COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 18 July 2012

To all support PFS

CIRCULAR CSSF 12/544

Re: **Optimisation of the supervision exercised on the "support PFS" by a risk-based approach**

Ladies and Gentlemen,

This circular applies to all PFS exercising one or several support PFS activities as defined in Articles 29-1, 29-2, 29-3 or 29-4 of the law of 5 April 1993 on the financial sector **and** classified as "I" by the CSSF (please refer to the identification numbers published on the website www.cssf.lu).

The CSSF's mission is to protect the financial stability of the supervised entities and of the financial sector as a whole as well as to ensure compliance with the financial laws and regulations applicable to the supervised entities.

Support PFS provide services which are operational and technical rather than financial and are not professionals of the financial sector by nature. Their services may be provided to any type of undertakings whether they belong to the financial sector or not. The fact that they provide services to financial professional clients qualifies them as professionals of the financial sector and subjects them to the supervision by the CSSF.

But this service provision can increase or trigger certain risks in the financial sector. The degree of risk that every support PFS puts the financial sector at may vary greatly from one support PFS to another depending, among others, on the nature of the provided services as well as on the market share and organisation of the support PFS concerned. For clarity reasons, we would like to specify that the risks are not those of financial professional clients of the support PFS, such as dependence on providers, loss of expertise, etc. which shall be dealt with by the financial professional clients themselves, but the risks of support PFS which can have a direct or indirect impact on financial professional clients and thus representing a risk for the latter.

The CSSF's findings led it, in April 2008[1], to note that it became crucial for it, as well as for support PFS, to refocus the prudential supervision as regards the issues and risk exposures exclusively brought upon the financial sector and that the CSSF was reflecting on this matter. Thus, the CSSF recommended to support PFS to "prepare for the implementation of risk assessment and management process for the provision of service to the financial sector".

The materialisation of the CSSF's reflection in this matter is the result of its will to optimise the supervision exercised on support PFS by introducing a new concept of risk-based approach. This will is in line with the increasing number of support PFS since the creation of the relevant statuses and with the diversity of the activities provided by them.

This refocusing of the supervision as regards the issues and risks generated in the financial sector[2] relies on:

1. the application of the principle of proportionality according to the importance of the activity exercised in the financial sector by the support PFS: the importance of the activity may be qualified, on the one hand, from the financial sector's point of view (importance of the activities outsourced to support PFS for clients) and, on the other hand, from the support PFS' point of view (weight of the financial sector in the total number of clients of the support PFS);

2. self-assessment and management taken into account by the support PFS as regards risks they put the financial sector at and which are subject to an annual **risk assessment report (RAR)** by the support PFS; a description of the activities exercised in the financial sector, the organisation and infrastructure of the support PFS - to be provided annually in a **descriptive report (DR)** - will facilitate the comprehension and analysis of the risks reported in the RAR. Pursuant to the principle of proportionality, the CSSF expects the volume of the DR to be proportional to the volume of the activity exercised in the financial sector by the support PFS;

3. the definition of the practical rules concerning the mission of *réviseurs d'entreprises agréés* (approved statutory auditors) of these entities and the drawing-up of a **long form audit report (LFR)**. The purpose of the LFR is to report the main observations of the *réviseur d'entreprises agréé* allowing a precise and justified assessment of the organisation, the internal control system, the financial situation and the risks incurred by the audited support PFS which may have a direct or indirect impact on financial professional clients. Pursuant to the

[1] Circular CSSF 08/350 regarding details relating to the amendments introduced by the law of 13 July 2007 on markets in financial instruments to the PFS statuses referred to in Articles 29-1, 29-2, 29-3 or 29-4 of the law of 5 April 1993 on the financial sector (the "LFS") and referred to as “support PFS”; Amendment to the prudential supervisory procedures for support PFS.

[2] The terms "financial professionals" or "financial sector" include, in this circular, the insurance and reinsurance undertakings clients unless otherwise mentioned. The risks encompass those for Luxembourg and foreign financial professional clients of the support PFS.

principle of proportionality, the CSSF expects the volume of the LFR to be proportional to the volume of the activity exercised in the financial sector by the support PFS.

This refocusing of the supervision includes two stages.

This circular (stage 1) specifies, first, the content of the risk assessment report and, second, the content of the descriptive report, knowing that these two documents constitute an important information source for the management of the support PFS in the framework of the management function as well as for the CSSF in the framework of its prudential supervisory mission.
In the final and transitional provisions, the circular sets out the submission of the first risk assessment reports and descriptive reports to the CSSF as from 2013.

A second circular (stage 2) will define the practical rules as regards the mission of *réviseurs d'entreprises agréés* of support PFS and the content of the long form audit report, completing thus the procedure for the optimisation of supervision.

CONTENTS

I. General Principles

The support PFS draws up annually:

- a report on its risk management system and its self-assessment on the risks as regards the financial sector ("risk assessment report" or "RAR");

- a report describing its administrative and accounting organisation, its internal control system, its IT infrastructure (for internal usage or supporting the services to clients), its activities and its financial situation ("descriptive report" or "DR").

The support PFS is responsible for the truthfulness of all the elements included in these two reports. Therefore, the management[3] shall sign these reports.

The RAR and DR are issued for the management and administrative bodies of the support PFS concerned and for the CSSF. The minutes of the board of directors (or management board) shall include the transmission of the RAR to the members of the board.

Generally, the support PFS is the main compiler of the RAR and DR. However, the support PFS may, if it wishes, take an external support in order to draw up some descriptive parts, without limiting, however, its own responsibility as regards the truthfulness of all included elements.

The support PFS shall send the RAR and DR to the CSSF within three months at most as from the end of the financial year[4].

As soon as it comes to their attention, the support PFS shall inform the CSSF of any reported delays and indicate the reasons for and the probable duration of the delay.

The RAR and DR shall be transmitted to the CSSF on paper **and** electronically. A circular will be dedicated to the electronic transmission methods.

II. Risk assessment report regarding the financial sector ("RAR")

The support PFS[5] includes in its risk assessment report:

- a description of its risk management system;
- its self-assessment of the risks at which it puts its clients of the financial sector.

[3] "Management" means in this circular "the persons responsible for the daily management and authorised pursuant to Article 19(2) of the LFS".

[4] Please refer to the final and transitional provisions as regards the deadline applicable for the first year.

[5] Each time the term "support PFS" is mentioned in the provisions of Part II.A. and II.B hereunder, it means "support PFS, including its branches".

II.A. Management system of risks for the financial sector

The support PFS provides a description of its management system of risks for the financial sector which includes at least the following elements:

- the roles and responsibilities of the various stakeholders (actors) to this system;
- the implemented methods and procedures for the identification, assessment, validation, limitation, monitoring and reporting of risks;
- the tools which are possibly used for the management and documentation of risks.

As regards the role and responsibilities, the support PFS notably indicates:

- the member of the management responsible for risk management;
- if the risk management function is internally entrusted to one or more person(s). These persons must have the necessary independence, from a hierarchical point of view, in order to adequately take on the responsibility;
- if the risk management function is entrusted to an external expert in risk management and the latter's name.

