Microsoft

Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud

Published: 5 September 2018

Overview

Recent guidance by financial supervisors and privacy authorities is becoming increasingly focused on the digital transformation that is happening in the financial service institution (FI) system. Cloud computing is a cornerstone of this transformation process, and regulatory guidance on this domain is being released at a high pace. Regulators are not only focusing on managing the risks involved with cloud computing, but they also understand the need for the finance industry to adapt their risk governance and management practices to take advantage of a new world where cloud computing is the norm. A good example on the quick pace of new regulation being released, and on their strong focus on governance processes is found within the EU: the European Banking Authority (EBA) released EU-wide cloud guidance in December 2017, and will also publish in 2018 its new general guidance on outsourcing, which replaces the former.

This document explains how to establish an efficient governance model that is optimized to meet regulatory requirements in a cloud-enabled world and how to efficiently evaluate risks for Microsoft's cloud solutions while meeting applicable financial regulatory requirements. Following the guidance in this document will enable your organization to assess and approve Microsoft cloud services such as Azure, Dynamics and Office 365; and help you understand the need to engage with financial and privacy supervisors as part of this assessment process.

Target audience

This whitepaper is for decision makers and risk and compliance managers in financial institutions that have decided to deploy Microsoft cloud services, or for those who remain unsure about assessing its risks. Presenting conclusions to regulatory authorities can be time consuming and complex and this paper will help your organization to optimizing your internal risk governance processes for cloud services, as well as assist in the assessment of Microsoft cloud services. This is a starting point for newcomers to Microsoft cloud solutions for financial institutions and references a variety of supporting materials that will help you with your risk assessments.

In a hurry?

Jump to Step-by-step guide for assessing Microsoft cloud services.

How to use this document?

Several Microsoft resources are referenced throughout this document and many more exist on the Microsoft website. To help you with the initial assessment and support reading of this document we have created a reference table with useful links with a short description in Annex I of this document.

Scope and purpose of a risk assessment

The following are the two most important types of risk assessments:

1. **General risk assessment**
   The goal of a general risk assessment is to ensure that the system and data that are considered for migration to the cloud do not introduce any new or unidentified risks into the enterprise. The focus is to ensure confidentiality, integrity and availability of information processing and to keep identified risks below the internal risk appetite threshold.

2. **Compliance assessment**
   Compliance is a key part of any risk assessment, although with a specific focus. A compliance assessment focuses on meeting both internal compliance requirements and applicable external regulations. Compliance assessments also involve dealing also with (often standardized) contractual terms associated with cloud services and is closely linked to the procurement process for the cloud service.

Key areas of regulation

There are many relevant regulations that must be considered when moving to a cloud solution, and the regulatory landscape keeps evolving, making it difficult to provide a list of all applicable regulations. However, we wanted to point out some important areas of regulation to the reader for further consideration in your projects.

Regulation domain	**Examples**	**Impact on cloud deployments**
General Banking and Insurance regulations	MIFID II, Solvency II, Anti Money Laundry (AML)	Transaction recording and record keeping requirements are common. These may pose challenges to cloud deployments (e.g. voice recording requirements). These regulations also contain specific data retention and logging requirements.
Broker-dealer specific regulations	SEC 17a-4	These often require very specify and expensive logging and brokerage surveillance processes to be implemented within the service.
Cloud and Outsourcing regulations	FFIEC guidelines (US); EBA and PRA Guidelines on cloud outsourcing (EU/UK)	All financial supervisors see cloud computing as a form of outsourcing. These regulations are a primary focus when moving applications into the public cloud, and a broad range of risks are addressed in these regulations. Many of them appear as soft law (guidelines) or exist on a country-by-country basis, which may make the assessment process more complicated for multinational FI's.
Privacy regulations	General Data Protection Regulation (GDPR)	These define very specific requirements to protect the privacy of personal information that is processed by the cloud service.

Microsoft cloud solutions offer a wide range of features which allow FI's to build or configure services that are compliant with these requirements. This is where our solutions offer a unique benefit compared to many of the on-premise counterparts that often need to rely upon third party products to reach the same level of compliance.

Cloud risk assessments: considerations

Most FI's have mature models in place for assessing security of internal systems, but when it comes to making use of cloud services where this data is moved outside of the perimeter and under the control of a cloud service provider (CSP), these existing processes may require a different approach.

Below are some of the key considerations concerning cloud computing:

- **Shared Responsibility:** Cloud deployments can be done as Infrastructure as a Service (IAAS), Platform as a Service (PAAS) or Software as a Service (SAAS). Depending upon the applicable cloud service model, the level of responsibility over the solutions security controls will shift between the CSP and the FI.

  Note that even SAAS solutions such as Office 365 and Microsoft Dynamics, part of the ownership remains with the FI. Depending upon the choice of license, a long list of built-in product features may be available to enhance the level of security and compliance of your deployments. It is up to the FI to make the right design choices for their service deployments and to configure these in context of your local environment so that they can help in maintaining end-to-end risk control and oversight over the service. The CSP at the other hand must ensure these features help meet the FI's compliance requirements.

