# Navigating your way to the cloud

A practical guide for financial institutions in Denmark

# Contents

## Navigating your way to the cloud

# Moving to the digital economy

Cloud computing is fast becoming the norm, not the exception, for financial institutions (FIs) in Denmark. The Danish Financial Supervisory Authority (FSA) has not imposed any specific restrictions on the use of cloud services by FIs. The European Banking Authority's (EBA) Recommendations on Outsourcing to Cloud Service Providers have provided the necessary clarity for FIs wishing to adopt and reap the benefits of cloud computing, while ensuring that risks are appropriately identified and managed.

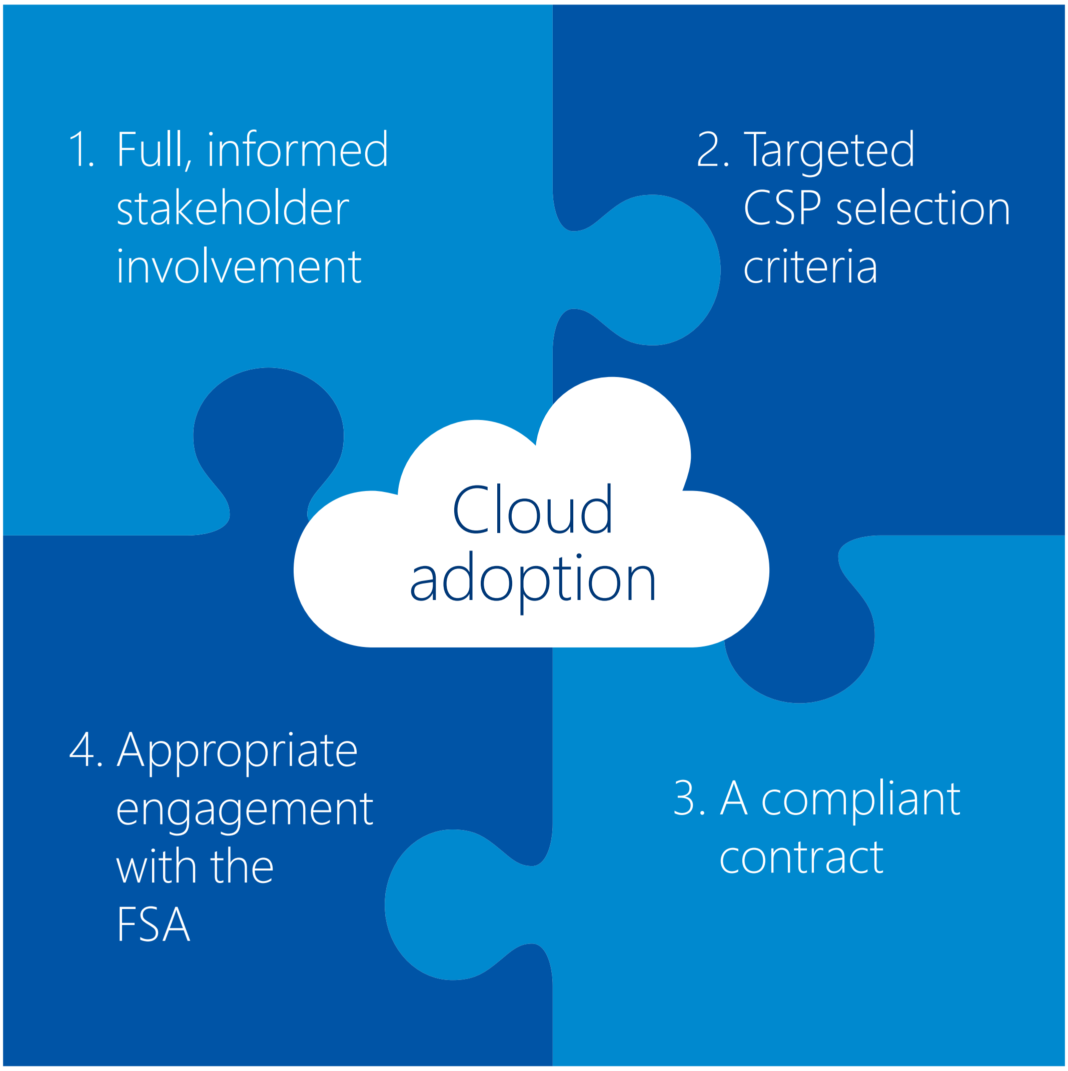
Microsoft is pleased to have been involved in the discussions with EBA that have led to these positive developments. Microsoft's approach to regulatory compliance for FI customers directly aligns with the EBA's underlying Recommendations, which should help FIs in the EU feel confident when moving to the Microsoft Cloud.