Smaller-sized institutions carrying out a low-risk activity, are authorised to renounce entrusting the risk management function to a service or full-time employee. These institutions may use external experts in risk management provided that the CSSF issues prior authorisation for such an outsourcing.

The outsourcing of the risk management shall not jeopardise the principle of continuity of the risk management process, by limiting oneself for example to one single risk assessment exercise per year.

The risk management cannot in any case be entrusted to a *réviseur d'entreprises agréé* or internal auditor of the support PFS or its group. Upon the support PFS' request, its *réviseur d'entreprises agréé* may thus only be in charge of the description of the risk management system; he cannot be in charge or support the risk management (including the identification, assessment, validation, limitation, monitoring and reporting of risks).

II.B. Self-assessment of direct and indirect risks for the financial sector

The support PFS must provide a description and self-assessment of the risks, whether direct or indirect, its financial sector clients may incur as defined under points II.B.1 and II.B.2 respectively.

It shall assess the materiality, or, in other words, the criticality of each identified risk and shall therefore consider the following two variables:

- the occurrence probability of the risk (P), and;
- the impact of the risk (I) if it occurred, knowing that it may be of several types: financial, legal and regulatory, operational etc.

The support PFS shall determine the probability level and the level(s) of impact(s) applicable to the probability and impact ladders provided for in **Annexe 1**. The materiality of a risk will be then determined by multiplying the applied probability level by the applied impact level (P x I). If several types of impacts are applicable for one risk, the support PFS will chose the highest for the calculation of the materiality of the risk.

Thus, for example, if a risk has an occurrence probability of 4, a financial impact of 3 and a legal impact of 5, the materiality of the risk will be 4 (probability) multiplied by 5 (legal impact because it is the highest), i.e. a materiality equivalent to 20.

For each identified risk, the support PFS will calculate:

- the gross materiality of risk, i.e. the existing controls are not taken into account (gross risk);
- the net materiality of risk, i.e. the existing means to reduce or transfer the risk are taken into account (net risk); if no means exist at the time of assessment, the net materiality is equal to the gross materiality;
- if applicable, the expected materiality of risk, i.e. by anticipating the effects of an action plan proposed to decrease or transfer the risk when the net materiality of risk was considered as too high, i.e. unacceptable.

The risks to be included in the risk analysis report[6] will be limited to 20 direct risks (as defined under point 1.1. hereafter) and 5 indirect risks (as defined under point 1.2. hereafter). The risks to be reported are those which received the highest scores during the calculation of the net materiality (the highest results of the transactions (P_{net} x $I_{net\ the\ highest}$)).

Nevertheless, any direct or indirect risk the net impact of which is equal to or higher than six and which has at the same time a net probability equal to or higher than five is also to be reported, even if the limits of 20 and 5 risks mentioned in the previous paragraph are reached.

A risk reported in the RAR may not be reported the following year if the mitigation measures implemented in the meantime classify the risk as not to be reported in accordance with the criteria mentioned above or if the risk is no longer relevant due to a change of activities or organisation. Any deletion of a risk from one RAR to the other shall be subject to an explanation reasoning this deletion.

For all the risks to be included in the risk analysis report, the following information shall be reported in a risk sheet (an example is available in **Annexe 2**):

- a risk number (identification):
- the name of the risk;
- a brief and clear description of the risk;
- an indication if this risk concerns all the financial sector professional clients of the support PFS or only some of them; in the latter case they shall be named;
- the risk category, to be chosen among the categories presented under points 1.1. and 1.2.;

[6] Please refer to the final and transitional provisions as regards the risks to be included in the first risk analysis report.

- the probability level, the impact level(s) and the materiality of the risk (P x I) determined by the PFS without taking into account the existing risk controls (gross risk) and a justification of this materiality (the materiality for the financial sector professional clients assessed by the PFS shall be considered and not the materiality for the support PFS);
- the existing means implemented by the PFS to reduce (mitigation) or transfer (insurance) and monitor the risks;
- the reference to the internal audits carried out to check the existence and efficiency of these mitigation aspects;
- the probability level, the impact level(s) and the materiality of the risk (P x I) determined by the PFS after taking into account the existing means to reduce or transfer the risk (net risk); if there are no means at the time of the assessment, the net risk is equal to gross risk;
- the argued response strategy in relation to risks having regard to its net materiality: accept the risk (because it has low materiality or is outside the control of the PFS), implement an action plan to reduce (mitigation) or transfer the risk (insurance), avoid the risk (by discontinuing an activity for example);
- a brief and clear description of the future action plan to reduce or transfer the risk, when it is deemed unacceptable;
- the expected materiality (P x I) of the risk when the action plan is realised.

The risk sheets will be provided in the order of the risk identifiers.

A risk register (an example is available in **Annexe 3**) shall present a summary of the risks according to the decreasing net materiality.

Any event occurring during the year and significantly changing the financial sector risk profile of the PFS (e.g. a new emerging significant risk or upward reassessment of the materiality of a risk already identified) shall be reported to the CSSF by the support PFS without waiting for the issue of the next risk analysis report. The report shall include a description of the new or reassessed risk(s) in the form of a risk sheet as presented above.

1. Direct risks

Direct risks are risks directly related to the activities carried out in the financial sector and which have a direct impact on the clients benefiting from these activities.

The risk analysis shall relate to the following risk categories:

- **D1 ("direct 1") - Strategic risks / commercial policy:** Example: the main market of the PFS is not the financial sector, the latter not having thus the priority as regards the means implemented to provide quality services.

- **D2 - Operational risks - Human Resources**: the personnel directly required to provide services to the financial sector is concerned. Examples: understaffed, unqualified personnel, excessive use of temporary employees, absence of replacement for a key function, etc.

- **D3 - Operational risks - Processes**: the processes directly linked to the service provision to the financial sector. Examples: absence of documentation for key procedures, insufficient internal control, etc.

- **D4 - Operational risks - Continuity of operations**: operations required for the delivery of the services to the financial sector are concerned. Examples: non-existing / incomplete / not tested Business Continuity Plan; non-existing / incomplete / not tested Disaster Recovery Plan; absence of coordination with the client's, possibly the group's or subcontractor's etc. BCP/DRP.

- **D5 - Operational risks - Cascade outsourcing:** the outsourcing to a third company (outside or intra-group) of operations required for the provision of financial sector services is concerned. Examples: insufficient control of the cascade outsourcing (insufficient control by the PFS of the quality of the provided services; compliance with professional secrecy; service agreement between the PFS and its subcontractor), etc.

- **D6 - Operational risks - Information systems**: the information systems for external use as described under point 3.3. of Section III.B. are concerned. The risks relating to the following areas shall be considered:

    - **D6.1 - Information security** (confidentiality, integrity, continuity, traceability): Examples: absence/inadequacy of security, management and monitoring policy; of physical and logical segregation of clients environments in case of mutualisation; of physical security; of logical security of the systems and incoming and outgoing communications, management of security failures, etc.;

    - **D6.2 - Acquisition, development and maintenance of systems** (adequacy of solutions according to the client's needs): Examples: absence/inadequacy of acquisition or development procedures for new applications, change of already existing applications, quality and startup control, documentation, etc.;

    - **D6.3 - Operating procedures** (management of batch processing, backups, printing of reports, etc.): Examples: absence/inadequacy of planning, sequencing and control procedures; control procedures for outputs and processing; backup, restoration and archiving procedures; management procedures for incidents, etc.;

    - **D6.4 - Technical support of information systems:** Examples: absence/inadequacy of maintenance procedures of basic software; maintaining and administering databases; typology of the internal network; maintaining and supervising communication networks; user and computer-related technology support, etc.