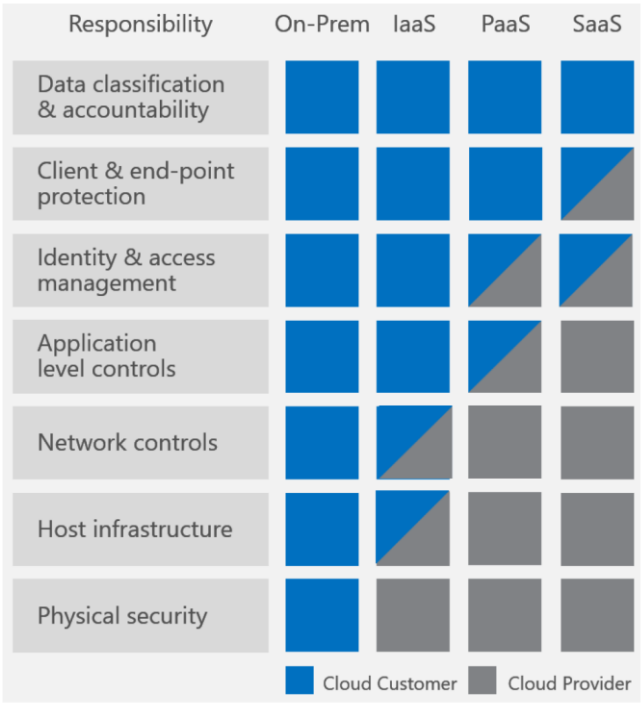

Figure 1: Shared responsabilities for different cloud service models

- **Transparency:** Information on the design of the cloud solution and how security controls are implemented may not be available. Without detailed information on the design of the cloud solution and on how different security controls are implemented by the CSP, it becomes very difficult for the risk teams to perform their assessments. Microsoft provides detailed transparency on how we manage and secure your data in the cloud and is committed to continue to do so also in the future.
- **Data location and Applicable law:** Another consideration concerns where your data will be managed. The CSP may be in a different country from your primary operations and governing law may also be different from your local jurisdiction. Microsoft services let you choose in which region the data is stored. It is important to understand which law governs the contract, including where data may reside, and that you have done an assessment concerning applicable law involving use of cloud services.

- **Privacy:** Regulations such as the General Data Protection Regulation (GDPR) ensure a high level of control over the processing of personal data of individuals. It is extremely important that both data controllers and data processors comply with this regulation to support secure processing of personal data and protecting the privacy of individuals. When assessing a cloud service, executing a Data Protection Impact Assessment (DPIA), and making sure the system is set up to deliver privacy by design are essential steps to consider. During a cloud risk assessment, we recommend to start by reading our Getting Started Guide for GDPR accountability. Next to this, our Trust Center also provides a very extensive GDPR overview, an overview of MS GDPR solutions built into each product, a GDPR FAQ and a set of GDPR resources such as whitepapers & videos.
- **Service standardization:** Inherent to the concept of cloud, most of the service technology as well as its contractual terms have been standardized. This standardization distinguishes cloud computing from more traditional outsourcing processes where the service may be customized to meet unique requirements of the FI. The standardized terms offered by major CSP's may be perceived as barriers for the adoption of cloud computing. Microsoft addresses this challenge by providing specific contract amendments for the financial services industry and by offering the optional Microsoft Cloud Financial Services Compliance Program (FSCP), both of which have been designed to address specific FI needs.
- **Legacy IT and integration:** When it comes to connecting to external cloud solutions some challenges may arise when integrating with internal identity- and authorization systems; when setting up data flows between cloud and on-premise environments; as part of some migration scenarios or when setting up (temporary) coexistence environments. Microsoft has the experience, tools and resources to assist you in working out migration scenarios that meet these challenges. To assist customers transition to the cloud, Microsoft provides direct support through Microsoft FastTrack and migration partners with a strong track record of helping FI customers in successfully meeting these challenges and realizing their cloud projects.
- **Risk Management:** With any model of cloud computing, part of an organizations control is transferred to the cloud service provider (see Figure 1 above). The CSP will have to demonstrate that they can meet the organizations' internal security (control) requirements. Because of differences in the control frameworks between the CSP and FI, gaps may occasionally appear. This creates the need for a financial institution to consider alternative risk mitigation scenarios or to deal with risk exceptions. Setting up a mature internal governance process that can deal with risk exceptions is a key success factor when dealing with cloud computing, otherwise cloud deployments risk getting stopped early in the process due to a perceived high risk that is attributed to them. In practice, the CSP may apply a set different controls to mitigate and manage the same underlying risks.
- **Service resilience and business continuity:** With data and processes being transferred externally the end-to-end complexity of an information system increases significantly. Different actors become responsible for different components. FI's will need to demonstrate that their services remain fully resilient in accordance with their internal business processes in the event of operational failures or during disaster scenarios. Internal disaster recovery and business continuity processes must consider both the cloud service as part of their test plans, and the FI must prepare exit scenarios that can be executed if the CSP fails to deliver its services. To support FI assessment, Microsoft provides transparency on continuity testing on the Service Trust Portal.
- **Extended supply chains (chain outsourcing):** most cloud providers will rely upon other third parties to deliver their services. Within Microsoft, we are committed to meet all applicable regulations and remain fully transparent on how we rely upon third parties for managing cloud services. From a FI perspective, the outsourcing to major cloud providers such as Microsoft may happen indirectly. For example, Azure Marketplace offers hundreds of third-party services that run on Azure. The challenge for the FI now becomes ensuring continued security and visibility over the end-to-end service throughout what may be an extensive service supply chain, so that their services continue to meet internal requirements. Note that the use of such chain outsourcing is not new to cloud computing, but it is more common in relative comparison.

Security risk assessment in the cloud: opportunities

Cloud solutions often have a very strong business case and offer great benefits to the FI when looking beyond the risk and compliance challenges above. But even when we look at risk and compliance, moving to a cloud solution also offers opportunities to improve a system's security and compliance:

- **Increased security:** The large economies of scale at which Microsoft operates gives us the ability to rapidly develop best-in-class security measures into our products. It is no surprise that many FI's find opportunities to reduce overall risk to their business services by leveraging our security solutions, especially when doing a 1-on-1 comparison against their (not always optimally secured) legacy on-premises environment. More and more we see that security is becoming a positive argument supporting a cloud business case rather than being a concern.
- **Compliance improvements:** The cost of compliance for FI's has increased significantly in recent years with the release of several new regulations that govern FI's or personal data. These regulations define strict requirements which are not always easy to comply with, and many FI's struggle to close the gaps for their on-premises environments. Microsoft cloud services offer a wide range of built-in compliance functions[1] allowing FI's to structurally increase their overall level of compliance by moving to the cloud, often saving on always increasing costs for investments in on-premises compliance measures.
- **Higher reliability and resilience:** Cloud services are often built on the newest technology combined with a high level of service automation. This results in the CSPs typically offering a very high level of service availability across multiple availability zones worldwide (links in Annex). Opportunities arise within the FI to make their services more fault-tolerant and resilient against failures by leveraging these cloud technologies. The FI has the responsibility to ensure it configures CSP features to meet or exceed the FI's requirements.

