Outsourcing to Blanco Investment firms

August 2021

(machine translation)

Inhoud

1. Introduction

Outsourcing is an important issue, both for you on a day-to-day basis and in the eyes of supervisors. In the sector letter of November 2019, the AFM wrote:

"Outsourcing of work takes place a lot and usually follows from a striving for more efficient management by a company. Outsourcing can, for example, contribute to an improvement in quality and/or a reduction in service costs. However, outsourcing also involves risks. Companies must ensure that the risks arising from outsourcing are managed, regardless of the reason for outsourcing. The core of outsourcing risks lies in the fact that a company does not carry out the work itself, but remains responsible for it. Responsibility (and therefore liability, if any) cannot be transferred to a third party.

A company can only mitigate the risk that a third party does not carry out the work or carries out the work of insufficient quality by maintaining (continuous) control over this work. This means that a company is expected to 1) have a full understanding of all work carried out by third parties, 2) have knowledge of all outsourcing rules that apply to it and 3) have taken the necessary measures to control the risks arising from the outsourcing."

Because Blanco and AIRS (hereafter together referred to as 'Blanco') would like to be good outsourcing partners, we think it is only logical to offer you some support with your outsourcing. With this 'Blanco-paper' we would like to give you some text and explanation about your (general) obligations and the way in which Blanco can help you meet these obligations when you outsource to Blanco.

We realise that the size of the document is not really inviting, but unfortunately outsourcing is an extensive subject about which much has been written. We have tried to structure this information for you in the best possible way, so that it might be easier for you to find your way through all the publications that are available.

2. Legislation and regulation

2.1. Outsourcing, yes or no?

Let us start at the beginning. As an investment firm, you must comply with the outsourcing rules set out in MiFID II (and implemented in national law). But to determine whether you need to comply with the outsourcing rules, it is important to first determine when there is actually outsourcing as referred to in the law.

Outsourcing occurs when critical and important operational functions of an investment firm are performed by a third party. This is an agreement between the investment firm and a third party under which the third party performs a process, service or activity that would otherwise be performed by the investment firm itself. As an example: depositing funds and financial instruments with a custodian bank is not an outsourcing, because this process (in most cases) is not part of your own licence.

This is also confirmed bty the AFM. But beware! If your custodian bank also provides other services, it is possible that this is outsourcing. The law also gives examples of tasks that do not qualify as outsourcing, such as legal advice and the purchase of price information services. The use of a portfolio management system, for example, does qualify as outsourcing. It is therefore advisable to take a critical look at the parties you use and to determine for each party whether the service qualifies as outsourcing, as purchasing or as a collaboration.

2.2. Legislative requirements

If you have established that there is indeed outsourcing as referred to in the law, you must comply with the legal requirements set out in Article 31 MiFID II Delegated Regulation. We will go into more detail on these legal obligations in this document, but if you are interested in the literal text of the legal obligation, it reads as follows:

1. Investment firms that outsource critical or important operational functions shall remain fully responsible for discharging all their obligations under Directive 2014/65/EU and shall comply with the following conditions:
a) outsourcing does not result in the delegation by management of its responsibility;
b) the relationship and obligations of the investment firm towards its clients under Directive 2014/65/EU are not modified;
c) the conditions with which the investment firm must comply in order to obtain and maintain authorisation in accordance with Article 5 of Directive 2014/65/EU are not undermined;
d) none of the other conditions under which the firm's authorisation has been granted shall be removed or modified.

2. Investment firms shall exercise due skill, care and diligence when entering into, managing or terminating any agreement to outsource critical or important operational functions to a service provider and shall take the necessary steps to ensure that the following conditions are met:

a) the service provider has the ability, capacity, sufficient resources, appropriate organisational structure to support the performance of the outsourced tasks and any authorisation required by law to perform the outsourced tasks reliably and professionally;

b) the service provider implements the outsourced services effectively and in compliance with the applicable legislative, regulatory and administrative requirements and, to that end, the undertaking has put in place methods and procedures to assess the level of performance of the service provider and to monitor on an ongoing basis the services provided by the service provider;

c) the service provider adequately supervises the performance of the outsourced tasks and adequately manages the risks associated with the outsourcing;

d) appropriate action is taken if it appears that the service provider is not performing the tasks efficiently and in compliance with the applicable legal and regulatory requirements;

e) the investment firm effectively supervises the outsourced functions or services and manages the risks associated with the outsourcing and, for that purpose, retains the necessary expertise and resources to effectively supervise the outsourced functions and manage those risks;

f) the service provider has informed the investment firm of any development that may materially affect his or her ability to perform the outsourced functions efficiently and in compliance with applicable laws, regulations and administrative requirements;

g) the investment firm may, if necessary, terminate the outsourcing agreement with immediate effect where this is in the best interests of its clients, without prejudice to the continuity and quality of its services to clients;

h) the service provider cooperates with the competent authorities of the investment firm in relation to the outsourced functions;

i) the investment firm, its auditors and the relevant competent authorities have effective access to data relating to the outsourced functions and to the relevant premises of the service provider where necessary for the purposes of effective supervision in accordance with this Article, and the competent authorities may exercise those access rights;

j) the service provider shall protect any confidential information concerning the investment firm and its clients;

k) the investment firm and the service provider have established, implemented and maintained a contingency plan providing for contingency management and periodic monitoring of back-up facilities where this is necessary in view of the outsourced function, service or activity;

l) the investment firm has ensured that the continuity and quality of the outsourced function or service is maintained even in the event of termination of the outsourcing by either transferring the outsourced function or service to another third party or performing the outsourced function or service itself;

3. The respective rights and obligations of the investment firm and the service provider shall be clearly defined and set out in a written agreement. In particular, the investment firm shall retain its rights of instruction and termination, its right of information and its right of inspection and access to the books and business premises. The contract shall ensure that outsourcing by the service provider is only carried out with the written consent of the investment firm.

4. Where the investment firm and the service provider belong to the same group, the investment firm may, for the purposes of compliance with this Article and Article 32, take into account the extent to which the firm controls or is able to influence the actions of the service provider.

5. Investment firms shall make available to the competent authority, at its request, all information necessary to monitor compliance with the requirements of Directive 2014/65/EU and its implementing measures in the performance of outsourced functions.

3. Guidelines

Because legislation is often risk-based, and therefore leaves room for individual interpretation, it is sometimes difficult to determine when you meet the requirements of the law. That is why guidelines are published regularly by various supervisory authorities, such as the EBA, DNB and AFM.

3.1. EBA Guidelines on Outsourcing

The EBA has published the final guidelines on outsourcing in 2019. The guidelines can be found on the following page: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements. The guidelines prescribe various governance requirements when entering into outsourcing arrangements. It is a very voluminous document, but can help you form a better idea of what can be expected of you as an investment firm.
To make it easier for you - as far as possible - we have included a table in Appendix 1 of this document that lists the various guidelines. You can use this table to indicate per guideline how you are compliant, or you can indicate that a certain guideline

does not apply to your situation. Where possible, we have also included a note in the table about how Blanco can help you meet requirements in relation to an outsourcing to Blanco.
It is also worth noting that the Guidelines emphasise that companies must (may) take into account the principle of proportionality.
You can request the table in Word version from us.

3.2. ESMA Guidelines on outsourcing to cloud service providers

ESMA published guidelines on outsourcing to cloud service providers in the summer of 2021. The Guidelines can be found on the following page: https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-providers. These guidelines apply with effect from 31 July 2021 to all outsourcing agreements regarding cloud services that enter into force, are extended or are amended on or after that date. Enterprises should review and amend existing outsourcing agreements regarding cloud services accordingly to ensure compliance with these Guidelines by 31 December 2022.
Annex 2 of this document also includes a table listing the various ESMA guidelines. You can use this table to indicate how you are compliant with each guideline, or you can indicate that a particular guideline does not apply to your situation. Where possible, we have also included a note in the table about how Blanco can help you meet requirements in relation to an outsourcing to Blanco.

You can request the table in Word version from us.

4. The obligations

4.1. Policy

Any investment firm that outsources or plans to outsource activities should have a sound outsourcing policy. In accordance with EBA guidelines, an outsourcing policy should cover the life cycle of outsourcing arrangements and define the principles, responsibilities and processes in relation to the outsourcing. See Appendix 1, Guideline 41 and further for more information on outsourcing policies.

In its recent question on outsourcing, the AFM also gave an indication of the elements that can be included in the outsourcing policy and/or with which the outsourcing policy must comply:

The outsourcing policy...

- is in line with the strategy of the organisation;
- is established at senior level, for example by the board or a delegated officer;
- is defined at group level;
- prescribes that a business case is determined for each outsourcing;
- prescribes that the requirements for the supplier and the service provision are defined for each outsourcing;
- requires decision-making at senior level for each outsourcing;
- requires a risk analysis for each outsourcing;
- requires measures to be taken to mitigate unacceptable risks;
- requires compliance to be involved in the decision to outsource;
- requires that for each outsourcing, legal requirements are identified and weighed and that a due diligence investigation is carried out prior to each outsourcing;
- requires rights, obligations and responsibilities to be contractually defined;
- requires contractual provisions to be reviewed in advance by compliance, JZ and the business;
- requires statutory provisions such as right to examine and right to audit to be included in outsourcing agreements, where applicable;
- contains guidelines for the service levels to be agreed;
- contains guidelines for the reports to be agreed and frequency of reporting;
- requires that continuity risks are periodically identified and evaluated;
- requires continuity guarantees from suppliers to be assessed at least annually;
- requires a continuity plan to be drawn up for each outsourcing;
- stipulates that in relation to continuity risks and guarantees, subcontractors are also included in the scope;
- prescribes that the follow-up of wishes and requirements with regard to the provision of services must be assessed periodically;
- requires that for each outsourcing, assurance on the system of internal control is provided periodically;
- prescribes that information security is part of the periodic assurance provided by the service provider about the services provided;
- requires that, for each outsourcing, the company records that it owns the data and ensures access to that data;
- requires that data portability of the data is contractually established;
- requires the service provider to provide an up-to-date insight into the location of the data;

- contains guidelines for an exit strategy.

It is important to regularly evaluate and update the outsourcing policy so that it is always in line with the investment firm's organisation and developments in legislation and regulations.

4.2. Selection and evaluation procedure

Because as an investment firm you remain responsible for the outsourced activities, you should carefully select your service providers. In accordance with EBA guidelines (number 70), the service provider must have a number of characteristics. In order to help you on your way with regard to your outsourcing to Blanco, we are happy to provide you with input that can help you test the properties. Of course it is also up to you to critically assess Blanco and to ask us for extra information if you need it for your assessment.

Property in accordance with EBA guidelines	Blanco
A good reputation	Blanco has a good reputation. Blanco has many satisfied customers; we are therefore enormously proud of our high retention score! On our website https://www.useblanco.com you can find some testimonials from satisfied customers. And perhaps unnecessarily, but important to mention: none of Blanco's stakeholders (directors, supervisory directors, employees, investors, etc.) have ever received negative publicity, and all have a good reputation.

Appropriate and adequate competencies	In order to be the perfect partner for our licensed clients, Blanco itself is (almost entirely) set up as a regulated company and we have people with the right specialties on board: certified compliance officers, EDP auditors, privacy professionals and risk experts.
Expertise	Blanco has extensive experience and expertise in the relevant market. Blanco employs many people with a background in banking and/or experience in the sector, so that they can think along with the client and offer appropriate services.
The capacity	Blanco builds scalable and innovative solutions that automate key processes within a licensed organisation. This means that less manual work is required, reducing the need for human resources, both in the customer and in Blanco itself. Of course, Blanco will always ensure that it has a large and knowledgeable team in place to properly service all of its clients
The resources (human, IT, financial)	Staff: Blanco ensures that there is always sufficient staff on board to serve customers well. IT: Blanco develops and runs in the cloud at Amazon (AWS). The great advantage of this is that the latest technology can be used and the data capacity is infinitely scalable. Financial: Blanco is largely funded by professional venture capital parties, such as KBC Focus Fund, Volta Ventures and Dutch Founders Fund. For more information see: https://www.useblanco.com/about- us#investors

The organisational structure	In its organisational structure, Blanco takes into account the fact that its clients are all financial enterprises. Blanco therefore has all relevant disciplines in house to be able to serve its clients optimally. For more information see also: https://www.useblanco.com/governance
If applicable, the required legal licence or registration.	Not applicable. Blanco does not carry out any licensed activities itself.

The AFM also indicated in its 2019 sector letter what should be considered when using a selection procedure. In addition to the EBA's suggestions, the following points of attention are mentioned:

Focal points AFM	Blanco
The appointment of third parties does not lead to uncontrollable concentration risks	Because Blanco is a 'one-stop-shop', supporting various processes within your organisation, there could be a concentration risk. However, the existence of a risk does not have to be an immediate problem, provided good control measures are in place. To help you substantiate the control measures with regard to this concentration risk, we have made a start with mitigating measures further on in the document (and specifically in Annex 3).

The third party has adequate technical and organisational measures in place for the protection of personal or confidential information of the enterprise	As an IT provider and a processor of personal data, Blanco has of course implemented adequate technical and organisational measures. In summary, Blanco has taken the following measures: • Blanco has implemented an information security policy and framework; • Blanco personnel are screened and a confidentiality agreement is part of the employment contract; • Blanco has implemented physical and logical access control. Two-factor authentication is used where possible. In addition, there are special access restrictions; • Blanco has an incident and data breach policy and will immediately inform the client of personal data breaches and other serious security incidents; • Blanco is responsible for appropriate logging and control of access to personal data; • Blanco regularly tests compliance with the policy and the quality of the security measures. Information security and privacy are topics that are in scope of the ISAE3402 of Blanco, and are therefore audited by an independent auditor. On request, we can provide you with further information on how Blanco has organised its information security.

