without your instructions.

4. A. If the IT supplier is to process personal data for the company, it is important that they meet the requirements set in relation to the Personal Data Regulation (GDPR) and the Danish Data Protection Act when they are to act as a data processor for the company. Please be aware that processing is not only storage, but also simply "viewing" access.

4. B. It is important that conditions related to the General Data Protection Regulation (GDPR) are in place before you start using a new IT supplier. The IT supplier must be able to state where and how personal data is stored and whether it uses subcontractors for processing.

The IT supplier must also be able to explain the procedure for deleting personal data

As a minimum, the IT supplier must ensure that any sub-data processors are located within the EEA, one of the EEA's list of safe countries or are protected by other authority. Furthermore, they must be able to explain the exact deletion routines. Data must be deleted when the processing is no longer relevant.

4. C. The IT supplier should be able to explain which of their employees will have access to the solution, e.g., in connection with support and whether they sign a confidentiality statement. They should also be able to explain how they manage and monitor access to the solution, so that only relevant employees gain access. At a minimum, the IT supplier should ensure that everyone who has access to personal data is subject to confidentiality and there should be restrictions on which employees have access to this data.

4. D. Should a breach of security involving personal data occur, this must be reported to the Danish Data Protection Agency within 72 hours of discovering the breach. The IT supplier must be able to explain how and how quickly your company is notified if there is a security breach involving personal data.

The IT supplier should at least ensure that your company can report security breaches within 72 hours of discovering the breach. They must therefore notify you within 48 hours and be able to assist in reporting the breach.

The General Data Protection Regulation (GDPR) has a large number of specific requirements and interpretations for further information, including examples of data processing agreements. Please refer to the Danish Data Protection Agency, which in Denmark is responsible for supervision and compliance with the GDPR. For further information on this, please go to www.datatilsynet.dk.

5. What is the division of responsibility between you as a customer and the IT supplier?

5. A. In the case of on-premise solutions, it is basically your company that is responsible for all matters, i.e., both the physical and technical security measures. This means, for example, that it is your responsibility to provide physical security, maintenance and updating, just as you must ensure that backups are made and tested. You may want to put a service agreement in place with your IT supplier.

The IT supplier must be able to explain the distribution of responsibilities, i.e., which security measures your company is responsible for and which ones they are responsible for. They should also be able to explain what services they can offer in connection with this.

5. B. Managing user accounts requires special attention, as it is often easy to forget to remove resigned users, users who retain old rights when they change jobs or similar situations.

The IT supplier must be able to explain which parts of the configuration you yourself are responsible for when it comes to both the implementation and operation of the solution. Typically, your company will be responsible for the data that is loaded into the solution, just as it is your responsibility to control which of your users have access to the solution.

5. C. Many cloud services contain quite advanced and well-developed security functions, but these are often not switched on by default. Therefore, it is important that you and your supplier together investigate which security functions the supplier offers and ensure that all relevant functions are switched on.

Many cloud services offer the option of so-called two-factor or multi-factor authentication, where instead of a simple password, users receive, for example, a message or popup on their mobile phone to be able to log into the solution. If this feature is found in the solution, it is important that it is switched on and used for all users, as the vast majority of security breaches in cloud services are due to breaches of login security.

For solutions that contain critical data, the IT supplier should at least offer the option of two-factor or multi-factor authentication.