Notes

to the licence application form for exchange institutions

DeNederlandscheBank

EUROSYSTEEM

Notes
to the licence application form for exchange institutions

These notes describe what DNB wants to see when considering your application for a licence. In addition to these notes, we have also listed all relevant sections of the law. See the PDF document "Relevant sections of the law for licence applications for exchange institutions" on Open Book on Supervision, under "Applying for licence". Please also keep these at hand when filling in the form and check carefully whether you comply with all requirements. This will help you submit a complete and correct application.

Table of contents

1 General information

1.1 Company data

We would ask you to provide us with a number of details about your company. Please submit all the required annexes, including a certified copy of the notarial deed stating the company's articles of association. Please ensure that the objectives described in the articles of association actually reflect the services that the company plans to provide. The description of the company's objectives may not include activities that require another licence, 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 Contact details of external consultant

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 his or her particulars.

1.3 Are you already active as an exchange institution or an exempt exchange institution?

You may already be operating as an exchange institution. If this is the case, we assume that you have made sure that you do not provide any services that are subject to a licence requirement. If you state that you are already active under the Exemption Regulation under the Wft (*Vrijstellingsregeling Wft*), please state the date on which you were registered as an exempt exchange institution. Please explain if you are currently active as an exchange institution, but not registered as an exempt exchange institution.

1.4 Conditions for licence applications

An exchange institution is an institution that performs exchange transactions in a professional capacity. This definition is based on Section 1:1 of the Wft. In order to determine whether your company qualifies as an exchange institution, the following questions must be answered.

1) Do the proposed activities qualify as exchange transactions?
2) Does the company intend to "pursue the business of" exchange transactions?
3) Does your company qualify for the Exemption Regulation under the Wft?

Does your company perform exchange transactions within the meaning of Section 1:1 of the Wft?

The Financial Supervision Act describes exchange transactions as all transactions involving the exchange of coins and banknotes of one currency for coins and banknotes of another currency and disbursement of coins or banknotes upon presentation of a credit card or in exchange for paper cheques or comparable documents.[1] Other activities may also be designated as exchange transactions by Order in Council. This follows from the definition of exchange transaction in Section 1:1 of the Financial Supervision Act. We would advise you to examine this closely together with a legal consultant.

Does your company provide exchange transactions on a commercial basis?

Your company is subject to the licence requirement if it performs exchange transactions on a commercial basis. You are always subject to the licence requirement if you actively promote your services, e.g. by advertising. Providing services to various customers is also an indication that these services are provided in a professional capacity. If your company provides exchange services on a one-off or very incidental basis, it does not qualify as an exchange institution.

Is your company subject to the Exemption Regulation under the Wft?

Exemption is possible for companies performing the business of a hotel, and who are registered as an accommodation providing business in the register of the Dutch industry board for Hospitality and Catering. This must involve the exchange of coins or banknotes and the disbursement of coins or banknotes upon presentation of a credit card or in exchange of one or more paper cheques. The counter value of these transactions must not exceed € 500 per guest per night and they may only available to natural persons to whom the hotel provides accommodation against payment.[2]

You are not required to apply for a licence as an exchange institution if already hold a licence as a bank or payment institution.

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

1 See Section 1:5a(2) under (g) of the Wft.

2 You will find the conditions for exemption under Section 1h of the Exemption Regulation under the Financial Supervision Act (*Vrijstellingsregeling Wft*).

2 Business plan

6 Your company's business plan must include a number of specific elements.

- A diagram of your activities and possible cash flows.
- The company's strategy, including
  - its targeted market share;
  - the envisaged origin of payment service users;
  - well-considered growth ambitions;
  - a SWOT analysis;[3]
  - outsourcing of processes;
  - the partners.
- A translation of your corporate strategy into financial projections for at least three years ahead (the current financial year and the three following years), including a full profit and loss account and a balance sheet, detailing the following items:
  - the company's expected own funds;
  - the assumptions and calculations underlying your financial projections, such as investment costs, outsourcing costs, management costs, contributions and your envisaged market share;
  - different 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;
  - an estimate of the company's liquidity position.