- **D7 - Other relevant risk categories** considering the activities carried out by the support PFS for its financial sector clients.

2. Indirect risks

Indirect risks are risks related to the organisation and administration of support PFS or its provisions outside the financial sector **and** whose impact creates an indirect risk for its financial sector professional clients.

The risk analysis shall relate to the following risk categories:

- **I1 ("Indirect 1") - Strategic and governance risks:** Examples: failure/disengagement risk of the PFS following a management decision, a development, repurchase or maladapted restructuring strategy (decided locally or at group level if applicable), absence (or inefficiency) of its own risk management system, etc.

- **I2 - Financial risks**: Examples: failure/disengagement risk due to a bad financial situation (profitability), risky investments, etc.

- **I3 - Legal and regulatory risks**: Examples: failure/disengagement risk due to legal proceedings/sanctions or loss of the support PFS authorisation, etc.

- **I4 - Operational risks - Human Resources**: the personnel required for the organisations and administration of the support PFS is concerned. Examples: major organisational troubles due to understaffed, unqualified personnel, absence of replacement for a key function, etc.

- **I5 - Operational risks - Processes**: the processes linked to the organisations and administration of the support PFS are concerned. Examples: major organisational troubles due to the absence of documentation for key procedures, insufficient internal control, etc.

- **I6 - Operational risks - continuity of operations**: the operations required for a sound organisation and administration of the support PFS are concerned. Examples: Non-existing / incomplete / not tested Business Continuity Plan; non-existing / incomplete / not tested Disaster Recovery Plan; where applicable, absence of coordination with the group's or a subcontractor's BCP/DRP (no redundancy of the communication line to the outsourced accounting system, no premises/replacement materials), etc.

- **I7 - Operational risks - Cascade outsourcing**: the outsourcing to a third company (outside or intra-group) of operations required for a sound organisation and administration of the support PFS is concerned. Examples: insufficient control of the cascade outsourcing (insufficient control by the PFS of the quality of the provided services; information confidentiality; service agreement between the PFS and its subcontractor; etc.).

- **I8 - Operational risks - Information systems**: the information systems for internal use as described under point 2.8. of Section III.B. are concerned. The risks relating to the following areas shall be considered:

  - **I8.1 - Information security** (confidentiality, integrity, continuity, traceability): Examples: absence/inadequacy of security, management and monitoring policy; of physical security; of logical security of the systems and incoming and outgoing communications; of management of security failures, etc.;

  - **I8.2 - Acquisition, development and maintenance of systems** (adequacy of solutions according to the PFS' needs): Examples: absence/inadequacy of acquisition or development procedures for new applications, change of already existing applications, quality and startup control, documentation, etc.;

  - **I8.3 - Operating procedures** (management of batch processing, backups, printing of reports, etc.): Examples: absence/inadequacy of planning, sequencing and control procedures; control procedures for outputs and processing; backup, restoration and archiving procedures; management procedures for incidents, etc.;

  - **I8.4 - Technical support of information systems:** Examples: absence/inadequacy of maintenance procedures of basic software; maintaining and administering databases; typology of the internal network; maintaining and supervising communication networks; user and computer-related technology support, etc.;

- **I9 - Risks related to a provision outside the financial sector:** Examples: financial risk (fees on an important contract etc.), indirect reputational risk (reputational spillover), in case of failure of a major non-financial sector project which was given media coverage, etc.

- **I10 - Other categories of relevant risks** according to the organisation and administration of the support PFS or its group and whose impact for the support PFS creates an indirect risk for its financial sector professional clients.

The CSSF reserves the right to assess and comment on the quality of the risk management system of the support PFS and whether or not the risk mitigation measures implemented by the support PFS are sufficient.

III. Descriptive report ("DR")

III.A. Format of the descriptive report

The descriptive report must be drawn up according to the format below. The format in question corresponds to the minimum information that must be provided by the support PFS in its report. It may be adapted to the nature and complexity of the activities, as well as to the structure of the company. Where applicable, the support PFS shall supplement the format by aspects it deems appropriate. Where a specific item of the format does not apply to the support PFS, the latter explicitly mentions it.

1. Significant events

2. Organisation and administration
   - 2.1. Description of the shareholders
   - 2.2. Management in charge of the daily management
   - 2.3. Organisation chart of the support PFS and of the group to which it belongs
   - 2.4. Central administration
   - 2.5. Administrative organisation
   - 2.6. Accounting function
   - 2.7. Internal control
   - 2.8. Information system for internal use

3. Activities carried out in the financial sector
   - 3.1 Description of the activities carried out
   - 3.2 Partnerships / cascade outsourcing
   - 3.3 Information system for external use
   - 3.4 Business Continuity Plan and Disaster Recovery Plan (BCP/DRP)

4. Periodic reports to be communicated

5. Analysis of annual accounts

6. Professional obligations as regards the prevention of money laundering and terrorist financing

7. Professional obligations as regards the rules of conduct

8. Relations with affiliated undertakings

9. Branches abroad

10. Subsidiaries abroad

III.B. Comments relating to the descriptive report

1. Significant events

The support PFS shall indicate, where applicable, the significant events which took place during the year under review and which may impact its situation. These events represent, for example, decisions on strategies, important reorganisation, launch or discontinuation of activities, merger/acquisition operations or collaboration/partnership.

Significant events which may trigger risks for financial professional clients of the support PFS shall be included in the risk analysis report of support PFS as requested in Chapter II of this circular (i.e. they are taken into account in the risk management system as described under point II.B.1 and detailed in the risk self-assessment as described under point II.B.2).

The support PFS shall specify where no significant events took place during the year under review.

2. Organisation and administration

The support PFS will provide under this item an overview of its operational, decisional and governance structure (outside the risk management system covered in the risk analysis report).

2.1. Description of the shareholders

The support PFS shall describe its direct shareholders, as well as those of the group to which it belongs; this structure will be presented in the form of an organisational chart with capitalistic links.

A copy of the report on annual accounts, the annual accounts and the management report of the direct majority shareholder shall be appended to the descriptive report.

In case its direct majority shareholder is not subject to the obligation to provide a management report, the support PFS shall, however, provide - with the report on annual accounts and the annual accounts of its direct majority shareholder - information on the development of the business and the situation of the shareholder and indications on this shareholder concerning:

- any important events that have occurred since the end of the financial year;
- the company's likely future development;
- activities in the field of research and development;
- information prescribed by Article 49-5(2) of the law of 10 August 1915 on commercial companies, as amended, as regards acquisitions of own shares;
- the existence of branches of the company.