Through its partnership with FIs in Denmark, Microsoft has developed deep experience of delivering solutions that meet all applicable compliance requirements. We understand that it is our role as cloud service provider (CSP) to Denmark's FIs to help facilitate compliance with the underlying guidelines and, as part of that, have developed a range of materials to help our cloud customers in the financial services sector. Microsoft will continue to provide support for Denmark's FIs to meet compliance requirements in a developing technological and regulatory environment.

By following the practical steps outlined in this paper, FIs in Denmark can navigate their way to the Microsoft Cloud with confidence and enjoy the benefits of digital transformation.

# Four essential steps to a successful cloud adoption and deployment

Microsoft's experience of working with FIs in Denmark has shown that a successful cloud adoption requires four inter-related and inter-dependent steps.



1. Full, informed stakeholder involvement
2. Targeted CSP selection criteria
Cloud adoption
3. A compliant contract
4. Appropriate engagement with the FSA

# Step 1: Full and informed stakeholder involvement

A smooth cloud adoption requires informed stakeholder involvement from the outset, with decisions being based on a full understanding of the proposed cloud solution. As a CSP, Microsoft takes responsibility for providing detailed product and service information to assist your key decision makers.

## Key actions

### 1. Build the core stakeholder team and develop the business case

**Establish a multi-disciplinary team from day one.**

Put your technology and procurement teams in charge of developing the business case, with a focus on the operational and commercial factors driving the decision to adopt cloud services.

This would include conducting an initial assessment of the benefits and risks associated with using cloud services, including whether the use of cloud services is consistent with your risk appetite and long-term business strategy.

Ensure your legal, risk and compliance teams are involved in these discussions from the outset. They'll need to map the proposed solutions against legal and regulatory requirements. Many technology projects have been delayed due to involving legal and compliance functions too late.

The board and senior management will typically require early reassurance regarding the business case for cloud services and the oversight, review, reporting and response arrangements with the CSP. And finally, they'll need to provide final sign-off, both as a matter of good corporate governance and because the responsibilities for maintaining effective oversight and governance of outsourcing arrangements, managing outsourcing risks, and implementing an adequate outsourcing risk management framework rest with the board and senior management.

Appendix 1 sets outs the records that FIs should maintain to help manage risk and facilitate oversight.

### 2. Obtain detailed product and service information

In addition to building the core stakeholder team and understanding the technical solution, the FI is expected to understand the cloud product being considered and the implications of the use of such cloud product for its particular organisation. In Microsoft's experience, successfully demonstrating this level of knowledge is dependent on the CSP's willingness and ability to share specific product and service information.

### 3. Perform due diligence

**Perform appropriate due diligence on the CSP and consider, at minimum the CSP's:**

- Business background, reputation and strategy;
- Financial performance and condition;
- Operational capabilities, risk management, and internal controls; and
- Ability to ensure the availability, reliability, integrity, and confidentiality of data.

Appendix 2 sets out the resources Microsoft makes available to help FIs conduct due diligence.

### 4. Understand the technical solutions available

Microsoft has prepared a summary of the different types of cloud delivery and deployment models to support your core team and assist with the early scoping of any cloud project.