3 This is an analysis of your company's strengths and weaknesses, opportunities and threats, presenting, in matrix form, the potential success of your proposed services. Based on a SWOT analysis, you can define objectives and subsequently devise a strategy for achieving these objectives.

3 Sound business operations

You are required to set up your business operations in a way that guarantees sound operational management. This means that you must analyse the operational risks that your company is exposed to and take measures to mitigate these risks.

DNB always reviews sound business operations proportionally. This means that we base ourselves on the risks relevant to your organisation when assessing whether you comply adequately with the requirements pertaining to sound business operations.

As part of our assessment of sound business operations, we look at:

- general principles of operational management;
- a clear, balanced and adequate organisational structure;
- information supply and communication systems (adequacy);
- segregation of duties (adequacy);
- prompt and complete records and administration;
- information systems and security;
- risk management and risk control function;
- compliance function;
- internal audit function;
- outsourcing;
- controlled remuneration policy;
- oath or affirmation;
- training and education.

We will explain this in more detail below.

3.1 General principles of operational management

As a minimum, your company must base its operating procedures on the following six principles:

- a clear, balanced and adequate organisational structure;
- a clear, balanced and adequate distribution of duties, authorities and responsibilities (governance);
- adequate recording of rights and obligations;
- unambiguous reporting lines;
- an adequate information supply and communication system;
- a transparent definition of the company's operational management, which is subjected to regular reviews.

3.2 A clear, balanced and adequate organisational structure

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 organisation. The reporting lines must be in line with the organisational structure.

The division of tasks and the 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 to ensure that these are remedied.

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 grouped together with your company in a formal or actual governance structure. This prevents undermining of your organisation's sound business operations.

The organisation and management of business processes must be aligned as closely as possible if (i) the interconnectedness of activities and/or (ii) the activities of subsidiaries or other companies affiliated with your company in a formal or factual governance structure have a substantial influence on the financial performance, position, continuity or reputation of your company.

Please state in the application form whether your company has one or more director-major shareholders (DMSs), or a comparable control structure. A structure of this kind warrants special attention to balanced corporate governance. 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.

In our interpretation of a control structure involving one or more DMSs, a DMS is a natural person who is both a major 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 your company has one or more DMSs, you must provide evidence in your application for licence 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 a director-major shareholder.

3.3 Adequate information supply and communication systems

To ensure that communication systems are adequate, the company must have well-functioning internal communication channels, designed to ensure that all relevant information reaches the right staff members and functions at the right time. It is also important that the management board and line management are informed promptly and receive reliable information on the company's objectives and the relevant operational processes.

3.4 Adequate segregation of duties

The duties, authorities and responsibilities of both individual staff 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 staff members 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 adequate segregation of duties is difficult to achieve due to having a small number of staff, you must take alternative measures. One option is to outsource activities to third parties to compensate for the lack of internal segregation of duties.

3.5 Prompt and complete records and administration

You must record your company's rights and obligations in a dedicated administrative system. Your company is responsible for ensuring that the turnover and the financial rights and obligations to be recorded in the accounts are accurate and complete.

3.6 Information systems and security

Your company must have an information system in place that enables you to manage business processes effectively and that meets your internal and external information requirements. The information system 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.

Electronic data processing must be an integrated part of the company and electronic data must be available at all times. Consequently, companies using electronic data processing must take measures and implement procedures, including back-up copies and recovery measures, and a calamity plan that must be updated at regular intervals and tested for proper functioning. Your company must also have procedures and measures in place that safeguard the integrity of electronic data processing. And last but not least, segregation of duties within electronic data processing must be compatible with the organisation structure.

3.7 Risk management and risk control function

Your company must structure its policies to ensure adequate control of the relevant risks. Here you may think of credit risk, market risk, interest rate risk, concentration risk, liquidity risk, operational risk, insurance risk, and the risks associated with the macroeconomic environment in which the company operates and with the phase of the economic cycle.

