Licence application for payment service providers

DeNederlandscheBank

EUROSYSTEEM

Notes to the (draft) licence application form for payment service providers – PSD2

De Nederlandsche Bank

Under the Financial Supervision Act (*Wet financieel toezicht – Wft*), De Nederlandsche Bank (DNB) is charged with the prudential supervision of payment institutions and with deciding whether to allow payment institutions access to the financial market. Within the context of its supervisory tasks, DNB has the statutory authority to share information with the Dutch Authority for the Financial Markets (AFM) and, once the revised Payment Services Directive (PSD2) has entered into force, also with the Dutch Data Protection Authority (DPA). This includes sharing information about licence applications.

Autoriteit Financiële Markten

Under the *Wft*, the AFM is responsible for conduct supervision of payment institutions, which can be relevant to certain parts of the licence application process.

Autoriteit Persoonsgegevens

Under the Personal Data Protection Act (*Wet bescherming persoonsgegevens – Wbp*) and the General Data Protection Regulation (GDPR), the DPA is responsible for supervision of personal data processing, which can be relevant to certain parts of the licence application process.

Contents

1 General information

1.1 Company data

We would like you to provide us with a number of details about your company. Please submit to us all required annexes, including a certified copy of the notarial deed containing the company's articles of association. Ensure that the objective described in the articles of association actually reflects the services that the company will provide. The description of the company's objective may not include activities that require another licence requirement, unless you already hold a licence for these activities. If you do not yet have a copy of the notarial deed containing the company's articles of association, a final draft version will suffice for the purpose of processing your application. Please note that we will not decide on your application until we have received a certified copy of your company's articles of association.

1.2 External consultant contact details

We recommend that you engage the services of a consultant to assist you in the application process. Practice has shown that applications are often more complete and of a substantially higher quality if the applicant has sought expert advice, for example from a legal expert who specialises in the Dutch Financial Supervision Act (*Wet op het financieel toezicht – Wft*). We can assess complete and well-substantiated applications faster and more thoroughly. If you decide to use the services of an external consultant please also provide us with this consultant's particulars.

1.3 If you are already operating as a payment service provider or exempt payment service provider

You may already be operating as a payment service provider or exempt payment service provider. If so, we assume that you have ascertained that you do not provide any services that are subject to a licence requirement. If you indicate that you are already operating under the Exemption Regulation under the *Wft* (*Vrijstellingsregeling Wft*), we would ask you to state the date of your registration as an exempt payment service provider. If you are active as a payment service provider but not registered as an exempt payment service provider, please specify. If you already hold a licence as a payment institution, please state to which payment services this applies.

1.4 If you are under supervision of a foreign supervisory authority

Please state whether your company is under financial supervision of another, foreign, supervisory authority. If this is the case, please specify the type of financial activities involved, the country, and the name of the supervisory authority in question. If you used to be under financial supervision of a foreign supervisory authority, please state this and specify why this is no longer the case.

1.5 Conditions for licence application

A payment service provider is a company whose business it is to provide payment services. This definition is based on Section 1:1 of the *the Financial Supervision Act (Wet op het financieel toezicht – Wft)*. These services are provided to persons making payments (consumers) or parties using the payment services (retailers), or both. So a payment service provider acts as an intermediary between the two.
To determine whether a company qualifies as a payment service provider, the following questions must be answered:

1. Do the proposed activities qualify as a payment service? Please note that there are specific services that the *Wft* explicitly does not qualify as payment services. These services are excepted from the licence requirement.
2. Will it be your company's "business"* to provide payment services?
3. Is your company subject to the Exemption Regulation under the *Wft*?

Check whether any of the statutory exceptions apply
Several specific services explicitly do not qualify as payment services under the *Wft*. They are listed in Section 1:5a(2). Examples include commercial agents and limited networks. Please consult the FAQs on Open Book on Supervision for more details on these exceptions.

Does your company provide payment services within the meaning of Section 1:1 of the Wft?
First you must verify that your company is a payment service provider within the meaning of Section 1:1 of the *Wft*.

There are eight types of payment services. These services may be provided as a single service or in any combination.

They are listed and defined in the Annex to the revised Payment Services Directive (EU) 2015/2366 (PSD2). The *Wft* refers to that Annex.

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account. These services enable users to pay cash (coins and banknotes) into a payment account held with the service provider.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account. These services enable users to withdraw funds in cash from a payment account held with the service provider.
3. Execution of payment transactions, including funds transfers on a payment account held with the user's payment service provider or with another payment service provider:
   - execution of direct debits, including one-off direct debits;
   - execution of payment transactions by means of a payment card or a similar device; and
   - execution of credit transfers, including standing orders.

   These services entail executing payment transactions on the payment accounts of payment services users as meant in the description of services 1 and 2, or on the user's payment account held with another payment service provider.

   This also includes services enabling users to withdraw or deposit cash using a cash dispenser or cash deposit machine, with the equivalent amount being debited from or credited to a payment account.
4. Execution of payment transactions where the funds are
   - covered by a credit line granted to a payment service user:
   - execution of direct debits, including one-off direct debits;
   - execution of payment transactions by means of a debit card or a similar payment instrument; and
   - execution of credit transfers, including standing orders.

   A credit line may include a situation in which the payment service provider advances the amount due.
5. Issuing and/or acquiring of payment instruments and/or acquiring of payment transactions
   A payment instrument is a means or method to initiate a payment order, including physical objects, such as credit cards. Acquiring payment transactions means that a company guarantees the settlement of transactions by means of an agreement concluded with the beneficiary, e.g. an online retailer. The acquiring entity handles payments to the beneficiary based on the payment orders received. Companies providing services to retailers, including online retailers, for the acceptance of payment instruments provide type 5 services.
6. Money remittance
   Money remittance services (money transfers) are involved if a payment institution receives funds from a payer for the sole purpose of transferring the corresponding amount either directly to a payee or to another payment service provider who pays out the funds to the ultimate beneficiary. No payment account is created in the name of the payer. In practice, money remittances are used mainly to transfer funds to beneficiaries abroad, in particular in countries with less sophisticated banking systems and a less widespread use of bank accounts. They are also sometimes used to effectuate unexpected urgent payments.
7. Initiating payment services at the request of payment service users with respect to payment accounts held with other payment service providers.
8. Account information services
   Providing consolidated information on one or more payment accounts held by a payment service user with one or more other payment service providers.

You are advised to explore the options available to you with a legal consultant.

Please state in the application form whether you intend to provide intermediation services for products and services. For the provision of intermediation services in financial products, you may need a licence issued by the AFM. For more information go to www.afm.nl

The application form contains the following three verification questions to ensure you apply for the correct licence for the payment services and to check whether you would require an additional licence :

1. Does your company intend to offer intermediation services for products and services at any point?
2. Does your company intend to offer lending services at any point?
3. Will your company manage customer accounts at any point?

Will your company provide payment services as a business?

Payment service providers are subject to the licence requirement if they provide payment services. Providing services to several customers is an indication that these services are provided as a business. You are in any case subject to the licence requirement if you are actively promoting payment services, e.g. by advertising. If a company provides payment services on a one-off or very incidental basis, it does not qualify as a payment service provider.

If you are in doubt about the legal qualification of your proposed activities, we would advise you to consult a legal expert.

Does your company intend, for the next three years, to provide or already provides business activities other than payment services?

Please state in the application form whether you intend to provide other business activities and, if so, include a description of the type and expected volume of the activities.

2 Business case

2.1 Business plan

When applying for a licence, you must submit a business plan on behalf of the company, including a programme of operations. You must also submit a budget estimate for the first three financial years, which demonstrates that you have appropriate systems, resources and procedures in place that allow you to operate in a financially sound and healthy manner.

You can submit the business plan and budget estimate as a single document, but please bear in mind that this information must be consistent with the information to be submitted in the templates described in Section 11 regarding Minimum own funds and solvency. We expect you to submit at least the following elements:

- a diagram of your company's activities, specifying each payment service, and how these payment services will be provided. We also want to receive a list of your company's other activities (including activities not subject to the licence requirement).
- A description of operational and closely related ancillary services, as referred to in Article 18 (1) of PSD2. Ancillary services are services related to the payment services. You must also describe any ambitions to provide such services for the coming three years.
- The company strategy, including
  - the intended market share for each payment solution
  - the intended origin of payment service users
  - a well-considered description of the company's growth ambitions;
  - a SWOT analysis.[1]
  - contracting out of processes (outsourcing).
  - the company's professional partners (e.g. acquirers, customer referrals).
- For existing companies: certified financial statements over the past three years, or an overview of the financial situation if the company has not yet issued financial statements.
- Based on the company strategy, a projection of your company's financial position and estimated results for the current financial year and the next three years, including a full profit and loss account and a balance sheet, detailing the following aspects.
  - The expected own funds of the company, in connection with the information to be submitted in the templates described in Section 11 regarding minimum own funds and solvency.
  - The assumptions and calculations underlying your financial projections, such as investment costs, outsourcing costs, management costs, contributions and your envisaged market share;

1 This is an analysis of your company's strengths and weaknesses, presenting the potential success of your proposed services in diagram form (e.g. in a matrix). S = Strengths, W = Weaknesses, O = Opportunities, T = Threats. Based on a SWOT analysis, you can define objectives and subsequently devise a strategy for achieving these objectives.

