www.pwclegal.ch

EBA Outsourcing Guidelines – an exciting topic which will significantly affect the financial industry

It was expected, or at least there was wishful thinking, that MiFID II (2014/65/EU) and GDPR (Regulation (EU) 2016/679) would be the regulatory summit for our high mountain region. However, the European Regulator is continuing to pursue its overall goal of strengthening the regulatory framework in the European Union, which, in turn, is having a major impact on the Swiss financial industry.

This paper gives you an easy to read, but also fundamental, overview of the complexity and impact of this major topic, and prepares you for the new obligations in this field. The following key points are discussed:

a) Executive summary
b) Background and looking ahead
c) Key topics to understand
d) Target Operating Model
e) Conclusion and impact on the financial industry
f) Legal background

On the 22nd of June 2018, the EBA published its draft version for the new EBA Outsourcing Guidelines (EBA/CP/2018/11) that will be applicable from 30 June 2019. These Guidelines will replace the current CEBS Guidelines of 2006(GL02/2006) and will repeal the Recommendation on Outsourcing to Cloud Service Providers of 20 December 2017 (EBA/REC/2017/03).

The EBA has taken the latest developments with regard to the financial markets and regulatory initiatives as an opportunity to redefine the outsourcing standards and guidelines in order to comply and align with the various requirements of CRR/ CRD IV (Regulation (EU) 575/2013), GDPR (Regulation (EU) 2016/679), PSD II (2015/2366/EU), BRRD (2014/59/EU), and MiFID II (2014/65/EU). Furthermore, it also addresses **internal as well as external outsourcing** as well as **cloud** outsourcing.

An important difference as compared with the FINMA Circular 2018/3 is that the EBA Guidelines apply to all outsourced functions, not only to those deemed to be "critical and important", to cite the wording used in MiFID II and Commission Delegated Regulation (EU) 2017/565 supplementing MiFID II in which it is used solely for the purpose of identifying services, activities or functions falling within

the scope of outsourcing arrangements. Furthermore, the FINMA circular consists of 6 pages whereas the EBA Guidelines provides around 50 pages of exciting reading.

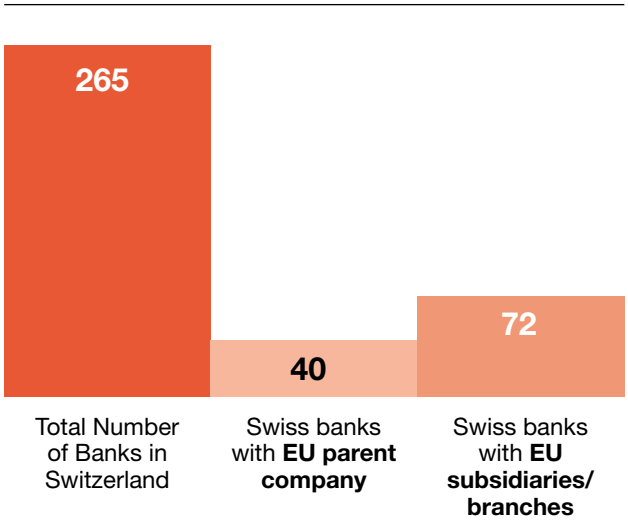
The new guidelines require external service providers in a third country to apply the regulatory requirements in almost the same way as EU domiciled banks. How to do so, and what it means can be found in the outlines below.

1. Executive summary

The EBA Guideline set out the internal governance arrangements that credit institutions, payment institutions and electronic money institutions should implement when they **outsource internal services, activities or functions.** Due to the increasing complexity of outsourcing solutions and technological developments, it is becoming ever more important to regulate the quality of these solutions.

Since not all providers of technical solutions (FinTechs/RegTechs/AnyTechs) **can be regulated directly,** the approach taken by the EBA in the recent Draft Guidelines on Outsourcing Arrangements is to **indirectly regulate them by applying higher and very formalistic standards to those companies to which those standards apply – the financial industry.**

This is also true for most third country firms outside the EEA.



The illustration above indicates that 42% of all Swiss banks are impacted directly by this new standard. The indirect impact is of course much higher.

1.1 Scope

Who should read this paper?

This paper is **applicable** to you, if you are

- a credit institution as defined in CRR;
- a post office giro institution which is entitled, under national law, to provide payment services as defined in PSD II;
- the ECB or a national central banks when not acting in your capacity as a monetary authority or other public authority as defined in PSD II;
- an electronic money institution as defined in the e-Money Directive

or

- one of your subsidiaries/branches is one of the above mentioned regulated institutions in the EU; or,
- a FinTech/RegTech inside or outside the EU providing any outsourcing services to an investment firm as defined in MiFID II (banks, asset managers, and providers of financial services such as investment advice or portfolio management);