In addition, you must have a clear perspective of the risks that your company is exposed to. The policy principles following from you risk perception must state how your company intends to manage its risk exposure.

Your risk management policy must be recorded in the form of procedures and measures, which must be tuned to the nature, size, risk profile, and the complexity of the company's activities, and include

- licence procedures
- limit allocation
- limit monitoring
- emergency procedures and measures

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

They must be clearly defined and recorded, e.g. in a policy plan, and must be consistently communicated, preferably in writing, to all units of the exchange institution exposed to these risks.

Your company must have an independent risk management function in place that ensures systematic, independent risk management. Risk management must focus 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.

3.8 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 shape of the compliance function depends on the nature and size of the exchange institution. "Independent" at least means that the compliance function is not influenced by commercial or other interests. Compliance duties must be recorded in a compliance charter, and the necessary activities must be further detailed in an annual compliance plan.

3.9 Internal control function

The effectiveness of the organisational structure and the procedures and measures in place must be tested independently in-house (at least once a year). By "independent" 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. Any shortcomings found must be adequately addressed. The board of supervisors is the (internal) client/principal of the internal audit function and carries (end)responsibility for its effectiveness.

3.10 Outsourcing

DNB must be enabled to exercise supervision of all activities and business processes of your company, also if these have been outsourced. This is why it is important that that you provide us with all information we need to assess whether all activities (also those outsourced) are performed in conformity with Part 3 of the Financial Supervision Act on the prudential supervision of financial enterprises.

Your company is permitted to outsource activities unless doing so hampers adequate compliance with the rules and regulations to which it is bound. This limitation only applies to outsourcing of important activities, which are taken to mean activities that may seriously harm the company's compliance with the requirements of its licence, its financial results, or the solidity or continuity of its services and activities if your company performs them incompetently or inadequately. There are also activities that you are not permitted to outsource, i.e. the duties and activities of staff members determining the 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 control structure relationship with your company will consequently harm embedding the quality of internal control.

If your company decides to outsource its internal audit function, audits must be performed by a third party under your company's management and supervision. This is because your company must at all times be able to render account of the structure and effectiveness of its operational management. It is essential to explicitly consider the risk of conflicts of interest when selecting the third party to perform the audit and the staff member within your company who will be responsible for managing and supervising the audit.

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.

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. Here you may think of procedures to be followed and measures that may be invoked to remedy deficient services by the third party, and calamities. It is important for companies that outsource activities on a permanent basis to analyse the risks associated with outsourcing. Risk analysis is an essential element for assessing whether or not activities are suitable for outsourcing.

To assess outsourced activities adequately, your company must have sufficient information at its disposal about the company to which it outsources these activities. The outsourcing company 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.

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

3.11 Sound remuneration policy

As part of sound operational management, your company must pursue a sound remuneration policy that must be recorded in writing. In short, the policy must include the requirement that remuneration does not include incentives to take more risks than acceptable in view of the company's solidity.

The remuneration policy must structurally and logically describe possible unwanted incentives as part of risk management, and describe how your company prevents and mitigates these incentives. Obviously, developing a sound remuneration policy requires in-depth analysis of possibly 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. It could also cover positive incentives arising from clawback provisions. Your remuneration policy must include the following three elements.

- The applied fixed-to-variable remuneration ratios appropriate to the enterprise. This includes the aspects that are generally important to remuneration policies, e.g. the nature of the company's activities, the size of the company, and the effect of remuneration on customer treatment. When formulating the appropriate ratio, the company must remain within the boundaries set by the bonus cap.
- The ratio between awarded remuneration and distributed variable remuneration.

- The criteria and performance on which variable remuneration is based, including the performance of natural persons working under the institution's responsibility, the business unit and the institution as a whole. So it is not just about the performance and results of individual staff members receiving the variable remuneration, but also about the performance of their business unit, and those of the institution as a whole. Performance assessments or individual staff members must also include non-financial criteria, e.g. to what extent the following objectives have been achieved: strategic goals; customer satisfaction; compliance with policies relating to risk management; compliance with internal and external rules; leadership; management skills; cooperating with other staff and business units; creativity; motivation; sustainability, and corporate social responsibility.