2.2. Management in charge of the daily management

The support PFS shall describe the responsibilities of the management in charge of the daily management and the scope of powers necessary for the good performance of its mission that the board of directors (or management board) will confer on it.

It specifies, among others, if there are:

- possible limits imposed on the local decisions of the support PFS by the board of directors (or management board) involving a group;
- the decisions of the board of directors (or management board) locally imposed on support PFS and which may infringe the Luxembourg laws and regulations.

If the limits and/or decisions are likely to create a direct or indirect risk for the activities carried out in the financial sector by the support PFS, the latter shall include them in its risk analysis report as requested in Chapter II of this circular (i.e. they are taken into account in the risk management system as described under point II.B.1 and detailed in the risk self-assessment as described under point II.B.2).

2.3. Organisation chart of the support PFS and of the group to which it belongs

The support PFS shall provide as a graph:

- its internal organisation chart by indicating hierarchical and functional lines and the number of employees per service;
- the organisation chart of its group showing its position within the group.

2.4. Central administration

The support PFS shall briefly describe the organisation of its central administration.

2.5. Administrative organisation

The support PFS shall briefly describe its administrative organisation.

In case the support PFS outsources the administrative services, it shall also briefly and precisely describe:

- if this outsourcing is subject to a contract (SLA);
- the supervision in place at the PFS in order to monitor the services subject to outsourcing;
- if the outsourcing is clearly mentioned in the general terms and conditions of the contracts with the financial sector clients, in case this outsourcing resulted in the localisation abroad of data concerning financial sector professional clients[7], or the access from abroad to these data.

2.6. Accounting function

The support PFS shall briefly describe the operation of the accounting function.

[7] For example, the name of the client.

In case the support PFS outsources the accounting function, it shall also briefly and precisely describe:

- if it is able to have permanent access to the accounting documents and financial statements;
- if this outsourcing is subject to a contract (SLA);
- the supervision in place at the PFS in order to monitor the services subject to outsourcing;
- if the outsourcing is clearly mentioned in the general terms and conditions of the contracts with the financial sector clients, in case this outsourcing resulted in the localisation abroad of data concerning financial sector professional clients[7], or the access from abroad to these data.

2.7. Internal control

The support PFS shall describe the way in which its internal control system is organised.

2.7.1 Internal procedures

The support PFS indicates under this item if there is a procedure manual covering all the activities carried out within the company and which may directly or indirectly impact on the financial sector professional clients.

The support PFS also mentions if, pursuant to its obligations:

- there is indeed a training programme for its employees in place notably in relation to the compliance with the confidentiality of the financial sector professional clients' data and the prevention of money laundering and terrorist financing;
- the contracts used indeed include a confidentiality clause, as well as a reference to criminal proceedings incurred in case of violation of the professional secrecy[8].

2.7.2 Internal information and management control systems

The support PFS shall describe the internal information and management control systems, in particular, the management information system (MIS).

2.7.3 Audit committee

In the event the support PFS has its own audit committee[9] (a possible audit committee at group level is not concerned here), it shall describe the composition, functioning modalities, the frequency and agenda of this committee's meetings.

[8] As laid down in Article 41(1) of the LFS.

[9] In accordance with point 6 of Circular IML 98/143 and Article 74 of the law of 18 December 2009 concerning the audit profession.

2.7.4 Internal audit

The support PFS shall describe the internal audit function (in-house, support of the parent company, use of an external expert or of a third professional in which case the coordination with the person responsible for the follow-up of works shall be described).

2.7.5 Reports

The support PFS shall include the following two reports appended to the descriptive report[10]:

- the written report of the management on the state of the internal control;
- a copy of the summary report on the controls carried out by the internal audit during the previous financial year[11]. The summary report shall be presented in the form of a table summarising the main recommendations. The report shall be divided into two parts: the purpose of the first part will be to follow up the recommendations issued during the interventions of the internal audit for the financial year under review; the purpose of the second part will be to follow up the recommendations issued during the interventions of the internal audit carried out during the past financial years. As previously mentioned, each of these two parts shall be presented in the form of a table. The columns of the table shall at least mention in the following order:
  - the date of the assignment;
  - the perimeter or area of the assignment;
  - the reference (number) of the observation;
  - the observation;
  - the risk level (for example: "high, medium or low");
  - the recommendations;
  - the comments from the management of the support PFS;
  - the implementation deadlines;
  - if applicable, the reference of the related risk identified in the risk analysis report of the support PFS.

The support PFS shall also append the following documents:

- a copy of the letter(s) of assignment entrusted to the internal auditor;
- the multiannual programme of the internal audit approved by the management and/or board of directors (or management board); the audit programme shall necessarily cover, among others, the decreasing aspects (mitigation) of the main risks identified in the risk analysis report of the support PFS;
- the internal audit charter.

The support PFS shall also append a table relating to the persons designated as being responsible for certain functions pursuant to the CSSF circulars[12].

[10] In accordance with point 8 of Circular IML 98/143.

[11] In accordance with points 5.4.7.d) and 5.4.9 of Circular IML 98/143.

[12] To that end, the PFS can refer to table B 4.6 as defined in Circular CSSF 09/424.

Finally, the support PFS shall append an up-to-date list of the members of the management in charge of daily management.

2.8. Information systems for internal use

The support PFS shall describe the IT systems and processing for internal use.

The systems supporting the support PFS' organisation and administration are considered as information systems for internal use. Thus, they do not belong to the IT infrastructure which partially or exclusively supports the activities carried out for the support PFS' clients.

For example and without them representing an exhaustive list, the following systems are considered as information systems for internal use: accounting systems, staff and payment management of the support PFS; management systems for clients' orders, purchase management, client relationship management but also email servers, the internal files servers, internet website of the support PFS (not the one used for services provided to its clients), the personnel's workstations.

2.8.1 Summary table

The support PFS shall provide a summary table of the information systems for internal use (cf. an example in **Annexe 4**) linking the main functions necessary for the internal functioning of the support PFS with the IT elements operating them. These IT elements shall be broken down into physical or virtual infrastructure elements (IT platforms and their operating system) and software elements (IT applications or programme systems).

2.8.1.1. Physical infrastructure

The main physical hardware elements (computers and peripheral equipment) operating one or several main functions shall be identified by their brand, model, operating system (including number of the version), their redundancy mode (none, hot/cold standby, cluster etc.) and the reason for redundancy (criticality of functions, distribution of the charge, mixed).

When the provided information is the same for several elements, the summary table shall present it once by indicating the identification number or name and the total number of the elements concerned.

The workstations shall not be included in the description if they do not operate at least one main function of the activity.

2.8.1.2. Virtual infrastructure

a) The main physical hardware elements that support the virtual machines operating one or several main functions shall be identified by the same information as those mentioned in the first paragraph of point 2.8.1.1. above.

   When the provided information is the same for several elements, the summary table shall present it once by indicating the identification number or name and the total number of the elements concerned.

   It shall also specify the number of virtual machines hosted by each physical machine.

   The workstations shall not be included in the description if they do not operate at least one main function of the activity.

b) The main virtual hardware elements operating one or several main functions shall be subject to a simplified description that specifies} at least the type of virtual machine (VM, XEN, etc.) and their operating system (including the version number).