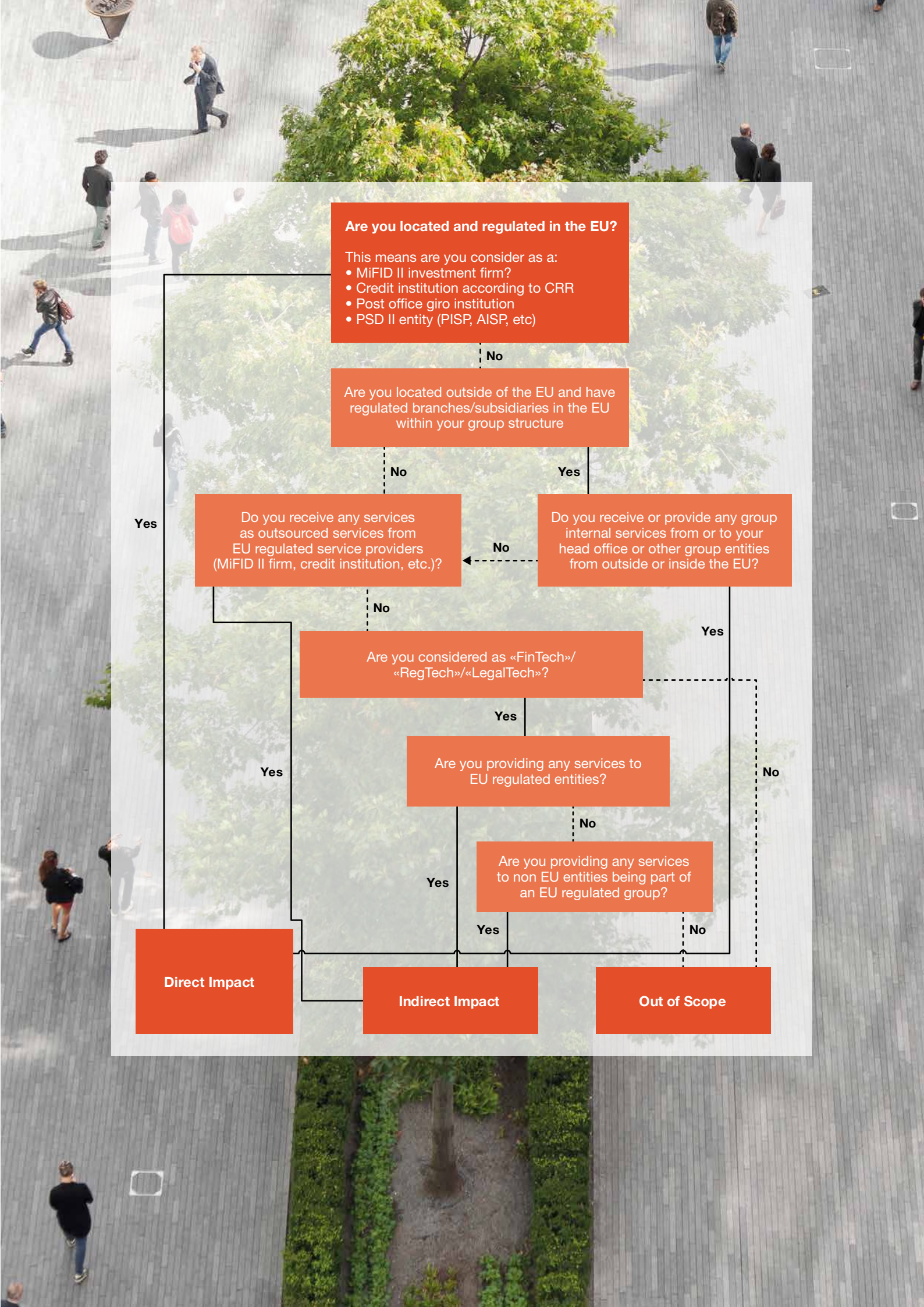
1.2 Why read it?

This paper is essential for the business of investment firms and payment institutions in order to both be aware of the new standards and, while being aware, be able to reduce costs and continue improving their own flexibility and efficiency in the financial market.

Under the Draft Guidelines, **liability lies at all times with the financial institution's governing body.** Therefore, it is crucial that investment firms and payment institutions continue to retain and **build adequate competences and resources to be compliant.**

Moreover, they must ensure that they have **sufficiently skilled human resources to provide appropriate support** to ensure that their additional responsibilities as regards the risks and management of their outsourcing arrangements are met.

From now onwards, it is essential to be able to effectively **control and manage the quality and performance of outsourced processes, services and activities** and carry out ongoing monitoring and (formal and informal) risk assessments.