The third party enters into an agreement that clearly defines the rights and obligations of the company, including a guarantee that the company will be able to continuously fulfil its monitoring and control obligations after outsourcing.	See the topic 'Contract' in this document for more information on the Blanco Agreement.
The Company has established methods and procedures for assessing and reviewing material developments at and the performance level of the third party on an ongoing basis	It is of course up to you to assess the level of performance of Blanco. Blanco has included service levels in the agreement, which can help you to assess the service.
The company ensures that sufficient expertise and resources are retained within the company to effectively supervise the outsourced activities and to understand and control the outsourcing risks.	You need to ensure that sufficient expertise and resources are retained. We would like to emphasise that at Blanco we believe in a symbiosis between man and machine. Our smart fintech solutions save a lot of time and money, but always integrate the human factor: we don't want to impose our technology 'from above', but rather to let it serve the people. This means that you can make active use of the software yourself and, in this way, directly supervise the work and immediately identify (operational) risks.
The company guarantees that the continuity and quality of the work will be maintained when the outsourcing is terminated by transferring the work to a third party or by taking it over itself. a third party or taking it over itself.	The agreement with Blanco contains an exit clause that includes agreements on the termination of the relationship. For more information, see the subject 'Contract' in this document.

Risk analyses

An important part of the outsourcing process is to make a risk analysis and perform a due diligence on the new service provider. In its recent questionnaire on outsourcing, the AFM provided an indication of the elements that may be included in the due diligence procedure.

The due diligence procedure...

- requires assessment of financial risks, including the financial situation of the service provider
- requires assessment of risks for the (quality of service to the) client and for society
- requires assessment of the risk of vendor lock-in
- requires assessment of continuity risks
- requires an assessment of concentration risks
- requires an assessment of conflicts as a result of cultural differences between your company and the supplier
- requires an assessment of information security risks
- requires an assessment of political risks such as risks related to the location of data
- requires assessment of risks due to conflicts of interest
- distinguishes between intra-group outsourcing and regular outsourcing
- requires that at least JZ, Risk, Compliance and the business are involved in the due diligence
- tests whether the service provider can comply with at least all legal requirements
- assesses whether and to what extent the service provider can meet the wishes and requirements of the organisation.

The main risks have been included by DNB in a 'risk analysis template for outsourcing'. Investment firms can use this template and supplement it with other risks where necessary. See for more information: https://www.toezicht.dnb.nl/5/50- 237322.jsp In Annex 2 of this document, the template of DNB is included and we have also made a remark about mitigating measures when outsourcing to Blanco, where possible. And again: we are happy to think along with you, but you will have to perform a critical analysis yourself.

3.2. Contract

Based on guideline 75 of the EBA guidelines, the outsourcing contract must contain at least the following topics. Please indicate below whether the (standard) agreement with Blanco addresses the subject and if so, how.

EBA-guidelines	Blanco
A clear description of the outsourced function to be performed.	The Agreement (Delivery Agreement) with Blanco contains a description of the delivered software and/or service.
The start date and end date, if any, of the contract and the notice periods for the service provider and the institution or payment institution	The agreement always contains a start and end date, including termination clause(s).
The legislation applicable to the agreement	The applicable law is always part part of the agreement.
The financial obligations of the parties	The financial obligations are always part of the agreement.

Whether the sub-outsourcing of a critical or important function, or material parts of such a function, is permissible and, if so, the conditions applicable to the sub-outsourcing as set out in Section 13.1	Subcontracting is possible under the Agreement; a good example of subcontracting at Blanco is the cloud provider (Maincubes and AWS). In addition, Blanco uses its platform to access services from third parties, such as ComplyAdvantage, the Chamber of Commerce and Mitek. Not all conditions for subcontracting are made concrete in the Agreement, but Blanco must always inform the customer on the basis of the Agreement if after the commencement of the services a new party is subcontracted. In that case, Blanco can always be asked for additional information regarding the party in question and if the subcontracting is not approved, the client has the possibility to not use or use differently a part of the service or to terminate the agreement. Blanco always conducts a thorough investigation into the parties to whom work is subcontracted.

The location(s) (i.e. regions or countries) where the critical or important function will be performed and/or where the relevant data will be held and processed, including the possible storage location, and the conditions to be met including the requirement to notify the institution or payment institution if the service provider proposes to change the location(s)	Blanco processes data in the Netherlands and Belgium, using the services of Maincubes (Netherlands) and of AWS (Frankfurt region - Germany). Other third parties and the location of data processing are included in the Delivery Agreement. The processing agreement includes the technical and organisational measures that Blanco takes. These measures and others are in scope of the ISAE3402. On request, Blanco can provide further information regarding the information security.
Where relevant, provisions on the accessibility, availability, integrity, privacy and security of the data concerned, as set out in Section 13.2;	See above. Information security is a very important topic within Blanco and is part of the ISAE3402. On request, Blanco can provide further information about the information security.
The right of the institution or payment institution to monitor the performance of the service provider on an ongoing basis;	The customer acquires this right in various ways. Firstly, a service level agreement is agreed upon. In addition, the agreement contains a right to audit and the client can view the ISAE3402 report. Of course, the client can also check the performance on a daily basis and contact us if the service is not satisfactory.

The service provider's obligations regarding reporting to the institution or payment institution, including the reporting by the service provider of any development that may have a material impact on the service provider's ability to perform the critical or important function effectively in line with agreed service levels and in accordance with applicable laws and regulations and, if applicable, the obligation to provide reports from the service provider's internal audit function	The agreement provides that Blanco will inform the client if there are any changes that may impact on the service.
Whether the service provider is subject to compulsory insurance against certain risks and, if so, the required level of insurance cover	The obligation to insure is not included in the Agreement, but Blanco does, of course, have professional liability insurance. Upon request, inspection of the policy can be obtained.

Provisions to ensure access to data owned by the institution or payment institution when the service provider is insolvent, in the process of being wound down or ceases its business activities	The agreement stipulates that the customer's data remains the property of the customer. The client has an instruction right with regard to its data, as included in the processing agreement. In case of bankruptcy of Blanco, a continuity measure has been contractually agreed upon, whereby a foundation temporarily takes over the services of Blanco, so that the investment firm can select another supplier or can decide to carry out the services itself. The continuity agreement also includes a right to instruct.
The obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them	This obligation is part of the agreement.
For institutions, a clear reference to the powers of the national resolution authority, in particular to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'material liabilities' of the contract within the meaning of Article 68 of that Directive	This provision is generally not applicable.

The unrestricted right of institutions, payment institutions and competent authorities to inspect and monitor the service provider, in particular in respect of the critical or important outsourced function, as stated in paragraph 13.3	This obligation is part of the agreement.
Termination rights, as set out in section 13.4	In the agreement, agreements are made about termination of the agreement. There is also a provision with regard to exit assistance, whereby Blanco indicates it will facilitate a transfer to a successor service provider.

If you have concluded a contract with Blanco or AIRS some time ago, it could be that (partly due to the entry into force of new legislation or publication of additional guidelines) your contract does not contain all the information as mentioned above. In that case you can ask us for the required information or you can conclude a new contract with us - obviously without any substantial changes to its contents as regards, for example, its duration or rates.

3.2. Notification of supervisory authority

Investment firms must report to the AFM any material activities that the investment firm has outsourced. This concerns activities that relate to the primary process of the firm. The notification must be made before the activity is outsourced to a service provider. For more information and the notification form, see: https://www.afm.nl/nl-nl/professionals/onderwerpen/uitbesteding-doorlopend-melden-bobi

Almost all the information you need can be found in this document and/or in the agreement you conclude or have concluded with Blanco. Additional information can always be requested.

Evaluation of the outsourcing

During the term of the agreement, you should regularly evaluate your service providers. This includes evaluating changes that occur at the service provider, such as a significant change in ownership, strategy or profitability. (As indicated above, the Blanco Agreement already provides that Blanco will inform you of relevant changes in the business and/or product as they occur).

In order to structure the evaluation of your service providers, it is recommended to set up an evaluation procedure. In its recent questionnaire on outsourcing, the AFM gave an indication of the elements that may be included in the evaluation procedure.

The quality assessment...

- states that quality requirements for outsourced services are measurably defined
- states that quality requirements for outsourced services have been agreed and laid down in writing in service level agreements
- states that for each outsourcing, it must be agreed what steps/procedures and consequences follow if the agreed quality levels are not met
- requires the service provider to provide the enterprise with insight into the actual service levels achieved within the agreed frequency
- Requires that the enterprise has the right and opportunity to investigate the service provider on the quality of service delivery.
- obliges the service provider to report incidents in relation to the service at a frequency agreed in advance
- prescribes the steps/procedures that the enterprise follows when the service provider does not meet the contractual requirements
- prescribes that continuity risks are periodically identified and evaluated
- requires that continuity guarantees from suppliers be assessed at least annually
- requires periodic evaluation of the follow-up of service wishes and requirements
- requires that for each outsourcing, assurance on the system of internal control is provided periodically
- requires that information security is part of the periodic assurance that the service provider provides on the services offered.

With regard to the outsourcing to Blanco, we have already indicated above that Blanco tries to facilitate the evaluation of the services in various ways. In the first place, a service level agreement is agreed upon, which is also reported on. The agreement also contains a right to audit and the client can view the ISAE3402 report. In addition, the customer can of course check the performance on a daily basis and contact the service provider if it is not satisfactory.

https://www.afm.nl/nl- nl/professionals/onderwerpen/uitbesteding-doorlopend-melden-bobi

3.3. Register

Investment firms should keep a register with information on all outsourcing. According to the EBA guidelines (Guideline 54), this register should contain the following information:

a) a reference number for each outsourcing arrangement
b) the start date and, if applicable, the next renewal date, end date and/or notice period for the service provider and for the institution or payment institution
c) a brief description of the outsourced function, including the data which is outsourced and whether personal data is transferred or not (e.g. indicating yes or no in a separate data field), or whether processing is outsourced to a service provider
d) a category assigned by the company reflecting the nature of the function as described in point (c) (e.g. information technology (IT), control function), which facilitates the identification of different types of arrangements
e) the name of the service provider, the trade register number, the legal entity identification code (if available), the registered address and other relevant contact details, and the name of the parent company (if available)
f) the country or countries where the service is to be provided, including the location (i.e. country or region) of the data
g) whether the outsourced function is regarded as critical or important (yes/no) and, if so, a brief summary of the reasons why the outsourced function is regarded as critical or important
h) in the case of outsourcing to a cloud service provider, the models for the cloud services and deployment, i.e. public/private/hybrid/common, and the specific nature of the data to be retained and the locations (i.e. countries or regions) where those data are stored
i) the date on which the criticality or importance of the outsourced function was last assessed.

For the purpose of outsourcing critical or important functions, the register shall contain at least the following additional information:

a) the institutions, payment institutions and other undertakings within the prudential consolidation or the institutional protection scheme, as the case may be, which benefit from the outsourcing
b) whether the service provider or sub-service provider belongs to the group or is part of the institutional protection scheme or is owned by institutions or payment institutions within the group or is owned by the members of an institutional protection scheme
c) the date on which a risk assessment was last carried out and a brief summary of its main findings;

d) the person or decision-making body (e.g. the management body) in the institution or payment institution that has approved the outsourcing arrangement;
e) the legislation applicable to the outsourcing arrangement
f) the dates of the most recent and subsequent scheduled audits, if applicable
g) where applicable, the names of subcontractors to whom material parts of a critical or important function have been subcontracted, including the country in which the subcontractors are registered, where the service will be provided and, where applicable, the location (i.e. country or region) where the data will be stored
h) the outcome of the assessment of the substitutability of the service provider (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the institution or the payment institution or the impact of termination of the critical or important function;
i) alternative service providers in accordance with point (h);
j) whether the outsourced critical or important function supports time-sensitive business activities
k) the estimated annual budget cost.