   When the provided information is the same for several elements, the summary table shall present it once by indicating the identification number or name and the total number of the elements concerned.
   It shall also specify the identification number or name of the physical machine hosting the virtual machines.

2.8.1.3. The software elements

As regards the software elements operating one or several main functions, the summary table shall provide information on:

- the name of the software or software package;
- development:
  - development (with or without use of outsourcing);
  - software package (with the indication of the provider’s name);
  - modified software package (if over 20% of the functionalities were modified) with an indication of the participants in the modifications (internal, provider, mixed).
- significant modifications made since the previous financial year.

2.8.1.4. Outsourcing and localisation of systems

Outsourcing[13] the internal IT systems or processing, as well as the localisation of the systems shall be specified for each system concerned. For each hardware element (physical or virtual), the summary table shall notably provide an answer to the following questions:

- Is the element intended only for the support PFS or shared with other entities?
- Does the PFS outsource and, if yes, what is the nature of the outsourcing (only hosting or operation provision)?
- Who operates the element: the PFS or a third service provider to be specified (an entity of the group shall be considered as third service provider)?
- Where is the system located? Indicate the locations (of the PFS, a third provider including an entity of the group?) and the country if the system is abroad.
- In case of outsourcing, is there a resumption plan (transfer to another provider or managing on its own), in the event the continuity or quality of the service provision is jeopardised?

2.8.2 Network architecture and external connections

The support PFS shall provide a description and/or a scheme of its network architecture comprising the main security elements (DMZ, firewalls, IDS, routers, proxy, etc.). In case it is impossible or useless to differentiate the network architecture required for the internal functioning of the PFS from that required for the activities carried out in the financial sector, please refer to point 3.3.3.

The support PFS shall list the connections useful for the internal functioning to or from the exterior (including with its group, where applicable), by specifying the control that it exercises of these accesses (separate Active Directory, opening/closing of the communication lines, logs, etc.) and the redundancy measures of these connections.

3. Activities carried out in the financial sector

3.1. Description of the activities carried out

The support PFS shall precisely describe the type and volume of its activities. On the one hand, a distinction shall be made between the activities carried out in the financial sector, insurance sector and other activities and on the other hand, a distinction between the activities requiring an authorisation as support PFS and those which do not.

The support PFS shall also specify, where appropriate, the mode of service provision. For example:

[13] Within the meaning of Circular CSSF 05/178

- for an administrative agent: "Business Process Outsourcing" services delivered on the support PFS' premises and on its own mutualised IT system;
- for a primary IT systems operator: making available and managing an "Infrastructure as a Service" located on its premises in a dedicated or shared mode;
- for a secondary IT systems operator: management of the network on the client's premises;
- for a client communication agent: impression and sending letters to clients of the financial professional client on its own systems and premises.

A change in the activities' nature, the cessation of an activity or the start of new activities or exceptional or significant events during the year under review should be reported under point 1. "Significant events".

The support PFS shall also provide a nominative list of its financial sector clients from Luxembourg or abroad for which it provides services requiring a PFS authorisation and specifying for each one of them:

- the activity sector concerned (finance/insurance);
- the country of residence (Luxembourg/abroad);
- the nature of the provision (main activities carried out);
- the location of the provision;
- and if it is offered through off-site or on-site.

For each type of support PFS authorisation it holds, the support PFS shall append a copy of the client agreement relating to the service provisions requiring such authorisation.

3.2. Partnerships / cascade outsourcing

The support PFS shall indicate the possible existence of a partnership or cascade outsourcing (with external companies or within the group) for carrying out activities in the financial sector and specify the nature (expertise, availability of profiles, provision requiring the authorisation).

It shall also specify:

a. its own staff (in number of full-time equivalent (FTE)) directly required for the provision of services to clients (all sectors);
b. the percentage of staff defined in point a. allocated to the provision of services in the financial sector (dedicated staff);
c. the percentage of the staff defined in point a. allocated at the same time to the financial sector services **and** services to other sectors (common staff);
d. the staff (in number of FTE) of possible subcontractors permanently used by the support PFS for the service provision in the financial sector;
e. the percentage of the staff available to the financial sector (staff defined in point b.) represented by subcontractors;
f. the percentage of the common staff available to the financial sector (staff defined in point c.) represented by subcontractors.

Finally, the support PFS shall describe the elements allowing it to manage this cascade outsourcing, such as:

- control by the PFS of the quality of services provided by the subcontractor (among others, checking the existence of performance measurement indicators);
- taking into account by the subcontractor of the risks for the client (existence of a risk analysis and transmission of the results to the support PFS);
- compliance with professional secrecy, notably if the subcontractor or partner does not himself have the status of support PFS;
- existence of a service agreement between the PFS and its subcontractor;
- information from the clients about the existence of this cascade outsourcing;
- maintenance of a sufficient PFS substance within the support PFS.

3.3. Information systems for external use

The support PFS shall describe the IT systems and processing for external use.

The following shall be considered as information systems for external use:

1. systems that partially or exclusively support the activities carried out for financial sector professional clients of the support PFS, irrespective of their belonging to the client of PFS or of their location;
2. and for which the support PFS is responsible as regards the sound functioning in relation to the client.

These two conditions are cumulative in order to determine if a system is qualified as system for external use within the meaning of this circular and is thus concerned by this section.

The term "system" may be limited here to a software if the provision is only about a software.

For example, an administrative agent which provides asset accounting services to professionals of the financial sector on its own accounting system and on its own premises - system which it already used and continues to use for its own activity - may, at first sight, consider this accounting system as an internal system. However, this system shall indeed be considered as an external system within the meaning of this circular, since it also supports the activity carried out in the financial sector, the administrative agent is responsible of its sound functioning and it has the power to decide on the system supporting the provision.

Similarly, an administrative agent which provides asset accounting services to professionals of the financial sector on its own accounting system, but which outsources the management of its system to a third party, shall consider this system as concerned by this section. Indeed, irrespective of the use of outsourcing, the administrative agent remains responsible towards the clients as regards the functioning of the system and may retain a decision-making power relating to the choice of the system supporting the provision.

3.3.1 Summary table

The support PFS shall submit a summary table (cf. the example in **Annexe 5**) linking the main functions (including techniques like firewalls, for example) necessary for the services it provides to the financial sector, with IT elements which operate them. These IT elements are broken down into physical or virtual infrastructure elements (IT platforms and their operating system) and software elements (IT applications or programme systems).

3.3.1.1. Physical infrastructure

The main hardware elements (computers and peripheral equipment) operating one or several main functions will be identified by their brand, model, operating system (including number of the version), their redundancy mode (none, hot/cold standby, cluster, etc.) and the reason for redundancy (criticality of functions, distribution of the charge, mixed).

When the provided information is the same for several elements, the summary table shall present it once by indicating the identification number or name and the total number of the elements concerned.

The total number of clients of the financial sector supported by each element shall be specified.

The workstations shall not be included in the description if they do not operate at least one main function of the activity.