## A summary of cloud delivery and deployment models

### Definition

**Cloud Computing, Cloud Services** or **Cloud** means on-demand network access to a shared pool of configurable computing resources. In other words, cloud services provide FIs with on-demand access, using a network connection, to information technology or software services, all of which a CSP configures to the needs of the FI.

### Cloud delivery models

1. **Software as a Service (SaaS)**
   Where the CSP makes software applications available to customers.
2. **Platform as a Service (PaaS)**
   Where the CSP provides a computing platform for customers to develop and run their own applications.
3. **Infrastructure as a Service (IaaS)**
   Where the CSP delivers IT infrastructure; e.g., storage space or computing power, and may include delivery of the operating system.

### Cloud deployment models

1. **Public Cloud**
   Infrastructure is owned and managed by the CSP and not located on the customer's premises. Although each customer's data and services are protected from unauthorised access, the infrastructure is accessible by multiple customers. Given the operational and commercial benefits to customers, public cloud is increasingly seen as the de facto deployment model.
2. **Private Cloud**
   Infrastructure is usually managed by the CSP (but sometimes by the customer). The infrastructure is located either on customer premises or, more typically, on the CSP's premises. The data and services are able to be accessed only by the particular customer.
3. **Community Cloud**
   Serves members of a community of customers with similar computing needs or requirements. The infrastructure may be owned and managed by members of the community or by a CSP. The infrastructure is located either on customer premises or the CSP's premises. The data and services are accessible only by the community of customers.
4. **Hybrid Cloud**
   A combination of two or more of Private Cloud, Public Cloud or Community Cloud.

## How Microsoft helps

Our cloud services span all of the above delivery and deployment models. Each of these services is supported with a range of materials, including product fact sheets, online trust centres and checklists, to help FIs make an informed decision. In addition, we have subject-matter experts available to meet with you and your core stakeholders. They'll provide specific and detailed information on the technical, contractual and practical aspects of your proposed cloud project.

# Step 2: Targeted CSP selection criteria

To verify that your proposed CSP can meet the applicable compliance, risk and security requirements, you'll need to develop selection criteria. Following the Danish outsourcing regime[1], FIs should ensure that these criteria include the seven listed below.

## Recommended selection criteria

### 1. Experience, capability and expertise

**The FI should assess the CSP's experience and capability to implement and support the cloud solution over the contracted period.**

- When it comes to assessing technical capability, industry standards are a useful objective tool for the FI to use. ISO/IEC 270012 and ISO/IEC 270183 have become an expected minimum within the industry around the world.
- A core aspect of technical capability is the security of the proposed cloud solution. There is now a growing acceptance that cloud services can meet or even exceed the highest on-premises security practices.
- Expertise and experience in financial services are also important as a CSP that has a deep understanding of the FI regulatory landscape in Denmark and extensive experience of working with FIs will be well-placed to proactively support the FI as part of a successful cloud adoption.

### 2. Financial strength and resources

In any technology procurement, the financial strength of the supplier provides comfort as to its ability to provide continuity of operations and to compensate the FI for any service failures or breaches of contract. Contractual promises carry little weight if the CSP cannot stand behind them financially. Accordingly, the FI will want to carefully consider the financial position of the CSP. It is common for FIs to request audited financial statements for at least each of the last three years and CSPs should be in a position to provide these.

### 3. Corporate governance, business reputation and culture, compliance and pending or potential litigation

- To lay the foundations for a successful long-term relationship you'll need to carefully consider the CSP's longevity and track record in Denmark and around the world.
- As part of due diligence, ask CSPs to demonstrate their track record through case studies of successful cloud projects they've undertaken with FIs in Denmark and around the world. A competent CSP will have all of the required information readily available.
- Ensure the CSP can demonstrate an understanding of and solution compatibility with FI culture and requirements.