  - Several stress scenarios demonstrating that your company's business case is sufficiently robust to meet the company's obligations also in the event of disappointing results or adverse circumstances.
  - The company's policy to ensure business continuity under normal, moderately adverse and highly adverse circumstances, see also Recovery plan (Section 3.3);
  - A detailed specification of estimated inward and outward cash flows, i.e. your liquidity position, for the next three years, presented in a flow chart.
- A marketing plan including an analysis of your company's competitive position and a description of the users for each of the payment services concerned and the proposed marketing activities and distribution channels.
- An estimate of the number and a description of the locations from which the company will be operating its payment services and related activities.

2.2 Funds flow chart

If your company exclusively provides payment services type 7 or 8, or both, this section does not apply to your company.

When assessing your application, we must have a clear picture of the cash flows related to your proposed activities. Please provide an overview of the anticipated cash flows for each type of payment service in the form of a flow chart, indicating for each payment instrument the number of transactions, the processing times and the parties involved.

2.3 Recovery and exit plans

You must draw up a recovery plan, setting out how you will recover from adverse financial circumstances. Such a plan must in any event describe the measures in place for detection of and timely recovery from any deterioration of the company's financial situation. The aim of this plan is to recover a stable financial situation as soon as possible. In addition to a recovery plan, you must draw up an exit plan in timely preparation for the potential termination or transfer of the company's business activities. If your company actually needs to be resolved, the plan ensures that liquid funds can be paid out or continue to be paid our in an orderly fashion and with the least adverse effects possible for payment service users and other stakeholders, and that relevant data will be removed. Although the recovery plan and exit plan serve different purposes, you can combine them in a single plan. This means you will only have to upload a single document. In the remainder of this text, we will therefore refer to the "recovery and exit plan". Obviously, the recovery and exit plan must be consistent with your business plan.

10 The recovery and exit plan must cover all of the company's business activities, products and processes. The resolution plan must have a clear responsible owner within the company, requires the prior approval of the management board and – if applicable – the supervisory board, and must be reviewed at least once a year. This must also be stated in the plan. The plan should be based on the principle of proportionality, and it is up to you as a company to determine the level of detail of the plan.

As part of our thematic examination into recovery and exit plans of payment institutions, we provided a guidance document to help you prepare these plans. The guidance document is available on our Open Book on Supervision pages (http://www.toezicht.dnb.nl/en/binaries/51-236219.pdf). Your company's recovery and exit plan must include all the elements described in this guidance document. In addition, the exit plan must specifically address the controlled management of payment service users' data in the event of the company's resolution.

We have also compiled a good practices document with advanced insights gained on the basis of the recovery and exit plans submitted by payment institutions. It may help you in preparing your company's own recovery and exit plan. The document is available on Open Book on Supervision (http://www.toezicht.dnb.nl/binaries/50-236731.pdf).

3 Sound business operations

Your company must be structured in such as way so as to ensure sound and ethical business operations. This means that you must analyse the operational risks that your company is exposed to and take measures to mitigate these risks.

If you use a customer accounts foundation to safeguard the funds entrusted by the users of your payment services, you must also include this foundation in your risk analysis. Any outsourced activities must also be included in the risk analysis.

Our assessment of sound business operations includes the following elements:

- Risk analysis for the purpose of managing operational processes and operational risks.
- Risk management framework
- A clear, balanced and adequate organisational structure
- Compliance function
- Internal control function
- Procedures manual
- External audit
- Outsourcing
- International services
- Information systems, infrastructure and security
- Authentication
- Secure communication
- Data collection
- Incident management
- Business continuity management
- Sound remuneration policy
- Oath or affirmation
- Training

We will explain this in more detail below.

3.1 Risk analysis for the purpose of managing operational processes and operational risks.

You must submit a recent, comprehensive analysis of the risks that are inherent to your company and the services it provides, so that we can determine whether your company's operational organisation is appropriate to the risks it is exposed to. The analysis must also include an assessment of the measures and control mechanisms in place to mitigate these risks. You should base your risk analysis on the risk management framework designed by your company.

12 Sound operational management as a payment services provider starts with identifying the relevant risks. Such a risk analysis is a precondition for the adequate organisation of sound business operations. The analysis must be verifiable, i.e. recorded in a separate document. Your risk management framework must be based on the outcome of the risk analysis. You should apply a clear quantification method. The risk analysis is based on gross (inherent) and net (residual) risks and analyses the likelihood and impact of these risks. The size of the net risks must be clear and the measures and procedures must have a plausible effect. In analysing the net risks, you should also consider your company's risk appetite. See also Section 4.2, regarding the risk management framework.

As a minimum, the risk analysis contains an analysis of the risks that are relevant to your company, such as the following categories: credit risk, market risk, interest rate risk, concentration risk, liquidity risk[2], operational risk (including IT and outsourcing risk), insurance risk and integrity risk (a systematic integrity risk analysis or SIRA must be submitted separately under Section 5, regarding the structure of business operations so as to ensure ethical business operations). The analysis must address the underlying inherent risks for each of these categories and, these risks if they are high, show the measures in place to mitigate them. In particular, it must address the risks related to the payment services and include a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data. To this end, you must draft a security policy, see Section 4.10.

Your procedures and measures must be verifiably connected with the specific risks identified in the risk analysis. The control measures must be demonstrably appropriate to the nature, size, complexity and risk profile of the activities of your company and must meet the minimum requirements set out above.

3.2 Risk management framework

Please describe your company's risk management framework. This policy document must address your company's policy aimed at managing relevant risks, including a description of the company's risk appetite. It must also address the design and set-up of the risk management function and describe how the policy is translated into procedures and measures to manage relevant risks, as well as how it is integrated into the company's operational processes (see also the Section on Procedures manual). You should also demonstrate that this risk management framework enables your company to guarantee controlled business operations. We also expect the other components described in this section to be in line with your company's risk management framework.

2 The liquidity risk management procedures and measures must focus on management of the company's current and future net financial position and requirements.

Your company must have a policy in place aimed at managing relevant risks. It should include a description of your company's risk appetite for each of the relevant risk areas, such as credit risk, market risk, interest rate risks, foreign exchange risk, concentration risk, liquidity risk, operational risk (including IT and outsourcing risk), and insurance risk.

Your risk management policy must be translated into procedures and measures, which must be appropriate to the nature, size, risk profile, and the complexity of the company's activities, and address at least the following four areas:

- licence procedures
- limit allocation
- limit monitoring
- procedures and measures for emergency situations.

The procedures and measures must be clearly documented, for example in a procedures manual (see Section 4.6). They must be communicated to all payment institution units exposed to the risks, preferably in writing.

Your company must have an independent risk management function that is responsible for systematic risk management within the organsiation, focussing on identifying, measuring and evaluating risks that the company is or may be exposed to. Risk management covers the company's operations as a whole as well as those of its individual business units. The risk management function must be given the required authority and access to all information necessary for the performance of its tasks. The description of the risk management framework must include an explanation of the structure of the risk management function. We also expect you to provide a description of the periodic and permanent control measures that your company has in place, including their frequency, staffing (in FTEs) and resources (in EUR).

Your company must establish an effective operational IT and security risk management framework, which should be approved and reviewed, at least once a year, by the management body and, where relevant, by the senior management. This framework should focus on security measures to mitigate operational and security risks and should be fully integrated into the PSP's overall risk management processes. See also the section on the management of operational IT and security risks.

3.3 A clear, balanced and adequate organisational structure

In setting up its business operations, your company must base its operational management (including a possible customer accounts foundation), on the following six principles.

- A clear, balanced and adequate organisational structure.
- A clear, balanced and adequate distribution of duties, authorities and responsibilities (governance).

- The rights and obligations within your company are adequately recorded.
- Your company has clear and unambiguous reporting lines.
- An adequate information supply and communication system.
- A transparent definition of the company's operational management, which is reviewed at regular intervals.

Your company must have a clear, balanced, and adequate distribution of duties and authorities in place at all levels and in all units of the company. Reporting lines must be in tune with the organisational structure.

The division of tasks and reporting lines must be documented and communicated throughout the company to ensure that all levels of the company have full knowledge of their duties, authorities and responsibilities, their role in the organisation and the control process, and how they are held accountable.

If we find any shortcomings or deficiencies, you must ensure that the organisational structure and the procedures and measures are changed so that these are remedied. Companies with a director-majority shareholder (DMS) or a complex international structure or group structure should pay special attention to balanced corporate governance. We expect you to include appropriate notes if this applies to your company.