The importance of finding a suitable cloud governance model

In recent years, financial regulations have placed an increasing emphasis on the importance of establishing a strong governance framework for FI's when using cloud services. For instance, the European Banking Authority (EBA) produced high-level guidance for FI's on cloud outsourcing in their recently published recommendations which introduces several concepts that may require FI's to adapt their governance models. These include a requirement for FI's to maintain a register of cloud outsourcing activities, the concept of materiality assessments for cloud services, and a requirement around regulatory notification each time a material cloud service is introduced.

A sample governance model that is optimized for cloud is available in Figure 2 below.

Throughput time for approval

When you assess a major cloud service for the first time, this process may take a long time to complete, especially when dealing with critical workloads (e.g. core banking systems) or important data sets (e.g. transaction records, customer data, personal information). We recommend starting this process as soon as possible before the planned deployment date, even if a lot of details are not yet understood at that time. The length of the timeline also depends on the different actors that are involved in the assessment process. However, for a FI with a firm governance model in place for cloud computing, it is possible to considerably shorten this timeframe.

[1] A good example of this is the extensive set of GDPR-related solutions and features built into our products

Important considerations when governing cloud computing

The orange highlighted boxes in Figure 2 below represent some of the essential components of a strong cloud governance model:

- **The case for cloud:** Before deciding to move to the cloud some initial steps may take place such as evaluating the product, creating an initial high-level design, assessing the vendor (including associated costs and benefits), and collecting any other information that can support your decision to move to a cloud solution.
- **Materiality assessment:** Financial regulators have introduced the concept of materiality and FI's will benefit from a clear definition on what is defined as being a material service. Already existing internal FI processes such as the Data Protection Impact Assessment (DPIA) or Business Impact Assessment (BIA) may also be leveraged to determine materiality. Financial supervisors may also define specific criteria that must be used for assessing materiality[2].
- **General risk assessment:** This is the central part of your cloud assessment. We recommend adopting one of the existing industry frameworks for this process, such as ISO27001:2013, CSA CCM[3], or FFIEC guidance. This can speed up the process since Microsoft is certified in several standard frameworks and offers control mappings to others (such as FFIEC), making it easier for FI's to assess the vendor side of the cloud service. The risk assessment should not only assess the vendor solution, but also assess risks as they appear in the end-to-end deployment including the FI's own systems and processes.
- **Compliance assessment:** Within global multinational enterprises, local and regional considerations on cloud outsourcing must be also considered since these may include some very specific requirements[4]. To help in the process, Microsoft has recently created some excellent compliance checklists on a country-by-country basis, available on the Data Protection section within our Service Trust Portal (STP).
- **Case approvals and exception management:** It's important that FI's can demonstrate that all the risks involved with cloud computing have been addressed, and that any risk or control exceptions[5] are formally approved. We strongly recommend that for material outsourcing each FI approves the cloud service at the highest management levels to demonstrate ownership and accountability. In Microsoft's experience, regulators frequently ask "who signed off on the risk?" This is typically not a statement of concern about the risk itself, but that the FI has internal risk management processes robust enough to manage the cloud project.
- **Supervisory notification:** Many jurisdictions require FI's to notify financial supervisors about outsourcing arrangements, and mandate that the FI maintains ownership and responsibility for the application and data. In some jurisdictions, actual approval may be required. Microsoft engages directly with regulators to provide insight into the operation of our cloud services and learn about the areas regulators would like us to make improvements. Each FI should, regardless of whether a regulation requires it, notify at least their primary regulator concerning selection of a vendor for material outsourcing, including for cloud.

---

[2] See: EBA recommendations on outsourcing to cloud service providers paragraph 4.1 (page 5) and the CEBS guidelines on outsourcing page 2 (applicable to EU member states). MIFID II regulation and more recent guidance by EBA refers to critical or important outsourcing, but his involves a similar concept and is referred to as materiality within this document.

[3] Cloud Security Alliance (CSA) is an independent non-profit organization that promotes the use of best practices for providing security assurance within cloud computing. Next to education and research, they also provide a popular set of security controls within the Cloud Controls Matrix v. 3.0.1 (CSA CCM).

[4] Common local requirements include requirements to inform supervisors on cloud outsourcing arrangements (notification duty); requirements to notify supervisory authorities in case of security incidents and specific requirements on contractual provisions in context of cloud outsourcing.

[5] Risk exceptions should be temporary in nature. Control exceptions, where a specific control is not in place, may also occur. However, the lack of a such a control does not necessarily imply an increase in risk (this would depend upon alternative – compensating – measures that have been established in this context).

- **Updating of business continuity plans:** Business resilience is a key concern for financial regulators and several guidelines require the creation of contingency or exit plans for the rare event that the service would become unavailable. This implies working out an exit strategy from the cloud, as well as ensuring the cloud services are included in end to end business continuity and disaster recovery tests.