### 4. Security and internal controls, audit coverage, reporting and monitoring environment

CSPs should be appropriately certified and maintain robust security measures and security policies that meet or exceed international standards. CSPs should make available appropriate information regarding their certifications and security controls to FIs as part of the FIs diligence process.

[1] The Danish regulatory regime on outsourcing includes the following: the Danish Act on Financial Institutions; the Executive Order on outsourcing of significant areas of activity; the Guideline for executive order on outsourcing of significant areas of activity; and Guidance on Use of cloud services as part of IT-outsourcing.

| | |
|---|---|
| 5. Risk management framework and capabilities | The FSA expects the FI to assess the CSP's risk management framework and capabilities, which includes technology risk management and business continuity management in respect of the outsourcing agreement. |
| 6. Disaster recovery arrangement and track record | FIs should consider the CSP's own disaster recovery capabilities. CSPs should make available appropriate information regarding their disaster recovery metrics as part of the FIs diligence process. |
| 7. Reliance and success in dealing with subcontractors | FIs should evaluate the CSP's standard subcontractor agreement and subcontractors should be subject to equivalent controls as the CSP. The CSP must ensure that the requirements of the Executive Order apply to subcontractors. Information regarding the CSP's subcontractor policies should be made available to the FI. |

## How Microsoft helps

Microsoft confirms its ability to meet all of the criteria specified above and therefore can meet applicable compliance, risk and security requirements placed on CSPs of FIs. Additionally, Microsoft makes available a rich set of resources to customers to conduct due diligence (set out in Appendix 2). We're also confident that our understanding of the FI environment is market-leading in Denmark and around the world, with a proven track record of successful cloud deployments that comply with financial services regulatory requirements and global security and risk standards. Microsoft has large dedicated teams consisting of hundreds of lawyers, software engineers and policy experts whose sole mission is to identify and implement new cloud security and privacy standards across Microsoft's portfolio of cloud services. We also have a long track record of being one of the first CSPs to implement major new cloud standards, including recent examples such as ISO/IEC 27018 and ISO/IEC 19086.

- Microsoft's Financial Services Compliance Program extends the compliance features of Microsoft Azure, Office 365, Microsoft Dynamics and Intune to provide FIs with deeper, ongoing engagement with Microsoft, including:
  - Customer access to additional information from Microsoft subject matter experts (SMEs).
  - Access to additional compliance-related information developed by Microsoft over time.
  - The opportunity for one-to-one discussions with Microsoft's third-party auditors.
  - Participation in webcast walk-throughs of ISO and SSAE audit reports with Microsoft SMEs.
  - The ability to view the Microsoft control framework for the cloud services.
  - The opportunity to recommend future additions to the audit scope of the cloud service.
  - Access to detailed reports of external audit penetration tests conducted on the cloud service.

# Step 3:
# A compliant contract

Pursuant to the Danish outsourcing regime, FI's outsourcing agreements with CSPs should include specific items set out below.

## Terms to address in your contract

| | |
|---|---|
| 1. Scope | The FI's agreement with the CSP should clearly describe the services to be provided by the CSP, including providing sufficient clarity on the scope and duration of those activities. |
| 2. Performance and risk management standards | There should be a service level agreement specifying the service levels the CSP is required to meet, with defined consequences if performance falls below the agreed standard. |
| 3. Confidentiality and security | The agreement should include provisions on security and confidentiality. This includes setting out the procedures of data protection, receipt, transmission and storage as well as the consequences if data is disclosed to third parties. |
| 4. Business continuity management | The agreement should include plans for business continuity and dealing with emergencies. |
| 5. Monitoring and control | The agreement should refer to cloud control systems, including performance and incident-reporting obligations. It should also include a requirement on the CSP to notify the FI of any significant change that may affect the CSP's compliance with the agreement. |
| 6. Audit and inspection | The agreement should include the FI's right to audit and monitor the CSP, including through regular information reports and through access to independent audit reports. The agreement should also specify that audit information available to FIs may be shared with the FI's regulators. There must be a provision specifying that disclosure of information to the Danish FSA is permitted by a grant of access to the CSP. |