Director-majority shareholder (DMS) structure

Please state in the application form whether your company has a DMS structure or a comparable control structure. Corporate governance is defined as the distribution of duties, responsibilities and authorities aimed at balancing the influence of those directly involved in the company and its operations, particularly its executive and supervisory directors, and capital providers. It is important that the company at all times has expert and balanced operational management with adequate checks and balances and appropriate incentives.

A DMS structure involves a natural person who is both a majority shareholder (even if indirectly) and a managing director. In the absence of adequate countervailing power (checks and balances), a DMS may exercise an unduly heavy influence on the company's day-to-day management. DMSs may find themselves in a situation where they let their own interests as a shareholder prevail over the long-term interests of the company or its stakeholders. Apart from potential conflicts of interest, there is also a risk that a DMS identifies with the company to such an extent that he or she is unable to demonstrate and safeguard the objectivity and independence required in that capacity, for example in the event that the company faces critical problems.

We judge the admissibility of a control structure involving one or more DMSs on a case-by-case basis. If such a structure exists in your company, you must provide evidence in your

licence application that you have sufficiently mitigated the vulnerabilities attached to a control structure of this kind. This may include establishing a supervisory board or putting adequate arrangements in place to ensure that carefully considered decisions are taken in case of conflicting interests between the company and the DMS.

Complex international structure

For complex international structures we expect you to provide evidence of an adequate risk analysis and appropriate mitigation measures. This may for example include establishing a supervisory board. If your company is part of a group of companies, you are responsible for ensuring that its organisational structure and business processes are adequately aligned with those of its subsidiaries and other companies joined together with your company in a formal or actual governance structure. In this way, you will prevent the controlled business operations of your company from being undermined.

If your company has a Supervisory Board or intends to establish one, it is essential that this Supervisory Board is able to function independently. For more detailed information, see http://www.toezicht.dnb.nl/en/3/51-226002.jsp#.

Organisation chart

We require you to provide a recent organisation chart showing all divisions, departments and other structural units. We expect you to include a list of the people in charge of these divisions, departments and other structural units, with special attention to the individuals in charge of internal control functions (e.g. risk management, management business, compliance, audit) and possible departments. If these people are not yet known, you should include a detailed job profile for these functions/positions. The organisation chart must be accompanied by a description of the functions and responsibilities of the divisions, departments and other structural units, including an estimate of the number of staff and FTEs for the next three years. You should also indicate in the chart which functions are outsourced and which staff members occupy multiple roles.

Segregation of duties

The duties, powers and responsibilities of both individual staff members and departments in your company must be distributed to control the risk of errors and inappropriate use of assets or data. For instance, job descriptions must not include powers enabling one single person to enter into transactions or liabilities uncontrolled, to authorise, process and settle transactions, to have free access to assets, or to manipulate financial or other data. If your company is small, it may be challenging to realise internal segregation of duties. However, simply stating that it is a challenge in a small organisation does not suffice. We expect you to take alternative measures in this case. One option is to outsource activities to third parties to compensate for the lack of internal segregation of duties. We expect you to be sufficiently in control, and to explain in your application how you intend to safeguard this. See also Section 4.8 on outsourcing.

3.4 Compliance function

Your company must have an organisational unit in place that performs an independent and effective compliance function. It is important to have an independent compliance function in place in order to supervise compliance with legislation and regulations and internal rules, requirements and procedures. Supervision of compliance with rules, requirements and procedures for instance includes assessing new legislation and verifying whether new products and procedures comply with rules and regulations. The actual set-up of the compliance function depends on the nature and size of the payment institution. "Independent" at least means that the compliance function is not influenced by commercial or other interests. Compliance duties and responsibilities must be recorded in a compliance charter, and the necessary activities must be further detailed in an annual compliance plan. While submission of the compliance charter and the annual compliance plan is not mandatory, it may contribute to a more comprehensive substantiation of your licence application.

Compliance charter (optional)

The compliance charter must include the following elements:

- Definition and scope
- Compliance mission
- The compliance officer's job profile, including key tasks, powers and responsibilities
- The compliance function's special status in your company
- Safeguards for segregation of duties
- The names of the internal and/or external compliance officer(s)/staff member(s)

The compliance charter is available to the entire organisation as well as to external parties such as supervisory authorities, and clearly sets out the various roles and responsibilities and what can be expected from the compliance function, the management and other senior staff as regards the safeguarding of sound and ethical business operations.

Annual compliance plan (optional)

The annual compliance plan is based on a risk analysis. The plan presents a visible account of the capacity to be deployed, and the compliance function compiles the plan in consultation with the management. The compliance function must also ensure that any other stakeholders agree with the contents of the plan.

3.5 Internal control function

Your company must have an organisational unit that performs the internal control function. The effectiveness of the company's organisation and the procedures and measures must be assessed internally and independently. By "independently" we mean independent of the line management and independent of the control measures integrated in the different operational processes.

Independent internal control is an ongoing process that includes changing internal and external circumstances, new products and services, and support processes. An internal audit must be performed at least annually. You must describe how your company ensures that any shortcomings identified are eliminated.

As you can read in the sections on External audit (4.7) and Outsourcing (4.8), the internal control function can also be outsourced. If this is the case, we expect you to include an adequate description, in which you address the annual plan of internal control activities.

3.6 Procedures manual

The risk management framework, the organisational structure, the compliance function, and the internal control function are the main components of your operational management to ensure sound business operations. The overall structure of your operational management is also important, however. you should record your company's general procedures and measures to support sound business operations in a single clear and accessible document: the procedures manual. The procedures manual translates the structure of your company (the policies that your company pursues) into tangible procedures and measures for operational management. It also includes the procedures outlined in your company's risk management framework for performing periodic and ongoing audits, including their frequency and the staff allocated to these duties. If you have not yet explained the procedures and measures that your company has in place in the risk management framework, the organisational structure, the compliance function and/or the internal control function, we expect you to do this in your procedures manual.

You must compile a procedures manual to translate your organisation's policy into practicable procedures and measures. The procedures manual describes the administrative organisation of your company, by which we mean the systematic collection, recording and processing of data for the following three components of your operational management:

- organisational governance of a payment institution;
- operation of a payment institution;
- accountability for operation of a payment institution;

A procedures manual serves the following objectives.

1. Transparency: it provides an overview of the structure of the administrative organisation. The procedures manual describes how processes are structured and the guidelines that apply.
2. Efficiency and effectiveness: the procedures manual is the starting point for an administrative organisation based on efficient and effective processes.
3. Knowledge transfer: the procedures manual can be used for training and induction of new staff members, while a clear and uniform description of processes will ensure a consistent approach throughout the organisation.
4. Authorities and responsibilities: authorities and responsibilities within processes are clearly delineated. For example, signing authority. This will help mitigate risks.
5. Control: the procedures manual contributes to a well-structured and adequately implemented internal control system.
6. IT: the procedures manual provides basic input for IT systems, e.g. authorisations.

3.7 External audit

This section only applies if your company offers type 8 payment services.

The instruction to the external auditor to audit the institution's or branch's annual accounts must include an instruction for a review and general assessment of the adequacy of the organisational structure and risk management. The external audit must also focus on the management of risks that may be of material influence on the company's financial performance, position and ability to continue as a going concern, The external audit must be integrated in the year-end audit of the financial statements as much as possible. The auditor's report must include an opinion of the company's operational management. Please include a copy of the engagement agreement with your licence application.

3.8 Outsourcing

As we are responsible for the prudential supervision of all activities and business processes of your company (also if these have been outsourced), it is important that you provide us with all information based on which we can assess whether all activities (including those that are outsourced) are performed in conformity with the law.

Your company is permitted to outsource activities, unless doing so hampers adequate compliance with the applicable rules and regulations. There are also activities that you are not permitted to outsource, i.e. the duties and activities of staff members determining the company's day-to-day policy, including policy adoption and accountability for the policies pursued.

The internal control function must have professional expertise, detailed knowledge of the structure of the organisation and must be available at all times. Outsourcing this function to a company that has no formal or actual governance structure relationship with your company will consequently harm embedding of the quality of internal control. This means that if the internal control function is outsourced, the activities must still be performed under your company's management and supervision. Your company must at all times be able to render account of the structure and effectiveness of its operational management. The risk of conflicts of interests should be explicitly considered when determining which third party will be selected to perform the audit, and which staff member within the company will be made responsible for management and supervision.

Outsourcing policy

Your company must pursue an adequate policy and have adequate procedures and measures in place regarding structural outsourcing of processes, and it must have satisfactory procedures and measures and sufficient expertise and information available to be able to assess the performance of structurally outsourced activities. Your company must always enter into written agreements with the third parties to which it outsources activities on a permanent basis. Please include a copy of your outsourcing policy with your licence application.