3.3.1.2. Virtual infrastructure

a) The main physical hardware elements that support the virtual machines operating one or several main functions shall be identified by the same information as that mentioned in the first paragraph of point 3.3.1.1. above.

   When the provided information is the same for several elements, the summary table shall present it once by indicating the identification number or name and the total number of the elements concerned.

   It shall also specify for each physical machine the number of hosted virtual machines, the total number of clients and the number of supported financial sector clients or any other information relevant for the risk concentration assessment of clients on the same machine (for instance, the volume of transactions dealt with on this machine).

   The workstations shall not be included in the description if they do not operate at least one main function of the activity.

b) The main virtual hardware elements operating one or several main functions shall be subject to a simplified description that shall specify at least the type of virtual machine (VM, XEN, etc.) and their operating system (including the version number).

When the provided information is the same for several elements, the summary table shall present it once by indicating the identification number or name and the total number of the elements concerned.

It shall also specify the identification number or name of the physical machine hosting the virtual machines.

Finally, it shall specify the total number of clients and the number of financial sector clients supported by every virtual machine or any other information relevant for the risk concentration assessment of clients on the same machine (for instance, the volume of transactions dealt with on this machine).

3.3.1.3. Software elements

The software elements operating one or several main functions shall be subject to a simplified description indicating, where available, information regarding:

- data management: type of management (database, indexed files, sequential files, combination of different types) and name of the product;
- the type of environment, programming language;
- the processing mode: real-time, batch or mixed; the latter case shall indicate the functions processed as batch;
- the architecture: client-server and number of levels with an indication, per level, of the functions used (for example client-server at three levels: presentation, application, data) and the identification of the material supporting each function;
- development:
  - development (with or without use of outsourcing);
  - software package (with the indication of the provider’s name);
  - modified software package (if over 20% of the functionalities were modified) with an indication of the participants in the modifications (internal, provider, mixed).
- significant modifications made since the previous financial year.

3.3.1.4. Outsourcing and localisation of systems

Outsourcing[14] the external IT systems or processing, as well as the localisation of the systems shall be specified for each system concerned. For each hardware element (physical or virtual), the summary table shall notably provide an answer to the following questions:

- Is the element dedicated to the support PFS (and, by extension, to its clients in the framework of its service provisions) or shared with other entities?
- Does the PFS outsource and, if yes, what is the nature of the outsourcing (only hosting or operation provision)?
- Who operates the element: the PFS or a third service provider to be specified (one entity of the group shall be considered as third service provider)?
- Where is the system located? Indicate the premises (of the PFS, a third provider including an entity of the group?) and the country if the system is abroad.
- In case of outsourcing, is there a resumption plan (transfer to another provider or managing on its own), in the event the continuity or quality of the service provision is jeopardised?

3.3.2 Functional scheme of the flows

The main links (interfaces) which exist between the functions and, consequently, the reported systems pursuant to point 3.3.1 shall be described in a functional scheme of flows by the support PFS.

Where all functions are included within one single software functioning on a single hardware (for example, the banking software package), it is not necessary to detail the internal flows but only the flows entering and coming out of the system.

3.3.3 Network architecture and external connections

The support PFS shall provide a description and/or a scheme of the network architecture comprising the main security elements (DMZ, firewalls, IDS, routers, proxy, etc.).
It shall list the useful connections according to the activities carried out in the financial sector towards or from outside (including with its group, where applicable), by specifying the control it exercises on these accesses. It shall briefly describe the security mechanisms implemented on physical (firewall, router, etc.) as well as on logical (intruder detector, anti-virus, client authentication, communication confidentiality, integrity and non-renouncing the transactions, etc.) and organisational (monitoring log history, configuration of the security equipment, generating keys or authentication certificates of client, monitoring systems, etc.) level.

[14] Within the meaning of Circular CSSF 05/178

3.4. Business Continuity Plan and Disaster Recovery Plan (BCP/DRP)

The support PFS shall describe the business continuity plan that it set up in case of disaster on its own premises or in case the access to its premises is impossible (group solution, specialised undertaking, regular tests, security measures, etc.).

It shall also describe the broad outline of the emergency plan in place which shall allow normal functioning in case of breakdown of its IT system, including as regards external connections (use of several communication lines providers, line redundancy).

4. Periodic reports to be communicated

The support PFS shall describe the system implemented in order to draw up periodic prudential reports for the CSSF and the internal control measures aiming to guarantee that the data submitted to the CSSF are complete, accurate and drawn up according to the applicable rules as well as transmitted within the allotted deadlines, including for the final figures.

5. Analysis of annual accounts

The support PFS shall analyse annual accounts, including the specific comments and explanations on important items and significant developments of the financial situation.

It should be noted that, instead of the annexe to annual accounts, relevant supplementary information (e.g. justification of unusually low or high accounts due, for example, to a cash-pooling activity for the group; European consolidation activity for the group) shall be indicated under this point.

The support PFS shall also mention the elements subsequent to the end of the financial year which are such that they influence the assessment of its economic and financial situation.

6. Professional obligations as regards the prevention of money laundering and terrorist financing

The support PFS shall describe the procedures set out in order to prevent money laundering and terrorist financing[15] and, notably, the following procedures:

- "Know Your Customer" policy;
- predefined internal suspicion denunciation procedure;
- reporting procedure to the State Prosecutor of the Luxembourg district court and the CSSF.

[15] Please refer to the CSSF website (www.cssf.lu) under section "AML/CFT - Financial sanctions".

The support PFS shall also specify if it implemented:

- regular training sessions for its employees;
- the review and validation of the procedures by the management;
- information and communication of all the procedures to the support PFS' personnel;
- availability of the procedures on a medium.

7. Professional obligations as regards the rules of conduct

The support PFS shall briefly describe its internal procedures for applying rules conduct and dealing with customer complaints.

8. Relations with affiliated undertakings

The support PFS commits itself to ensuring that the intra-group transactions are carried out at arm's length.

The following shall notably be described and commented upon:

- the type of executed intra-group transactions;
- the guarantees issued to the benefit of/received from the affiliated companies;
- the prices charged for provided and received services;
- etc.

All the transactions not executed under market conditions shall be reported and detailed.

9. Branches abroad

The support PFS shall provide for each branch:

- an organisation chart;
- a description of the activities;
- a description of the internal control procedures;
- if applicable, the serious deficiencies that the internal audit noticed at the branch;
- a description of the administrative and accounting organisation;
- an indication on the existence of procedures regarding compliance with the rules of conduct and prevention of money laundering and terrorist financing;
- explanations on the accounting integration of the branch.

10. Subsidiaries abroad

The support PFS shall provide an annual report or, otherwise the annual accounts of the subsidiaries or majority holdings on a yearly basis.

IV. Communication to third parties

The support PFS is authorised to communicate to its clients and potential clients the risk self-assessment as set out under point II.B of Chapter II and the relevant analysis documents provided that no modification is made in them and to communicate them in their entirety.

Alternatively, the support PFS may provide them a summary of its self-assessment provided that the latter always has the same risk profile as the one from the self-assessment communicated to the CSSF. A copy of this summary shall then be sent to the CSSF.