| | |
|---|---|
| 7. Notification of adverse developments | The agreement should have provisions to address notification of adverse developments. There should be an obligation on the CSP to notify the FI if it becomes aware of any security incident or any event which would negatively impact the CSP's existing or future ability to perform the services. |
| 8. Default termination and early exit | The agreement should specify what happens on termination of the cloud services and should have provisions to address early exit. |
| 9. Subcontracting | The agreement should define the extent to which the CSP may use subcontractors, identify any subcontractors that the CSP will use, and provide for subcontractors to be subject to equivalent controls as the CSP. The CSP must ensure that subcontractors are subject to the requirements of the Executive Order. |
| 10. Choice of law and dispute resolution | The agreement should include appropriate choice-of-law and dispute resolution provisions. |
| 11. Delivery on time | The agreement should include provisions specifying that delivery of the services must be on time and according to the agreed requirements. |

## How Microsoft helps

To make the contract review process easier for you, Microsoft provides a checklist of the contractual terms that the FSA expects and explains where they are addressed in the Microsoft contract. This is available from your Microsoft contact upon request. This checklist gives you the confidence that your contract with Microsoft meets the applicable regulatory requirements.

# Step 4: Appropriate engagement with the FSA

A successful cloud adoption requires that the FI with the support of the CSP (where necessary) engages openly with the FSA. To streamline this process, we have provided details on the regulatory environment along with practical steps you can take.

## Overview of the FI Regulatory Environment in Denmark

| | |
|---|---|
| Who is the regulator? | The Danish Financial Supervisory Authority (FSA)<br>The Ministry of Industry, Business and Financial Affairs |
| Are cloud services permitted? | Yes, the regulatory framework in Denmark permits the use of cloud services, including public cloud services. |
| What regulations and guidance are relevant? | • Danish Act on Financial Institutions<br>• Executive Order on outsourcing of significant areas of activity<br>• Guideline for executive order on outsourcing of significant areas of activity<br>• Guidance on "Use of cloud services as part of IT-outsourcing" |
| Are transfers of data outside of Denmark permitted? | Yes. Transfer of data outside of Denmark is permitted.<br>The GDPR, which comes into force on 25 May 2018, allows trans-border dataflows, subject to certain restrictions. |

| | |
|---|---|
| Is regulatory approval required? | No, the FSA does not require prior approval in relation to outsourcing arrangements. However, with respect to regulation of the cloud, the outsourcer shall no later than eight (8) business days after entering into an outsourcing agreement notify the FSA. The notification shall be made in writing by use of a specific form available at the website of the FSA. |
| Are there particular forms or questionnaires the FI needs to complete? | No, there is no mandatory requirement for FIs to complete a checklist to adopt Microsoft cloud services. However, Microsoft has developed a checklist that maps the relevant requirements against Microsoft's contractual terms and conditions. |

## How Microsoft helps

Microsoft's expert team is on hand to support you throughout your cloud project. Microsoft has developed various materials that directly map its cloud services against the applicable regulatory criteria, including a checklist populated with detailed information about Microsoft's cloud services and contractual terms, which is available from your Microsoft contact upon request.

# Appendix 1: Maintaining appropriate records of the CSP relationship

To manage risk and facilitate oversight, FIs and CSPs should maintain records that document all stages of the CSP relationship. FIs should document compliance with applicable legal and regulatory requirements, as well as the principles set forth in this document.

## FI records should include:

1. Initial plan and risk assessment.
2. All contracts between the FI and CSP.
3. Any business plans.
4. Findings, results, and recommendations that result from the due diligence process.
5. Analyses of the costs associated with the CSP and outsourcing cloud services.
6. Periodic risk analyses performed over the course of the CSP relationship.
7. Documentation of the FI's oversight activities (e.g. reports to the board).
8. Any report that the CSP provides to the FI.
9. Dispute resolution documents.