In order to be able to pursue an adequate policy with respect to structurally outsourced activities, it is important that your company takes into consideration the influence that outsourcing of activities has on controlled business operations. For example, by having procedures and measures in place to deal with inadequate service provision by the third party or emergency situations. Payment institutions that outsource activities must systematically analyse the risks associated with outsourcing. Systematic risk analysis is an essential element for assessing whether or not activities are suitable for outsourcing.
You must perform a separate risk analysis for each of the service providers concerned.
The procedures manual must describe how the outsourcing risk analysis is compiled, and you must submit risk analyses for all outsourced material activities, i.e. activities that, if they are not completely or adequately performed, may seriously harm the company's compliance with the requirements of its licence, its financial results, or the solidity or continuity of its payment services.

Outsourcing agreement

To assess outsourced activities adequately, your company must have sufficient information at its disposal about the company to which it outsources these activities. You must also have sufficient in-house expertise to be able to assess this information adequately.
The outsourcing agreement must at least provide for the following:

- the exchange of information between the company and the third party about unlocking information required by the supervisory authorities as part of the performance of their statutory tasks;

- the option for your company to make changes at any time to how the third party performs the outsourced activities;
- the obligation incumbent on the third party to enable your company to keep meeting the requirements ensuing from primary and secondary legislation;
- the possibility for supervisors to perform, directly or by proxy, examinations on the premises of the third party;
- the manner in which the agreement is terminated and how, after termination, it is ensured that your company can again perform the activities concerned itself, or have such activities performed by another third party.

These requirements also apply if the service provider to which your company has outsourced the activities has subcontracted these activities.

However, if the activities are outsourced to companies that have their registered office in a Member State and that are part of the group to which your company belongs, you do not need to submit the policy documents, procedures and outsourcing agreements of these companies. The activities must meet the requirements of sound operational management, and we expect you to describe how your company is in control of performance of the activities.

In accordance with our policy on cloud computing [available in Dutch only], you must always notify us of outsourcing activities to cloud-based service providers in connection with concentration risk.

And finally, when outsourcing activities the company must verify that the fact of outsourcing does not compromise its duties towards its customers and the legal rights of its customers.

By the end of 2018 we will provide more information about outsourcing on our Open Book on Supervision pages. Please make sure to check these pages on a regular basis.

3.9 International services

Payment institutions that have their registered office in the Netherlands can operate in any other country of the European Economic Area (EEA) on the basis of the licence granted by DNB, without having to apply for a licence in the other EEA country concerned. Payment institutions are required to notify DNB of this. You can find the background and types of notification here.

If applicable, and to ensure timely processing of your notifications, please describe how your company plans to provide these international services in the near future. You should list the EEA countries and any third countries to which your company plans to provide services, as well as describe how you intend to monitor and check agents and branch offices as part of your

company's internal control system, with particular emphasis on the monitoring and control processes related to financial crime and compliance with sanctions legislation. If your company uses agents, we expect you to also provide an overview of the IT systems, processes and infrastructure used by these agents to perform activities on your behalf.

3.10 Information systems, infrastructure and security

PSD2 requires a stronger focus on the management of operational and security risks. Subsections 4.10 to 4.15 set out our expectations regarding the management of these risks, which means there will be some overlap with the other subjects described in this section. You do not have to submit the same document again for each of these subsections, but we ask you to include clear references as to where the requested information can be found in your application.

You company should have in place an information system and information infrastructure to support operational processes. They should meet all internal and external information requirements. There must be effective management of operational and security risks. The information system and infrastructure must be set up to ensure that transactions and entries in data files can always be retraced to authorised source files or data processing by authorised staff or systems.

Electronic data processing (EDP) and the related infrastructure must be an integrated part of the organisation, and the data must comply with the requirements relevant to the nature of the activities and statutory regulations.

A company using electronic data processing and offering EDP-based services must implement measures and procedures to ensure the integrity of the electronically processed data, protect the data from unauthorised access or processing and safeguard the availability of data and EDP.

The description of measures and procedures to manage operational and security risks must address the following.

a. The company's IT strategy, IT policy and security policy.
b. The IT landscape, the information systems and their infrastructure, including internal and external links.
c. The information systems, infrastructure components and links that are classified as critical, including the applicable classification criteria and a substantiation.
d. The operational and security risk management framework.
e. The risk and risk management model, including a detailed risk analysis.
f. Identification and classification of operational functions, processes and resources, with a focus on the availability, integrity and confidentiality of systems, infrastructure, data and processes.

g. The measures in place to protect the data, information systems and information infrastructure as well as the integrity of these information systems, information infrastructure and data, using security measures and logical and physical access security, possibly including multiple layers of protection.
h. Continuous monitoring and detection of internal and external threats and vulnerabilities that could have an impact on the information systems and the information infrastructure, and how this is approached.
i. The policy, process (with its relevant procedures) and specification of logical access security, providing insight into the organisational segregation of duties with respect to the security of logical access to information systems and the information infrastructure.
j. Ongoing monitoring for variations and unauthorised activity in the information systems and information infrastructure.
k. Testing of security measures to assess their robustness and effectiveness, including regular vulnerability scans and penetration tests (at least once a year).
l. The process with its relevant procedures for making changes to the information systems, information infrastructure and security measures, including the implementation of short-term emergency changes.
m. The process providing continuous insight into the vulnerabilities at security and operational levels in IT and the financial sector that could impact the company's information systems and information structure and (if necessary), sharing of insights with the sector.
n. Training staff members in the area of security and information security.
o. Informing users/customers about security and information security.
p. The process with its relevant procedures for secure sharing of data and secure submission of obligatory reports.
q. The process of independent assessment of the security measures by auditors with expertise in the area of IT security and payments, who are operationally independent within or with respect to your company.

3.11 Authentication

The purpose of authentication is to establish the identities of payment service users and others. If your company has direct contact with payment service users, you must apply strong customer authentication (SCA). SCA means authentication based on combining two or more elements categorised as knowledge (i.e. something only the user knows), possession (i.e. something only the user possesses), and inherence (e.g. a user's biometrical characteristics), resulting in a unique authentication code.
The procedures manual must address the following aspects of authentication.

- the use and control of customer authentication instruments
- the supporting processes and resources (hardware and software)

- the protection of the authentication code in accordance with Commission Delegated Regulation (EU) 2018/389, the European Regulatory Technical Standards (RTS) on strong customer authentication.

If you believe your company is exempted from applying SCA, you must be able to substantiate this.

When authorising a payment transaction, the unique authentication code generated specifically for the payment transaction must be linked to this payment transaction (i.e. the dynamic linking requirement laid down in the RTS). The procedures manual must describe your company's process and security measures related to customer authentication.

You must test the customer authentication process and security measures on a regular basis, and ensure that they are assessed and checked by auditors with expertise in the area of IT security and payments, who are operationally independent within or with respect to your company.

3.12 Secure communication

Your company uses electronic (digital) means to communicate with third parties. This means you must take the necessary measures to safeguard the availability of communication and ensure data confidentiality and integrity. The procedures manual must describe the measures you have taken and the processes and procedures to manage them.

As a payment service provider, you must ensure secure identification in the communication between the equipment of payers and payees used for accepting electronic payments. You must also ensure that the risk of communication towards unauthorised parties is limited as far as possible. You must describe how you do so in the procedures manual.

As a payment service provider, you must have procedures in place to safeguard that all payment transactions and other interactions with payment service users, other payment service providersand other entities (including traders) can be traced, ensuring that all events that are relevant to the electronic transaction, in all stages, can be identified.

You must ensure that all communication sessions with payment service users, other payment service providers and other entities (including traders) include each of the following elements.

a. A unique session identifier.
b. Security mechanisms for detailed transaction logging, including a transaction number, time stamp and all relevant transaction details.
c. Time stamps that are based on a time reference system and synchronised with an official time signal.

Your company's procedures manual must include a description of how this is ensured in your organisation.

If your company uses cryptographic means, you should also describe the technologies used and how these means (e.g. keys and certificates) are stored and managed.

3.13 Data collection

Due to the nature of the proposed activities, your company will be dealing with sensitive payment data, i.e. data that could be abused for fraudulent purposes. This in any event includes personal security details[3].
Sensitive payment data must never fall into the wrong hands, which is why you must provide a description of your company's process for storing, monitoring and tracing sensitive data and for restricting access to such data. You should include the following four elements in this description:

- A description of the data flows in proportion to your business model.
- A description of the storage process for collected data. If you provide type 7 services only, this is not required, since type 7 service providers are not permitted to store sensitive payment data.
- A description of the expected internal and external applications, including a description of any third parties involved in this, with respect to collected and stored data. If you provide type 7 services only, this is not required, since type 7 service providers are not permitted to store sensitive payment data.
- A list of the individuals, operational units and committees with access to the sensitive payment data, including explanatory notes.

Please note that the list above is not exhaustive.

If your company is granted a licence, the following applies to your organisation with respect to data protection.