Negative performance on non-financial criteria, especially in case of unethical or non-compliant behaviour must cancel out positive results on financial criteria. In such cases, variable remuneration should be reduced to zero. At least 50% of variable remuneration must be based on non-financial criteria. Moreover, variable remuneration must be capped. For more information on this point, we refer you to Sections 1:121 and following of the Wft. The rules pertaining to remuneration policies are further defined in the Regulation on Sound Remuneration Policies (*Regeling beheerst beloningsbeleid Wft 2014*).

3.12 Training and education

Adequate implementation of processes and procedures largely depends on the level of knowledge and experience of staff. This is why knowledge and experience of 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.

Your institution is required to offer its staff members training courses to ensure that they are acquainted with the provisions of the *Wwft* and the SW, to enable them to perform customer due diligence fully and correctly and to identify unusual transactions. These programmes should focus on money laundering and terrorist financing techniques, methods and trends, on the international context and standards, and on new developments in this area. To enable staff to keep abreast of new developments and to improve awareness in the long term, training courses must be provided at regular intervals and at different levels, rather than as on-off sessions. The compliance function is also advised to attend additional training courses to keep up to date on new developments in national and international legislation and regulations, and risks of money laundering and terrorist financing.

4 Ethical business operations

The integrity of your company is one of the pillars of trust and, hence, a precondition for its proper functioning. It is essential that you prevent your company from becoming involved in unlawful or socially unacceptable acts. Management of integrity risks is the pivotal issue here. Integrity risks include money laundering and terrorist financing.

Your company is required to pursue an adequate policy to ensure ethical operational management. The integrity policy must be detailed and implemented in clear and readily accessible procedures and measures, recorded in a procedures manual. This procedures manual must also include (a reference to) the procedures required pursuant to the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels - Bpr*).

The regulatory framework for adequate integrity policies is risk-based, meaning that your company must implement all measures that the law requires. The intensity with which you do this, however, depends on the risks that your company is exposed to. These measures may for instance be related to the nature and background of customers, the type of product or service provided, the combination of customer and product, and how customer contact takes place (delivery channels).

You must assess the risks that your company is exposed to and formulate sufficient mitigating measures. 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 its risk exposure. These risk categories vary from low to high risk, and the classification is based on objective and identifiable indicators. The higher the risks, the more efforts the institution should make to mitigate them. You must also indicate which risks you find unacceptable.

The following points should at least be discussed:

- systematic integrity risk analysis;
- preventing conflicts of interest;
- dealing with and reporting of incidents;
- propriety of staff in integrity-sensitive positions;
- customer due diligence;
- *Sanctions Act of 1977*;
- transaction monitoring and reporting of unusual transactions;
- complaints procedure.

These points are discussed in detail below.

4.1 Systematic integrity risk analysis (SIRA)

Your company's integrity policy and its implementation starts with identifying your integrity risk exposure. The systematic integrity risk analysis (SIRA) is a precondition for ensuring ethical operational management.

As risks change continuously, the SIRA has a sell-by date, i.e. a date by which the analysis must be updated. The SIRA to be considered together with the licence application must at least be up to date. It must include instructions stating the situations in which business units need supplementary review, or when the review must be brought forward.

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 of the following risks: conflicts of interest; money laundering; terrorist financing; breach of sanctions legislation, and internet fraud and scams. Your SIRA must also include an analysis of risks associated with the products and services provided to customers 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). You must show that this always carries high risk and your analysis must reflect how 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/50-234068.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

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

This policy should make clear how you approach

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

4.3 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 these acts. These may be staff members, managing directors, members of the supervisory body, or natural persons or legal entities 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. The incident policy must at any rate include the following elements:

- 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.

4.4 Propriety of staff 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.

Integrity-sensitive positions include:
- management directly below policymakers and co-policymakers;
- positions with powers that pose real risks to ethical business operations.