In any case, the support PFS shall ensure that the documents communicated to its clients and potential clients are anonymous.

This communication is under the exclusive responsibility of the support PFS which commits itself as regards the truthfulness of the communicated information. The support PFS, may under no circumstances, pride itself on any validation by the CSSF of the communicated information and documents.

V. Final and transitional provisions

The circular enters into force on the day of its publication and initially refers to the financial year 2012 for the support PFS closing their financial year on 31 December 2012.

The first risk analysis report ("RAR") shall be submitted at the latest three months after the closing date, i.e. in 2013. The risks to be included in this first report are:

a) pursuant to the provisions of Chapter II (point II.B) of this circular, the 20 direct and 5 indirect risks which received the highest scores during the calculation of the <u>net</u> materiality (the highest results of the transactions (P_{net} x $I_{net\ the\ highest}$)). Nevertheless, any direct or indirect risk the net impact of which is equal or higher than 6 and which has at the same time a net probability equal or higher than five is also to be reported, even if the limits of 20 and 5 risks mentioned above are reached;

b) and, in addition, the 20 direct and 20 indirect risks which are the most material before taking into account the mitigation measures, no matter the net materiality of these risks.

For the second and all subsequent risk analysis reports, the support PFS shall only report the risks referred under point a) above, in accordance with the provisions of Chapter II (point II.B) of this circular.

Moreover and as a reminder, any event occurring during the year and significantly changing the financial sector risk profile of the PFS (e.g. appearance of a new significant risk or reassessment increasing the materiality of the risk already identified) shall be communicated to the CSSF in the form of a risk sheet as presented under point II.B by the support PFS without waiting for the issue of the next risk analysis report.

The CSSF encourages the support PFS to prepare their risk analysis report during 2012. During this year, they may seek the CSSF to discuss about their first risk analysis elements before the submission of the reports.

The first descriptive report ("DR") shall be submitted at the latest seven months after the closing date 2012. The following years, the DR shall be submitted at the same time as the RAR.

As a reminder, the support PFS shall also spontaneously, and without a request to that effect, communicate to the CSSF the documents relating to the end of their financial year. In any case, the support PFS have a maximum time limit of seven months[16] as from the end of the financial year in order to send to the CSSF the reports and written comments issued by the *réviseur d'entreprises agréé* in the framework of its control of annual accounting documents[17].

The table below summarises the deadlines given to support PFS for the submission of the required documents to the CSSF.

Documents to be submitted	**In 2013**	**After 2013 and before the entry into force of the second circular <u>(Note 1)</u>**	**From the entry into force of the second circular**
Risk analysis report (RAR)	At the latest three months after the closing date 2012	At the latest three months after the closing date	At the latest three months after the closing date
Descriptive report (DR) **<u>(Note 2)</u>**	At the latest seven months after the closing date 2012	At the latest three months after the closing date	At the latest seven months after the closing date
Documents relating to the accounting closing date	At the latest seven months after the closing date 2012	At the latest seven months after the closing date	At the latest seven months after the closing date

[16] Consistent with Articles 9 of the law of 10 August 1915 on commercial companies, 79(1) of the law of 19 December 2002 concerning the trade and companies register, as well as the accounting and annual accounts of companies and 55(2) of the LFS which impose the filing of regularly approved annual accounts with the trade and companies register within the month of their approval, and at the latest seven months after the end of the financial year, and their publication in the *Mémorial* within two months as from the filing.

[17] In accordance with Article 54(1) of the LFS.

Note 1: It is the second circular (stage 2) mentioned in the introduction. It will define the practical rules as regards the mission of *réviseurs d'entreprises agréés* (approved statutory auditors) *vis-à-vis* support PFS and the content of the long form audit report.

Note 2: The documents requested in Part III of this circular[18] - as summarised below – shall be appended in the descriptive report:

- a copy of the report on annual accounts and annual accounts of the direct majority shareholder as well as, where applicable, of its management report;
- the written report of the management on the state of the internal control;
- a copy of the summary report on the controls carried out by the internal audit during the previous financial year;
- a copy of the letter(s) of assignment entrusted to the internal auditor;
- the multi-year plan of the internal audit confirmed by the management and/or the board of directors (or management board);
- the internal audit charter;
- a table relating to the persons designated as responsible for certain functions pursuant to the CSSF circulars;
- an up-to-date list of the members of the management in charge of the daily management;
- a summary table of the information systems for internal use;
- a nominative list of Luxembourg or foreign financial sector clients for which the support PFS provides services requiring a PFS authorisation;
- a copy of a client agreement on the service provision requiring a PFS authorisation for each different PFS authorisation that the support PFS has;
- a summary table of information systems for external use;
- a functional scheme of the flows;
- the annual report or otherwise, the annual accounts of the subsidiaries or majority holdings.

[18] Please refer to Part III for details on the required content of these documents.

As soon as it comes to their attention, the support PFS must inform the CSSF of any reported delays and indicate the reasons for and the probable duration of the delay.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON	Andrée BILLON	Simone DELCOURT	Jean GUILL
Director	Director	Director	Director General

Annexe 1: Probability scale and impact
Annexe 2: Example of risk sheet
Annexe 3: Example of register of direct and indirect risks in the financial sector
Annexe 4: Example of a summary table of information systems for internal use
Annexe 5: Example of a summary table of information systems for external use

Annexe 1

Probability scale and impact

Probability scale

Value	Informative description
0	Does not occur / never occurs
1	Does not take place *a priori* / very improbable
2	Isolated / rare event
3	
4	Repetitive / possible event
5	
6	Recurring / probable event
7	
8	Common / very probable event
9	
10	Constant / certain event

Impact scales

- Impact on the reputation

Value	Informative description
0	No impact
1	
2	Rumour(s), worry of isolated client(s)
3	
4	Coverage in national press Many information requests from clients
5	
6	Coverage in specialised press Loss of some clients or a strategic client
7	
8	Coverage in all national broadcasting media Mass departure of clients
9	
10	Coverage in international press/media Departure of all clients

- Operational impact

Value	Informative description
0	No impact
1	
2	Minor incident(s) without any impact on clients
3	
4	Isolated incident(s) with manageable impact(s) on clients
5	
6	Isolated incident(s) with significant impact(s) on clients / interruption of an entire process
7	
8	Systemic incident(s) with impact(s) on several clients / partial stop of activities
9	
10	Complete stop of activities

- Legal impact

Value	Informative description
0	No impact
1	
2	Reminder(s) by CSSF Minor / isolated complaint of client(s)
3	
4	Deficiency letter / request by CSSF to state its position Commercial dispute(s) / creation of provisions
5	
6	Regular breach - threat to fine / injunction by CSSF Civil case / dispute with isolated client
7	
8	Serious breach - fine / dismissal of management / threat by CSSF to withdraw authorisation Criminal case / dispute with mass clients
9	
10	Loss / withdrawal of authorisation by CSSF Payment suspension / liquidation of the company

- Financial impact

Value	Informative description
0	No impact
1	
2	Minor loss(es)
3	
4	Loss(es) moderately impacting the quarterly profit and loss
5	
6	Loss(es) significantly impacting the profit and loss of the financial year
7	
8	Major loss(es) annihilating the profit and loss of the current and/or following financial years
9	
10	Major and irrecoverable loss(es) threatening the perenniality of the company and/or resulting in bankruptcy

Annexe 2

Example of risk sheet

Risk ID: 1	Category: D6.1	Title: Mutualisation - Segregation of uninsured environments

Description of risk:
In the context of mutualisation, risk that the segregation of the clients' environments is uninsured.