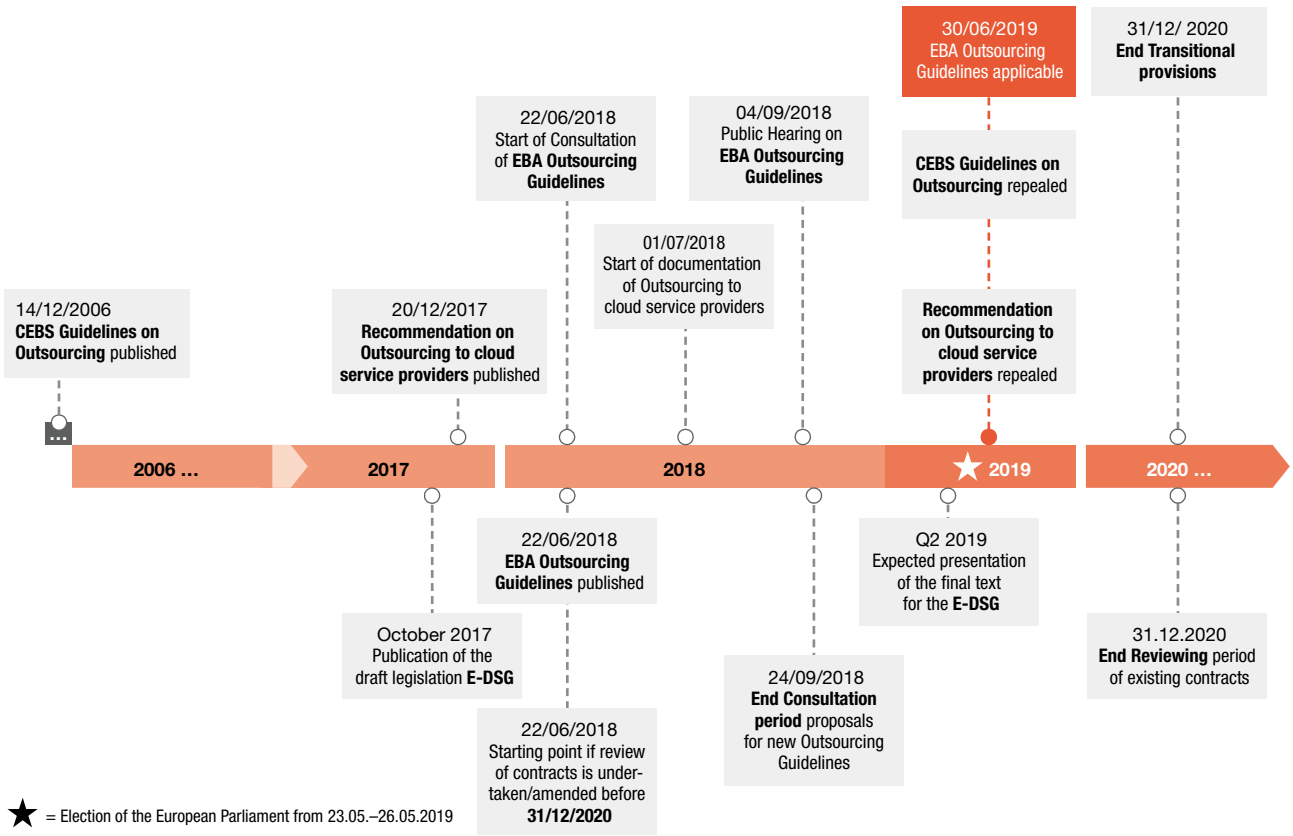

Are you located and regulated in the EU?
This means are you consider as a:
• MiFID II investment firm?
• Credit institution according to CRR
• Post office giro institution
• PSD II entity (PISP, AISP, etc)
No
Are you located outside of the EU and have regulated branches/subsidiaries in the EU within your group structure
No
Yes
Yes
Do you receive any services as outsourced services from EU regulated service providers (MiFID II firm, credit institution, etc.)?
No
Do you receive or provide any group internal services from or to your head office or other group entities from outside or inside the EU?
No
Yes
Are you considered as «FinTech»/ «RegTech»/«LegalTech»?
Yes
Yes
Are you providing any services to EU regulated entities?
No
No
Yes
Are you providing any services to non EU entities being part of an EU regulated group?
Yes
No
Direct Impact
Indirect Impact
Out of Scope

1.3 Effective date and next steps

- **ATTENTION:** already in force: Document on Cloud Outsourcing on 1 July 2018

- The consultation period was closed on 24 September 2018.
- The EBA is now in the process of finalizing these Guidelines.
- Unless specified otherwise, the Guidelines will **enter into force on 30 June 2019,** with the exception of the cloud recommendation.
- **Finalization of the document on all other services – 31 December 2020**
- If contracts are to be reviewed or amended **before 31 December 2020,** this date is applicable

What has happened so far and what can be expected? New Outsourcing Guidelines



1.4 Direct vs indirect impact on Financial Intermediaries

Who is directly affected?

Institutions directly affected are those institutions listed below that are registered and supervised in the EEA:

- investment firms as defined in MiFID II (banks, asset managers, providers of financial services such as investment advice or portfolio management);
- credit institutions as defined in CRR;
- post office giro institutions that are entitled, under national law, to provide payment services as defined in PSD II;
- the ECB and national central banks, when they are not acting in their capacity as monetary authority or other public authority as defined in PSD II;
- electronic money institutions as defined in the e-Money Directive.

Who is indirectly affected?

Institutions indirectly affected are the following:

- all institutions above that have their head office located outside the EEA but provide internal services to their EEA subsidiaries **(internal outsourcing);**
- all **cloud solutions provided to EEA institutions** but managed and maintained from outside the EEA (not where the servers are hosted);
- **IT/FinTech/RegTech/LegalTech providers of services to EEA institutions;**
- IT/FinTech/RegTech/LegalTech providers of **services to non-EU institutions who host their service in a cloud accessible for EEA regulated entities;**
- IT/FinTech/RegTech/LegalTech providers of services to non-EU institutions who **distribute their service to the institutions' EEA subsidiaries/branches.**

What does it mean?

For directly affected financial intermediaries it means:

- setting up a sound (clear and transparent) outsourcing framework (due diligence, oversight of outsourced functions, risk assessment and management of outsourcing arrangements, exit plan(s));
- putting in place a legally compliant outsourcing agreement;
- setting up appropriate SLAs for group outsourcing;
- reviewing/amending existing outsourcing relationships;
- identify, disclose and maintain all outsourcing activities/partners in an outsourcing register.

For indirectly affected FinTechs/RegTechs (not directly regulated) it means:

- ensuring that all processes/functionalities are in line with the regulatory requirements (e.g. ISAE 3000, ISAE 3402, Type 1 and Type 2);
- ensuring that contractual obligations are met in full;
- drawing up a Sub-Outsourcing Framework Agreement;
- concluding Outsourcing Agreements with Sub-Outsourcing Providers.

Overlay with the Swiss Outsourcing Circular and RegTech Regulation

- The Swiss Outsourcing Circular is principle based, whereas the EBA Outsourcing Guidelines is rule based (FINMA circular 6 pages vs. EBA Guidelines 50 pages).
- **An important difference as compared with FINMA Circular 2018/3 is that the EBA Guidelines apply to all outsourced functions, not just those deemed as "critical and important".**

2. Background and looking ahead

In this new era of increasing digitalization and growing importance of new financial technology providers (FinTech and RegTech), financial institutions are adapting their business models to embrace such technologies. Some have increased their use of FinTech/RegTech solutions and have launched projects to improve their cost efficiency as intermediation margins from the traditional banking business model are put under pressure. Outsourcing is a way of gaining relatively easy access to new technologies and of achieving economies of scale.