- If your company offers payment services types 1 through 7, you may only access payment service users' personal details with their express consent, and only process and store these details to the extent that you need them for the provision of payment services[4].
  Your company's procedures manual must include a description of how this is ensured in your organisation, taking into account temporary storage of payment data, security and authentication data, and how consent is recorded.
- If your company offers type 8 payment services, you may only provide these services with the express consent of the payment service user.[5]

3 The account holder's name and account number do not qualify as sensitive payment data in relation to the activities of payment initiation service providers and account information service providers.

4 Proposed new Section 26e of the Decree on Prudential Rules for Financial Undertakings (*Besluit Prudentiële regels Wft – Bpr*).

5 Proposed new Section 26j of the Decree on Prudential Rules for Financial Undertakings (*Besluit Prudentiële regels Wft – Bpr*).

Your company's procedures manual must include a description of how this is ensured in your organisation, taking into account temporary storage of payment data, security and authentication data, and how consent is recorded.

3.14 Follow-up of incidents

Operational or security incidents

Operational or security incidents are events that endanger the availability of your company's services, the confidentiality or integrity of the data entrusted to your company, or both. Given the impact of such incidents on your operational management, you must have measures in place to minimise the risk of such incidents occurring.

This is why your company must have policy, procedures and measures in place to address operational or security incidents. The following procedures and measures must be described as a minimum.

- Incident recording.
- Classification mechanism based on criteria determined by law, distinguishing between major and non-major incidents and providing for an adequate analysis of the internal and external impact of incidents, including the impact for fellow payment institutions inside or outside the Netherlands.
- Notification to DNB of major incidents within four hours and in accordance with the set procedure and the required information.
- Procedure for updating DNB on the progress of resolving incidents.
- Performing a root cause analysis after incidents have been resolved.
- Fully informing DNB based on the prescribed procedure.
- Your company must have a complaints procedure enabling payment service users to report potential or actual security risks and incidents.

We are obliged to notify the European Banking Authority (EBA) and the European Central Bank (ECB) of any operational or security incidents, and these bodies may contact your company directly on the basis of this information (see EBA-GL-2017-10).

You must describe your company's policy, procedures and measures regarding operational and security incidents in the procedures manual.

Your company is responsible for notifying any other relevant authorities (e.g. the DPA) in the Netherlands in the event of operational or security incidents.

Integrity incidents

An incident is defined as behaviour or an event that poses a serious threat to ethical pursuit of business operations. Because of the repercussions that incidents can have on a company, it is important that you organise your operational management so as to ensure that the risk of incidents occurring is limited to the best possible extent. The company must be prevented from being implicated in criminal offences, or committing acts that conflict with commonly accepted practices. It makes no difference who commits said acts; they may include behaviour of staff members, executive directors, supervisory board members, or of natural or legal persons working for your company. This includes both displaying and refraining from specific behaviour.

This is why your company must have procedures and measures in place to deal with incidents. This entails the following:

- Recording of incidents;
- Procedures for dealing with incidents;
- Supply of information to the supervisory authorities.

Your incident records enable us to assess whether your company handles incidents in the appropriate manner. From your records, we should be able to distil the characteristics of the incident, the perpetrators causing the incident or aggravating the situation, and the measures taken. You must notify us promptly of any incidents.

Fraud reporting

Payment institutions are obliged to collect data on fraud and report these to DNB in a prescribed format and on a regular basis, i.e. you must submit an overview of quarterly fraud data every six months.

Your company must have procedures and measures in place to record the correct data and meet the fraud reporting requirements. The procedures and measures must be described in the procedures manual.

Please consult the EBA website for more information, since the requirements have not yet been finalised. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

3.15 Business continuity management

Your company must have a business continuity management (BCM) system in place to enable the recovery of its services following serious internal or external disruptions as soon as possible in accordance with the agreements made and socially expected recovery time.

The BCM system must be described in the procedures manual and must address at least the following eight elements.

- The BCM policy, describing the organisation during disruptions, disruption classification, maximum recovery times for systems and processes, internal and external communication, escalation, notification of authorities, loss of data, etc.
- A business impact analysis, taking into account the internal and external impact of incidents.
- The measures in place to implement the policy and the agreements made, and how these measures were formulated.
- The various disruption scenarios in use.
- A communications plan.
- A crisis management plan.
- The human factor.
- A testing plan for the BCM system, setting out the method and frequency of testing, demonstrating that the company is able to comply with its own policy at all times.

3.16 Sound remuneration policy

As part of controlled operational management, your company is required to pursue a controlled remuneration policy that must be recorded in writing, in a separate document (and not in the Procedures Manual). In short, the remuneration policy must include the requirement that remuneration does not contain incentives to take more risks than acceptable in view of the company's solidity.

The remuneration policy must in a structured and logical way describe possible unwanted incentives as part of risk management, and describe how your company prevents and mitigates these incentives. Obviously, developing a controlled remuneration policy requires in-depth analysis of possible inappropriate incentives contained in remuneration structures and components. This analysis should pay explicit attention to the incentives that may arise as a result of variable remuneration components. Positive incentives as part of claw back options can also be included in the analysis.

The description of your company's remuneration policy must answer the following four questions:

- Is the fixed-to-variable remuneration ratio applied appropriate to your company?
  This includes the generally important aspects to remuneration policies, e.g. the nature of the company's activities, the size of the company and the consequences for customer treatment. When formulating the appropriate ratio, the company must remain within the boundaries set by the bonus cap.
- What is the ratio between awarded remuneration and distributed variable remuneration?
- What is the composition of variable remuneration?
- What are the criteria and performance on which variable remuneration are based?
  You should not just describe the performance and results of the individual staff members receiving the variable remuneration, but also the performance of their business unit, and those of the company as a whole. Performance assessments of individual staff members must also include non-financial criteria, e.g. to what extent objectives such as the following have been achieved: strategic goals; customer satisfaction and compliance with policies relating to risk management, compliance with internal and external rules, leadership, management skills, cooperation with other staff and business units, creativity, motivation, sustainability, and corporate social responsibility. Negative performance on non-financial criteria, especially in the case of unethical or non-compliant behaviour must cancel out positive results on financial criteria. In such cases, variable remuneration should be lowered to zero. At least 50% of variable remuneration must be based on non-financial criteria.
  Please note that variable remuneration is subject to a cap under Section 1:121 ff of the Wft. We further defined the rules pertaining to remuneration policies in the Regulation on Sound Remuneration Policies (Regeling beheerst beloningsbeleid Wft 2014) (see www.overheid.nl; in Dutch only)

Please enclose your remuneration policy as an annex to the application form. We also ask you to briefly state in your own words how your company's remuneration policy does not encourage staff to take more risks than acceptable in view of the company's solidity.

3.17 Oath or affirmation

Your company must have procedures and measures in place to ensure that natural persons working in the Netherlands under the responsibility of your company, whose activities may have a material impact on the company's risk profile, or who are directly involved in the provision financial services, take the oath or affirmation in conformity with the 2015 Regulation on the Financial Sector Oath or Affirmation (Regeling eed of belofte financiële sector 2015).

Adequate implementation of processes and procedures largely depends on the level of knowledge and experience of staff. This is why knowledge of and experience with risk management (including money laundering and terrorist financing) are important preconditions

for developing an adequate control framework. Staff training courses are important instruments to communicate and embed knowledge of the Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft) and the Sanctions Act 1977 (Sanctiewet 1977 – SW) and integrity principles and procedures.

3.18 Training

Your company is required to offer its staff and board members training courses to ensure that everyone within your company is acquainted with the provisions of the Wwft and the SW, to enable staff to perform customer due diligence fully and correctly and to recognise unusual transactions. These training courses must cover money laundering and terrorist financing techniques, methods and trends, the international environment and standards and new developments in this area. In order to enable staff to keep abreast of new developments and to improve awareness in the long term, training courses are usually not one-off sessions, but should be offered at regular intervals and at different levels. The compliance function is also advised to attend additional training courses in order to remain aware of new developments in the area of international legislation and regulations, and money laundering and terrorist financing.

Please enclose your company's training programme with your application. We also ask you to submit a description of how your company has organised its training scheme to guarantee sound and ethical business operations. The description can be part of the company's procedures manual or be included in a separate document. Please state in the application form where we can find the relevant information.

4 Ethical business operations

Ensuring ethical business operations is one of the pillars of confidence and, hence, a precondition for your company's proper functioning. It is essential that you prevent your company from becoming involved in unlawful or socially unacceptable acts. You should focus on managing integrity risks and combating financial and economic crime in particular in this respect. Money laundering, terrorist financing and conflicts of interests are key examples of financial and economic crime.

The requirement of ethical business operations is based on Sections 3:10 and 3:17 of the *Wft* as further elaborated in the *Bpr*. The applicable integrity legislation is the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en het financieren van terrorisme – Wwft*) and the Sanctions Act (*Sanctiewet 1977 – Sw*). Your company must pursue an adequate policy to ensure ethical operational management. This integrity policy must be detailed and implemented in clear and readily accessible procedures and measures, recorded in a procedures manual.