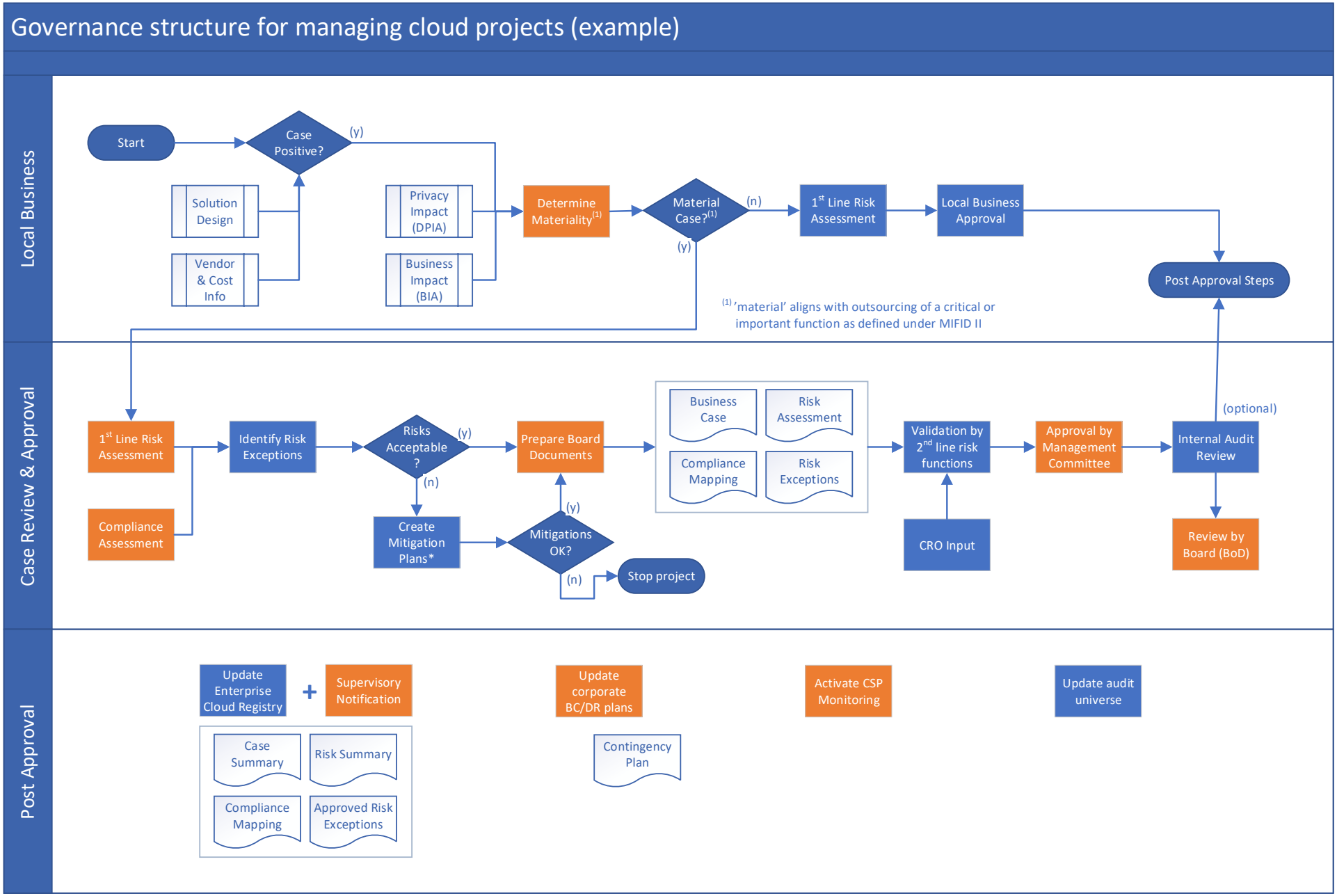

Figure 2 Example governance structure for managing cloud projects

The different actors and stakeholders within a FI

Within most FI's, three lines of defense are applied as part of their corporate governance model. The 1st line encompasses the business and several risk functions within this business. The 2nd line typically reports to the Chief Risk Officer (CRO) and operates with a significant level of independence from the business. The 3rd line of defense is internal audit, which operates independently and is not part of the day-to-day control environment of a FI. To strengthen their independence, the audit department will often not report to the CEO of the company but to the audit committee (part of the external board for a publicly listed company).

To ensure the development of a smooth risk management process for a FI, we recommend involving all the stakeholders below early in the process and clearly defining their individual involvement in the assessment process:

- **1st Line (Risk) Management:** The 1st line evaluates the cloud service from a business perspective, determining its materiality, its business impact, and the risk that the solution brings to the organization. This includes all aspects of the cloud service, including cyber, security, contractual, compliance, resilience, adequacy of the solution. The accountable business management area will review this risk assessment and decide whether the service is acceptable, especially in cases where they are the only user for the service (very often this is not the case for material cloud services, which is why enterprise-wide decision bodies may be involved). The 1st line risk team is also supported by other 1st line risk functions:
    - **Procurement:** The procurement officer is not only involved in price negotiations, but they often function as a control point for validating the adequacy of the vendor (the cloud provider). They will screen contracts for compliance against existing regulations such as GDPR or outsourcing guidelines, making sure everything stays compliant.
    - **Cloud architect and technology design:** A technology or cloud architect will obtain a deep understanding of the service and how it integrates with the FI's internal systems. Security design is an important part of this process. As such, they are an essential part of each cloud assessment process, documenting how security controls are embedded in the future solution.
    - **Legal:** The 1st line functions may seek legal advice on how to best implement the applicable regulation or to research the steps needed to achieve compliance (especially in cases where regulation hasn't been translated into internal policy)
- **2nd Line Risk Management:** The main reason for creating additional lines of defense is to increase the level of control and get an independent opinion on the adequacy of the proposed solution and its risk to the business and the enterprise. They may also advise on, or even approve, risk exceptions when the cloud service provider is unable to meet internal standards. Support from these risk functions is considered beneficial to the further approval process:
    - **Operational risk:** The 2nd line risk function is involved with managing all non-financial risks within a FI, including information security-, data protection-, cyber-, business continuity-, governance and cloud related risks. Their involvement may be very limited, depending upon the FI's risk management structure and the maturity and experience of the 1st line risk functions involved.
    - **Compliance:** The compliance department is mostly involved in keeping track of external regulations and translating these into internal policy guidance. They define internal policies (or policy requirements) to ensure cloud, privacy, and outsourcing regulations are respected in each deployment. A compliance function may also advise on a case-by-case basis, especially in the case of cloud computing (for instance when no internal cloud policy exists yet).

- **3rd Line Internal Audit:** The main reason for this functions to get involved is to deliver an independent opinion on how the change will ensure compliance for the FI now and in the future. Their focus will typically incorporate review of the end-to-end solution including the FI internal support models and documentation.
- **Top-level management decision bodies:** For material cloud services, especially services that operate across several business functions, it is important to ensure decisions are taken at the appropriate level within the organization. For enterprise-wide services such as messaging and collaboration, it is recommended to approve these at the highest management levels internally (e.g. in an Executive Committee Meeting, or an Enterprise Risk Committee). Furthermore, in case of doubts about the risks, an independent opinion by 2nd line risk and/or audit may be requested.