The EBA is updating the CEBS Guidelines on Outsourcing issued in 2006 (GL02/2006) that applied solely to credit institutions and needed to be replaced by guidelines to achieve a more harmonized framework for all financial institutions that fall within the scope of the EBA's mandate and to resolve the existing high-level barrier of uncertainty for institutions **using cloud services** as well as supervisory expectations. Moreover, the landscape of **FinTech and RegTech firms,** which is currently unregulated, will be **regulated indirectly** by applying these standards.

Furthermore, the Recommendation on Outsourcing to **Cloud Service Providers** (EBA/REC/2017/03), published in December 2017, has been integrated in these Guidelines.

The 2006 Guidelines on Outsourcing **will be repealed when the EBA Guidelines come into force on 30 June 2019.**

3. Key topics to understand

3.1 Which activities are deemed to be outsourcing and what are the different types of outsourcing?

The key question is what is deemed to be an outsourced service?

In contrast to what we are familiar with, the Outsourcing Guidelines will not only cover "critical or important functions", but **all functions that are outsourced externally or internally.** The definition of outsourcing for the purposes of the Guidelines is the following:

Outsourcing means an arrangement in any form between a credit institution, payment institution or electronic money institution and a service provider under which that service provider performs a process, service or activity, or parts thereof that would otherwise be undertaken by the credit institution, payment institution or electronic money institution itself.[1]

The latest **FINMA Circular 2018/3** for example only deals with "critical or important" functions, whereas the EBA obligations **extend far beyond** this.

The outsourcing of the operational tasks of internal functions is divided into:

- **intragroup outsourcing;**
- **outsourcing within groups** – where no waivers are granted to institutions and payment institutions which are subsidiaries of an EU parent undertaking or a parent undertaking in a Member State; and,
- **institutional protection schemes** – which means internal governance arrangements, processes and mechanisms in subsidiaries, including payment institutions, at all levels.

[1] In comparison, the FINMA Circular 2018/3 defined outsourcing as follows: "Outsourcing […] occurs when a company mandates a service provider to perform all or part of a function that is significant to the company's business activities independently and on an ongoing basis."

3.2 General outsourcing principles and intra-group outsourcing

Regardless of the degree of outsourcing and the criticality of outsourced processes and functions, the **management body remains liable at all times for all activities –** thus, a proper understanding and adequate skillset, oversight and management are required internally. The EBA refers to this as the avoidance of **"empty shell"** or **"letter-box"** entities. It can be avoided by having an appropriate outsourcing framework in place that ensures:

1. clearly **assigned responsibilities** internally for the **documentation** and **control** of outsourcing;
2. the **availability of sufficient resources** to ensure compliance with all regulatory requirements;
3. an **assigned outsourcing officer** with senior management responsibilities;
4. appropriate **oversight of all outsourced activities** at all times;
5. proper **risk management** for the risks arising from outsourcing – especially with regard to **third-party IT providers** (FinTechs/RegTechs/LegalTechs) – as well as appropriate flows of relevant information;
6. that **internal controls are defined,** measured and implemented on an ongoing basis;
7. that there is a **plan B for critical or important outsourced functions** that either:
   - transfers the function to an **alternative service provider;** or,
   - **reintegrates** the function into the institution's own structure.

Moreover, these requirements also apply to **intra-group outsourcing,** which is a common feature of **centralised group structures. This becomes even more significance when services are obtained from a head office that is located in a third country that is not part of the EU – such as Switzerland.**

3.3 The Cloud

The first and probably most important information is, that EBA outsourcing standards for cloud outsourcing are **applicable since 1 July 2018** (EBA/REC/2017/03).

Based on the definition given, there are four different types of Clouds:

- the **Public Cloud,** where the Cloud infrastructure is available for open use by the general public;
- the **Private Cloud,** where the Cloud infrastructure is available for exclusive use by a single institution;
- the **Community Cloud,** where the Cloud infrastructure is available for exclusive use by a specific community of institutions, including institutions of a single group;
- the **Hybrid Cloud,** where the Cloud infrastructure is composed of two or more distinct Cloud infrastructures.

However, the enhanced obligations outlined in the Outsourcing Guidelines encompass the Cloud in general and are aimed at ensuring that all the Clouds abide by EU standards.

This means that the following, inter alia, needs to be documented in the **Outsourcing Register** and **regularly assessed to assure ongoing compliance with EU law:**

- **risk** assessments;
- the **locations** where sensitive data is processed;
- all **decision makers** who decided on the procurement of outsourcing solutions;
- the last and next **audit dates;**
- assessments of **substitutability** and of the possibility of **re-integrating** the outsourced service (only if critical or important);
- the **Cloud service and deployment model** (private, public, hybrid, community);
- the estimated **yearly costs;**
- the Parties **receiving outsourcing services** under the outsourcing agreement.

It is of major importance that the Cloud service provider complies with **GDPR standards** – this is especially critical if the Cloud service provider's servers are **located outside the European Union** in countries where data protection **standards are not equivalent** – such as in Switzerland, for example.

4. Outsourcing target operating model to avoid "empty shell" entities

To assure compliance with the Outsourcing Guidelines, and thus, also indirectly with standards such as **MiFID II** (2014/65/EU), **PSD II** (2015/2366/EU), **BRRD** (2014/59/EU), **e-Money Directive** 2009/110/EC, etc., it is crucial to have a **sound outsourcing framework** in place.

One major criterion is that all liability must rest with the financial institution and may not be passed on to providers of outsourced services (see 4.1 Liability) if investment firms or payment institutions are to continue to be licensed and not become "empty shell" entities. For institutions to remain fully liable and ensure compliance with the regulatory standards, a sound framework must be in place that will make it possible to **enforce compliance and appropriately manage third-party risk on an ongoing basis.**

To assist with establishing that sound framework, a description is provided below of how the **lifecycle** of an outsourcing relationship must be managed and overseen, and a list of the component elements to be integrated into the institution itself in order to achieve a proper framework structure.