You must determine which positions in your company qualify as integrity-sensitive, and thoroughly assess the staff members holding these positions. This also applies to temporary staff.

4.5 Customer due diligence (CDD)

You are not permitted to start providing services to customers before you have identified and verified the customer and the ultimate beneficial owner, by means of customer due diligence. Your procedures manual should explain the procedures and measures contained in the customer due diligence exercise. The procedures and measures for customer acceptance must be in line with your company's integrity policy, the risk analysis performed, and the applicable statutory requirements, including the *Wwft* and the *Sw* 1977.

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.
- 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.
- Your company is required to keep all such information in readily accessible form for at least five years after it has ceased providing services, or terminated the business relationship.
- In principle, your company does not provide numbered accounts and "hold mail" accounts.
- All customer data and files relating to the customer and the ultimate beneficial owner must be kept in a central place accessible to the compliance and other relevant staff.

Procedures and measures 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. Some categories of customer relationships require the explicit consent of senior management.

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 divide customers into 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. Customer acceptance is 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 hits 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.

See our "Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act and Counter-Terrorist Financing Act and the Sanctions Act" for more information.
http://www.toezicht.dnb.nl/en/binaries/50-212353.pdf

4.6 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 offered, broken down by countries, natural persons, legal entities and groups governed by sanctions legislation. There must also be 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 you regularly check your customer base for matches with the entities targeted by sanctions legislation. The procedures must provide for risk-based monitoring of domestic and international services. Your procedures and measures must take account of the standards and objectives of the different sanctions regulations. These procedures and measures must be structured to ensure that if a hit 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. The company must have adequate measures in place to guarantee that any hits are reported without delay to the responsible central person or department and, if acknowledged as a hit, reported to DNB.

Please note: your procedures with respect to the Sanctions Act 1977 must also include other customer relationships, e.g. sub-licence holders, authorised representatives, and payments to related companies.

See our "Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act and Counter-Terrorist Financing Act and the Sanctions Act" for more information.
http://www.toezicht.dnb.nl/en/binaries/50-212353.pdf

4.7 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 stipulating how transactions are monitored and how to act if transactions are made that may qualify as unusual, and you must make motivated and logical choices between electronic monitoring and manual monitoring. If you have large numbers of transactions, electronic monitoring will be the obvious choice, but this stops at detecting possible unusual transactions. Suspected unusual transactions are not performed before they have been manually verified. Your procedural descriptions must state which members of staff are authorised to perform manual checks, and which cases require the involvement of the compliance officer.

You must have policies and procedures in place to report detected unusual transactions to FIU-Netherlands without delay. And your company must notify all relevant business units of the policies, procedures and measures relating to the subjects mentioned above. Your company is also responsible for

- implementation and systematic testing of policies, procedures and measures;
- independently monitoring the implementation of the policies, procedures and measures relating to ethical business operations.

And finally, your company must have

- procedures in place to ensure that detected deficiencies or shortcomings are reported to the officers entrusted with that duty (independent compliance function);
- procedures in place to ensure that the detected deficiencies or shortcomings relating to ethical business operations are appropriately remedied under the supervision of an independent compliance function.

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.

5 Propriety of policymakers and co-policymakers

5.1 Executive directors, internal supervision, and co-policymakers

The propriety of the policymakers in your company (managing directors, and internal supervision, if applicable) must be guaranteed beyond any doubt. This requirement also applies to the individuals that have a say in your company policies.

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

In principle, propriety assessments are a one-time procedure. Appointees 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. 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, nor the specific post the appointee will take up.

Propriety assessments are performed based on information provided by the company, and our review of that information.

5.2 Qualified shareholders

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 interest or control in the company of 10% or more. Persons who are able to exercise actual influence on the company's day-to-day management are also designated as co-policymakers.

6 Transparent control structure

Your company must have a transparent governance structure. In short, this means that your company's 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 makes it impossible for us to supervise your company adequately. This includes identifying your company's risk exposure, or assessing whether its operational management is sound and prudent.

Group relationships

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

DeNederlandscheBank
EUROSYSTEEM

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