The regulatory framework for adequate integrity policies is risk-based, meaning that your company must implement all measures that the law requires. The focus of these measures depends on the risks that your company is exposed to. They may e.g. follow on from the nature and background of your customers, the type of product (iDEAL, debit card terminal, money transfer, etc.) or the type of service (types 1 to 8). You must assess the risks that your company is exposed to and formulate appropriate mitigating measures.

The following points should be addressed in this assessment:

- Systematic integrity risk analysis
- Preventing conflicts of interests
- Dealing with and reporting of incidents
- Propriety of staff in integrity-sensitive positions
- Customer due diligence[6]
- Sanctions Act
- Transaction monitoring and reporting of unusual transactions[7]
- Complaints procedure.

These points are explained in greater detail below. National and European regulations regarding payment services and risks such as money laundering and terrorist financing are constantly changing. You are responsible for updating your policy and procedures in accordance with the applicable rules and regulations.

6 We have prepared Q&As on customer due diligence for type 7 and 8 services. You will find these Q&As on our PSD2 web page: http://www.toezicht.dnb.nl/4/1/50-236570.jsp

7 We have prepared Q&As on transaction monitoring for type 7 and 8 services. You will find these Q&As on our PSD2 web page: http://www.toezicht.dnb.nl/4/1/50-236570.jsp.

4.1 Systematic integrity risk analysis (SIRA)

Your company's integrity policy and its implementation starts with identifying your integrity risk exposure. Such a systematic integrity risk analysis (SIRA) is a precondition for ensuring ethical operational management. The analysis must be verifiable, i.e. recorded in a separate document, and the integrity policy must be based on the outcome of the SIRA, and you must use a comprehensible quantification method. The SIRA is based on gross (inherent) and net (residual) risks and analyses the likelihood and impact of these risks. The size of net risks must be clear and the measures and procedures must have a plausible effect.

The SIRA must at any rate include an analysis, for different scenarios, of the following risks: conflicts of interest; money laundering; terrorist financing; breach of sanctions legislation, and internet fraud and scams. Your company's SIRA must also include an analysis of risks associated with your customers' products and services and you must include this in the customer profiles that you intend to use. You are also required to pay extra attention to on-line customer acceptance (if applicable). This inherently carries high risk and your analysis must specify the measures with which your company intends to offset this elevated risk.

Your procedures and measures must be verifiably connected with the specific risks identified in the SIRA. The control measures set out in the SIRA must be in line with the nature, size, complexity and risk profile of your company's operations. You will find more information on the SIRA in our user manual for producing an adequate SIRA: "Integrity risk analysis: more where necessary, less where possible": http://www.toezicht.dnb.nl/en/binaries/51-234068.pdf

4.2 Preventing conflicts of business and private interests

Conflicts of interest or the semblance thereof may negatively affect your company as well as its customers. Your company must therefore have procedures and measures in place to prevent conflicts between its own business interests and the private interests of specific groups, i.e.

- policymakers
- group directors
- supervisory board members
- other staff members or individuals who permanently work for the company.

This policy should make clear how you approach e.g.

- personal, professional, and financial interests in relation to contacts with customers and other stakeholders
- handling confidential information,
- customer relationship management
- private financial transactions
- secondary activities

4.3 Propriety of staff working in integrity-sensitive positions

In addition to the positions of managing director or member of the supervisory body, there are other positions that may influence ethical business operations. These are known as integrity-sensitive positions. You must determine which positions in your company qualify as integrity-sensitive, and thoroughly screen the staff members holding these positions. This also applies to temporary staff.

The following positions always qualify as integrity-sensitive:
- the management layer directly below policymakers and co-policymakers;
- positions with powers that pose fundamental risks to ethical business operations.

4.4 Customer due diligence

You are not permitted to start providing services to customers before you have identified and verified the customer and the ultimate beneficial owner (UBO), i.e. before you have performed customer due diligence. Your procedures manual should explain the procedures and measures contained in the customer due diligence exercise. Procedures and measures relating to client acceptance must be in accordance with the company's integrity policy, the outcome of the SIRA and legal requirements.
The frameworks of the *Wft* (ethical operational management) and the *Wwft* assume that a company allocates its customers to risk categories, based on the nature and size of risk exposure. These risk categories vary from low to high risk, and the classification should be based on objective and identifiable indicators. The higher the risks, the more efforts your company should make to mitigate them. You must also indicate which risks you find unacceptable.

When performing customer due diligence, you must take account of the following points.
- Your company must verify the identity of all customers based on independent and reliable documents. If legal entities are concerned this also includes their representatives and ultimate beneficial owners (UBOs).
- Your company is sufficiently familiar with the customer's or legal entity's ownership and governance structure.
- Your company is well aware of, and has adequately documented, why and with what intention the customer wants to use its services, and sees that this is incorporated in the customer's risk profile.
- All customers must undergo politically exposed person (PEP) screening and sanctions screening.
- Your company is required to file all such information in readily accessible form for at least five years after it has ceased providing services, or terminated the business relationship.

All data and files relating to the customer and the ultimate beneficial owner must be kept in a central place and can be accessed by compliance and other relevant staff. Your company must also record when enhanced customer due diligence is required and which measures it intends to take in such cases, and document whether customers, prospective customers or ultimate beneficial owners are politically exposed persons. You must assign customers to risk categories, stating your reasons for allocating customers, products or services to specific risk categories. This classification must be adequate and in line with the SIRA mentioned above. Customers are accepted subject to screening against sanctions lists, PEP lists and any other relevant lists. You must record positive matches in the relevant customer file and take action where needed. These matches must also be mentioned in the customer's risk profile and must be reported to us. And finally, an exit policy must be put in place for customers who cannot or do not want to be identified, or whose identity cannot be verified in the prescribed manner. When such cases occur, they must be verifiably followed up.

Procedures and measures must document how and by whom customer due diligence is to be performed. The relevant staff must be made aware of the internal and statutory requirements imposed on customer due diligence. Customer acceptance must be approved by authorised staff or management based on the four-eyes principle. See our Guidance on the *Wwft* and the *Sw* for more information on this topic. http://www.toezicht.dnb.nl/en/binaries/51-212353.pdf.

4.5 Sanctions Act 1977 (*Sanctiewet 1977 – Sw*)

Your procedures manual must include your policy and procedures on sanctions legislation. These procedures must guarantee the existence of a comprehensive and up-to-date inventory of services provided, broken down by countries, natural persons, legal entities and groups governed by sanctions legislation. You must also have a procedure in place for the receipt and internal distribution of sanctions lists (at least with respect to the Netherlands sanctions lists and the EU regulations).

These procedures and measures must ensure that the customer base is regularly screened on matches with the entities targeted by sanctions legislation. The procedures must provide for risk-based monitoring of domestic and international services. The procedures and measures take account of the standards and objectives of the various sanctions regulations (governing sanctions against persons/entities or against countries).

The procedures and measures must be structured to ensure that if a match is detected financial assets may be frozen, or financial resources or services can be prevented from being made available to persons or entities mentioned on the sanctions list. Your company must have adequate measures in place to guarantee that any matches are reported without delay to the responsible central person or department and, if acknowledged as a match, reported to DNB.

See our Guidance on the *Wwft* and the *Sw*, http://www.toezicht.dnb.nl/en/binaries/51-212353.pdf and "Getting around in sanctions regulations" on our Open Book on Supervision pages: http://www.toezicht.dnb.nl/en/2/51-221960.jsp, for more information on this topic.

4.6 Transaction monitoring and reporting of unusual transactions

Your company must have procedures and processes in place to monitor customers' accounts, activities and transactions so as to gain and retain insight into the nature and background of customers and their financial behaviour, and to detect non-standard transaction patterns, including unusual transactions and transactions that by their nature entail increased risk of money laundering or terrorist financing. You must have procedures and processes in place specifying how transactions are monitored, which alerts and red flags are used, and how to act if transactions are made that may qualify as unusual, and you must make motivated and appropriate choices between electronic monitoring and manual monitoring. Electronic monitoring may be applied for large numbers of transactions. You must have policies and procedures in place to report detected unusual transactions to FIU-Netherlands without delay.

See our Transaction Monitoring Guidance document for more information on this point. http://www.toezicht.dnb.nl/en/binaries/51-236852.pdf

5 Fit and proper assessment of policymakers and co-policymakers

5.1 Fitness of policymakers

The policymakers[8] in your company must be fit to occupy this position. You must therefore take care to nominate individuals whom you expect to pass DNB's fit and proper assessment. When assessing fitness, we determine whether a candidate has sufficient relevant knowledge and skills, and displays the required professional behaviour to perform the job, and establish this based on education, work experience and competences.

As the fitness assessment is linked to position, we consider
- the details of the candidate's proposed position,
- the nature, scope, complexity and risk profile of the company, and
- the composition and performance of the control structure.