4.1 Liability Responsibility

Under the new Guidelines, it will not be possible to delegate liability. **The institution`s management body remains fully responsible and accountable for** compliance with all of the regulatory obligations at all times when outsourcing.

In the light of this, it is highly important for investment firms and payment institutions not only that service providers within the group are chosen carefully but the performance and quality of the Cloud service provider`s delivery are borne in mind. Moreover the provider's ability to protect the confidentiality, integrity and availability of data (both in transit and at rest) and of the systems and processes used for processing, transferring and storing those data are reflected and managed properly.

Given these considerations, **overseeing the outsourcing of any critical or important function must be the key focus** of the institution at all times to ensure compliance.

With regard to oversight, institutions are fully responsible and accountable for the following:

- meeting, on an **ongoing basis,** the conditions to be complied with retaining the license and the conditions imposed by the competent authority;
- **internal organisation;**
- identification, assessment and **management** of **conflicts of interest;**
- putting in place **strategies and policies,** e.g. a business model, risk appetite and risk management frameworks;
- **day-to-day management** and management of the risks associated with outsourcing;
- the **oversight role of the management body** in its supervisory role.

Under the EBA Guidelines, institutions must:

- clearly assign responsibilities;
- **allocate sufficient resources to ensure compliance with the Guidelines;**
- establish an **outsourcing officer;**

- set up the appropriate **register** without undue delay (in which all existing outsourcing arrangements are listed and maintained centrally within a group) and ensure that all outsourcing arrangements, including outsourcing arrangements with service providers inside the group, are included in that register;
- ensure that operational tasks are performed effectively, including on the basis of appropriate **reports** (especially with regards to the monitoring and auditing of outsourcing arrangements where operational tasks relating to **internal control functions** are outsourced to a service provider within the group);
- ensure **independent monitoring of the service provider** applying due skills, care and diligence; have appropriate oversight, including through reports on centralised monitoring functions; ensure timely information on relevant changes being planned with regard to centralised service providers (if within a group or a member of an institutional protection scheme);

  – When relying on an exit plan –
- Examine the respective plan, ensure that it can be effectively implemented and take the plan into account in taking the decision to make use of the outsourcing arrangement (if the outsourcing is within a group, institutional protection scheme or central body).

4.2 Outsourcing life-cycle management

The obligation to manage the outsourcing risk starts from the outset and ends when the contract terminates.

An outline of the obligations applicable to you is given below.

Before entering into an outsourcing agreement, a **pre-outsourcing analysis** should be performed on the basis of the checks indicated below.

Step 1 – Assessment of the criticality or importance of the process

Crucial to the management and monitoring of the risks incurred in outsourcing specific services is whether a service is considered to be **"critical or important"**.

This must therefore always to be checked especially when:

- a defect or failure in performance of the service would **materially impair continuing compliance** with the conditions for the institution's authorisation and with its **regulatory obligations,** its **financial performance** or the **soundness or continuity of its banking and payment services** and activities;
- operational tasks relating to **internal control functions** are outsourced;
- the intention is to outsource **banking or payment services** that must be licensed by a competent authority.

Thus, a service is considered as "critical or important", if:

1. internal controls functions services are outsourced;
2. banking or payment services that require a license under European Union law are outsourced;
3. any service outsourced where a defect would materially impact on compliance with any of the following regulations:
   - CRR
   - CRD IV
   - PSD II
   - e-Money Directive;
   - MiFID II
4. activities are outsourced that relate to the **core business lines of critical functions,** as defined in the Recovery and Resolution Planning Directive, i.e.:
   - activities, services or operations which, if discontinued, are likely to lead to the disruption of services that are essential to the real economy or of financial stability due to the size, market share, external and internal interconnectedness, complexity or **cross-border activities** of an institution or group, with particular regard to the degree to which those activities, services or operations could be substituted for;
   - business lines and associated services that are **material sources of revenue,** profit or franchise value for an institution or for a group of which an institution forms part.

     What constitutes a core business line depends on an institution's internal organisation, its corporate strategy and how much those business lines contribute to the financial results of the institution

     Indicators of core business lines include, but are not limited to, the following:
     a. the revenue generated by the business line as percentage of overall revenue;
     b. the profit generated by the business line as percentage of overall profit;
     c. the return on capital or assets;
     d. the total assets, revenue and earnings;
     e. the customer base, geographic footprint, brand and operational synergies of the business with other group businesses;
     f. the impact that ceasing the business line would have on costs and earnings where it is a source of funding or liquidity;
     g. the growth outlook of the business line;
     h. the attractiveness of the business line to competitors as a potential acquisition;
     i. the market potential and franchise value.

Core business lines may rely on activities, which do not generate a direct profit for the institution, but which support core business lines, thereby contributing indirectly to the institution's profits.

If a service is considered to be “critical or important”, then the relevant risk has to be **quantified** by applying a highly standardized process involving a prescriptive list of minimum risk assessment criteria (e.g. GDPR compliance, substitutability, compliance with legal and regulatory standards, etc.).

Step 2 – Due diligence

Before entering into an outsourcing arrangement it has to be assured in the selection process, that the service provider has appropriate and sufficient ability, capacity, resources, organisational structure and, if applicable, regulatory authorisation(s) to perform the critical or important function in a reliable and professional manner.

This is especially important in the case **of third parties located outside the European Union** where no **equivalent legislations** are applicable. It is likely, especially for critical and important functions, that an **audit assurance based on ISAE 3000 and ISAE 3402 Type 1 & 2 reports** will be required in this regard.