Bijlage 1 – EBA Guidelines on outsourcing

	Guidelines	Implementation at investment firm (Input blanco when performing analysis)
	Title I - Proportionality: application within groups and institutional protection schemes	
	1. Proportionality	
18.	Institutions, payment institutions and competent authorities shall take into account the principle of proportionality when complying with, or monitoring compliance with, these guidelines. The objective of the proportionality principle is to ensure that governance arrangements, including those concerning outsourcing, reflect the individual risk profile, the nature and business model of the institution or payment institution and the size and complexity of its operations, so that the objectives of the regulatory requirements are effectively met.	Take into account the principle of proportionality

19.	Institutions and payment institutions shall, when applying the requirements of these guidelines, take into account the complexity of the outsourced functions, the risks posed by the outsourcing arrangements, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their operations	Take into account the principle of proportionality
20.	When applying the principle of proportionality, institutions, payment institutions and competent authorities shall take into account the criteria set out in Title I of the EBA guidelines on internal governance in accordance with Article 74(2) of Directive 2013/36/EU.	Take into account the principle of proportionality
	2. Outsourcing by groups and institutions affiliated to an institutional protection scheme	
21.	In accordance with Article 109(2) of Directive 2013/36/EU, those guidelines shall also apply on a sub-consolidated and consolidated basis, taking into account the scope of prudential consolidation. To this end, EU parent undertakings or the parent undertaking in a Member State shall ensure that internal governance arrangements, processes and mechanisms in their subsidiaries, including payment institutions, are consistent, well-integrated and adequate so as to ensure the effective application of these guidelines at all relevant levels.	This section is often not applicable

22.	Institutions and payment institutions in accordance with point 21 and institutions using centrally imposed governance arrangements as members of an institutional protection scheme shall comply with the following: a. Where such institutions or payment institutions have an outsourcing arrangement with intra-group service providers or the institutional protection scheme, the management body of such institutions or payment institutions shall remain fully responsible, including for this outsourcing arrangement, for compliance with all regulatory requirements and the effective application of these guidelines. b. Where those institutions or payment institutions outsource the operational functions of internal audit to an intra-group service provider or institutional protection scheme in order to monitor and control outsourcing arrangements, the institutions shall ensure that, also with regard to those outsourcing arrangements, those operational functions are carried out effectively, including by receiving appropriate reports	This section is often not applicable

23.	In addition to point 22, institutions and payment institutions within a group which do not benefit from exemptions have been granted in accordance with Article 109 of Directive 2013/36/EU and Article 7 of Regulation (EU) No 575/2013, institutions which are a central body or which are permanently affiliated to a central body for which no exemptions have been granted under Article 21 of Directive 2013/36/EU, or institutions that are members of an institutional protection scheme, take into account the the following: a. Where operational monitoring of outsourcing is centralised (e.g. as part of a framework contract for the monitoring of outsourcing arrangements), institutions and payment institutions shall ensure that, at least for critical or important functions which are outsourced, both the independent monitoring of the service provider and appropriate supervision by each institution or payment institution are possible, including by means of - at least annually and upon request from the centralised monitoring function - reports containing at least a summary of the risk assessment and performance monitoring risk assessment and performance monitoring. In addition, institutions and payment institutions shall receive from the centralised monitoring function a summary of the relevant audit reports on the outsourcing of critical or important functions and, upon request, the full audit report. b. Institutions and payment institutions shall ensure that their management body is properly informed of the relevant planned changes to the service providers being centrally monitored, and the potential impact of those changes on the critical or important functions performed important functions, including a summary of the risk analysis, including legal risks, compliance with regulatory	This section is often not applicable

	requirements and impact on service levels, so that the management body to assess the impact of these changes;. c. Where those institutions and payment institutions within the group, institutions affiliated to a central body institution or institutions belonging to an institutional protection scheme, rely on a centralised prior assessment of outsourcing arrangements as referred to in Chapter 12 each institution and payment institution shall receive a summary of the assessment and shall take into account its specific structure and risks in the decision-making process. d. Where the register of all existing outsourcing arrangements, as referred to in Chapter 11, is established and maintained centrally within a group or institutional protection scheme, competent authorities, all competent authorities, all institutions and payment institutions are able to obtain their individual register without undue delay. This register shall cover all outsourcing arrangements, including outsourcing arrangements with service providers within that group or institutional protection scheme. e. Where those institutions and payment institutions rely on an exit plan for a critical or important function drawn up at group level, within the institutional protection scheme or by the central body, all institutions and payment institutions shall receive a summary of the plan and satisfy themselves that the plan can be implemented effectively.	

24.	Where exemptions have been granted pursuant to Article 21 or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013, the provisions of these Guidelines shall be applied by the parent undertaking in a Member State for itself and its subsidiaries, or by the central body and its affiliated institutions as a whole.	This section is often not applicable
25.	Institutions and payment institutions which are subsidiaries of an EU parent undertaking or a parent undertaking in a Member State which has not been granted an exemption under Article 21 or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013 shall ensure that they comply with those guidelines individually.	This section is often not applicable
	Title II - Assessment of outsourcing arrangements	
	3. Outsourcing	
26.	Institutions and payment institutions shall determine whether an arrangement with a third party falls within the definition of outsourcing. In making this assessment, the extent to which the function (or part of the function) outsourced to a service provider is performed by the service provider on a periodic or ongoing basis and whether this function (or part of the function) is usually among those which could realistically be performed by institutions or payment institutions, even if the institution or payment institution has not historically performed this function itself, shall be taken into account.	See also chapter 2 of the Blanco paper
27.	Where an arrangement with a service provider involves multiple functions, institutions and payment institutions shall consider all aspects of the arrangement in their assessment, e.g. if the service provided includes the provision of hardware for data storage and the back-up of data, both aspects shall be considered together.	Always carry out a risk analysis prior to outsourcing, looking at all relevant aspects of the total outsourcing in context.

28.	As a general principle, institutions and payment institutions shall not consider the following as outsourcing a. a function which by law must be carried out by a service provider, e.g. a statutory audit; b. market intelligence services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch); c. global network infrastructures (e.g. Visa, MasterCard); d. clearing and settlement arrangements between clearing houses, central counterparties and settlement houses and their members; e. global financial messaging infrastructures supervised by the relevant authorities; f. correspondent banking services; and the purchase of services which would not otherwise be performed by the institution or payment institution (e.g. architectural consultation, legal advice and representation before courts and administrative bodies, cleaning, gardening and maintenance services relating to the institution's or payment institution's premises, medical services, maintenance of company cars, catering, vending machine services, administrative, travel or postal services, receptionists, secretaries and telephonists), goods (e.g. plastic cards, card readers, office supplies) and services (e.g. banking, insurance, insurance, securities). plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line).	For information/no remarks

	4 Critical or important functions	
29.	Institutions and payment institutions shall always consider a function to be critical or important in the following situations: a. where a defective or deficient performance would have a material adverse effect on: their continued compliance with the conditions of authorisation or other obligations to which they are subject under Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2014/65/EU, Directive (EU) 2015/2366 and Directive 2009/110/EC, and with their regulatory obligations; their financial performance; or the soundness or continuity of their banking and payment services and activities; b. where operational functions of internal control functions are outsourced, unless the assessment concludes that it would not impair the effectiveness of the internal control function if the outsourced function were not performed or performed improperly;where they plan to outsource functions of banking activities or payment services to the extent that it requires approval by a competent authority as referred to in Section 12.1.	For information/no remarks
30.	In the case of institutions, particular attention shall be paid to the assessment of the criticality or importance of functions where the outsourcing concerns functions related to core business lines and critical functions as defined in Article 2(1) points 35 and 36 of Directive 2014/5918 and identified by institutions on the basis of the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778. Functions that are necessary to carry out core or critical functions are considered critical or important functions for the purposes of these guidelines unless the institution's assessment shows that it would not have an adverse impact on the operational continuity	For information/no remarks

	of the core or critical function if the outsourced function were not provided or provided in an improper manner.	
31.	In assessing whether an outsourcing arrangement concerns a critical or important function, in addition to the results of the risk assessment as set out in Section 12.2, institutions and payment institutions shall take into account at least the following factors a. whether the outsourcing arrangement is directly related to the conduct of banking business or the provision of payment services for which they are authorised; b. the potential impact on them of any disruption to the outsourced function or of the service provider not continuously providing the service at agreed service levels: i. short- and long-term financial resilience and viability, including, where applicable, their assets, capital, costs, funding, liquidity, profits and losse ii. business continuity and operational resilience iii. operational risk, including conduct, information and communication technology (ICT) and legal risks iv. reputational risks; v. Where applicable, recovery and resolution planning, resolvability and operational continuity in the event of early intervention, recovery or resolution; c. The potential impact of the outsourcing arrangement on their ability to: identify, monitor and manage all risks; comply with all legal and regulatory requirements; conduct appropriate audits of the outsourced function;	For information/no remarks

	d. the potential impact on the services they provide to their customers; e. any outsourcing arrangements, the aggregate exposure of the institution or payment institution to the same service provider and the potential cumulative impact of outsourcing arrangements in the same area of activity f. the size and complexity of each area of activity involved; g. the possibility of scaling up the proposed outsourcing arrangement without replacing or revising the underlying agreement; h. the extent to which it would be possible to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and timeframe for doing so ("substitutability"); i. the extent to which it is possible to reintegrate the outsourced function into the institution or payment institution, if necessary or appropriate j. data protection and the potential impact of a breach of confidentiality or ensuring availability and integrity of data on the institution or payment institution and its customers, including but not limited to compliance with Regulation (EU)2016/67921.	
	Title III - Framework for governance	
	5. Robust governance arrangements and third party risks	
32.	As part of the overall internal control framework, including internal control mechanisms, institutions shall have a holistic institution-wide risk management framework covering all business lines and internal units. Under that framework, institutions and payment institutions shall identify and manage all their risks, including those posed by third-party arrangements. The risk management framework shall also enable institutions and payment institutions to make well-informed	Provide an institution-wide risk management framework that extends to all business units. Examples include a risk management process that is run periodically, performing periodic integrity risk analyses, and continuously monitoring and/or controlling processes that are performed both internally and by an outsourcing partner.

	decisions about entering into risks and shall ensure that risk management measures are properly implemented, including with regard to cyber risk	
33.	Institutions and payment institutions shall, taking into account the principle of proportionality in line with Chapter 1, identify, assess, monitor and manage all risks arising from third-party arrangements to which they are or might be exposed, regardless of whether those arrangements constitute outsourcing arrangements. The risks, notably the operational risks, of all arrangements with third parties, including those referred to in points 26 and 28, shall be assessed in accordance with section 12.2.	The outsourced services should be part of the internal risk management.
34.	Institutions and payment institutions shall comply with all the requirements of Regulation (EU) 2016/679, including as regards their arrangements with third parties and outsourcing arrangements.	For information/no remarks
	6. Robust governance arrangements and outsourcing	
35.	Outsourcing of functions shall not result in the delegation of the management body's responsibilities. Institutions and payment institutions shall remain fully responsible and accountable for complying with all their regulatory obligations, including for the ability to oversee the outsourcing of critical or important functions.	For information/no remarks

36.	The management body shall at all times be fully responsible for and accountable for at least the following a. ensuring that the institution or payment institution complies at all times with the conditions for its authorisation, including any conditions imposed by the competent authority b. the internal organisation of the institution or payment institution c. the identification, assessment and management of conflicts of interest d. Determining the strategies and policies of the institution or payment institution (e.g. business model, risk appetite, risk management framework); e. overseeing the day-to-day management of the institution or payment institution, including the management of all risks associated with outsourcing; and f. the supervisory role of the management body, including overseeing and monitoring management decision-making.	For information/no remarks
37.	Outsourcing shall not result in lower suitability requirements for the members of the management body of an institution, the directors and persons responsible for the management of the payment institution and key personnel. Institutions and payment institutions shall have adequate professional competencies and sufficient and properly trained staff to properly manage and supervise the outsourcing arrangements.	For information/no remarks

38.	Institutions and payment institutions a. clearly allocate responsibilities for documentation, management and monitoring of outsourcing arrangements b. allocate sufficient resources to ensure compliance with all legal and regulatory requirements, including these guidelines and the documentation and monitoring of all outsourcing arrangements; c. shall establish an outsourcing function or designate a senior member of staff who is directly accountable to the management body (e.g. a key function holder within an audit function) and is responsible for managing and monitoring the risks of outsourcing arrangements as part of the institution's internal control framework and for overseeing the documentation of outsourcing arrangements, all subject to Chapter 1 of these guidelines. Smaller and less complex institutions or payment institutions shall at least ensure a clear allocation of tasks and responsibilities for the management and monitoring of outsourcing arrangements and may allocate the outsourcing function to a member of the institution's or the payment institution's management body.	For information/no remarks
	Institutions and payment institutions will always retain sufficient content and not become "empty shells" or "letterbox companies". To this end: a. they shall comply at all times with the conditions of their authorisation, including that the management body exercises effectively its responsibilities as described in point 36 of these guidelines; b. maintain a clear and transparent organisational framework and structure that allows them to comply with legal and regulatory requirements; c. exercise appropriate oversight and be able to manage the risks arising from outsourcing of critical or important functions where the operational functions of internal control functions are outsourced (e.g.	For information/no remarks

	in the case of intra-group outsourcing or outsourcing within institutional protection schemes); and d. have sufficient resources and capabilities to comply with points (a) to (c).	

40.	When outsourcing, institutions and payment institutions shall in any event ensure that a. they can take and implement decisions relating to their business activities and critical or important functions, including those outsourced b. they continue to conduct their business and provide banking and payment services in an orderly manner; c. the risks related to the existing and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (FinTech); d. appropriate arrangements are in place for the confidentiality of data and other information e. an adequate flow of relevant information is maintained with service providers; f. as regards the outsourcing of critical or important functions, they can perform at least one of the following, within an appropriate timeframe: transfer the function to alternative service providers; reintegrate the function; or cease the business activities that depend on the function.	For information/no remarks

	g. where personal data are processed by service providers in the EU and/or third countries, appropriate measures are taken and the data are processed in accordance with Regulation (EU) 2016/679	
	7. Outsourcing policy	
41.	The management body of an institution or payment institution which has, or plans to have, outsourcing arrangements shall adopt, regularly review and update a written outsourcing policy and, where appropriate, implement that policy on an individual, sub-consolidated and consolidated basis. For institutions, the outsourcing policy shall comply with Chapter 8 of the EBA Internal Governance Guidelines, in particular with the requirements set out in Chapter 18 (New products and material changes) of those Guidelines. Payment institutions may also align their policies with Chapters 8 and 18 of the EBA Internal Governance Guidelines.	See also paragraph 4.1 of the Blanco paper

42.	The policy shall cover the key stages of the outsourcing arrangements life cycle, outlining the principles, responsibilities and processes relating to the outsourcing. In particular, the policy shall include at least the following a. the responsibilities of the management body in accordance with point 36, including its involvement, where appropriate, in the decision-making process for outsourcing critical or important functions b. the involvement of business units, internal audit functions and other persons in relation to outsourcing arrangements; c. the planning of outsourcing arrangements, including: the definition of business rules for outsourcing arrangements; the criteria, including those set out in chapter 4, and processes for determining critical or significant functions the identification, assessment and management of risks in accordance with section 12.2; due diligence checks on potential future service providers, including those required pursuant to Section 12.3; procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with Chapter 8; business continuity planning, in accordance with Chapter 9; Method of approval of new outsourcing arrangements; d. The implementation, monitoring and management of outsourcing arrangements, including the ongoing assessment of the service provider's performance in accordance with chapter 14; the procedures for notifying and responding to changes in an outsourcing arrangement or service provider (e.g. in its financial position, organisational or ownership structures, sub-contracting) the independent review and monitoring of compliance with legal and regulatory requirements and policies the renewal procedures;	See also paragraph 4.1 of the Blanco paper

	e. the documentation and record keeping, subject to the requirements set out in Chapter 11; f. the exit strategies and termination procedures, including a requirement for a documented exit plan for each critical or important function to be outsourced, where such an exit is deemed possible, taking into account possible service disruptions or the unexpected termination of an outsourcing arrangement.	