We apply the Policy Rule on Suitability 2012. For more information, please refer to the relevant page on Open Book on Supervision: http://www.toezicht.dnb.nl/en/4/2/16/51-229353.jsp

Supervisory boards (whether or not required by DNB) must act independently, as part of the company's sound and ethical operational management. For more information, please refer to the relevant page on Open Book on Supervision: http://www.toezicht.dnb.nl/en/3/51-226002.jsp
You can use the Initial assessment application form available from our Digital Supervision Portal (DLT) to present a candidate for assessment. We frequently see that application forms are not filled in completely, which causes unnecessary delays. Our website has tips to help you prepare for the screening procedure: http://www.toezicht.dnb.nl/en/4/2/16/51-229355.jsp

Please note that for management board and supervisory board members a maximum number of supervisory roles applies under the Management and Supervision Act (*Wet bestuur en toezicht*).

5.2 Propriety of policymakers and co-policymakers

The propriety of the policymakers and co-policymakers in your company (managing and supervisory directors, if applicable) must be guaranteed beyond all doubt.
Individuals holding direct or indirect qualifying share holdings are classified as co-policymakers. Owners of a qualifying holding are natural persons or legal entities that have a direct or indirect shareholding or controlling interest in the company of 10% or more. Individuals who are able to exercise actual influence on the company's day-to-day management are also designated as co-policymakers.

8 The company's policymakers are the members of its Management Board and – if applicable – the members of its Supervisory Board. Co-policymakers are not subject to the fitness assessment. The section "Propriety of policymakers and co-policymakers" below sets out which staff members are classified as co-policymakers.

DNB verifies whether the propriety of the candidate is beyond doubt, Candidates' intentions, actions and antecedents must not stand in the way of performing the duties of the job.
In particular, we review criminal, financial, tax compliance, supervisory, tax administrative law antecedents and other relevant information.

In principle, propriety assessments are a one-time procedure. Candidates who have passed the assessment will not require reassessment. Our decision will stand unless a change in the relevant facts or circumstances provides reasonable grounds for a propriety reassessment.

A propriety assessment is related only to the candidate individually. This means that – unlike in initial fitness assessments – our decision does not depend on circumstances such as the composition of the management board, the type of company that the proposed appointment pertains to or the specific post the appointee will take up. A propriety assessment is performed based on information provided by the company and an assessment by DNB
For more information, see: http://www.toezicht.dnb.nl/en/4/2/16/51-229351.jsp

6 Two day-to-day policymakers working from the Netherlands

The day-to-day management of your company must be in the hands of at least two natural persons. These two individuals must work from the Netherlands, in order to ensure compliance with the four-eyes principle, or the principle of dual day-to-day management. The rule that two or more natural persons must be responsible for the day-to-day management of a payment institution, guarantees continuity and observance of the quality standard of the company's operations and services.

7 Transparent governance structure

Your company must have a transparent governance structure. In short, this means that its formal control structure must be the same as its actual control structure. The governance structure must not obstruct adequate supervision. This occurs if, as a result of the governance structure, individuals are employed by the company who are subject to the laws of non-EU states. The aim of this statutory provision is to prevent the organisational structure within which the activities of the control structure are performed from deviating sharply from the legal structure in which the activities are embedded. An organisational structure of this kind impedes adequate supervision of your company. This includes identifying your company's risk exposure, or assessing whether its operational management is sound and prudent.

Please provide a diagram of the legal structure (UBO, parent company, any subsidiaries and affiliated companies) of which your company (as a payment institution) is a part. It must reflect the actual situation clearly and accurately. The diagram must include the identities of the persons and entities possessing a qualifying holding in your company, as well as the size of such holdings. Owners of a qualifying holding include natural persons or legal entities that have a direct or indirect shareholding or controlling interest in the company of 10% or more. The overview must also show the identity of the ultimate beneficial owners, and the managing directors of all legal entities and companies and firms that are part of the group.

Group relationships

If your company is part of a national or international group or a group of affiliated companies operating within or outside the EU, we would like to see a description of the group decision-making tree and the role that your company plays in this.

8 Qualifying holdings

This section does not apply to your company if you provide payment service type 8 only.
Companies wanting to acquire or enlarge a qualifying shareholding or a controlling interest in your company must obtain our prior permission. They must do so by applying for a declaration of no-objection (DNO) as meant in Section 3:95 of the *Wft*.

What do we mean by a qualifying holding?

A qualifying holding, which is subject to a declaration of no objection (DNO), applies in the following cases.

- A legal entity or natural person acquires or will acquire a direct or indirect holding representing 10% or more of your company's issued share capital.
- A legal entity or natural person can exercise directly or indirectly 10% or more of the voting rights in your company, or have comparable control.

In determining the number of voting rights of holders of participating interests in a company, we also take into account the votes that the holder has or is taken to have. Control comparable with voting rights may comprise special rights in respect of appointment, dismissal or suspension of management or supervisory board members of your company.

Separate DNO procedure

Before your company can be issued a licence, you must have all qualifying holdings approved by a DNO. To issue DNOs for qualifying holdings, we need relevant details from the qualifying shareholders.

Note: the qualifying shareholders must submit these details by means of a separate form, available from the DLT. The DNO procedure runs parallel to the licence application. For complex shareholder structures, e.g. if more parties are required to submit DNO applications at the same time, we recommend that you contact us first. You can contact the expert centre at: markttoegang@dnb.nl

Deadlines

The statutory consideration period for a DNO application is 62 business days. This may be suspended for up to [20/30] working days if we need further information to consider your application. The consideration period starts on the first business day after we have received the complete DNO application (all required information).

Fee

We charge a fee for considering applications for licences or DNOs. The fees charged are listed in Annex I to the Financial Supervision Funding Act (*Wet bekostiging financieel toezicht*). The fees charged depend on the number of hours spent on processing the application. The fee for a DNO application is charged to the party acquiring or increasing the qualifying holding and applies regardless of whether DNB issues or rejects the application, the applicant withdraws the application during the procedure, or we cease consideration during the procedure.

9 Securing the funds of payment service users

This section does not apply to you if you only provide payment service types 7, 8 or both.
If your company provides payment services 1 through 6, you must safeguard that the funds of payment service users remain separated from your company's own funds. This prevents the payment service users' funds from being seized by creditors in the event of bankruptcy, for example. Your company has two options for securing these funds.

Method 1: customer accounts foundation

The funds are paid into a separate account that cannot be touched by your company's other creditors. In practice, this means that a separate, independent custodian must be appointed to manage the funds entrusted by payment service users – known as a customer accounts foundation. In order to guarantee as much as possible the independence of the customer accounts foundation, the foundation must meet the following conditions.

- Propriety of the managing directors of the customer accounts foundation. Their propriety must be beyond all doubt.
- Appropriate and concise description of objectives: the articles of association clearly and accurately describe the objective of the customer accounts foundation, i.e. receiving, managing and distributing customer funds.
- No commercial activities. Following from its objective, the customer accounts foundation is not permitted to develop commercial activities, issue loans or enter into other financial obligations. This will prevent claims from being made on the foundation by third parties.
- Prudent handling of payment service users' liquid assets: any funds invested during the period of securing must be invested in safe and liquid low-risk assets. The company must also ensure that the liquid assets of the customer accounts foundation at any time at least equal the company's liabilities to the payment services users (reconciliation). Finally, the customer accounts foundation is not permitted to issue bridging finance, i.e. when the foundation pays out funds to the user before the foundation has received these funds.

Adequate segregation of duties and prevention of conflicts of interests between the payment institution and the customer accounts foundation is crucial. This means the managing directors and the staff members working for the customer accounts foundation may not also work for the business unit responsible for effecting payment transactions or bear final responsibility for this business unit.

If you opt for this method, we expect you to submit a statement specifying your company's extent of compliance with Article 10 of PSD2. You must include a list of the persons having access to the protected accounts and their positions. You must also include a description of the accounting and coordination process for safeguarding that the funds of payment service users are protected, in these users' interests, from claims of other creditors of the payment institution, especially in the event of insolvency.

Method 2: insurance policy or comparable guarantee

If you opt for method 2, we require a statement that the funds entrusted are covered by an insurance policy, or a comparable guarantee from an insurance company or a bank that is not part of the same group as your company. The policy or guarantee covers the risk that you fail to meet your obligations with respect to the funds. We also require a detailed description of the reconciliation process demonstrating that the insurance policy or guarantee offers sufficient coverage and quality to ensure that your company is able to meet its obligation to secure funds at all times.

10 Minimum own funds and solvency

10.1 Minimum own funds

This section does not apply to your company if you provide payment service type 8 only.
When applying for a licence, your company must at least have own funds on a par with the highest outcome of the following two calculations.

Your company's initial capital amounts to

EUR 125,000 for the provision of payment services
- 1 through 5, or
- 1 through 5 with 6 and/or 7 and/or 8

EUR 50,000 for the provision of payment service
- 7, or
- 7 with 6 and/or 8

EUR 20,000 for the provision of payment service
- 6, or
- 6 and 8.