When conducting due diligence checks on a potential service provider, certain factors must be taken into consideration, such as:

- its business model;
- nature;
- scale;
- complexity;
- financial situation; and, if applicable,
- group structure.

In addition to these factors, it must be ensured that the service provider chosen acts within the values and code of conduct of the investment firm or payment institution.

Step 3 – Risk assessment

A key factor for the regulator is that prior to outsourcing to any third party (or even internally), **all potential operational risks are identified, managed, monitored and reported,** applying the principle of proportionality. This means that all the requirements imposed under the Guidelines must be applied in a manner that is appropriate, allowing in particular for the institution’s size, internal organization and nature, scope and complexity of its activities.

Having said that, a full scenario analysis needs to be undertaken focusing on risk factors such as:

- the Concentration risk;
- the Aggregation risk;
- the Step-in risk;
- measures implemented by the institution;
- the Sub-outsourcing risk;
- the Third-country/different-country outsourcing risk;
- the risk of log and complex chains of sub-outsourcing;
- the Performance risk;
- the Political and legal risks;
- the Functions, data and systems protection risks;
- the IT security risk;
- the Geographical risk (EU vs non-EU);
- the Conflicts of Interest risk.

The risk assessment (both the scenario analysis and the outcome) must be documented thoroughly and transparently and, in case of any **sub-outsourcing or multiple outsourcing,** provided to the customer who outsources the services concerned (e.g. in a intra group setup, where the head office located in Switzerland provides services to an EU subsidiary).

The reason for this is the need for greater certainty as regards **Cloud outsourcing** given that it is more dynamic, more standardised in an automated manner and on a larger scale so that services can be provided to a larger number of different clients than the old traditional way of providing outsourced services.

The risk assessment should **regularly be updated** and consistently reported to the management body when any risk is identified in respect of the outsourcing of critical or important functions.

Step 4 – Contractual Phase – Setting up the Outsourcing Agreement

For **each** outsourcing relationship, **not only for critical or important functions,** there must be a sound outsourcing arrangement in writing in place that clearly allocates the rights and obligations of the institution concerned.

Agreement must set out **general terms,** such as:

- a clear description of the services concerned;
- the start and end dates for the agreement;
- the applicable law
- the sub-outsourcing permit;
- the location(s) where the critical or important functions will be provided;
- where relevant data will be kept and processed, including possible storage locations;
- the conditions to be met, including the requirement to notify the institution concerned if the service provider proposes to change location(s);
- liability clauses;
- termination rights; and,
- cooperation with competent authorities.

The following conditions must also be encompassed:

- **Sub-outsourcing:**
  a. whether or not the sub-outsourcing of critical or important functions is permitted;.
  b. confirmation of any change in use made of a sub-outsourcing provider based on a properly conducted risk assessment of the sub-outsourcing provider concerned;
  c. full compliance by the sub-outsourcing and direct outsourcing provider with all applicable regulations in the country where the commissioning institution is established.

- **IT and data security:**
  a. detailed data and system security requirements and ongoing compliance monitoring procedures (appropriate data security standards);
  b. procedures for monitoring GDPR compliance
  c. the agreed **location of data storage** and processing facilities (EU and non-EU).

- **Access, information and audit rights:**
  a. the grant of full **access** to the accounts and relevant business premises (head offices and operational centres), including to all devices, systems, networks, information and data used for providing the outsourced service, financial information, personnel and the service provider`s external auditors (“access rights”), to:
     i. the **outsourcing institution;**
     ii. the **national competent authority;**
     iii. the **outsourcing institution’s auditor.**
  b. the grant to the outsourcing institution of the right to inspect and audit the outsourcing provider.

For **critical and important functions** that are outsourced, the following must, inter alia, likewise be covered:

- ongoing monitoring of the service provider’s performance;
- precise **quantitative and qualitative** definitions of performance targets **(KPIs);**
- reporting requirements in the event of any defect and any foreseen changes potentially affecting the service provided;
- the **financial obligations** of the parties;
- mandatory insurance to cover given risks;
- the implementation and testing of business contingency plans;
- termination rights;
- data access in the event of the insolvency of the service provider.

These principles must be followed **for all new contracts as from 1 July 2019.** Existing contracts that do not comply with these standards **must be amended** on the first review data but no **later than 31 December 2020.**

Step 5 – Ongoing assessment – Oversight requirements and information duties

Outsourcing arrangements have to be **monitored constantly** applying the aforementioned principle of proportionality. The focus shall be on critical or important functions which are outsourced.

Nevertheless, it is imperative to integrate the risk assessment criteria indicated above and that have to be **applied ex-ante,** in the ongoing risk management process. This can be done by the integration into the internal controls system **(ICS)** and by defining key control indicators **(KCIs).**

The measurement and management of third-party risks has then to be **reported regularly to senior management.**

Step 6 – Duty to inform and audit and access rights

The whole framework is aimed at increased transparency and **more effective risk management.** Information is therefore the key.

Hence, investment firms and payment institutions must make **available to the competent authorities** the **register of all existing outsourcing arrangements** in a common data base format **as part of each supervisory review** and evaluation process undertaken every three years or on request by the competent authority. They should also **inform the competent authority** in a timely manner when they plan to enter **into a new outsourcing agreement,** and likewise notify it promptly and adequately if a function became **critical or important.** Finally if material changes and severe events could have a material impact on the continuing provision of business activities.

In addition, the right to unilaterally collect information through **on-site visits and or audits** is also a very efficient measure for ensuring proper third-party risk management.