43.	The outsourcing policy distinguishes between: a. outsourcing of critical or important functions and other outsourcing arrangements b. outsourcing to service providers licensed by a competent authority and service providers not licensed by a competent authority c. Intra-group outsourcing arrangements, outsourcing arrangements within the same institutional protection regime (including entities owned, individually or collectively, by institutions within the institutional protection regime) and outsourcing to entities outside the group; and outsourcing to service providers in a Member State or third country.	See also paragraph 4.1 of the Blanco paper
44.	Institutions and payment institutions shall ensure that the identification of the following potential effects of critical or material outsourcing arrangements is part of the policy and is taken into account in the decision-making process: a. the risk profile of the institution; b. the ability to supervise the service provider and manage the risks;	See also paragraph 4.1 of the Blanco paper

	c. the business continuity measures; and the conduct of their business.	
	8. Conflicts of interest	
45.	Institutions and payment institutions shall identify, assess and manage conflicts of interest in relation to their outsourcing arrangements in accordance with Chapter 11 of Title IV of the EBA Internal Governance Guidelines.	As an investment firm, you should have a conflict of interest policy which covers conflicts of interest in cases of outsourcing.
46.	Where outsourcing creates material conflicts of interest, including between entities belonging to the same group or institutional protection scheme, institutions and payment institutions shall take appropriate measures to manage those conflicts of interest.	For information/no remarks

47.	Where functions are performed by a service provider belonging to a group or to an institutional protection scheme, or owned by an institution, payment institution, group or institutions affiliated to an institutional protection scheme, the terms and conditions, including financial terms, for the outsourced service shall be determined in conformity with market conditions. Synergies resulting from the provision of the same or similar services to several institutions within a group or an institutional protection scheme may be taken into account in the pricing of services, as long as the service provider remains viable on a stand-alone basis; within a group this should be independent of the failure of any other entity of the group.	For information/no remarks

	9. Business continuity plans	
48.	Institutions and payment institutions shall have appropriate business continuity plans in place for outsourced critical or important functions, maintain them and test them periodically, in line with the requirements of Article 85(2) of Directive 2013/36/EU and Title VI of EBA Guidelines on Internal Governance28 . Institutions and payment institutions within a group or institutional protection scheme may rely on centrally prepared business continuity plans for their outsourced functions.	As an investment firm, you are required to have business continuity plans in place, which include outsourcing.
49.	Business continuity plans shall take into account the possibility of the outsourced critical or important function deteriorating to an unacceptable level, or not being performed at all. They shall also take into account the possible consequences of insolvency or other forms of failure of service providers and, where relevant, political risks in the jurisdiction of the service provider.	For information/no remarks
	10. Internal audit function	
50.	The activities of the internal audit function shall include an independent review, based on a risk-based approach, of outsourced activities. The audit plan and programme shall cover in particular the outsourcing arrangements for critical or important functions.	For information/no remarks
51.	With regard to the outsourcing process, the internal auditor shall at least ensure the following a. that the institution's or payment institution's outsourcing framework, including the outsourcing policy, is properly and effectively implemented and in compliance with the applicable laws and regulations, the risk strategy and the decisions of the management body b. that the assessment of the criticality or importance of the functions is adequate, qualitative and effective;	For information/no remarks

	c. that the risk assessment of outsourcing arrangements is adequate, high quality and effective and that the risks remain consistent with the institution's risk strategy; d. the appropriate involvement of governing bodies; and e. that outsourcing arrangements are appropriately monitored and managed.	
	11. Documentation requirements	

52.	As part of their risk management framework, institutions shall keep records of all outsourcing arrangements of the institution and, where applicable, at sub-consolidated and consolidated levels, as mentioned in Chapter 2. They shall properly document all current outsourcing arrangements, distinguishing between outsourcing of critical or important functions and other outsourcing arrangements. Subject to national legislation, institutions shall retain for an appropriate period of time the documentation related to the discontinued outsourcing arrangements in the register and supporting documentation.	See also paragraph 4.7 of the Blanco paper
53.	Subject to Title I of these guidelines and the conditions set out in point 23(d), if institutions and payment institutions are part of a group, institutions that are permanently affiliated to a central body or institutions belonging to the same institutional protection scheme, the register may be operated centrally.	See also paragraph 4.7 of the Blanco paper

54.	The register shall contain at least the following information on all existing outsourcing arrangements a. a reference number for each outsourcing arrangement; b. the start date and, where applicable, the next renewal date, end date and/or notice period for the service provider and for the institution or payment institution c. a brief description of the outsourced function, including which data is outsourced and whether personal data is transferred or not (e.g. by stating yes or no in a separate data field), or whether processing is outsourced to a service provider; d. a category assigned by the institution or payment institution which reflects the nature of the function as described in point (c) (e.g. information technology (IT), audit function), thereby facilitating the identification of different types of arrangements; e. the name of the service provider, the trade register number, the legal entity identification code (if available), the registered address and other relevant contact details, and the name of the parent company (if available) f. the country or countries where the service is to be provided, including the location (i.e. country or region) of the data; g. whether the outsourced function is considered (yes/no) critical or important, plus, if applicable, a brief summary of the reasons why the outsourced function is considered critical or important h. in the case of outsourcing to a cloud services provider, the models for the cloud services and the roll-out of the cloud, i.e. public/private/hybrid/common, and the specific nature of the data to be retained and the locations (i.e. countries or regions) where such data will be stored; i. the date on which the criticality or importance of the outsourced function was last assessed.	See also paragraph 4.7 of the Blanco paper

55.	For the purposes of outsourcing critical or important functions, the register shall contain at least the following additional information a. the institutions, payment institutions and other undertakings within the prudential consolidation or the institutional protection scheme, as applicable, which benefit from the outsourcing; b. whether the service provider or sub-service provider is part of the group or is a member of the institutional protection scheme or is owned by institutions or payment institutions within the group or is a member of an institutional protection scheme c. the date on which a risk assessment was last carried out and a brief summary of its main findings; d. the person or decision-making body (e.g. the management body) in the institution or payment institution that has approved the outsourcing arrangements e. the legislation applicable to the outsourcing arrangement f. the dates of the most recent and next scheduled audits, if applicable g. if applicable, the names of subcontractors to whom material parts of a critical or important function have been subcontracted, including the country in which the subcontractors are registered, where the service will be provided and, if applicable, the location (i.e. country or region) where the data will be stored h. the outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a critical or important function into the institution or the payment institution or the impact of terminating the critical or important function; i. alternative service providers in accordance with h); j. whether the outsourced critical or important function supports time-sensitive business operations; the estimated annual budget cost.	See also paragraph 4.7 of the Blanco paper

56.	Institutions and payment institutions shall make available on request the complete record of all existing outsourcing arrangements or specified parts thereof, such as information on all outsourcing arrangements falling into one of the categories referred to in point 54(d) of these guidelines (e.g. all IT outsourcing arrangements). Institutions and payment institutions shall provide this information in a processable electronic format (e.g. a commonly used database format, comma separated values).	For information/no remarks
57.	Institutions and payment institutions shall make available to the competent authority, on request, all information which is necessary to enable the competent authority to supervise the institution or payment institution effectively, including a copy of the outsourcing agreement, if necessary.	For information/no remarks
58.	Institutions, without prejudice to Article 19(6) of Directive (EU) 2015/2366, and payment institutions shall notify the competent authorities or engage in a supervisory dialogue with the competent authorities, as appropriate and in a timely manner, of the planned outsourcing of critical or important functions and/or where an outsourced function has become critical or important, and shall provide at least the information set out in point 54.	See also paragraph 4.5 of the Blanco paper
59.	Institutions and payment institutions shall inform the competent authorities in good time of any material changes and/or serious events related to their outsourcing arrangements which could have a significant impact on the continuation of the business of the institutions or payment institutions.	See also paragraph 4.5 of the Blanco paper

60.	Institutions and payment institutions shall properly document the assessments made under Title IV and the results of their ongoing monitoring activities (e.g. service provider performance, compliance	For information/no remarks

	with agreed service levels, other contractual and regulatory requirements, update of risk assessment).	
	Title IV - Outsourcing process	
	12. Analysis before outsourcing	
61.	Before entering into an outsourcing arrangement, institutions and payment institutions shall act as follows: a. They shall assess whether the outsourcing arrangement concerns a critical or important function as set out in Title II. b. They shall assess whether the supervisory conditions for outsourcing set out in Section 12.1 are met. c. They identify and assess all relevant risks of the outsourcing arrangement in accordance with Section 12.2. d. They conduct appropriate due diligence on the potential future service provider in accordance with Section 12.3. e. They identify and assess conflicts of interest that the outsourcing may cause in accordance with Section 8.	See also paragraph 4.2 of the Blanco paper
	12.1 Supervisory conditions for outsourcing	
62.	Institutions and payment institutions shall ensure that the outsourcing of functions of banking activities or payment services, in so far as the performance of those functions is subject to authorisation by or registration with a competent authority in the Member State where they are authorised, to a service provider located in the same or another Member State takes place only if one of the following conditions is met a. The service provider is authorised or registered by a competent authority to provide such banking activities or payment services. Or b. The service provider is otherwise authorised to perform such banking activities or payment services in accordance with the relevant national legal framework.	Not applicable for investment firms

63.	Institutions and payment institutions shall ensure that the outsourcing of functions of banking activities or payment services, in so far as the performance of those functions is subject to authorisation or registration by a competent authority in the Member State where they are authorised, to a service provider located in a third country takes place only if the following conditions are met a. The service provider is authorised or registered to provide that banking activity or payment service in the third country and is subject to supervision by a relevant competent authority in that third country ("supervisory authority"). b. There is an appropriate cooperation agreement, e.g. in the form of a memorandum of understanding or college agreement, between the competent authorities responsible for the supervision of the institution and the supervisory authorities responsible for the supervision of the service provider. c. The cooperation agreement referred to in point (b) shall ensure that the competent authorities are at least able to: obtain, on request, the information necessary to carry out their supervisory duties under Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive (EU) 2015/2366 and Directive 2009/110/EC; obtain adequate access to data, documents, locations or personnel in the third country relevant to the exercise of their supervisory functions receive, as soon as possible, information from the supervisory authority in the third country to investigate apparent breaches of the requirements of Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive (EU) 2015/2366 and Directive 2009/110/EC; and cooperate with the relevant supervisory authorities in the third country in enforcement actions for breaches of applicable regulatory requirements and national legislation in the Member State. The cooperation should include, but not necessarily be limited to,	Niet van toepassing voor beleggingsondernemingen

	receiving information on possible breaches of applicable regulatory requirements from the supervisory authorities in the third country as soon as practically possible.	
	12.2 Assessing risks of outsourcing arrangements	
64.	Institutions and payment institutions shall assess the potential impact of outsourcing arrangements on their operational risk, take into account the assessment results when deciding whether to outsource to a service provider, and take appropriate measures to prevent unnecessary additional operational risk before entering into outsourcing arrangements.	See also section 4.2 and 4.3 of the Blanco paper

65.	The assessment shall include scenarios of possible risk events, including very serious operational risk events, where appropriate. Within the scenario analysis, institutions and payment institutions shall assess the potential impact of service failures or inadequacies, including the risks caused by processes, systems, people or external events. Institutions and payment institutions shall, taking into account the principle of proportionality referred to in Chapter 1, document the analysis performed and its results, and estimate the extent to which their operational risk would increase or decrease as a result of the outsourcing arrangement. Subject to Title I, small and non-complex institutions and payment institutions may use a qualitative approach to risk assessment, whereas large or complex institutions shall use a more sophisticated approach, including, where available, the use of internal and external loss data as a source of information for the scenario analysis.	See also section 4.2 and 4.3 of the Blanco paper

66.	In the risk assessment, institutions and payment institutions shall also take into account the expected benefits and costs of the proposed outsourcing arrangement, including the weighing of risks that can be mitigated or better managed against risks that might arise from the proposed outsourcing arrangement. In doing so, they shall consider at least: a. concentration risks, including as a result of: outsourcing to a dominant service provider that cannot be easily replaced; and multiple outsourcing arrangements with the same service provider or service providers that are closely related; b. the aggregate risks stemming from outsourcing various functions across the institution or payment institution and, in the case of groups	See also section 4.2 and 4.3 of the Blanco paper

	of institutions or institutional protection schemes, the aggregate risks on a consolidated or institutional protection scheme basis; c. in the case of large institutions, the entry risk, which is the risk that might result from the need to provide financial support to a service provider in distress or to take over its business activities; and d. the measures taken by the institution or payment institution and the service provider to manage and mitigate risks.	
67.	Where the outsourcing arrangement allows the service provider to subcontract critical or important functions to other service providers, institutions and payment institutions shall take into account a. the risks of subcontracting, including the additional risks which may arise if the subcontractor is located in a third country or a country other than the service provider b. the risk that long and complex chains of sub-outsourcing reduce the ability of institutions or payment institutions to supervise the outsourced critical or important function and the ability of competent authorities to supervise them.	See also section 4.2 and 4.3 of the Blanco paper