Gross assessment (before controls):

Probability (P)	Impacts (I)				Importance
	Reputational	Operational	Legal	Financial	(PxI$_{\text{the highest}}$)
7	6	8	8	8	7*8 = 56

Argumentation:
Risk for confidentiality and integrity of the clients' data that might have serious operational impacts for clients and legal impacts (e.g. professional secrecy not observed) for clients and the PFS.

Financial sector clients concerned:
Clients X, Y and Z concerned by the mutualised offer.

Measures to decrease or transfer and monitor risk:

- Duplication of applications on one operating system.
- Technical robustness of partitioning: proper, documented, regularly controlled implementation, monitoring of vulnerabilities and regular corrective updates.

Net development (after controls):

Probability (P)	Impacts (I)				Importance
	Reputational	Operational	Legal	Financial	(PxI$_{\text{the highest}}$)
1	6	8	8	8	1*8 = 8

Response strategy (including argumentation if the choice is to accept the risk): Reduce

Action plan (including deadlines):
Cryptography of partitions at operating system level (deadline: MM/YY)

Expected materiality:

Probability (P)	Impacts (I)				Importance
	Reputational	Operational	Legal	Financial	(PxI$_{\text{the highest}}$)
1	4	4	6	2	1*6 = 6

Risk ID: 12	**Category I1**	**Title: Decisions imposed by the group put our activities or our PFS status at risk**

Description of risk:
Given the current economic context, the group could impose on us to decrease staff by 15% mainly impacting our internal and administrative organisation and our capacity to comply with the regulatory requirements (central administration).

Gross assessment (before controls):

Probability (P)	Impacts (I)				Importance
	Reputational	Operational	Legal	Financial	(PxI$_{\text{the highest}}$)
7	6	4	8	6	7*8 = 56

Argumentation:
Reputation risk and loss of market shares, risk of non-compliance with the regulations. Indirectly, operational risks for our clients.

Financial sector clients concerned:
All clients.

Measures to decrease or transfer and monitor risk:
Consciousness-raising action by the group as regards the support PFS status and the relevant requirements.

Net development (after controls):

Probability (P)	Impacts (I)				Importance
	Reputational	Operational	Legal	Financial	(PxI$_{\text{the highest}}$)
6	6	4	8	6	6*8 = 48

Response strategy (including argumentation if the choice is to accept the risk): Reduce

Action plan (including deadlines):
Continue the consciousness-raising actions (deadline: MM/YY); agree on a governance policy with the group (deadline: MM/YY).

Expected materiality:

Probability (P)	Impacts (I)				Importance
	Reputational	Operational	Legal	Financial	(PxI$_{\text{the highest}}$)
4	6	4	8	6	4*8 = 32

Annexe 3

Example of register of direct and indirect risks in the financial sector

Cat.	ID.	Title of risk	Gross development			Net development			Response strategy
			P	I	Imp.	P	I	Imp.	Response strategy
Direct risks									
D6.1	1	Mutualisation - Segregation of uninsured environments	7	8	56	1	8	8	Reduce
…	…	…							…
D5	5	…							Accept
…	…	…							…
Indirect risks									
I1	12	Decisions imposed by the group put our activities or our PFS status at risk	7	8	56	6	8	48	Reduce
…	…	…							

Annexe 4

Example of a summary table of information systems for internal use

Function	Software elements	Physical material elements	Virtual material elements
PFS FUNCTION: • *GENERAL ACCOUNTING (function outsourced to group)*	**NAME OF SOFTWARE (and provider if software package):** **Development:** internal, software package (less than 20% of adaptations of the standard product), mixed **Changes since the previous financial year:**	**Brand:** **Model:** *PC* **OS** (operating system): name and version **Redundancy mode:** Cold standby **Redundancy reason:** Low criticality (maximum 48H halt) **Number:** 2 **Identification:** PC01, PC02 **Virtual Machine (VM):** 2 VM per element	**Type of VM:** VMware **OS** (operating system): name and version **Number:** 4 **Identification and hosting:** VM01 and VM02 on PC01 VM03 and VM04 on PC02
	Outsourcing: yes, hosting of the physical infrastructure in the parent company in the USA and administration of VM and software by a sister company in the UK **Dedicated/shared:** Software mutualised with other entities of the group (Multiple Entities Single Instance mode). Physical and virtual material elements shared with other entities of the group. **Operated by:** parent company (physical materials) and sister company in the UK (VM and software) **Location:** Los Angeles, USA, parent company **Existence of a resumption plan:** yes, internal resumption plan (terms included in the contract with the group)		
TECHNICAL FUNCTION: • *FIREWALL*	**NAME OF THE SOFTWARE:** *"trusted OS"*	**Brand:** **Model:** *PC* **OS** (operating system): name and version **Redundancy mode:** Clustering **Redundancy reason:** Criticality (maximum 1 minute of halt) **Number:** 1 **Identification:** FW1 **VM:** N/A	**N/A**
	Outsourcing: no **Dedicated/shared:** dedicated **Operated by:** the support PFS **Location:** Premises of the PFS **Existence of a resumption plan:** N/A		

Annexe 5

Example of a summary table of information systems for external use

Function	Software elements	Physical material elements	Virtual material elements
FUNCTION CLIENT: - *ASSET ACCOUNTING*	**NAME OF SOFTWARE (and provider if software package):** **Data management:** type and name of the DMS product **Analysis and programming:** type (Classic, Object-Oriented, mixed) and name of the languages and/or CASE tools **Mode:** Real-time transaction, batch, mixed **Architecture:** simple or client-server with a number of levels (2, 3 or more) and link with the used material **Development:** internal, software package (less than 20% of adaptations of the standard product), mixed **Changes since the previous financial year:**	**Brand:** **Model:** **OS** (operating system): name and version **Redundancy mode:** **Redundancy reason:** **Number:** 2 **Identification:** PC01, PC02 **VM:** 2 VM per element **Total number of clients:** - On PC01: - On PC02: **Number of financial sector clients:** - On PC01: - On PC02:	**Type of VM:** VM **OS** (operating system): name and version **Number:** 4 **Identification and hosting:** VM01 and VM02 on PC01 VM03 and VM04 on PC02
	Outsourcing: yes, hosting and operation of the infrastructure (physical and virtual) in an OSIP PFS (to be named). **Dedicated/shared:** Software dedicated to a support PFS and offered to its clients in Saas mode. Mutualised physical and virtual material elements (Iaas mode). **Operated by:** software operated by the support PFS. Infrastructure operated by the OSIP PFS **Location:** Premises of the OSIP PFS **Existence of a resumption plan:** yes, transfer to another provider (terms included in the contract with current provider)		