- **Access** – provision must be made in outsourcing contracts and in the overall framework for the investment firm, its auditor and the national competent authority to be able to access the data of the company providing the outsourced service and even premises used for provision of that service.
- **Internal audit** – to ensure that the quality of the provided services is compliant with the applicable standards, such as GDPR, MiFID II, PSD II, CRR, etc., the investment firm must be granted the right to perform audits on the premises of company providing the outsourced service.

	Non-critical or unimportant	Critical or important
ISAE 3000	Y	N
ISAE 3402 – Type 1	Y	N
ISAE 3402 – Type 2	N	Y

- **External audit** – provision must be made for external audits to be conducted by audit firms, on the basis of the following audit standards.

Step 7 – Exit strategy

Institutions must include a clearly defined exit strategy for all outsourcing of critical or important functions in their outsourcing policy that allows, at the very least, for the possibility of terminating the outsourcing arrangements in the event of:

- the failure of the service provider; and/or
- a material deterioration in the service provided.

They must be able to exit any outsourcing arrangements to **avoid any negative impact** on their business, **adverse effects on their compliance with the regulatory framework** or detriment to the continuity and quality of its service provision to clients.

It is therefore important to put in place:

- **Exit plans:** based on objectives, developed and implemented, comprehensive, documented and sufficiently tested, and that include the performance of business impact analyses, and well-defined indicators to be used for monitoring of the outsourcing arrangement;
- **Alternative solutions:** identified and developed transition plans;
- **Roles, responsibilities** and **sufficient resources**
- **Success criteria**
- Proper **resource planning:**

4.3 Outsourcing framework

Ongoing monitoring and the well-balanced assignment of responsibilities and duties to the corresponding resources in an organization calls a **highly efficient outsourcing framework.** The more complex a group of financial institutions is, the greater the importance of a sound framework is.

This is especially true when **the corporate structure deviates from the functional structure,** which is frequently the case in centralised group organizations.

A sound framework must encompass the deliverables, roles and responsibilities set out below.

Outsourcing Policy

As always, a policy with its underlying processes is the key to implementing a defined ruleset differentiating between:

- **Outsourcing of critical or important function** and other outsourcing arrangements;
- **Outsourcing to service providers** authorised by a competent authority and those which are not;
- **Intra-group outsourcing arrangements,** outsourcing arrangements within the same institutional protection scheme, including entities fully owned individually or collectively by institutions within the institutional protection scheme, and outsourcing to entities outside the group;
- **Outsourcing to service providers** located within the EU/EEA and **outside** the **EU/EEA.**

It is essential that the policy can be implemented and therefore be applicable on a **consolidated, sub-consolidated and individual basis** to all institutions in a group.

A generic "table of content" is given below, but it goes without saying that it has to be tailored to the individual setup of the group concerned.

Outsourcing Policy 1.0

Table of content

New roles and responsibilities

A new role, that of an **Outsourcing Officer,** is introduced.

This function is responsible for the proper functioning of the entire outsourcing framework. It is important that conflicts of interests are avoided and thus it is likely that the outsourcing officer will be found in the **2nd level of defence.**

Moreover, **it is the clear responsibility of the senior management to ensure that the EBA Outscoring Guidelines are implemented and that the institution's governance is working properly. The Outsourcing Officer has a regulatory duty to report (monthly) to the senior management to address any issues and/or risks.**

The senior management and the Outsourcing Officer must ensure that sufficient resources – internally or externally – are available to comply with the Guidelines.

For **each and every outsourcing relationship, one person has to be accountable** and thus needs to be assigned to this role and disclosed in the **outsourcing register.**

Third-party risk management

Risk assessment of third parties is a key measure in the entire outsourcing framework. The complexity arises when an investment firm has many outsourcing partners, especially from **non-EU countries and FinTech companies** that are not regulated.

Therefore, a sound and **well-organized third-party risk management** has to be put in place.

Register of all outsourcing activities

Institutions must maintain a register of all outsourcing arrangements at **institutional and group level,** and document and record **all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements.**

This is applicable to **all entities within a group** and the register must be kept at **individual entity** level **and at group level.**

The register must include the following at the very least and have the following structure.

Outsourcing register

Table of content

1 A reference number for each outsourcing arrangement.
2 A brief description of the function that is outsourced.
3 An indication of whether the function is considered to be critical or important, the reasons why this is the case and the date of the last assessment.
4 Whether or not personal and confidential data are processed, transferred or held by the service provider.
5 The institutions and other entities falling within the scope of prudential consolidation that make use of the outsourcing agreement, including their names.
6 Information on the outsourcing provider:
  6.1 Name and registered address;
  6.2 Country of registration and LEI, or if this is unavailable, the company registration number.
  6.3 The parent company, where applicable.
  6.4 Whether or not the service provider, or sub-service provider, is part of the institution's own group, based on the scope of accounting consolidation.
  6.5 The country or countries in which the outsourced function will be performed by the service provider, or the sub-service provider.
  6.6 The country or countries where the data will, or will potentially, be stored.
7 Information on outsourcing of critical or important functions and outsourcing to Cloud service providers.
  7.1 The date of the last risk assessment and a brief summary of the main findings.
  7.2 The individual or decision-making body or committee in the institution that approved the outsourcing arrangement (e.g. the management body).
  7.3 The law governing the outsourcing agreement.
  7.4 The start date and, as applicable, the expiry date and/or notice periods.
  7.5 The date of the last and next scheduled audit, where applicable.
  7.6 An assessment of the service provider's substitutability and/or the possibility of reintegrating the critical or important function back into the institution.
  7.7 Identification of alternative service providers in line.
  7.8 Whether the outsourcing of the critical or important function is considered time critical.
  7.9 In the case of outsourcing to a Cloud service provider, the Cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and locations where such data will be stored.
  7.10 The estimated yearly budget cost.