68.	When assessing the risks prior to outsourcing and during ongoing monitoring of the performance of the service provider, institutions and payment institutions shall in any case carry out the following actions a. They shall identify the relevant functions and associated data and systems and classify them according to their sensitivity and the security measures required. b. They shall perform a thorough risk-based analysis of the functions and related data and systems which they are considering outsourcing or have outsourced, and address the potential risks, especially the operational risks, including legal, ICT, compliance and reputational risks, and supervisory constraints related to the countries where the outsourced services are (likely to be) provided and where the data are (likely to be) stored. c. They consider the implications of the location of the service provider (within or outside the EU). d. They look at political stability and security in the relevant jurisdictions, including: the legislation in force, including laws on data protection; the existing law enforcement facilities; and the insolvency law that would apply in the event of non-compliance by a service provider and the possible limitations that would arise in the event of urgent recovery of the institution's or payment institution's data in particular. e. They shall define and decide on appropriate data confidentiality protections, the continuity of outsourced activities, and the integrity and traceability of data and systems in the context of the envisaged outsourcing. Furthermore, institutions and payment institutions shall consider the need for specific measures for data in transit, stored data and data at rest, such as the use of encryption techniques	See also section 4.2 and 4.3 of the Blanco paper

	(scrambling) in combination with an appropriate key management scheme. f. They shall consider whether the service provider is a subsidiary or parent undertaking of the institution, falls within the institution's accounting consolidation or is a member of or owned by institutions that are members of an institutional protection scheme and, if so, the extent to which the institution controls the service provider or can influence its actions in line with Chapter 2.	
	12.3 Due diligence	
69.	Before entering into an outsourcing arrangement and before looking at the operational risks related to the function to be outsourced, institutions and payment institutions shall ensure the suitability of the service provider during their selection and evaluation process.	See also section 4.2 and 4.3 of the Blanco paper
70.	With regard to critical and important functions, institutions and payment institutions shall ensure that the service provider has the business reputation, appropriate and sufficient skills, expertise, capacity, resources (e.g. human resources, IT, financial), organisational structure and, where applicable, the required legal licence(s) or registration(s) to perform the critical or important function in a reliable	See also section 4.2 and 4.3 of the Blanco paper

	and professional manner so as to meet its obligations throughout the course of the draft contract.	

71.	Additional factors to be considered when performing due diligence on a potential service provider include, but are not limited to a. its business model, character, size, complexity, financial situation, ownership and group structure; b. its long-standing relationships with service providers already assessed that provide services to the institution or payment institution; c. whether the service provider is a parent or subsidiary of the institution or payment institution, falls within the accounting consolidation of the institution or is a member of or owned by institutions affiliated to the same institutional protection scheme as the institution d. whether the service provider is subject to the supervision of the competent authorities	See also section 4.2 and 4.3 of the Blanco paper
72.	Where the outsourcing involves the processing of personal or confidential data, institutions and payment institutions shall ensure that the service provider implements appropriate technical and organisational measures to protect the data.	See also section 4.2 and 4.3 of the Blanco paper
73.	Institutions and payment institutions shall take the necessary steps to ensure that service providers act in a manner consistent with their values and code of conduct. In particular, as regards service providers in third countries and, where relevant, their subcontractors, institutions and payment institutions shall ensure that the service provider acts in an ethically and socially responsible manner and complies with international standards in the field of human rights (e.g. the European Convention on Human Rights), environmental protection and adequate working conditions, including the prohibition of child labour.	See also section 4.2 and 4.3 of the Blanco paper
	13. Contract phase	

74.	The rights and obligations of the institution, the payment institution and the service provider shall be clearly defined and set out in a written agreement.	See also paragraph 4.4 of the Blanco paper
75.	The outsourcing agreement for critical or important functions shall include at least the following a.a clear description of the function to be outsourced; b. the commencement and termination dates, if any, of the agreement and the notice periods for the service provider and the institution or payment institution c. the legislation applicable to the agreement; d. the financial obligations of the parties; e. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions applicable to the sub-outsourcing in Section 13.1 f. the location(s) (i.e. regions or countries) where the critical or important function will be performed and/or where the relevant data will be stored and processed, including the possible storage location, and the conditions to be met including the requirement to notify the institution or payment institution if the service provider proposes to change the location(s) g. where relevant, provisions on the accessibility, availability, integrity, privacy and security of the data concerned, as specified in Section 13.2 h. the right of the institution or payment institution to monitor the performance of the service provider on an ongoing basis; i. the agreed service levels, which shall include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met; j. the service provider's obligations regarding reporting to the institution or payment institution, including the service provider's	See also paragraph 4.4 of the Blanco paper

	reporting of any development that may have a material impact on the service provider's ability to perform the critical or important function effectively in line with agreed service levels and in compliance with applicable laws and regulations, and, if applicable, the obligation to provide reports from the service provider's internal audit function k. whether the service provider is required to obtain insurance cover against particular risks and, if so, the required level of insurance cover; l. the requirement to implement and test business emergency plans m. provisions ensuring that access can be obtained to the data owned by the institution or payment institution when the service provider is insolvent, in a process of resolution or ceasing its business activities; n. an obligation on the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them; o. for institutions, a clear reference to the powers of the national resolution authority, in particular to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'material liabilities' of the contract within the meaning of Article 68 of that Directive p. the unrestricted right of institutions, payment institutions and competent authorities to inspect and monitor the service provider, in particular as regards the critical or important outsourced function, as stated in Section 13.3 q. termination rights, as referred to in Section 13.4.	

	13.1 Subcontracting of critical or important functions	
76.	The outsourcing agreement shall specify whether the sub-outsourcing of critical or important functions, or material parts thereof, is permitted or not.	See also paragraph 4.4 of the Blanco paper
77.	Where the sub-outsourcing of critical or important functions is permissible, institutions and payment institutions shall determine whether the part of the function being sub-outsourced is critical or important as such (i.e. a material part of the critical or important function). If this is the case, they shall record this in the register.	See also paragraph 4.4 of the Blanco paper

78.	If the sub-outsourcing of critical or important functions is authorised, the written agreement shall contain the following requirements: a. All types of activities excluded from subcontracting shall be identified. b. The conditions to be met in the case of sub-outsourcing shall be specified. c. It shall state that the service provider has an obligation to supervise services which it has subcontracted, in order to ensure ongoing compliance with the contractual obligations between the service provider and the institution or payment institution. d. The contract shall require the service provider to obtain the prior specific or general written consent of the institution or payment institution before subcontracting. e. It shall include a requirement for the service provider to inform the institution or payment institution of any planned sub-outsourcing, or material changes to it, in particular where it would reduce the service provider's ability to fulfil its responsibilities under the outsourcing agreement. This shall also cover any planned material changes as regards subcontractors and the notification period; in particular, the	See also paragraph 4.4 of the Blanco paper

	notification period shall be fixed so as to allow the outsourcing institution or payment institution at least to assess the risks of the proposed changes and to object to any changes before the planned subcontracting, or any material changes thereto, takes place. f. Where necessary, the contract shall provide that the institution or payment institution has the right to object to a proposed outsourcing, or to material changes to it, or that explicit approval is required. g. The contract shall provide that the institution or payment institution is contractually entitled to terminate the contract in the event of undue sub-outsourcing, for example if the sub-outsourcing would materially increase the risks to the institution or payment institution or if the service provider proceeds with sub-outsourcing without informing the institution or payment institution.	
79.	Institutions and payment institutions shall agree to sub-outsourcing only if the subcontractor undertakes to a. comply with all applicable laws, regulatory requirements and contractual obligations; and to grant the institution, payment institution and competent authority the same contractual access and audit rights as the service provider.	See also paragraph 4.4 of the Blanco paper
	13.2. Security of data and systems	
81.	Institutions and payment institutions shall ensure that service providers comply with appropriate IT security standards, where relevant.	See also paragraph 4.3 en 4.4 of the Blanco paper
82.	Where relevant (e.g. in the context of outsourcing cloud or other ICT services), institutions and payment institutions shall define data and	For information/no remarks

	system security requirements in the outsourcing agreement and monitor compliance with those requirements on an ongoing basis.	
83.	In the case of outsourcing to cloud service providers and other outsourcing arrangements which involve the processing or transfer of personal or confidential data, institutions and payment institutions shall adopt a risk-based approach with regard to the location(s) of data storage and processing (i.e. country or region) and information security considerations.	See also section 4.3 and 4.4 of the Blanco paper

84.	Without prejudice to the requirements of Regulation (EU) 2016/679, institutions and payment institutions shall take into account differences in national data protection provisions when outsourcing (in particular to third countries). Institutions and payment institutions shall ensure that the outsourcing agreement stipulates that the service provider must protect confidential, personal or otherwise sensitive information and comply with any legal data protection requirements applicable to the institution or payment institution (e.g. the protection of personal data and that banking secrecy or similar legal obligations of confidentiality with respect to customer information, where applicable, are respected).	See also section 4.3 and 4.4 of the Blanco paper
	13.3. Access, information and audit rights	
85.	Institutions and payment institutions shall lay down in the written outsourcing arrangements that the internal audit function may review the outsourced function using a risk-based approach	See also paragraph 4.4 of the Blanco paper
86.	The written outsourcing arrangements between institutions and service providers shall, irrespective of the criticality or importance of the outsourced function, refer to and ensure the rights of competent authorities and resolution authorities to information collection and examination under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU as regards service providers located in a Member State, and also as regards service providers located in third countries.	See also paragraph 4.4 of the Blanco paper

87.	Where the outsourcing of critical or important functions is involved, institutions and payment institutions shall stipulate in the written outsourcing agreement that the service provider will provide to them and their competent authorities, including resolution authorities, and to any other person designated by them or the competent authorities a. provide full access to all relevant business locations (e.g. headquarters and operations centres), including the full range of relevant equipment, systems, networks, information and data used to perform the outsourced function, including related financial information, personnel and the service provider's external auditors ("access and information rights"); and b. provide unrestricted rights of inspection and audit in relation to the outsourcing arrangement ("audit rights") to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.	See also paragraph 4.4 of the Blanco paper
88.	As regards the outsourcing of functions which are not critical or important, institutions and payment institutions shall ensure the access and audit rights referred to in point 87(a) and (b) and in Section 13.3 by adopting a risk-based approach, taking into account the nature of the outsourced function and the associated operational and reputational risks, its scalability, its potential impact on the ongoing performance of the activities related to the function, and the contractual period. Institutions and payment institutions shall take into account that functions may become critical or important over time.	See also paragraph 4.4 of the Blanco paper
89.	Institutions and payment institutions shall ensure that the outsourcing agreement or any other contractual arrangement does not prevent or restrict the effective exercise of the rights of access and audit, which may be exercised by themselves, by competent authorities or by third parties designated by them to exercise these rights.	See also paragraph 4.4 of the Blanco paper

90.	Institutions and payment institutions shall exercise their access and audit rights, determine through a risk-based approach the frequency of audits and the areas to be audited, and abide by relevant generally accepted national and international auditing standards.	For information/no remarks

91.	Without prejudice to their ultimate responsibility for outsourcing arrangements, institutions and payment institutions may use a. joint audits organised with other clients of the same service provider and carried out by them and those clients or a third party appointed by them in order to use audit resources more efficiently and reduce the organisational burden on the clients and the service provider; b. external certifications and external or internal audit reports provided by the service provider.	See also paragraph 4.4 of the Blanco paper
92.	As regards the outsourcing of critical or important functions, institutions and payment institutions shall assess the adequacy and sufficiency of the external certifications and reports referred to in point 91(b) to meet their regulatory obligations and not rely exclusively on those reports over time.	For information/no remarks

93.	Institutions and payment institutions shall use the method referred to in point 91(b) only if they: a. are satisfied with the audit plan for the outsourced function; b. ensure that the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and controls identified by the institution or payment institution as critical, and compliance with the relevant regulatory requirements c. Undertake an ongoing comprehensive review of the certification or audit report and verify that reports or certifications are not outdated; d. ensure that future versions of the certification or audit report cover key systems and controls; e. be satisfied with the suitability of the certifying or audit party (e.g. with regard to rotation of the certifying or audit organisation, qualifications, expertise, repetition of performance / check of documentary evidence in the audit file concerned) f. have satisfied themselves that certifications have been issued and audits carried out in accordance with generally accepted professional standards, and that they include an assessment of the operational effectiveness of the key controls present g. have the contractual right to request the extension of the scope of the certification or audit report to other relevant systems and controls; the number and frequency of such requests shall be reasonable and justified from a risk management perspective; and h. retain the contractual right to conduct separate audits on outsourced critical or important functions at their discretion.	For information/no remarks
94.	In accordance with the EBA Guidelines on the assessment of ICT risk under SREP, institutions shall ensure, where relevant, that they are able to conduct periodic penetration tests to assess the effectiveness of the cyber- and internal ICT security measures and processes implemented. Subject to Title 1, payment institutions shall also have in place internal ICT	Blanco has (for the KYC Suite) an ongoing bug bounty program at HackerOne. Ethical hackers then try to penetrate the software of Blanco (within a controlled environment), which is similar to a penetration test, but on an ongoing basis. The

	control mechanisms, including ICT security controls and risk mitigation measures.	HackerOne programme is in scope of the ISAE3402 certification.
95.	Prior to a scheduled on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution or competent authorities shall notify service providers a reasonable time in advance, unless this is not possible due to an emergency or crisis situation or would lead to a situation in which the audit would no longer be effective.	For information/no remarks

96.	When performing audits in a multi-client environment, risks to the environment of another client (e.g. impact on service levels, data availability, confidentiality issues) are avoided or mitigated.	For information/no remarks. This is always an important condition for Blanco to carry out an audit. This is also quite possible, given the segregated accounts.
97.	Where the outsourcing arrangement is particularly complex from a technical point of view, such as in the case of outsourcing of cloud services, the institution or payment institution shall verify that the person or persons carrying out the audit - its own internal auditors, or the pool of auditors or external auditors acting on its behalf - have the appropriate and relevant knowledge and skills to effectively carry out the relevant audits and/or reviews. The same shall apply to the institution's or payment institution's staff carrying out the external certification or the audits carried out by service providers.	For information/no remarks
	13.4 Termination rights	

98.	The outsourcing arrangement shall expressly allow the institution or payment institution to terminate the arrangement in accordance with the applicable law, including in the following situations: security measures and processes are in place. payment institutions also have internal ICT control mechanisms, including ICT security controls and risk mitigation measures. a. where the person performing the outsourced functions breaches applicable laws, regulations or contractual provisions; b. where obstacles are identified that may lead to changes in the performance of the outsourced function; c. where there are material changes that affect the outsourcing arrangement or the service provider (e.g. subcontracting or changes relating to subcontractors); d. where there are weaknesses in the management and security of confidential, personal or otherwise sensitive data or information; and e. where the competent authority of the institution or payment institution issues instructions, for example where, as a result of the outsourcing arrangement, the competent authority is no longer in a position to supervise the institution or payment institution effectively.	See also paragraph 4.4 of the Blanco paper
99.	The outsourcing arrangement shall facilitate the transfer of the outsourced function to another service provider or its re-assignment to the institution or payment institution. To this end, the written outsourcing arrangement shall include the following a. a clear description of the obligations of the existing service provider in case of transfer of the outsourced function to another service provider or back to the institution or payment institution, including the treatment of data; b. an appropriate transitional period during which, after termination of the outsourcing arrangement, the service provider continues to perform the outsourced function so as to limit the risk of disruption; and	See also paragraph 4.4 of the Blanco paper

	c. a requirement on the service provider to assist the institution or payment institution to transfer the function in an orderly manner when the outsourcing arrangement is terminated.	
	14. Supervision of outsourced functions	

100.	Institutions and payment institutions shall continuously monitor the performance of service providers with regard to all outsourcing arrangements using a risk-based approach, with a particular focus on outsourcing critical or important functions, including ensuring the availability, integrity and security of data and information. Where the risk, nature or scope of an outsourced function has changed in any material respect, institutions and institutions and payment institutions shall reassess the criticality or importance of that function in accordance with Chapter 4.	For information/no remarks
101.	Institutions and payment institutions shall exercise due skill, care and diligence when monitoring and managing outsourcing arrangements.	For information/no remarks
102.	Institutions shall regularly update their risk assessment in accordance with section 12.2 and periodically report to the management body on the risks they have identified in connection with the outsourcing of critical or important functions.	For information/no remarks
103.	Institutions and payment institutions shall monitor and manage their internal concentration risk arising from outsourcing arrangements, subject to Section 12.2 of these guidelines.	For information/no remarks

104.	Institutions and payment institutions shall ensure on an ongoing basis that outsourcing arrangements meet appropriate performance and quality standards in accordance with their policies, with a particular focus on critical or important functions outsourced. They shall do so by a. ensuring that they receive appropriate reports from service providers; b. assessing the performance of service providers using tools such as key performance indicators, key risk management indicators, service provision reports, self-certification and independent reviews; and c. assess any other relevant information from the service provider, including reports on business continuity measures and testing.	For information/no remarks
105.	Institutions shall take appropriate action if they detect deficiencies in the performance of the outsourced function. In particular, institutions and payment institutions shall take action where there is evidence that service providers are not performing the outsourced critical or important function effectively or in accordance with applicable laws and regulatory requirements. If deficiencies are identified, institutions and payment institutions shall take appropriate corrective or remedial action. If necessary, the outsourcing contract shall be terminated with immediate effect.	For information/no remarks
	15. Exit strategies	
106.	Institutions and payment institutions shall have a documented exit strategy during the outsourcing of critical or important functions which is in line with their outsourcing policy and business continuity plans, taking into account at least the possibility that a. Outsourcing arrangements are terminated; b. The service provider fails; c. The quality of the function performed deteriorates and that there is or may be business disruption caused by the function not being	For information/no remarks

	performed or being performed improperly;significant risks to the proper and continued performance of the job.	

107.	Institutions and payment institutions shall ensure that they are able to withdraw from outsourcing arrangements without undue disruption to their business operations, without reducing their compliance with regulatory requirements and without impairing the continuity and quality of their services to customers. To this end: a. develop and implement exit plans that are complete, documented and, where necessary, adequately tested (e.g. by analysing the potential costs, consequences, resources and time implications associated with the transfer of an outsourced service to an alternative service provider); and they shall seek alternative solutions and formulate transition plans enabling the institution or payment institution to remove outsourced functions and data from the service provider and transfer them to alternative service providers or back to the institution or payment institution, or to take other steps to ensure, in a controlled and sufficiently tested manner, the continuation of the critical or important function or business activity, taking into account the challenges that may arise from the location of data and taking the necessary steps to safeguard business activity during the transition phase.	For information/no remarks

108.	When defining an exit strategy, institutions and payment institutions shall act as follows: a. define the objectives of the exit strategy b. carry out a business impact analysis proportionate to the risk of the processes, services or activities outsourced, to identify the human and financial resources required to implement the exit plan and the time period involved; c. assign tasks, responsibilities and sufficient resources to manage exit plans and transfer activities; d. establish criteria for determining the successful transfer of outsourced functions and data; and e. define the indicators to be used for monitoring the outsourcing arrangement (as described in Chapter 14), including indicators based on unacceptable levels of service provision which should lead to an exit.	For information/no remarks
	Title V - Guidance on outsourcing addressed to competent authorities	
109.	When establishing appropriate methods to monitor the compliance of institutions and payment institutions with the conditions of their original authorisation, the aim of the competent authorities shall be to determine whether outsourcing arrangements entail a material change in the conditions and obligations under the original authorisation of institutions and payment institutions.	Aimed at supervisor.
110.	Competent authorities shall ensure that they can supervise institutions and payment institutions effectively, and also that institutions or payment institutions have stipulated in their outsourcing arrangements that service providers are required to provide audit and access rights to the competent authority and the institution, in accordance with 13.3.	Aimed at supervisor.
111.	The outsourcing risks of institutions shall be analysed at least within the framework of the SREP, or, where payment institutions are	Aimed at supervisor.

	concerned, as part of other supervisory procedures, including ad hoc requests, or during on-site inspections.	

112.	On the basis of the information contained in the register as referred to in Chapter 11, competent authorities may ask institutions and payment institutions for additional information, in particular in view of critical or important outsourcing arrangements, such as: a. the detailed risk analysis; b. whether the service provider has a business continuity plan appropriate to the services to be provided to the outsourcing institution or payment institution c. the exit strategy to be applied if one of the parties terminates the outsourcing arrangement or if there is a disruption of services; and the resources and measures in place to adequately monitor the outsourced activities.	Aimed at supervisor.
113.	In addition to the information required under Chapter 11, competent authorities may require institutions and payment institutions to provide detailed information on all outsourcing arrangements, even if the function in question is not considered critical or important.	Aimed at supervisor.
114.	Competent authorities shall assess the following through a risk-based approach a. Whether institutions and payment institutions properly monitor and manage particularly critical or important outsourcing arrangements; b. Whether institutions and payment institutions have sufficient resources to monitor and manage outsourcing arrangements; c. whether institutions and payment institutions identify and manage all relevant risks; and whether institutions identify, assess and properly manage conflicts of interest with regard to outsourcing arrangements, for example in the case of intra-group outsourcing or outsourcing within the same institutional protection scheme.	Aimed at supervisor.

115.	Competent authorities shall ensure that EU/EEA institutions and payment institutions do not operate as "shells", including situations where institutions use back-to-back or intra-group transactions to transfer part of the market and credit risk to a non-EU/EEA entity, and shall ensure that they have appropriate governance and risk management arrangements to identify and manage their risks.	Aimed at supervisor.

116.	During their assessment, competent authorities shall take into account all risks, in particular a. the operational risks of the outsourcing arrangement b. reputational risks; c. entry risk, which may require the institution to retain a service provider if the institution is a significant one; d. concentration risks within the institution, including on a consolidated basis, caused by the existence of multiple outsourcing arrangements with a single service provider or service providers that are closely related, or multiple outsourcing arrangements within the same business sector; e. concentration risk at sector level, for example where multiple institutions or payment institutions use a single service provider or a small group of service providers f. the degree of control which the outsourcing institution or payment institution has over the service provider or can influence its actions, the mitigation of risks which may result from a higher degree of control and whether the service provider is included in the consolidated supervision of the group; and g. conflicts of interest between the institution and the service provider.	Aimed at supervisor.
117.	Where concentration risks are identified, competent authorities shall monitor the evolution of such risks and assess both the potential impact on other institutions and payment institutions and on the stability of the financial market; where appropriate, competent	Aimed at supervisor.

	authorities shall inform the resolution authority of any new potentially critical functions identified during the assessment.	
118.	Where concerns are identified that an institution or a payment institution no longer has robust governance arrangements or does not meet the regulatory requirements, the competent authorities shall take appropriate measures, such as reducing the scope of outsourced functions or requiring the withdrawal from one or more outsourcing arrangements. In particular, since the institution or payment institution needs to operate on an ongoing basis, contract dissolution may be required if the monitoring and enforcement of regulatory requirements cannot be achieved by other means.	Aimed at supervisor.
119.	Competent authorities shall ensure that they can exercise effective supervision, especially where institutions and payment institutions outsource critical or important functions performed outside the EU/EEA.	Aimed at supervisor.

Annex 2 - ESMA Guidelines on outsourcing to cloud service providers

	Guidelines	Implementation at investment firm (Input Blanco when performing analysis)
	Guideline 1 - Governance, supervision and documentation	
12.	An enterprise should have a well-defined and up-to-date outsourcing strategy for cloud services consistent with the enterprise's relevant strategies and internal policies and processes, including with regard to information and communication technology, information security and operational risk management.	For information/no remarks

13	An undertaking must: a. clearly allocate responsibilities for documenting, managing and overseeing outsourcing arrangements for cloud services within its organization b. allocate sufficient resources to ensure compliance with these Guidelines and with all legal requirements applicable to its outsourcing arrangements for cloud services; c. establish a cloud service outsourcing oversight function or designate senior staff directly accountable to the management body and responsible for managing and monitoring the risks of cloud service outsourcing arrangements. When complying with this Guideline, undertakings should take into account the nature, scale and complexity of the underlying risks, including the risk to the financial system and the risks associated with the outsourced functions, and ensure that their management body has the necessary technical skills to understand the risks of cloud service outsourcing arrangements. Small and less complex undertakings should at least ensure a clear allocation of roles and responsibilities for the management and supervision of outsourcing agreements for cloud services.	For information/no remarks
14	An enterprise should monitor the performance of functions, security measures and compliance with agreed service levels by its cloud service providers. This monitoring should be risk-based and focus on critical or important outsourced functions.	For information/no remarks
15	An enterprise should periodically reassess whether its outsourcing arrangements for cloud services involve a critical or important function, and should also conduct such an assessment when there is a material change in the risk, nature or scope of the outsourced function.	For information/no remarks
16	An enterprise should keep an up-to-date register of information on all its outsourcing arrangements for cloud services, distinguishing between outsourcing of critical or important functions and functions not deemed critical or important. In doing so, it should briefly state why the outsourced function is or is not considered critical or important. Subject to national law, an undertaking should also keep a list of	For information/no remarks

	terminated outsourcing agreements for cloud services for an appropriate period.	

17	For cloud service outsourcing agreements for critical or important functions, the register must contain at least the following information a. a reference number b. the start date and, if applicable, the next renewal date of the contract, the end date and/or termination dates for the CSP and for the company c. a brief description of the outsourced function, including the outsourced data, and an indication of whether this data comprises personal data (for example, by entering Yes or No in a separate data field) d. a category assigned by the undertaking indicating the nature of the outsourced function (e.g. IT function, monitoring function), which should make it easier to identify the different types of outsourcing arrangements for cloud services e. indication of whether the outsourced function supports time-sensitive business activities f. the name and brand name (if applicable) of the CSP, the country in which it is registered, the trade register number, the identification code for legal entities (if applicable), the registered address, the relevant contact details and the name of the company's parent company (if applicable) g. the applicable law governing the outsourcing agreement for cloud services and, where applicable, the choice of jurisdiction h. the type of cloud services and implementation models and the specific nature of the data to be retained as well as the locations (i.e. countries or regions) where those data may be stored	See also chapter 4.7 of the Blanco paper

	i. the date on which the criticality or importance of the outsourced function was last assessed and the date of the next scheduled assessment j. the date of the most recent risk assessment/audit of the CSP and a brief summary of the main results, and the date of the next scheduled risk assessment/audit k. the person or decision-making body within the undertaking that approved the outsourcing agreement relating to cloud services; l. where applicable, the names of subcontractors to whom critical or important elements (or substantial parts thereof) have been subcontracted, including the countries in which the subcontractors are registered, where the subcontracted service will be provided and the location (i.e. countries or regions) where the data will be stored m. the estimated annual budget cost of the outsourcing agreement for cloud services.	
18	For outsourcing agreements of cloud services for non-critical or non-important functions, an enterprise should determine the data to be included in the register based on the nature, scope and complexity of the risks associated with the outsourced function.	See also section 4.2 and 4.3 of the Blanco paper

	Guideline 2 - Pre-outsourcing analysis and due diligence	
19	Before entering into an outsourcing agreement for cloud services, an undertaking shall a. assess whether the outsourcing agreement for cloud services relates to a critical or important function b. identify and assess any relevant risks of the outsourcing agreement for cloud services c. carrying out appropriate due diligence on the potential CSP; d. identify and assess any potential conflicts of interest arising from the outsourcing.	See also paragraphs 2.1, 4.2 and 4.3 of the Blanco paper
20	The analysis and due diligence carried out on the potential CSP prior to outsourcing should be proportionate to the nature, scale and complexity of the function that the enterprise wishes to outsource and the risks associated with that function. In any event, an assessment should be made of the potential impact of the outsourcing agreement for cloud services on the operational, legal, compliance and reputational risks for the company.	See also paragraph 4.2 of the Blanco paper

21	In cases where the outsourcing agreement for cloud services concerns critical or important functions, an undertaking shall also a. assess all relevant risks which may arise from the outsourcing agreement for cloud services, including risks relating to information and communication technology, information security, business continuity, legal, compliance, reputational and operational risks, as well as possible supervisory impediments to the undertaking arising from: i. the selected cloud service and the proposed implementation models; ii. the migration and/or implementation process iii. the sensitivity of the function and the data involved that the enterprise may wish to outsource and the security measures that would need to be taken iv. the interoperability of the company's and the CSP's systems and applications, i.e. their ability to exchange information and to use the information exchanged v. the portability of the enterprise's data, i.e. the ability to easily transfer enterprise data from one CSP to another provider or to the enterprise itself; vi. the political stability, security situation and legal system (including applicable law enforcement provisions, insolvency law provisions that would apply in the event of bankruptcy of the CSP , applicable data protection regulations and whether the conditions for transferring personal data to a third country under the AVG are met) of the countries (within or outside the EU) where the outsourced functions would be performed and where the outsourced data would be stored; in the case of subcontracting, the additional risks that may arise if the subcontractor is located in a third country or in a country other than the CSP and, in the case of a subcontracting chain, any additional risks that may arise, including as a result of the absence of a direct	Op verzoek stelt Blanco graag nadere informatie ter beschikking ten aanzien van de informatie- en communicatietechnologie, de informatiebeveiliging en de continuïteit. Uiteraard is het aan de onderneming zelf om de risico's in kaart te brengen en eventuele maatregelen te treffen. Zie tevens paragraaf 4.2. van de Blanco-paper

	agreement between the company and the subcontractor performing the outsourced function; vii. possible intra-company concentration (including at the level of the group to which the company belongs, where appropriate) caused by multiple outsourcing agreements for cloud services with the same CSP, and possible concentration within the EU financial sector due to multiple companies using the same CSP or a small group of cloud service providers. In assessing concentration risk, the undertaking should take into account all its cloud services outsourcing agreements with that CSP (and, where applicable, the cloud services outsourcing agreements at the level of the group of which it forms part); b. consider the expected benefits and costs of the cloud services outsourcing arrangement, including a balancing of the significant risks that may be mitigated or better managed against any significant risks that may arise as a result of the cloud services outsourcing arrangement.	

22	In the case of outsourcing critical or important functions, an assessment of the CSP's suitability should be part of the due diligence process. In assessing the suitability of the CSP, a company should ensure that the CSP has the business reputation, the skills, the resources (including human, IT and financial resources), the organisational structure and, if applicable, the necessary licence(s) or registration(s) to perform the critical or important function in a reliable and professional manner and to fulfil its obligations over the duration of the cloud services outsourcing agreement. Additional factors to be considered in any due diligence on the CSP include: a. the management of information security and, in particular, the protection of personal data and confidential or otherwise sensitive data; b. the support offered by the CSP, including support plans and support contacts, and incident management procedures; c. the business continuity and disaster recovery plans.	On request, Blanco will be happy to provide further information regarding information and communication technology, information security and continuity. An SLA is a standard part of the agreement with Blanco. See also paragraph 4.2. of the Blanco paper
23	Where appropriate and to support the due diligence carried out, a company may also use certifications based on international standards and reports from external or internal audits.	Blanco has an ISAE3402 Type 2 certification.
24	If a company identifies significant deficiencies and/or changes in the services provided or the situation of the CSP, the analysis and due diligence conducted on the provider prior to outsourcing must be reviewed immediately or re-examined as appropriate.	For information/no remarks
25	If a company enters into a new agreement with an already rated CSP or renews an existing agreement, it should use a risk-based approach to determine whether new due diligence is required.	For information/no remarks
	Guideline 3 - Essential contractual clauses	
26	The respective rights and obligations of a company and its CSP must be clearly set out in a written agreement.	Blanco concludes a written agreement with all clients.

27	The written agreement must expressly allow the company to terminate the agreement if necessary.	The agreement with Blanco contains an extensive 'duration and termination clause'. In principle, the contract has a fixed duration, but it is possible to terminate the contract prematurely under certain circumstances.

28	In the case of outsourcing of critical or important functions, the written agreement shall contain at least the following a. a clear description of the outsourced function; b. the start date and end date of the agreement, if any, and the notice periods for the CSP and the company c. the applicable law governing the agreement and, if applicable, the choice of law d. the financial obligations of the undertaking and the CSP e. whether sub-contracting is allowed and, if so, under what conditions, having regard to Guideline 7 f. the location(s) (i.e. countries or regions) where the outsourced function will be performed and data will be processed and stored and the conditions that must be met, including an obligation to notify the company if the CSP proposes to change the location(s) g. the provisions on information security and the protection of personal data, having regard to Guideline 4; h. the right for the undertaking to regularly monitor the performance of the CSP under the cloud services outsourcing agreement, having regard to Guideline 6 i. the agreed service levels, which should include quantitative and qualitative performance targets to allow for timely monitoring so that appropriate corrective management action can be taken without undue delay if the agreed service levels are not met j. the obligations of the CSP to report to the undertaking and, where appropriate, obligations to submit reports relevant to the safety function and critical functions of the undertaking, such as reports from the CSP's internal audit function k. the provisions on incident management by the CSP, including the obligation for the CSP to notify the undertaking without undue delay of any incidents that have affected the performance of the outsourced service of the undertaking	All the topics mentioned are included in the standard agreement with Blanco. See also paragraph 4.4. of the Blanco paper

	l. an indication of whether the CSP is required to take out insurance against certain risks and, if so, the level of insurance cover required m. the CSP's obligation to implement and test business continuity and disaster recovery plans n. the obligation of the CSP to provide the undertaking, the relevant competent authorities and any other person designated by the undertaking or the competent authorities with access rights and inspection rights (investigation and "audit" rights) in respect of the relevant information, sites, systems and devices of the CSP to the extent necessary to monitor the performance of the CSP under the cloud services outsourcing agreement and its compliance with applicable legal and contractual requirements, having regard to Guideline 6 o. provisions to ensure that data processed or stored by the CSP on behalf of the undertaking are accessible where necessary and can be restored and returned to the undertaking, having regard to Guideline 5.	

	Guideline 4 - Information security	
29	An enterprise should include information security requirements in its internal policies and procedures and in the written outsourcing agreement for cloud services and continuously monitor compliance with these requirements, also in order to protect confidential, personal or otherwise sensitive data. These requirements should be proportionate to the nature, scale and complexity of the function that the enterprise is outsourcing to the CSP and the risks associated with this function.	For information/no remarks

30	To this end, in case of outsourcing of critical or important functions, and without prejudice to the applicable requirements of the AVG, an enterprise should, through a risk-based approach, at least a. information security organisation: ensure that information security roles and responsibilities are clearly allocated between the enterprise and the CSP , including with regard to threat detection, incident and patch management, and that the CSP is able to effectively fulfil its roles and responsibilities; b. identity and access management: ensure that strong authentication mechanisms (e.g. two-factor authentication) and access measures are in place to prevent unauthorised access to the enterprise's data and back-end cloud resources c. encryption and key management: ensure that relevant encryption technologies are used where appropriate for data in transit, stored data, data at rest and data backups in combination with appropriate key management solutions to mitigate the risk of unauthorised access to encryption keys; in particular, when choosing a key management solution, the enterprise should pay attention to advanced technology and processes ; d. operational and network security: consider appropriate levels of network availability and separation (e.g. tenant isolation in the shared cloud environment, operational separation of web, application logic, operating system, network, database management system (DBMS) and storage layers) and processing environments (e.g. test, user acceptance test, development and production environments) e. application programming interfaces (APIs): consider mechanisms for integrating cloud services with enterprise systems to ensure security of APIs (e.g. by establishing and maintaining information security policies and procedures for APIs across multiple system interfaces, jurisdictions and business functions to prevent unauthorised disclosure, alteration or destruction of data)	The minimum information security measures are mentioned in the agreement. In addition to these general measures, Blanco takes further measures, depending on the module and/or suite that is purchased from Blanco. On request, Blanco can provide further explanation. Blanco has an information security policy that is in scope of the ISAE3402 of Blanco.

	f. business continuity and disaster recovery: ensuring effective business continuity and disaster recovery management measures (e.g. setting minimum capacity requirements, selecting geographically dispersed hosting options with the ability to switch between them, or requesting and reviewing documentation that shows the path taken by enterprise data between the CSP's systems, as well as considering the possibility of copying machine images to an independent storage location that is sufficiently isolated from the network or is offline) g. data location: adopt a risk-based approach to data storage and data processing location(s) (i.e. countries or regions); h. compliance and monitoring: verifying that the CSP complies with internationally recognised information security standards and has implemented appropriate information security measures (e.g. by asking the CSP to demonstrate that it implements relevant information security measures and by regularly reviewing and testing the CSP's information security measures).	

	Guideline 5 - Exit strategies	
31	In the event of outsourcing critical or important functions, an enterprise must ensure that it can terminate the outsourcing agreement for cloud services without undue disruption to its business operations and services to customers, and without prejudice to compliance with its obligations under applicable law and the confidentiality, integrity and availability of its data. To this end, an undertaking must: a. develop and implement exit plans that are complete, documented and sufficiently tested. These plans must be updated as necessary, including in the event of changes to the outsourced function b. identify alternative solutions and develop transition plans to remove the outsourced function and data from the CSP and, where applicable, any subcontractors, and transfer them to the other CSP as identified by the company or directly to the company. These solutions must be defined in view of the challenges that may arise due to the location of the data, and must include the necessary management measures to ensure business continuity during the transition phase c. ensure that the written outsourcing agreement for the CSP includes the obligation to transfer the outsourced function and related data processing in an orderly manner from the CSP and any subcontractors to another CSP, as specified by the company, or directly to the company itself in the event that the company initiates the exit strategy. The obligation to support the orderly transfer of the outsourced function and the related processing of data should also include, where relevant, the secure removal of the data from the systems of the CSP and any subcontractors.	Blanco has included an 'exit assistance' clause in the Agreement. In addition, the agreement contains provisions regarding the transfer and/or removal of (personal) data.

32	In developing the exit plans and solutions referred to in points a. and b. above ("exit strategy"), the firm must pay attention to a. the identification of the objectives of the exit strategy; b. identifying events that may trigger the exit strategy. This should at least include the termination of the outsourcing agreement for cloud services at the initiative of the undertaking or the CSP and the bankruptcy or other serious interruption of the CSP's business c. the carrying out of an impact assessment of the potential business damage proportional to the outsourced function in order to identify the human and other resources that would be required to implement the exit strategy d. the allocation of roles and responsibilities for managing the exit strategy e. testing the adequacy of the exit strategy through a risk-based approach (for example, through an analysis of the potential costs, consequences, resources and timing implications of transferring an outsourced service to another provider) f. the development of criteria for determining whether the transition has been successful.	For information/no remarks

33	An undertaking must include indicators of the events that may trigger the exit strategy in its ongoing monitoring and supervision of the services provided by the CSP under the outsourcing agreement for cloud services.	For information/no remarks
34	An undertaking should ensure that the written outsourcing agreement for cloud services does not restrict the effective exercise of access and audit rights and oversight options in relation to the CSP by the undertaking and the competent authority.	The standard agreement contains a right to audit and right to examine.
35	An enterprise should ensure that the exercise of access and audit rights (such as audit frequency and the areas and services to be audited) takes into account whether the outsourcing relates to a critical or important function and the nature and extent of the risks and consequences of the outsourcing agreement for cloud services for the enterprise.	For information/no remarks
36	In the event that the exercise of access or audit rights or the use of certain audit techniques poses a risk to the environment of the CSP and/or another customer of the CSP (e.g. by affecting service levels or the confidentiality, integrity and availability of data), the CSP must clearly identify why this would pose a risk and agree with the company on alternative courses of action to achieve a similar result (e.g. the inclusion of specific control measures tested in a specific report/certification of the CSP).	For information/no remarks. An audit will always be carried out in consultation, taking into account the rights and obligations of both the company and Blanco and other clients of Blanco.
37	Without prejudice to their ultimate responsibility for cloud service outsourcing arrangements, in order to make more efficient use of their audit resources and to reduce the organisational burden on the CSP and its customers, undertakings may use a. external certifications and external or internal audit reports provided by the CSP;	Blanco has ISAE3402 Type 2

	b. joint audits carried out jointly with other customers of the same CSP or by an external auditor appointed by several customers of the same CSP.	
38	In the case of outsourcing of critical or important functions, an undertaking should assess whether the external certifications and external or internal audit reports referred to in point 37(a) are appropriate and sufficient to fulfil its obligations under the applicable legislation, and it should endeavour not to rely exclusively on these certifications and reports over time.	For information/no remarks
39	In the case of outsourcing critical or important functions, an enterprise may use the external certifications and external or internal audit reports referred to in paragraph 37 a. only if it a. ensures that the certifications or audit reports cover the CSP's key systems (e.g. processes, applications, infrastructure, data centres), the key controls established by the firm and compliance with relevant applicable legislation; b. regularly reviews the contents of the certifications or audit reports and verifies that they are not outdated c. ensures that future versions of the certifications or audit reports cover essential systems and management measures of the CSP d. has ascertained the suitability of the certifying or audit party (e.g. qualifications, competence, recency of execution/control of documentary evidence in the audit file concerned and rotation of the certifying or audit organisation); e. satisfied that certifications have been issued, that audits have been performed to appropriate standards, and that they include a review of the effectiveness of the key management measures in place; f. has the contractual right to request the extension of the scope of the certifications or audit reports to other relevant systems and controls of the SPC, provided that the number and frequency of such	At the moment Blanco has two ISAE3402 reports; one for the KYC Suite and one for the PMS. The scope of the ISAE3402 with regard to the KYC Suite relates to information security, privacy and development processes. A large part of these processes are generic for the whole of Blanco. The ISAE3402 that relates to PMS mainly concerns data processing. Blanco is working towards a situation where both suites are covered by 1 ISAE3402 (expected in 2022). The reports are issued annually by an independent auditor.

	requests are reasonable and justified from a risk management perspective g. retain the contractual right to conduct individual on-site audits of the outsourced function at its discretion.	

40	A company must give the CSP prior notice of a site visit - including that of a third party appointed by the company (e.g. an auditor) - within a reasonable period of time, unless advance notice is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective. The notification shall indicate the location and purpose of the visit, as well as the personnel who will participate in the visit.	The standard agreement contains a right to audit and right to examine.
41	Since cloud services are technically very complex and present specific challenges in terms of competence, the personnel performing the audit - the company's internal auditors or auditors acting on its behalf - should have the appropriate skills and knowledge to assess the cloud services concerned and to conduct an effective and relevant audit. The same should apply to the company staff reviewing the CSP's certifications or audit reports.	For information/no remarks

	Guideline 7 - Subcontracting	
42	If sub-contracting of critical or important functions (or essential parts thereof) is permitted, the written outsourcing agreement for cloud services between the enterprise and the CSP must a. identify each part or aspect of the outsourced function that is excluded from potential subcontracting; b. specify the conditions that must be met in the event of sub-outsourcing c. specify that the CSP remains liable and must monitor and control the subcontracted services to ensure ongoing compliance with all contractual obligations between it and the company; d. include a requirement for the CSP to notify the undertaking of any proposed subcontracting or material changes thereto, in particular where it may affect the CSP's ability to meet its obligations under the cloud services outsourcing agreement with the undertaking. The notice period provided for in the written agreement shall allow sufficient time for the undertaking to carry out at least a risk assessment of the proposed subcontracting or any material modification thereof and to object to or expressly approve it, as set out in point (e) below e. ensure that the undertaking has the right to object to the proposed sub-outsourcing or any material modification thereof or that express approval is required before the proposed sub-outsourcing or any material modification becomes effective; f. ensure that the undertaking has the contractual right to terminate the outsourcing agreement for cloud services with the CSP in the event that it objects to the proposed sub-outsourcing or material changes thereto and in the event of unlawful sub-outsourcing (e.g. where the CSP proceeds with sub-outsourcing without informing the undertaking in advance) subcontracting without notifying the company or seriously violating the terms of the subcontracting as stated in the subcontracting agreement).	Blanco's standard agreement allows for services to be subcontracted. Particularly in the KYC Suite, Blanco uses service providers that specialise in a part of the service, for example digital signing, screening for sanctions and PEP lists or adverse media, and online verification of customer identity. Customers may object to subcontracting and may decide not to use certain functionalities (for which subcontracting is used). It is possible that the objection to certain subcontracting may result in termination of the agreement, for example if Blanco cannot reasonably accommodate the objection.

43	The company should ensure that the CSP has adequate supervision over the subcontractor.	Before subcontracting, Blanco will always investigate the relevant service provider and continue to monitor them during the provision of services.
	Guideline 8 - Written notification to competent authorities	
44	The undertaking must give timely written notice to the competent authority of planned outsourcing arrangements for cloud services involving a critical or important function. In addition, the undertaking must give timely written notice to the competent authority of those outsourcing arrangements for cloud services which concern a function which was previously classified as non-critical or non-important and subsequently became critical or important.	See also paragraph 4.5. of the Blanco paper.

45	The written notification from the undertaking shall include, subject to the principle of proportionality, at least the following information a. the start date of the outsourcing agreement for cloud services and, if applicable, the next date of the renewal of the contract, and the end date and/or notice periods for the CSP and for the undertaking b. a brief description of the outsourced function c. a brief summary of the reasons why the outsourced function is considered critical or important d. the name and brand name (if any) of the CSP, the country in which it is registered, the trade register number, the legal entity identification code (if any), the registered address, the relevant contact details and the name of the company's parent company (if any) e. the applicable law governing the outsourcing agreement for cloud services and, if applicable, the choice of law f. the deployment models for cloud services and the specific nature of the data to be retained by the CSP and the locations (i.e. countries or regions) where such data will be stored g. the date on which the criticality or importance of the outsourced function was last assessed h. the date of the most recent risk assessment or audit of the CSP and a brief summary of the main findings, and the date of the next scheduled risk assessment or audit i. the person or decision-making body within the undertaking that approved the outsourcing agreement regarding cloud services; j. where applicable, the names of the subcontractor to whom essential parts of a critical or important function have been subcontracted, including the country or region in which the subcontractors are registered, where the subcontracted service will be provided and where the data will be stored.	See also paragraph 4.5. of the Blanco paper. A prescribed notification form must be used for notifications to the AFM.

	Guideline 9 - Oversight of outsourcing agreements for cloud services	
46	As part of their supervisory review process, competent authorities should assess the risks arising from outsourcing agreements concluded by the undertaking regarding cloud services. This assessment should focus in particular on those agreements involving the outsourcing of critical or important functions.	Aimed at supervisor.

47	Competent authorities ensure that they can carry out effective supervision, especially when companies outsource critical or important functions outside the EU	Aimed at supervisor.
48	Competent authorities should assess on a risk-based approach whether firms a. have the necessary governance, resources and operational processes in place to enter into, implement and supervise outsourcing agreements relating to cloud services as appropriate and effective b. identify and manage all relevant risks associated with outsourcing of cloud services.	Aimed at supervisor.
49	Where concentration risks are identified, competent authorities should monitor the evolution of these risks and assess their potential impact on other undertakings under their supervision and on the stability of the financial market.	Aimed at supervisor.

Annex 3 - DNB Risk Analysis Template Outsourcing

Nr.	Topic	Explanation	Analysis	Chance	Impact	Risk	Measures	Residual risk
1	Vendor lock-in	The risk that it is not possible or not easy to switch to another service provider, e.g. because of technical limitations, because there are too few other service providers or because the current service provider is unable or unwilling to provide support in switching to a competitor.					Input Blanco: • Blanco wants to ensure as much as possible that data from customers is easy to transport and has an open architecture so that the software from Blanco can easily work together with other software that customers use. • The service agreement with Blanco can be terminated relatively easily contractually • In the event of the bankruptcy of Blanco, there is a contractual continuity measure in place, whereby a Foundation temporarily takes over the services of Blanco, allowing the investment firm to select another supplier or to decide to carry out the services itself.	

							• The investment firm may keep a list of potential parties that may take over (parts of) the services of Blanco's services if necessary.	

2	There are not enough resources to manage acquisitions and/or existing outsourcing agreements.	The institution needs resources (i.e. knowledge and personnel) for acquisition, for the application of outsourcing solutions and for monitoring suppliers. The latter involves the performance of the service provider, but also internal control, IT risk management and security. A lack of resources means that outsourcing is not (or no longer) managed, which can lead to undesirable risks for the institution that are not identified or dealt with. If one service provider delivers multiple outsourcing solutions, the overall impact of possible failures may increase with every additional activity the service provider delivers to the institution.				Input Blanco: • Blanco can periodically provide the investment firm with its ISAE3402 report, in which an external auditor gives an opinion on the IT environment of Blanco. • The agreement with Blanco contains mandatory clauses, e.g. regarding audit.	

3	Concentration					Input Blanco: • Blanco wants to ensure as much as possible that data from customers is easy to transport and has an open architecture so that the software from Blanco can easily work together with other software that customers use. • The service agreement with Blanco can be terminated relatively easily, if necessary. • In the event of a bankruptcy of Blanco, a continuity measure is contractually agreed, whereby a Foundation temporarily takes over the services of Blanco, allowing the investment firm to select another supplier or to decide to carry out the services itself. • Blanco is a solid company with a committed Supervisory Board and investors, with whom strategic and financial stability are	

						properly monitored and guaranteed • The investment firm may maintain a list of potential parties that may take over (parts of) the services of Blanco if necessary.	

4	Service provider ceases activities	The risk that data, systems and services become (immediately) unavailable once a service provider ceases its activities. The institution's daily operations may be disrupted and it may be difficult or impossible to retrieve data.					Input Blanco: • The agreement includes a provision on exit assistance • It is included in the agreement that the data remains property of the investment firm and that in case of termination of the agreement, the data will be deleted or transferred at the discretion of the investment firm. • In case of bankruptcy of Blanco, a continuity measure is contractually agreed upon, whereby a Foundation temporarily takes over the services of Blanco, so that investment firm can select another supplier.	

5	Compliance with laws and regulations	The institution shall retain responsibility for the outsourced activities and shall ensure that the service provider (and subcontractors) complies with applicable laws and regulations.					Input Blanco: • The Agreement stipulates that the Blanco software takes account of developments in legislation and regulations. • The agreement offers the possibility to test whether the software complies with laws and regulations and the service levels as agreed between the parties.	
6	Insufficient performance / results	The service provider does not comply with the quality standards or does not meet the agreements made, even though quantitative service levels are met. Or the service provider meets quantitative service levels, but quality standards are not met. Or qualitative and quantitative standards are not met. This involves monitoring and evaluation; certification, service level reports, assurance reports, audits.					Input Blanco • Where possible, Blanco reports on service levels and informs on developments within the organisation and with regard to the product. • Contractually the investment company can request an ISAE3402 Type II report.	

7	Data location	The data is subject to the legislation of the location where it is stored or passed. Such local legislation may differ from the Dutch legislation, which may pose a risk with regard to confidentiality requirements.					Input Blanco: • With regard to the PMS Module (AIRS), it currently uses a data centre in the Netherlands, which will be transferred to AWS data centre in the near future. • With regards to other products from Blanco, they are using AWS and have chosen the Frankfurt region for data storage. AWS will not move Blanco's data out of the selected regions without notifying Blanco, unless required to comply with the law or requests from government agencies. AWS fully complies with applicable EU data protection legislation. • A processor agreement is part of the agreement with Blanco. This agreement complies	

							with the requirements of the law. (AVG)	

8	Separation of environments	Facilities may be lost that provide separation of storage, memory, routing and may even impact the reputation of the various tenants of the shared infrastructure.					Input Blanco: • Blanco uses AWS and has conducted a cloud outsourcing analysis with respect to AWS. The following analysis is relevant in this context: Different instances running on the same physical machine are isolated from each other via the Xen hypervisor. AWS is active in the Xen community, which provides awareness of the latest developments. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors	

							have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms. Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer, so that one customer's data is never unintentionally exposed to another. In addition, memory allocated to guests is scrubbed (set to zero) by the hypervisor when it is	

							unallocated to a guest. The memory is not returned to the pool of free memory available for new allocations until the memory scrubbing is complete. In the Blanco-solution there is a logical seperation of data on tenants as well. They cannot cross-interfere because there is no capacity management needed per tenant or per solution.	
9	Data access	Is the data handled in a legally correct manner? This includes compliance with regulations, such as encryption standards, management of encryption keys, the four-eyes principle and authentication					Input Blanco: Blanco has an ISAE3402 Type 2 report, which includes the encryption strategy and an access & identity policy.	

10	Cyber attacks	All risks related to cyber attacks, such as DDoS attacks, data interception or leakage, social engineering, unauthorised access, unauthorised gain of rights and ransomware					Input Blanco: • Blanco uses AWS and has conducted a cloud outsourcing analysis with respect to AWS. The following analysis is relevant in this context: AWS API endpoints are hosted on large, Internet- scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS' networks are multi-homed across a number of providers to achieve Internet access diversity.	

							Blanco added AWS WAF (Web Application Firewall) for parts of the solution. This will help against DDOS. Also, Blanco can block specific countries if needed.	

Extra risico suggestie Blanco:

11	Lost backup	Due to insufficient physical security procedures, user facility vulnerabilities, user deprovisioning vulnerabilities.					Input Blanco: • Blanco uses AWS and has conducted a cloud outsourcing analysis with respect to AWS. The following analysis is relevant in this context: AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS	

							data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and	

							contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.	