Most FI's should expect a significant increase in the amount of cloud-based services in their organization in the future. As such, it is our recommendation to establish a multi-disciplinary advisory function across all the domains above (except internal audit) to speed up the approval process and increase efficiency. For instance, a **Cloud Advisory Board** could ensure that all the different stakeholders are simultaneously represented during each case evaluation.

The list of stakeholders at the decision-making level, in line with the functions above, is available in this table (it should be ensured that all these functions are informed of the intention to move to a cloud solution early on in this risk assessment process):

Role	Reason
CIO/CTO **(Chief Information/Technology Officer)**	Owner of the solution (=accountable), sponsoring the cloud project and accountable for the solution. Reports to the CEO and may be member of the Executive Committee. The cloud architect reports to this function. The CISO may report to this position.
CISO **(Chief Information Security Officer)**	Manages information security and cybersecurity risks. The 1st line risk functions report to the CISO.
CDO/DPO **(CDO - Chief Data Officer** **DPO - Data Protection Officer)**	Manages data protection related risks, deals with privacy and protection of personal/confidential information. The DPO is a mandatory role when processing personal information under the General Data Protection Regulation (GDPR).
CRO **(Chief Risk Officer)**	CROs are accountable to the Executive Committee and The Board for enabling the FI to balance risk and reward. 2nd line risk functions (above) also report to the CRO, and the CISO may sometimes report to the CRO making their involvement in the risk assessment decision essential.
Internal Audit **(Audit Manager)**	The Audit Manager may be asked to provide an independent assessment of the cloud solution to the Audit Committee Members which are part of the (external) Board. It is less common that they are involved in cloud projects[6] directly, unless for very specific reasons.
CFO **(Chief Financial Officer)**	Involvement depends upon the internal reporting lines of the different risk functions. The CRO, procurement, or other functions may report to the CFO of the enterprise.

Procurement	Involvement depends upon management structure. Often advise on contractual matters, financial viability of the CSP etc.
Compliance and Legal	The head of compliance often has a deep involvement due to the regulatory notification requirements and the evolving regulatory landscape around cloud computing. They are a key stakeholder in most cases. Legal is often involved as well in these processes (as a separate function).

In addition, specifically for software-as-a-service solutions such as Microsoft 365 that offer services such as messaging and collaboration across the entire enterprise, the following additional stakeholders may be involved from a functional perspective:

Role	Reason
Communications	May act as the business sponsor, ensuring the solutions user-friendliness or usability is not restrained by excessive security requirements. They may act as a counterbalance against some risk functions, representing the business's need to have a solution that offers best-in-class services without compromise.
HR	Similar as above, since HR touches all business lines, they may be involved as a business representative overseeing some functional needs for the solution. In addition, they will advise on the integration with internal joiners-movers-leavers processes ensuring this process is enhanced to deal with the new cloud solution.

Step-by-step guide for assessing Microsoft cloud services

This step-by-step guide is created for customers that want to execute an end-to-end risk analysis of Microsoft services in the most effective way possible, leveraging optimized tools and processes that will help in getting a qualitative assessment done as fast as possible whilst staying focused on the most important risks.

Prerequisite: Solution Security Design

When internal security and compliance requirements are unclear, or when no architecture design exists that defines how these are configured in practice, your assessment of the Microsoft cloud may become unnecessarily difficult. To avoid this, we recommend making a set of initial security design decisions prior to deployment that are later included in the risk assessment process. This design work implies choosing product features that must be enabled to meet all internal security and compliance requirements. While this may be an obvious step in IaaS/PaaS deployments, it is often overlooked for SaaS solutions such as Microsoft 365.

Microsoft provides customer guidance on how to secure SaaS solutions under the FAQ and White Papers section on the Service Trust Portal. A great starting point is the Microsoft Cloud Security for Enterprise Architects whitepaper. We also recommend to review the recommendations in the Microsoft 365 and the Office 365 Secure Score portals for your tenant.

Estimated time to complete: varies

Step 1: Identify internal stakeholders and decide a governance approach

Stakeholder management is a key success factor in any significant cloud deployment. A risk assessment of a major cloud project is therefore best treated as a miniature project, where the various internal stakeholders (see above) are brought together and agreements are made on their level of involvement within the broader process. This minimizes delays due to unavailability of internal stakeholders and therefore causing the risk that assessment would need to be reassessed, each time from a different risk perspective.

Equally important is to align and agree on the internal governance and approval process, including how to engage in later stages with financial and privacy supervisors. Because these topics are sensitive within FI's, it is recommended that rules of engagement are discussed upfront and considered throughout the entire assessment process.

Estimated time to complete: 1 week

Step 2: Choose an appropriate reference framework for your assessment

Your existing internal risk assessment models may not always translate well into the context of cloud computing where part of the service is now managed by the CSP. They also may not sufficiently address the specific challenges involved with cloud computing (see Cloud risk assessments:), and mapping your internal control requirements on the standard models as provided by Microsoft may become very time consuming.

As an alternative, try adopting an independent external model for addressing cloud risks such as the Cloud Security Alliance's Cloud Controls Matrix (CCM v3.0.1) which was specifically created for assessing cloud deployments, the

widely supported ISO 27001:2013[7] information security standard, or special publication NIST SP 800-53. Or, in case of privacy assessments, you may want to assess compliance against the GDPR.

The benefit of this approach is three-fold:

1. **Acceptance:** Because these frameworks address cloud-related risks so well they are also widely accepted in the FI industry and are recognized by many financial supervisors.
2. **Mapping:** These frameworks have been mapped on most of Microsoft's cloud services already, providing you with insights on how each control is managed by Microsoft. This way, a lot of time can be saved on fact finding, mapping, and researching how specific controls are implemented by Microsoft.
3. **Assurance:** Microsoft publishes assurance reports[8] for its cloud services that can be mapped onto these frameworks[9], allowing you to quickly verify for each control when it was audited the last time by an independent third-party auditor and what the level of compliance was.