## How Microsoft helps

Microsoft makes available a substantial amount of information and reports that financial institutions may use to document compliance with regulatory requirements and cloud computing principles through its online resources, including the Trust Center, the Service Trust Platform and the Financial Services Compliance Program. In addition, Microsoft can make additional resources available to customers as necessary.

# Appendix 2: Resources to help FIs conduct due diligence

Microsoft makes available a rich set of resources to customers to conduct due diligence through its online resources, including the Trust Center, the Service Trust Platform and the Financial Services Compliance Program. Should customers require additional information, Microsoft can make resources available to the customer to discuss the ways in which Microsoft achieves compliance and arrange meetings with its business and engineering teams and the customer's designated employee for CSP diligence and communications. Further, the customer can retain Microsoft Consulting Services for deeper engagements that require mutual investment of resources at any time during the customer's relationship with Microsoft.

The following are selected sources highlighting information Microsoft makes available to its customers to assist in due diligence:

- **Financial Reports.** Microsoft has a strong track record of stable profits, and its commercial cloud business is strong and growing. Microsoft's public financial reports are available on its Investor Relations website.

- **Policies and Procedures.** Microsoft policies and procedures regarding compliance, security, confidentiality, internal controls, audit, and escalation are made available to customers through various resources, including the Trust Center and Service Trust Platform. These resources include a substantial volume of information for customers regarding Microsoft's cybersecurity policy and internal controls; certifications and risk assessments; business continuity and disaster recovery metrics; and diagnostics for logging, auditing, and granular tracing. Microsoft Online Services are subject to multiple third-party audits, which are available to customers online.

- **Litigation and Regulatory Enforcement.** As of [March 2018], Microsoft has had no material litigation, regulatory enforcement actions, or consumer complaints related to the cloud principles, except for complaints received and addressed in the ordinary course of business.

- **Continuity of Service and Performance Metrics.** Microsoft guarantees 99.9% of uptime for most of its Online Services. Uptime guarantees are set forth in Microsoft's contracts with its customers, and if service levels are not maintained, customers may be eligible for a credit toward a portion of their monthly service fees.

- **Contingency and Business Operations Plans.** Microsoft includes standard terms for business continuity management and data recovery procedures in its contracts with customers. For example, Microsoft maintains emergency and contingency plans for each facility that houses customer data. Information regarding contingency planning and Microsoft's Enterprise Business Continuity Management Program is made available to customers through the Service Trust Platform.

- **Insurance Coverage.** Microsoft is self-insured and can make certificates of insurance available upon request.

- **Subcontractor Agreements.** Information regarding Microsoft's subcontractor policies is made available to customers on the Trust Center. Subcontractors that handle customer data must enter into additional agreements with Microsoft that are as stringent as Microsoft's own data protection terms. In addition, all subcontractors that handle customer personal information must join the Microsoft Supplier Security and Privacy Assurance Program, which is an initiative designed to standardise and strengthen the handling of customer personal information and to bring vendor business processes and systems into compliance with those of Microsoft.

Microsoft

## Find out more

**Trust Center**
microsoft.com/trustcenter

**Service Trust Portal**
aka.ms/trustportal

**Financial Services Amendment**
Contact your Account Manager

**Online Services Terms**
microsoft.com/contracts

**Compliance program for regulated financial services customers**
Contact your Account Manager

**Service Level Agreements**
microsoft.com/contracts

**SAFE Handbook**
aka.ms/safehandbook

This document is provided "as is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This paper is not intended to be a comprehensive analysis of all regulations and their requirements, nor is it legal advice; rather it is intended to be a summary and to provide guidance to FIs in Denmark on the types of issues they should consider. Microsoft, the Microsoft logo, Azure, Dynamics, Office 365 and Windows Intune are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.