Conflicts of interest

Where outsourcing creates material conflicts of interest, including between entities within the same group, institutions need to take appropriate measures to identify, assess and manage those conflicts of interest.

With regard to conflicts of interests identified, institutions should ensure that the decision on an outsourcing arrangement and the oversight are performed with sufficient objectivity to be able to **manage conflicting interests appropriately.**

For those institutions that are impacted by MiFID II and other EU regulations, such as MAD MAR, any conflicts need to be **disclosed publicly** on the webpage.

Business continuity planning

Institutions should have appropriate business continuity plans in place for the outsourcing of critical or important functions.

To comply with this requirement, a financial institution can **leverage the activities already performed to comply with the BRR Directive.**

Where any failure of a service provider to provide the critical or important function would lead to a severe business disruption, **institutions should incorporate the service provider in its business continuity planning** and establish, implement and maintain business contingency plans for disaster recovery.

Such plans should be tested periodically, including the testing of backup facilities, and involve the service provider when that is part of those plans.

Such plans should also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, the political risks in the service provider's jurisdiction.

Internal audit function

The EBA Outsourcing Guidelines place particular emphasis on the importance of the 3rd line of defence: the internal audit function applying a risk-based approach. An **independent review of the effectiveness of the system in place, and the contracts in particular, must for part of the annual audit planning.** In practice, the following checkpoints must be considered in the review (not exhaustive):

1. The outsourcing arrangements for critical or important functions.
2. The degree to which data protection measures are appropriate.
3. **The internal controls.**
4. The risk management and business continuity measures implemented by the service provider.
5. Information and audit rights are sufficiently ensured, in particular for the outsourcing of critical or important functions, and that the internal audit function is able to effectively enforce such audit rights.
6. The **framework** for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulations, the risk appetite and the decisions of the management body.
7. The adequacy, quality and effectiveness of assessment of criticality or importance.
8. The adequacy, quality and effectiveness of risk assessment for outsourcing arrangements and that the risks remain within the risk appetite.
9. The **risk appetite, risk management and control procedures** of the service provider are in line with the institution's strategy.
10. Appropriate involvement of governance bodies.
11. Appropriate monitoring and management of outsourcing arrangements.

5. Conclusion and impact on the financial industry

The impact for market players, irrespective of whether or not they are directly or indirectly affected, is relatively high due to the far-reaching consequences of this framework. Moreover, **it is virtually impossible to isolate an institution to avoid being affected in any way.** The reasons for this are set out below:

Impact on third-country firms

In third countries, there are two major players who are affected:

1. financial institutions outsourcing certain services to providers, and
2. outsourcing providers providing services to regulated financial institutions in the EEA.

In the first case, when a third-country financial institution is consuming services outsourced to a provider, the financial institution will be affected if it **has any regulated entities in the EEA.** Moreover,consuming services outsourced to an **EEA provider** might indirectly affect institutions since the EEA provider will apply its own contractual standards to your relationship.

In addition, financial intermediaries **claiming to be compliant with EU regulations such as MiFID II, IDD, BRRD, MAD MAR, PSD II,** etc., must apply the same standards since all of these regulations **refer to these new Guidelines** as laying down the standards to be met.

Thus, the impact is relatively high if an institution has any touchpoint with the EEA.

Impact on banks and payment service providers

For regulated financial intermediaries in the EEA, these Guidelines apply in full and must **form part of their audit plan;** the impact is thus very high.

This is also true for a **group with its head office outside the EEA but with responsibility for a regulated entity in the EEA** since the parent company must also apply these standards.

Impact on FinTechs/RegTechs

This is probably the most important and significant, but also the most surprising, impact of the new Guidelines as a whole.

Although the European regulator has not yet regulated FinTechs/RegTechs directly, they are now regulated indirectly since their clients (financial intermediaries) need to obtain assurance that all outsourced services comply with the regulatory standards applicable to financial intermediaries in the EU either through:

1. Internal audits; or,
2. External audits – ISAE 3000 or ISAE 3402

If a FinTech/RegTech wants to scale up its business and wants to **avoid having to persuade its clients each and every time that the outsourcing service provided is compliant** with the standards currently applicable, it must provide **ISAE reports** that set out, in a standardized manner, the level of compliance.

6. What is the legal ground?

- CRD IV – REGULATION (EU) No 575/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
- MiFID II – DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
- DIRECTIVE 2013/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC
- PSD II – DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
- e-Money Directive – DIRECTIVE 2009/110/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC
- Recommendation on Outsourcing to Cloud Service Providers – EBA/REC/2017/03
- BRRD – DIRECTIVE 2014/59/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council
- COMMISSION DELEGATED REGULATION (EU) 2016/778 of 2 February 2016 supplementing Directive 2014/59/EU of the European Parliament and of the Council with regard to the circumstances and conditions under which the payment of extraordinary ex post contributions may be partially or entirely deferred, and on the criteria for the determination of the activities, services and operations with regard to critical functions, and for the determination of the business lines and associated services with regard to core business lines
- GDPR (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Draft Guideline – EBA/CP/2018/11 of 22 June 2018 Consultation Paper on EBA Draft Guidelines on Outsourcing Arrangements

Contacts

Dr. Günther Dobrauz
Partner, Leader PwC Legal Switzerland
PwC Switzerland
+41 58 792 14 97
guenther.dobrauz@ch.pwc.com

Michael Taschner
Director, Head Strategic Legal Regulatory
PwC Switzerland
+41 58 792 10 87
michael.taschner@ch.pwc.com

Vanessa Dutzi
Assistant Consultant Legal
FS Regulatory and Compliance Services
PwC Switzerland
+41 58 792 47 59
vanessa.dutzi@ch.pwc.com

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00