Tip: for efficiency reasons we recommend choosing a framework that is supported in Compliance Manager (see also next step)

Estimated time to complete: 2 days

Step 3: Use Compliance Manager to assess risks

With Compliance Manager, you can assess your deployment in the Microsoft cloud against these standards, allowing you to distinguish between provider and customer-managed controls. Several standards are available per cloud service for assessment, and each control has been scored in accordance with their relative risk-weighted importance. The tool will allow you to quickly assess the service and offers a built-in workflow management system that also allows you to follow-up on the assessment of customer managed controls (the controls for which you as a customer remain responsible). Some of the compliance assessments focus exclusively on the steps Microsoft must take to meet compliance against a specified selected standard, but we recommend that you focus also on the assessments that are created to help you as a FI to become fully compliant with inclusion of customer controls. These customer controls are requirements you should meet when setting up the end-to-end solution so that you can be fully compliant. An example of a standard which includes a wide set of customer controls is GDPR.

Once your assessment is done, the results can be exported for further review and sign-off by the relevant decision bodies. More information can be found in the Compliance Manager FAQ or by taking the guided tour on the homepage.

Important note: Exceptions may become visible where specific controls failed during testing, which leads to a (temporary) exception state. These (control) exceptions must be carefully tracked and the relative risk that results from these gaps must be assessed and presented to management.

Estimated time to complete: 1 week

[7] The new and updated controls in ISO 27001:2013 reflect changes to technology affecting many organizations such as, for instance, cloud computing and are therefore a suitable standard also for cloud service assessments.
[8] See the Compliance Guides section on the Service Trust Portal
[9] Limitations may apply for certain products, but Microsoft continuously continues to increase its level of compliance.

Step 4: Use our compliance guides to assess regulatory compliance (per country)

Microsoft also created some excellent compliance guides on a country-by-country basis which are available on the service trust portal (STP, http://aka.ms/STP - direct link here). These guides can be leveraged to ensure that the cloud deployment is compliant with all relevant regulations in the countries where the service will be offered. These guides will also reference specific contract language locations that meet regulatory requirements within a country.

We recommend writing a compliance assessment summary[10] using these guides and adding this also in Annex to the decision memo for internal approval (same as for the risk assessment and risk exceptions) so that all information is available supporting informed decision making.

Estimated time to complete: 2-4 weeks

Step 5: Preparation of an exit strategy

A key element that is rapidly gaining in importance when consuming cloud services involves mitigating business continuity risks, and specifically how an organization can recover from major CSP failures (e.g. bankruptcy). More and more regulators require FI's to prepare a strategy document which explains how the FI would recover from such an event. The EBA guidance document on cloud outsourcing of December 2017 provides some basic guidance on how to prepare an exit strategy.

Our recommendation is to prepare a short principles-based document that is in line with these EBA requirements, and that is also validated or tested by walking through the different scenarios together with all stakeholders taking part in this exercise on a yearly basis. The document should list key threat scenarios that might lead to an exit taking place and detail strategies on how these can be achieved by the FI highlighting key process steps/phases, involved staff and their responsibilities, dependencies, timing, cost estimates etc. A good exit strategy document to a large extent mimics a project charter in its length, structure and level of detail.

Estimated time to complete: 3 weeks

Step 6: Risk action plans and service approval

The business case, risk assessment (or summary), compliance assessment (or summary), and the risk exceptions to be approved must now be joined up in a management letter asking formal approval to start consuming the cloud service. The exit plan – when ready – may also be included in this document set.

It is recommended that all stakeholders from step 2 are somehow involved in the review and approval process for using this cloud service, and that accountability and responsibility in the 1st line is clear and unambiguous. The case approval is strengthened further if a financial institution can demonstrate that 2nd line risk functions have been involved as well endorsing the deployment. Finally, optionally, internal audit may also be involved in the risk assessment of the cloud service, presenting their findings to the Audit Committee[11].

For critical or important case Executive Board/Committee approval should be considered, with further reporting to the (external) Board of Directors.

[10] This can be limited to a very short 2-page document, highlighting key regulations and how the service complies with these regulations. The difference with the risk assessment is that now the regulation is in focus, not the (risk) control set.

[11] In many cases this step will take place post deployment (unless audit involvement has been specifically requested by senior management).

Estimated time to complete: 2 days (+ lead time)

Step 7: Notify financial and privacy supervisors

As a last and final step, consider what notification and/or approval requirements may apply in your applicable jurisdictions for a new outsourcing arrangement, and notify your supervisors accordingly. For this step, our recommendation is to strive for maximal transparency by not just informing the regulators where notification is mandatory, providing them only with the minimum info as required but, instead, to inform all supervisors on the recently approved case.

The notification process must not focus on details, but explain:

- Which cloud service is being deployed and why
- Business case summary or benefits
- Risk governance and approval process that was followed
- Risk decisions that have been taken
- (optionally) Address key risks that have been assessed and explain how these are mitigated
- (optionally) Address key compliance requirements and explain how these are mitigated
- (optionally) Address the exit strategy highlights

We recommend notifying the financial supervisors after a risk approval has been obtained, and not to wait until moments before the expected deployment into production. A regulatory notification template is available in Annex II.

Estimated time to complete: 2 months

Tip: regulators will not formally approve use of a cloud service in writing, they only expect to be notified hereof. It is not uncommon for them to come back with questions in a Q&A process which can take some time to complete. However, a formal approval must not be expected at the end of this process and in the absence of an approval requirement responding to such questions can occur without holding up deployment of cloud services. This is because moving to the cloud is the institutions responsibility and decision, and in most cases the regulators role is primarily bound to keeping oversight (not granting approvals).

Step 8: (optional) Join the Microsoft Cloud Financial Services Compliance Program

The Microsoft Cloud Financial Services Compliance Program (FSCP) was specifically created to help financial services and regulated financial affiliates assess the risks of using Microsoft's cloud services. This (paid) FSCP program offers deep insights into Microsoft cloud services' capabilities, risks, and performance but is entirely optional for those customers that want to achieve the highest level of assurance over the service. The FSCP is available to FI customers using Microsoft 365, Microsoft Azure, Microsoft Dynamics 365, and Microsoft Intune.

Next Step: Production Deployment

The step-by-step risk assessment process ends with the production deployment of your cloud services, which can happen shortly after the financial supervisors have been notified in step 7. Other prerequisites that are typically part of a cloud migration but that have not been mentioned explicitly in this document such as technical preparations, data migration activities, upgrading network connectivity and modifying the security perimeter, IT training/transformation, internal Management of Change (MOC), preparation of end-user training etc. All these activities can take place in parallel with the risk assessment phase in order to keep the time needed to deploy

these services as short as possible. Therefore, when carefully planned, a successful first deployment of Microsoft cloud services can be achieved in a matter of months while staying fully compliant with all supervisory requirements.

Annex I: Useful Links for Evaluating Cloud Services

Security	
Microsoft Cloud - Security	This paper provides insight into what IT architects need to know about security and trust in Microsoft cloud services and platforms.
Data Management and Transparency within Microsoft	These links best describe how Microsoft manages your date including how data is governed, categorized, accessed and stored across the different cloud services. We are fully transparent on how we manage your data. Further info on how we protect your data, and where this data is stored is included in the additional links below.
Where is your data located?	Describes where your data is stored for all our Cloud services.
Microsoft Cloud - Encryption	Formerly a white paper, this link now describes for all cloud services how we protect your data using encryption at different levels.
Tenant Isolation in Office 365	An overview of our shared tenant infrastructure that explains how we ensure your data is isolated and secured from accidental disclosure to third parties.
Data Resiliency in Office 365	Resiliency sits at the core of our cloud services. An overview of service features that deliver this resilience is provided here.
Data Retention, Deletion, and Destruction in Office 365	Document that explains data governance such as setting of retention policies, data deletion and physical destruction of hardware media that were used for storing customer data.
Administrative Access Controls in Office 365	Explains that Microsoft engineers have zero standing access to customer content in O365 as well as the protocol we follow if such access is temporary required.
Office 365 - Auditing and Reporting features	Description of auditing, reporting and alerting features built into Office 365.
Protecting against DDOS attacks in Office 365	Description of protective measures against Distributed Denial of Service or DDoS attacks against our services.
Office 365 - Customer Security Considerations Workbook	Following the shared responsibility principle, some of the security configuration for securing your Office 365 deployments must be done by you. To guide you to this process we have created the Office 365 Customer Security Considerations workbook, designed to provide organizations with quick access to the security and compliance features in Office 365 and considerations for using them.
Office 365 - Customer Security Considerations User Guide	This document is a companion guide for the Office 365 Customer Security Considerations workbook. The Office 365 Customer Security Considerations workbook is designed to provide organizations with quick access to the security and compliance features in Office 365 and considerations for using them.
Azure Security & Compliance blueprint	Blueprint document addressing Microsoft Azure Security and Compliance.
Introduction to Azure security	Overview page with documentation on Azure security. Excellent starting point to learn about different capabilities, features & technology offered by Microsoft Azure.

Azure Security Whitepapers	This page links to a set of Azure Security Whitepapers on different topics. Rather than linking each of these individually, we recommend searching here when you are preparing for Azure deployments.
Dynamics 365 Security Overview	Benefit from Microsoft Dynamics 365 features such as identity and access management, encrypted connections, and data centers that provide security and data privacy in the Trusted Cloud. With Dynamics 365, you can control information access to maintain confidentiality, integrity, and availability of data.
Compliance	
Microsoft Cloud Compliance Offerings	Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider. This link allows you to search this offering per service and/or industry.
Microsoft Cloud Financial Services Compliance Program	Describes the Financial Services Compliance Program for Microsoft Cloud Services.
Microsoft Compliance Guidelines (per country)	This website includes a set of compliance checklists for almost all countries in the Asia Pacific region for regulated industries such as the finance industry.
Privacy	
Getting Started Guide for GDPR accountability	This guide helps FI's in preparing for GDPR compliance for internal systems and processes that rely upon our cloud services. It addresses the Data Protection Impact Assessment (DPIA), how we deliver tools to perform Data Subject Requests (DSR) etc.
GDPR Overview	Starting point on the Microsoft Trust Center. Review the different pages for a complete overview.
GDPR Solutions	This section lists the different technology solutions that we offer within each product to help you in your journey towards GDPR compliance.
GDPR FAQ	Frequently Asked Questions on GDPR.
GDPR Resources	Various resources such as whitepapers, videos and blog posts providing a deeper explanation and context into the topic.
Action Plan for GDPR	This article includes a prioritized action plan you can follow as you work to meet the requirements of the General Data Protection Regulation (GDPR), focusing on the first 30 days, 90 days and beyond.
How Microsoft responds to government and law enforcement requests to access customer data	This resource explains how Microsoft responds to law enforcement requests for access to customer data, as well as explaining our position on the Cloud Act.
Additional Resources	
Trust Center, STP, Compliance Manager	

Annex II: Regulatory Notification Template

See next page.

<Location>, *<Date>*

To *<Name of supervisory office>*,
Attn. Mr(s). *<Full Name>*, *<Function Title>*
<Department/Division>
<Name of regulatory body>

Notification on implementation of *<Microsoft Office 365 / Azure / Dynamics >* in *<Organization>*.

Dear <title>,

Further to the decision to *<decision summary>* approved by the *<accountable decision body name>* on *<date of decision>*, *<organization>* is preparing the production deployment of *<service or process name>* which is running on public cloud technology. This service *<does / does not>* involve a critical or important function (or material service)[12], within *<organization>*.

Info: The purpose of this notification cover letter is to inform the financial or privacy supervisor that appropriate internal due diligence processes have been involved prior to approving the service. There is no need to highlight individual risks & project details. Instead, the letter should explain the internal risk governance processes that have been followed, outline internal responsibility and ownership over the solution and its involved risks.

Recommended sections to highlight in the cover letter (2 to 3 pages):

1. *Context*
    - *Short service description*
    - *Scope & timeline of the project*
    - *Impact on data processing (type of data that is processed in the cloud, in which countries will this data be processed)*
    - *Internal ownership over the solution (IT, Business, group vs. local)*
2. *Benefits & decision*
    - *Key benefit of the solution, why was the decision made (context)?*
3. *Risk management*
    - *Summary of the internal risk assessment process & risk approval (which of the management functions have been involved in the approval, who chairs these decision body members etc.)*
    - *Applicable regulations that have been considered (include both financial as well as privacy regulations).*
    - *Statement on audit rights & right of access by financial supervisors*
    - *Statement on service resilience, business continuity & exit strategy*
4. *Annexes*
    - *Supervisory Notification Sheet (template)*

[12] Statement on the materiality of the service. The use of the name 'critical or important function' is derived from MIFID II regulation. Notification may only be required for materially important services, but you may decide to notify also for non-material services for transparency reasons.

Supervisory Notification Sheet Part 1 - Overview

SUPERVISOR QUESTIONS[13]	CLARIFICATION (ANSWER FIELD)
Unique Identifier or Reference	(optional) Provide a unique identifier linked to the outsourcing arrangement.
Description of outsourced activity (Process/Function/Activity)	Description of the outsourced activity and sub-activity within the FSI (e.g. Customer Relationship Management / Customer Acquisition, or Risk Management / Liquidity Controlling). Include a clear self-explanatory description, without use of jargon or abbreviations.
Does the outsourcing involve a material or critical service?	Whether the function is considered material, critical or important or not. ("Yes" / "No"). Note that different qualifications on materiality may be used in different parts of the world. They type of data under processing is often a key driver towards determining materiality of a service. Examples of material services: core banking (sub-)systems, trading systems, day-to-day risk management systems, customer CRM systems that process sensitive data, internal information systems for managing secret data, etc.
Name of the Cloud Service Provider (CSP)	Microsoft
Country where the CSP is registered	USA
Licensed Products in scope + number of users	Reference to the specific cloud services that are consumed, as well as the targeted use of license. Example: Microsoft 365 E3 + E5 features MS ATP & AD Premium P2 for an estimated total of 25,000 users.
Region where the service will be provided (incl. countries of data storage)	In which region and countries will the service be provided and where will the data at rest be stored? Example: European Union, Dublin IE & Amsterdam NL
Contractual service start date	There is no need to provide a copy of the contract to the financial supervisor. Including the basic contractual information in this template + maintaining a copy of this contract within your FSI should be enough.
Next contractual renewal date (or service end date)	Provide end date for the service, or contractual renewal schedule and date.
Applicable laws governing the contract	The law governing the contract, as defined in the contract.
Cloud deployment model (public/hybrid/private)	Public cloud (always the case when consuming MS cloud services)
Parties receiving cloud service under the outsourcing arrangements	These are the entities that are using the cloud service. This may be the name of the financial institution at group level, or a set of specific subsidiaries from the institution.

[13] List of questions is aligned with European Banking Authority (EBA) Guidelines on outsourcing to cloud providers published December 2017 (see also Registration template for guidelines on outsourcing to CSPs on the EBA website)

Approval date for the outsourcing + decision body	Highest decision body within the accountable business line. We highly recommend approving cloud outsourcing at level of Risk Management Committee, Executive Board/Committee and or Board of Directors for material or critical cloud services and reporting all of these in this line item.
Relationship Manager within the Bank	Individual responsible for managing the relationship/contract with the CSP
Relationship Manager within the CSP	Key contact person within Microsoft overseeing the CSP relationship (e.g. account manager)
Data Privacy Officer (DPO) within the Bank	Relevant only when processing personal data of EU citizens context of GDPR, otherwise use N/A to indicate that no personal data is processed in the system.
Data Privacy Officer (DPO) contact within the CSP	Relevant only when processing personal data of EU citizens context of GDPR, otherwise use N/A to indicate that no personal data is processed in the system.
Name(s) or list of subcontractors + countries where these are registered	Refer to the "We limit access by subprocessors" section on our webpage for more information as well as to the relevant contractual safeguards in your contracts (this is specific to each FI, but in many cases the contractual language on this topic may be found the Online Service Terms).
Date of the latest materiality assessment for the service in context of cloud outsourcing?	When was the business process or services that makes use of cloud technology assessed in terms of its materiality. If no materiality assessment process exists with the FI, we recommend establishing this using the guidelines in this document.
Does the service involve time-critical functions (y/n)?	Indication if the processes are time-critical, e.g. real-time banking environments would be classified as being time-critical, but this may also be the case for other interactive processing such as real-time video broadcasting.
Assessment of the outsourcing providers substitutability (easy, difficult)	The EBA guideline of 2017 suggested to provide an indication on how easy it is to switch to exit the outsourcing arrangement. Technical concerns but also contractual terms may prevent an immediate exit of the service. An indication of the difficulty should be provided to the financial supervisor, especially within the EU.
Identification of alternate service provider	See also above. Provide the alternative service provider or refer to on premise solutions in case of severe outsourcing issues that force the FI to engage their exit scenario.
Date of the latest risk assessment	When was the cloud service last assessed?

Supervisory Notification Sheet Part 2 – Overview Compliance with *<country>* Outsourcing & Privacy Guidelines

Sample only, these requirements will be different per country. Different tables or a table format covering multiple countries may be provided for each country where the service will be deployed.

KEY REQUIREMENT IN COUNTRY XXX	SOLUTION
Written Agreement	A common requirement says that a written agreement must be in place that sets out the responsibilities of both parties.
Right of Access; Right to Audit	The contract must allow the outsourcing institution's compliance and internal audit departments complete access to its data and its external auditors full rights of inspection of that data; and the contract should allow direct access by the outsourcer's supervisory authority to the outsourcer's relevant data and premises
Termination Rights	Terms on which the contract may be terminated as required by supervisory guidance.
Exit Provisions	The contract should include termination and exit management provisions which allow the activities to be transferred to another service provider or to be reincorporated into the FI.
Use of Sub-Contractors	The contract should take account of the risks associated with chain outsourcing.
Data Security	Description of appropriate security measures such as access controls, cryptographic protections, cybersecurity defences & monitoring that must be established within the national regulation.
Notification of Security Breaches	Contractual commitments to report security breaches within 72 hours (for instance under GDPR)
GDPR Compliance	Processing of personal information of European citizens must occur in compliance with the EU General Data Protection Regulation (GDPR).

Disclaimer: Supervisory requirements for cloud outsourcing & privacy are not globally harmonized and may be different in each country where the service is deployed. The list above is only provided as an example, listing common elements encountered in the most common regulations. Replace the requirements as appropriate for the countries where you will deploy your cloud service.