Your company's own funds must not fall below the required amount of initial capital. You must provide detailed information on your company's own funds with your application.

Please take account of the eligible capital instruments when calculating your required actual own funds. These are the capital instruments referred to in Article 26 of the Capital Requirements Regulation (CRR).

10.2 Required actual own funds as part of solvency

This section does not apply to your company if you only provide payment services type 7, 8 or both.
As part of solvency requirements, your company must hold a sufficient amount of actual own funds. The method to be used for calculating minimum actual own funds is determined based on the payment services that your company provides. The minimum level of actual own funds is generally calculated based on method B. In method B, the company's actual own funds depend on the volume of payments made. However, we would ask you to submit calculations based on all three methods A, B, and C.

You can find an own funds calculation template on the e-Line page on Open Book on Supervision: http://www.dnb.nl/en/statistics/eline-dnb/. Go to Payment institutions and electronic money institutions/user documentation/FIN&CO_REP prudentiële rapportages betaalinstellingen. Please complete the templates for the three years ahead, in line with your financial projections (see Section 3).

We want to remind you to take account of a number of deductible items when calculating your required actual own funds. These are the deductible items referred to in Article 36 *ff*. of the Capital Requirements Regulation (CRR). Intangible fixed assets for instance. These assets are regarded as "soft" assets that offer hardly any buffer against losses in times of stress. Other deductible items include earnings made in the current financial year that have not yet been confirmed by the auditor and deferred taxes encumbering future earnings. We would ask you to pay close attention to this, as we find these items are often overlooked.

For more information please consult the Manual for prudential reporting.

11 Indemnity insurance

This section does not apply to you if you only provide payment services type 7, 8 or both.
Please note: if your company also holds or is applying for a licence for services 1 through 6, the indemnity insurance requirement applies cumulatively to the minimum own funds and actual own funds requirements.

If your company intends to offer payment initiation services or account information services, you are required to take out professional indemnity insurance or a comparable guarantee. More information about the comparable guarantee can be found on our Open Book on Supervision pages: http://www.toezicht.dnb.nl/3/50-237165.jsp

The liability to be insured and level of coverage depends on the type of service provision. For example, for providing payment initiation services (type 7) you must be covered against non-permissible payment transactions and non-performance, inadequate performance or late performance of payment transactions. For providing account information services (type 8), you must be covered against claims from the account holding payment service provider for unauthorised or fraudulent use of account information.

Minimum level of coverage

The minimum level of coverage is calculated based on the following formula:

Minimum level of coverage = the amount appropriate to the risk profile + the amount appropriate to the type of activities + the amount appropriate to the size of activities.

Risk profile

The amount appropriate to the risk profile can be calculated by taking the total value of reimbursement requests by payment service users and/or account holding payment institutions over the past 12 months. If your company was already active in the past 12 months and no such requests were made, you may enter 0 here. If your company did not yet provide services in the past 12 months, you should enter an estimated aggregate value of the predicted reimbursement requests over a 12-month period. If you do not enter an estimate or if the predicted value is EUR 50,000 or lower, we will depart from a notional amount of EUR 50,000.

The risk profile includes the number of initiated transactions or the number of consulted accounts over the past 12 months. For payment initiation service providers this is calculated as follows:

- 40% of the first 10,000 initiated transactions
- plus 25% of the number of initiated transactions between 10,000 and 100,000
- plus 10% of the number of initiated transactions between 100,000 and 1 million
- plus 5% of the number of initiated transactions between 1 and 10 million
- plus 0.025% of the number of initiated transactions over 10 million.

If your company is not yet active, the predicted number of initiated transactions can be taken. If you do not enter an estimate or if the predicted number is 50,000 or lower, we will set the number at 50,000 transactions.
The same calculation method is applied with respect to the number of consulted accounts by an account information service provider. The number of initiated transactions can be read as the number of accounts consulted over the past 12 months.

Type of activities

The amount appropriate to the type of activities can be found as follows: if you are only applying for a licence for type 7 or 8 services, you can enter 0 here. If your company also holds or is applying for a licence for services 1 through 6, the indemnity insurance requirement applies cumulatively to the initial capital and own funds requirements. If your company also conducts other business activities in addition to providing payment services as meant in Annex 1 of PSD2, a value of EUR 50,000 is added to the formula unless your company can demonstrate, either by holding a guarantee or because the payment service provision activities are incorporated in a separate entity, that the risks do not impact service provision.

Size of activities

For payment initiation service providers, the amount appropriate to the size of activities is calculated as follows:

- 40% of the share of the total value of aggregate transactions over the past 12 months (*N*) between EUR 0 and EUR 500,000
- plus 25% of the share of *N* between EUR 500,000 and EUR 1 million
- plus 10% of the share of *N* between EUR 1 million and EUR 5 million
- plus 5% of the share of *N* between EUR 5 million and EUR 10 million
- plus 0.025% of the share of *N* over EUR 10 million.

If your company provides account information services, the amount to be entered is calculated as follows:

- 40% of the share of the total number of users over the past 12 months (*N*) between 1 and 100
- plus 25% of the share of *N* between 100 and 10,000 users
- plus 10% of the share of *N* between 10,000 and 100,000 users
- plus 5% of the share of *N* between 100,000 and 1,000,000 users
- plus 0.025% of the share of *N* over 1 million users.

If your company did not yet provide services in the past 12 months, you should enter estimated values and/or numbers. If you do not have an estimate available, or if the estimate is 50,000 or lower, you should enter 50,000.
The above calculations are based on the EBA's *'Final Guidelines on Personal Indemnity Insurance under PSD2'*, which can be found on the EBA website.

Annex
Overview of required annexes

If you do not yet have access to *e-Herkenning* and the Digital Supervision Portal (DLT), this overview lists all required Annexes referred to in the application form. Please note that this list is neither exhaustive nor detailed regarding all questions and explanations included in the application form. We recommend that you apply for *e-Herkenning* as soon as possible so that you can consult the form at the same time.

Plans

- Programme of operations and business plan
- Recovery and exit plan, including scenario analyses
- Marketing plan

Overviews

- Organisation chart
- Diagram of the legal structure

Analyses

- General risk analysis
- Systematic integrity risk analysis (SIRA)
- Business impact analysis
- Identification and classification of operational functions, processes and resources, with a focus on the availability, integrity and confidentiality of systems, infrastructure, data and processes.
- Completed FIN&COREP templates for the three years ahead (not applicable to type 7 and 8 services)

Agreements

- A copy of the engagement agreement issued to the auditor or audit firm (not applicable to type 8)
- Copies of any outsourcing agreements

Policy

- Risk management framework
- Compliance and compliance function charter
- Internal control and internal control function charter
- Outsourcing
- Incidents
- Business continuity management
- Remuneration policy
- Prevention of conflicts of private interests
- Integrity-sensitive positions
- Customer due diligence
- Sanctions regulations
- Monitoring and reporting of unusual transactions

Other

- Recent extract from the Trade Register of the Chamber of Commerce
- Certified copy of the company's articles of association
- Copy of the company's updated shareholders' register
- Funds flow chart (not applicable to types 7 and 8)
- List of outsourced activities
- Procedures manual (translation of policy into procedures and measures)
- Indemnity insurance (if applicable)
- Certified financial statements or auditor's opinion regarding compliance with the own funds and/or solvency requirement
- If there is a customer accounts foundation: 1) An extract from the Trade Register of the Chamber of Commerce of the customer accounts foundation. 2) A certified copy of the articles of association of the customer accounts foundation. 3) Details of the agreements made between the company and the customer accounts foundation or a copy of the agreement between the company and the customer accounts foundation. 4) A statement from your company certifying that the customer accounts foundation meets specific conditions. (not applicable to types 7 and 8)
- If there is an insurance policy or comparable guarantee: a copy of this policy or guarantee (not applicable to types 7 and 8)
- Documents evidencing the company's own funds, e.g. certified financial statements including the external auditor's opinion, memorandum of association, a bank statement showing the deposit of a specified amount of capital (not applicable to type 8)
- For existing companies you should include certified financial statements over the past three years, or an overview of the financial situation if the company has not yet issued financial statements (not applicable to types 7 and 8)

- Insurance policy or comparable guarantee (including terms and conditions)(not applicable to types 1 through 6)
- Calculation showing that the minimum level of coverage complies with EBA Guideline CB/2016/12 (not applicable to types 1 through 6)

Please note: In parallel to the licence application you must also submit the following applications separately through the DLT.

Fit and proper assessments for all relevant persons, with a separate form for each person to be assessed

- Application form for Initial Assessment
- Propriety Assessment Form (mandatory if not previously assessed on propriety) (not yet available through the DLT, see Open Book on Supervision http://www.toezicht.dnb.nl/en/4/2/16/51-229347.jsp

Separate declarations of no-objection for each shareholder (holders of a qualifying holding)

- Application for a declaration of no-objection (DNO) – Section 3:95 of the *Wft*

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl