Good practices
fighting corruption
Contents

Introduction

Part I – Controlling the risk of corruption

1.1 Systematic risk assessment
1.2 The risk control process
1.3 What risks?

Part II – Measures

2.1 Measures in the field of organisation and culture
2.2 Measures in the field of governance
2.3 Measures in the field of third-party risk
2.4 Three high-risk policy fields

Annex

2013 Thematic Examination on Corruption: notes on assessment framework
Introduction

This brochure reflects the outcomes of the thematic examination on corruption performed by DNB at banks and insurers in 2013. During that examination, it was found that many financial undertakings need more information and guidance in order to fight corruption effectively in their own organisation. DNB is pleased to meet this need. This is why you will find in this brochure the assessment framework developed by DNB for banks and insurers companies, illustrated by references to good practices.

The assessment framework consists of the risk control cycle that DNB proposes as the standard for all banks and insurers: four steps that enable your organisation to take the measures necessary to tackle the risks that may possibly affect it. The good practices provide you with examples of solutions, measures and ideas adopted by other organisations in fighting the different risks of corruption.

The need for information about ways of tackling corruption is due in part to the international attention focused on the fight against corruption. The extraterritorial effect of U.S. and British anti-corruption legislation is an extra reason for banks and insurers that operate internationally to take measures to combat corruption.

Corruption is a subject that comes within DNB’s supervision remit. These good practices serve as recommendations to banks and insurers for the application of the statutory framework in respect of sound and ethical operations designed to prevent corruption in the form of conflicts of interest and/or bribery. You may apply these good practices in your efforts to prevent corruption, although you are not required to do so. Your own circumstances may be taken into account in this connection. The possibility cannot be excluded that stricter application of the underlying rules is required. This is a matter for you to decide.

---

1 Sections 3:10 and 3:17 of the Financial Supervision Act (Wet op het financieel toezicht or Wft) and Articles 10-13, 17, 18, 21 and 29 Decree on Prudential Rules for Financial Undertakings (Besluit prudentiële regels Wft or Bpr).
Definition of corruption

Given the extent to which integrity can be compromised within the financial sector, we have adopted a broad definition of corruption which covers private and public corruption, active and passive corruption and corruption in the Netherlands and elsewhere. The risk of corruption is defined as follows:

‘the risk that financial undertakings in the Netherlands may be involved in forms of bribery and/or conflicts of interest that compromise the integrity of, and trust in, the undertaking concerned or in the financial markets.’

Bribery too may be either active or passive: the active form involves bribing employees of another business that provides products or services to the undertaking, and bribery qualifies as passive if the undertaking’s own employees accept bribes from third parties.

The brochure

Part I explains the four different phases in the risk control process, and Part II takes a more detailed look at one of these phases, i.e. taking appropriate measures to combat corruption. For your information we have included a set of good practices in each part, classified in each case according to the different types of risk.

We hope that the guidance given in this brochure will enable you to take appropriate measures in your own organisation to combat corruption.
Part I – Controlling the risk of corruption

Using this part of the brochure you can take the necessary steps to assess risks systematically and take appropriate measures to manage the risk of corruption. A list of good practices is included at the end of this part. A diagram illustrating the risk management process is included on page 8 of this brochure.

1.1 Systematic risk assessment

Only if you identify the risks facing your organisation can you take appropriate measures. What risks does your organisation incur in respect of both inherent corruption and implemented controls? We therefore urge that all financial undertakings carry out a thorough and systematic risk assessment. This is actually a statutory requirement. As part of sound and ethical operations, financial undertakings are required under Article 10 of the Decree on Prudential Rules for Financial Undertakings (Besluit prudentiële regels Wft, hereafter: Bpr) to prevent and combat involvement in corruption by performing a systematic assessment of integrity risks, including the risk of corruption.

Some undertakings decide to perform a separate corruption risk assessment where they consider this to be necessary, for example because of the nature, scope or international character of their activities. Undertakings may also decide to include corruption in their generic systematic assessment of integrity risks or to perform a separate corruption risk assessment. The basic principle is in any event that anti-corruption measures should form part of a periodic risk assessment process, the results of which are recorded.

1.2 The risk control process

The risk control process consists of four steps: risk identification, risk assessment, adoption of appropriate measures and, finally, risk monitoring. Where desired, the monitoring results in a review of the risk assessment.

Step 1: Identify risks

The undertaking identifies what risks may play a role. It is important to establish clearly in advance what the scope of the assessment is, what internal and external sources are to be used (including legislation and regulations), what parties are involved and to what period the assessment relates.

Step 2: Assess risks

In the next phase, the undertaking studies how the identified risks play a role within the organisation. Account should be taken in this connection of the different (functional) departments or business lines, products and services, international activities, operational processes and other internal and external factors that affect risk. How vulnerable the undertaking is to the corruption risk is determined by assessing the chance or likelihood of corruption occurring and what the impact will be if corruption does actually occur. Factors taken into account include
**STEP 1**
Identify risks

**STEP 2**
Assess risks

**STEP 3**
Take appropriate measures

**STEP 4**
Monitor risks and address weaknesses

**Good Practices**
- All risks
- Inherent risks and controls
- Collaboration
- All jobs and units concerned
- Extra risk assessment, where necessary
- Reproducible from record

**Good Practices**
- Senior management involvement
- Targeted screening
- Effective training
- Promote awareness
- Incidents can easily be reported
- Responsibilities clearly allocated
- Key role of compliance and internal audit
- Third parties properly identified
- Three high-risk policy fields
the financial, economic and macroeconomic, operational, legal and reputational risks.

**Step 3: Take appropriate measures**
Once the risks have been identified and recorded, appropriate measures are defined and taken to control that risk. Part II of this brochure explains in some detail the measures your undertaking can take.

**Step 4: Monitor risks and address weaknesses**
The next step is to monitor whether the measures taken actually work, i.e. whether they are effective and efficient. If weaknesses or faults are found in corruption risk control or it transpires that the procedures and measures are not fit for purpose, you are expected to address these appropriately.

1.3 What risks?
To carry out properly the first two steps of the risk control process (identification and assessment), it helps if you have a clear idea of all the different types of risks that are possible.

Both internal and external factors can influence the risk of corruption. Common risks are:
- geographical risk
- sector risk
- product or transaction risk
- third-party risk
- risk of personal networks and interests.

**Geographical risk**
Geography plays a role in determining corruption risks both within your undertaking and in relation to third parties. The degree of risk may also be affected by other elements such as corporate culture, local legislation and regulations (or the absence thereof) and political instability in the areas where your organisation operates.

**Sector risk**
As the literature and case histories show, some sectors are more prone to corruption because of their nature and related activities: examples are property, infrastructure, government and semi-government, pharmaceuticals, defence, commodity trading and energy.

**Product or transaction risk**
Certain products and services also entail a higher risk of involvement in corrupt practices for the financial sector. Four examples are:
• **Private banking**
  The generally large sums of money connected with these services tend to increase the risk of corruption, and as bankers often have a personal relationship with their clients they may not be fully objective.

• **Project financing**
  Major projects often involve such large sums of money that payments of bribes and the like may be less noticeable.

• **Specific types of transaction**
  Certain types of transaction, for example those relating to permits, authorisations, licences and public procurement, entail a higher risk.

• **Involvement of public officials**
  The involvement of public officials in transactions may point to a higher risk.

**Third-party risk**
Organisations in the financial sector must be aware of the possibility of becoming involved in corruption either through the actions of their own employees or through third parties. Undertakings may be held liable for corrupt acts committed by third parties. Third party is a very broad term and refers to all parties other than clients. It may include, for example, suppliers of physical goods such as office supplies, consultants and lawyers hired by the undertaking and proxies, agents and intermediaries used by it. Undertakings that operate internationally are especially likely to use the services of third parties to set up and expand their activities locally. For example, an undertaking may use agents and intermediaries to obtain and retain business and permits on its behalf. Other instances of actions that automatically result in the involvement of a third party are full outsourcing of activities and acquiring or merging with another business. In such cases, the undertaking must decide well before the transaction date what constitutes ethical business practices, including the measures taken by the third party concerned to prevent corruption. An example of third-party risk in connection with corruption occurs where lavish entertainment is provided for business contacts, particularly with a view to winning a large contract. There is also a risk of being caught up in bribery through third parties where activities are outsourced or use is made of the services of intermediaries and agents.

In assessing third-party risk, undertakings must also specifically allow for the possibility of conflicts of interest. Such conflicts may occur, for instance, where services are purchased from businesses directly or indirectly owned by, or related to, personal contacts or relatives of senior managers or employees concerned.

Various prominent cases in recent years have shown that conflicts of interest involving third parties are quite common in the financial sector. They may concern a direct or indirect interest or advisory or other function in a third party with which
business is transacted or with which a client relationship exists or the awarding of contracts or activities to parties with whom there is a personal relationship.

Risk of personal networks and interests
A higher risk of corruption exists where the interests of directors and employees may conflict with those of your undertaking. Financial undertakings have a duty to prevent conflicts (or apparent conflicts) of interest involving their employees. A systematic risk assessment should therefore include possible conflicts of interest through employees.

**Good practices**

- The undertaking assesses the geographical risk, transaction risk, sector risk, third-party risk and risk of personal networks and interests as part of its systematic risk assessment.
- Those responsible for compliance, risk management and the business collaborate on the implementation of the risk assessment.
- Senior management is involved in the risk assessment.
- The systematic risk assessment defines the risk appetite, in other words what the undertaking regards as an unacceptably high risk of corruption.
- The systematic risk assessment is not confined to a specific function, but identifies links between different functions and business units.
- The systematic risk assessment is carried out at regular intervals or in the intervening period where necessary. An example would be a standard annual cycle or a greater frequency where necessary.
- If a financial undertaking’s activities, environment or organisation change or it has new participating interests, this may be a reason for it to perform a risk assessment.
- The results of the systematic assessment of the risk of corruption are recorded in such a way that they can be reproduced.
- The record of the systematic risk assessment should include a note of those involved and the considerations and findings.
Once your organisation has properly identified what risks must actually be controlled, you can take appropriate measures by formulating and implementing policy and involving the right people at the right time.

This part of the brochure describes what measures you can take in the fields of organisation and culture, governance and third-party risk as well as three other policy fields. The good practices included in the various sections provide examples of measures already taken by other organisations in the financial sector.

2.1 Measures in the field of organisation and culture

In the field of organisation and corporate culture, DNB expects undertakings to control risks by taking measures to set the ‘tone at the top’, using HR tools, providing training when necessary, creating awareness, and ensuring that procedures are in place for quick and easy reporting of incidents. These measures contribute to a transparent and ethical corporate culture.

Senior management commitment and ‘tone at the top’
Initial responsibility for adopting the appropriate corporate culture rests with senior management, which must set the tone by creating the right framework and explicitly disseminating this decision. To ensure that the fight against corruption is solidly embedded within the organisation it is important to

- Senior management sets the tone by means of publications, newsletters and awareness emails sent to all managers and all staff within the organisation. At one of the larger banks, for example, the CEO regularly mentions quite explicitly in his weblog that any involvement in corruption is unacceptable.
- And the CEO of another financial undertaking explicitly reminds employees, in the case of major events such as the Olympics, of the prevailing rules on gifts, entertainment and hospitality.
- Elsewhere, undertakings communicate transparently about policy-related and operational developments connected with risk control in relation to corruption risk and the involvement of senior management in it, making clear that anti-corruption measures should not be dismissed simply as a ‘compliance thing’. The subject affects the business in its entirety and in full.
- At one of the larger banks the senior management themselves play an active role in the anti-corruption training sessions and related discussions.
have a clear and transparent allocation of the duties and responsibilities of senior management in preventing corruption. Senior management is naturally involved in establishing an anti-corruption programme and in all important decisions on this policy, and explicitly and visibly bears overall responsibility for the programme.

The correct ‘tone at the top’ is crucial for this purpose. By communicating clearly about the importance of compliance and integrity, particularly in relation to corruption, senior management visibly assumes this responsibility and thus helps to establish an anti-corruption culture. As it is important to encourage staff to act ethically and report unethical behaviour, expectations in this regard are clearly communicated.

Assessment of existing and new employees

Employees of financial undertakings, including management and senior management, are the weakest link in cases in which corruption occurs. The decision to engage in corrupt business practices is often motivated by greed. Every financial undertaking is therefore expected to scrutinise the character of its employees as a standard practice. This screening starts at the outset of the employment relationship when the undertaking assesses the knowledge, experience and integrity of job applicants. It should be clear what screening of new recruits (including managers) entails, what matters receive attention and what its purpose is.

The recruitment and selection of management and other staff could flag up personality traits that may make individuals susceptible to corruption, particularly in the case of jobs that involve a higher risk of corruption. Examples of such personality traits are narcissism, self-confidence, independence and emotional instability in combination with the social circumstances of the employee concerned. Knowledge of how involvement in corruption can be prevented is another part of the employee assessment. What knowledge is already available about the risk of corruption and what issues should receive immediate attention in the training and education of the employee in order to prevent involvement in corruption? In addition, the financial undertaking is expected to vet employees whose jobs may influence the ethical conduct of its business to see whether they have a criminal or financial record. Such a screening may also be risk-based. Conditions for re-screening should be clearly documented.

Article 13 of the Bpr provides that a financial undertaking wishing to appoint a person to an ‘integrity-sensitive position’ (i.e. a key position of special trust) should in any event make a reasoned assessment of the person’s trustworthiness.

This applies to all people who will perform an ‘integrity-sensitive position’, whether they are employed under a contract of employment or on some other basis.
**Good practices**

- A large insurer has set up a second panel to vet job applicants, besides the one that determines whether candidates meet the job requirements; the second panel assesses their suitability in terms of whether they meet the requirements of the code of conduct.
- Screening of new employees by reference to the programme or lists used in preventing money laundering and terrorist financing provides an additional insight into possible integrity risks affecting them.
- In-employment screening too is used when staff are promoted or transferred to a different (high-risk) job.
- A bank has identified integrity-sensitive jobs that trigger extra screening at the appointment of an employee or new employee.

**Training and other forms of communication**

Staff training is commonly used to create awareness of the importance of establishing an ethical and transparent corporate culture in which there is no room for corruption. Financial undertakings may establish a training course to make employees aware of the organisation’s integrity policy and clearly demonstrate that corruption is not tolerated. During the course, the undertaking’s position on bribery and conflicts of interest is explicitly communicated. This can be done by giving examples of what is meant by corruption, how this can be recognised and what action should be taken by employees. The curriculum is regularly revised and updated. The course encourages transparency and enables employees to recognise unethical conduct and respond adequately.

The subject of corruption is not only dealt with in special courses but is also a recurrent item in all integrity training courses. The courses are organised in such a way that in each case all relevant employees are trained in this field and that participation is monitored and registered by the ‘second line of defence’. The level and scope of the courses depend on the extent to which a position is corruption-sensitive. Failure to take part in compulsory courses should have consequences for the employee concerned. Nor should the need for follow-up be overlooked. An assessment should be made at the end of the course to determine whether the employee has understood the content, thereby increasing the chance that what has been learned will be put into daily practice.
**Good practices**

- Legal and Compliance work together with other departments such as HR, Security Affairs and, explicitly, the business to determine the content and form of the courses (e.g. e-learning or class teaching) and the target groups.
- Not long should elapse between the date on which a new employee joins the undertaking and the date of his or her attendance on the course, and the course should be repeated periodically.
- Integrity training is mandatory for every (selected) employee, and the training requirements should be clearly communicated.
- Management, including senior management, should take part (and be seen to take part!) in courses.
- An e-learning system is used at one of the larger banks to keep track of who has participated in the various modules and how long they have spent taking them. The data are recorded centrally.
- The effectiveness of the training courses is measured, for instance by reference to surveys or feedback requests.
- A large bank uses oversight flying squads to visit all its branches worldwide to give training courses and challenge policies.

**Awareness**

The establishment of an ethical and transparent corporate culture within an organisation starts with the definition of rules of conduct. This is broader than simply arranging for a coherent description of the policy and procedures required to control the risk of corruption. It is a general behavioural norm, often laid down in a code of conduct, which makes clear that corruption is unacceptable. The code of conduct should contain a clear definition of corruption (covering both bribery and conflicts of interest) that is comprehensible to every employee and clearly spells out the expectations and how these can be fulfilled. This establishes a basis for creating awareness within the organisation of the need to treat corruption as unacceptable.

To make the subject of anti-corruption policy accessible, the undertaking should clearly indicate whom employees should contact if they have questions about this subject and how they should do this. The communication should therefore focus not only on ‘getting the message across’, but also and above all on being open to signals and ideas from within the organisation, in order to be able to strengthen controls. It should be noted that although communication is aimed at the entire organisation, it also focuses on separate target groups that are more susceptible to corruption.
**Good practices**

- Each year a financial undertaking gives consideration to its code of conduct in one way or another. Besides continuous attention through the intranet, it uses communication techniques such as ‘fish bowl meetings’ and dilemma debates to emphasise that corruption is unacceptable.
- One bank arranges for the code of conduct to be signed by all employees, including senior management.
- Following DNB’s communication of its decision to make corruption a supervisory theme, one of the larger banks has also adopted this as a theme for its Compliance and Internal Audit Departments.
- The sanction for corrupt behaviour or failure to comply with measures taken by the financial undertaking to prevent corrupt behaviour is clearly indicated. One of the smaller banks, for example, has introduced a rule that an employee who twice misses the annual deadline for reporting their private interests will be let go.
- One of the smaller insurers has adopted a practice of putting subjects such as ‘challenging each other’ as principal themes on the annual strategy agenda, thereby emphasising the importance of transparency and open communication within the organisation.

**Ways of reporting incidents**

To promote transparent and ethical business practices and a culture of integrity, it is essential for financial undertakings to have in place a scheme for reporting incidents or suspected incidents. This may take the form of either a whistleblower scheme or an incident reporting scheme. Under Article 12 of the Bpr, a financial undertaking is actually required to have procedures and measures in place for dealing with and recording incidents. A clearly described and consistent process for dealing with incidents enables the financial undertaking to respond quickly and adequately. Such a scheme must clearly indicate who is responsible for reporting an incident, within what period the report must be made and that the findings (including follow-up) are clearly recorded.

Where necessary, sanctions must be taken against those concerned. If appropriate, measures based on the findings should be taken to prevent repetition, for example inclusion of the
findings in the systematic risk assessment or modification of the training programme.

If there is an act or event that seriously compromises the ethical conduct of its business, the undertaking must immediately report this to DNB. For this purpose too, a uniform and clear procedure is applied.

Alongside the mandatory reporting procedure, a whistleblower scheme makes it possible for allegations of corruption to be made confidentially within the organisation. This can include specific cases that are not covered by the definition of incident, but are of importance in tackling certain undesirable practices and behaviour. Such a scheme explicitly safeguards the confidentiality of the person reporting the incident and their legal position. The information from incident reports and whistleblower schemes can serve as input for procedures to expose certain developments in the culture of the organisation and/or integrity risks. This information can be used to make senior management and supervisory bodies (such as the supervisory board and internal auditors) aware of any trends and developments. The findings are in any event periodically included in management reports.

**Good practices**

- Integrity incidents, including corruption, are clearly described. This also includes ‘near misses’.
- Various financial undertakings make it possible to report incidents to different independent counsellors.
- The reporting procedure is clear and is regularly communicated through various media such as the code of conduct, news portals and posters.
- The reports are explicitly subdivided into themes, including corruption.
- An undertaking has a protocol for investigations into incidents and provides for a clear record to be kept of duties, powers and resources. This creates clarity for those involved in an investigation, and recording this in advance guarantees the independence of the researchers.
2.2 Measures in the field of governance

You can also arm your organisation against corruption risks in your governance structure, for example by scrutinising the duties, responsibilities and management information.

Duties and responsibilities

As noted in the section on organisation and culture, senior management involvement and the right ‘tone at the top’ are essential in creating a corporate culture in which corruption has – and can have – no place. Financial undertakings can therefore be expected to have clearly allocated the duties and responsibilities for drafting, amending and implementing policies on the prevention of corruption. Senior management has overall responsibility for preventing corruption and ensuring that the reporting lines have been clearly defined. Responsibility for drafting and maintenance of the anti-corruption policy is clearly allocated within the organisation, usually to Compliance, Risk Management, Legal or Security Affairs. An explicit question to be considered when drafting, amending and implementing the policy is whether the business is sufficiently involved. By involving the business in drafting the policy and organising the procedures at an early stage and not waiting until the moment when the policy is adopted, it is possible to take better account of the practical situation in which the activities are undertaken. In the context of the correct operation of the policy cycle, the organisational unit responsible for drafting the policy is also

---

**Good practices**

- Various business owners have been involved in providing feedback by reference to four questions:
  1. does the policy explain clearly and simply what is expected and why?
  2. does the policy take account of the situation in practice?
  3. is the policy aligned as closely as possible with existing business processes?
  4. should additional procedures be formulated for specific business units?
- The anti-corruption policy is explicitly approved and adopted by senior management.
- The entire organisation knows who is responsible for implementing the policy, including mandatory timelines. Often this responsibility is assigned to the business.
- Who is to implement the policy and what is expected for this purpose is clearly indicated. For instance in the case of third-party due diligence; in this process, there is a role not only for the business but also for procurement and/or HR, etc.
responsible for reviewing and updating it. Responsibility for monitoring the anti-corruption policy has been unequivocally allocated to the (senior) management.

**Role of Compliance and Internal Audit**
The Compliance and Internal Audit units have a key role in combating corruption. In the case of almost all undertakings in the examination, Compliance is either involved in, or possibly even responsible for, formulating policy and implementing and monitoring the anti-corruption programme. This guarantees the quality of the policy cycle and ensures effective organisation-wide support with implementation. Experience with, and knowledge of, preventing and combating corruption is so recorded and used centrally. In addition to Compliance, Internal Audit – as the ‘third line of defence’ in combating corruption – can play an explicit role as part

---

**Good practices**

- The subject of anti-corruption is explicitly included in periodic compliance reports (at least twice a year), which list:
  - identified weaknesses in respect of corruption;
  - (anonymised) corruption incidents;
  - developments and future developments concerning corruption.
- Compliance reports are also supplied periodically to the Supervisory Board/Audit Committee.
- At one of the larger banks, Internal Audit performs an impact analysis to assess the consequences of the UK Bribery Act and the US Foreign Corrupt Practices Act (FCPA), in particular the legal risk.
- The findings of audits performed by Internal Audit are reported in general terms to business owners, senior management and the Supervisory Committee/Audit Committee.
- Internal Audit has formulated explicit measures to rectify any identified weaknesses and monitor follow-up.
- The effectiveness of the anti-corruption policy is assessed not only by means of the review by Compliance and Internal Audit but also in other ways, for example by external parties on a recurrent or one-off basis.
- As regards the decisive points in the risk control process, the undertaking checks whether the internal supervisory bodies are kept sufficiently informed of anti-corruption measures.
- The external supervisors are sufficiently informed of the anti-corruption measures.
of its control function in prevention (policy and procedures, training, due diligence), detection (whistleblower scheme) and reaction (investigations). The findings of investigations carried out by Internal Audit are clearly reported to relevant business units and bodies.

2.3 Measures in the field of third-party risk

Third-party risk comes in two forms. First, it is part of the systematic risk assessment described in the first part of this brochure: to what extent, in what countries and for what activities does the undertaking use the services of third parties? Second, before entering into an individual relationship with a third party for a specific activity, an undertaking must assess the associated corruption risk. It does so by carrying out a risk-based due diligence review. Risk-based means that where there is greater risk of corruption additional measures should be taken to assess the integrity of the third party. Due diligence includes investigating the background, activities and reputation of the third party. Other factors to be taken into account are the geographical risk, sector risk and product/transaction risk. It is important to draw up clear rules covering at least five situations:

---

**Good practices**

- The third-party policy provides for an escalation procedure in cases where there is disagreement about the risk classification of a third party.
- Where there is a high risk classification, the financial undertaking takes extra measures by including a right-to-audit clause in the contract with the third party and obtaining a declaration from the third party that it complies with the financial undertaking’s code of conduct.
- Third-party data and payments are clearly recorded and updated centrally.
- All payments to third parties are authorised in accordance with the four-eyes principle.
- Checks are made to ensure that payments to a third party are at the going rate.
- Approval is given at a more senior level if this is warranted by the extent of third-party risk and the size of the payment.
- Payments to third parties are also monitored by means of random sampling ex-post facto.
- Employees who make payments to third parties are trained to watch for red flags.
- tendering process
- selection criteria
- payments to the third party
- enforcement of the supervision rules and norms applying to the financial undertaking (in the event of outsourcing)
- prevention of bribery and conflicts of interest arising, for example, as a result of gifts and personal relationships with the third party concerned.

As already noted, the due diligence should be risk-based and take account of complicating factors such as:
- a large number of third parties;
- the fact that the third party is established in a country where public information is unavailable or unreliable;
- information is available only in a foreign language.

2.4 Three high-risk policy fields

Besides third parties, three other policy fields also give rise to a higher-than-average risk of corruption and therefore warrant explicit attention in terms of the measures that can be taken.

Gifts, hospitality & entertainment

A high risk of corruption occurs in connection with gifts, hospitality & entertainment’ (GH&E). In accepting or offering GH&E, employees and the undertaking are in a vulner-
Good practices

- Explicit limits are set on the amounts that can be regarded as acceptable (often the limit is EUR 75).
- Where an undertaking operates internationally, it conducts a debate specifically about cultural aspects of GH&E and the desirability and necessity of explicitly deciding not to engage in certain cultural practices that can be regarded as a form of corruption. The outcome of this debate is clearly represented in policy and procedure, with attention being given to cultural differences and any differences in legislation and regulations.
- Attention is paid to red flags and dilemmas in the procedures and measures connected with GH&E.
- Exceptions to the GH&E policy can be made only in special situations and with the prior approval of Compliance and/or senior management (Managing Board).
- There is a uniform procedure for information to be supplied (such as the name of the offeror and recipient, offer date, acceptance date, type of GH&E, price, business purpose, circumstances and so forth).
- A central record is kept of GH&E that have been accepted, given or rejected in order to identify and assess the extent of the risk.
- An undertaking has created a decision framework for the acceptance of invitations, so that employees are aided in making the right decision and avoiding the appearance of corruption.
- A periodic assessment is performed by the ‘second line of defence’ in order to identify trends and patterns. Examples are an increase in reports in a certain period, excessive acceptance/offering of gifts by one employee or within any given organisational unit and so forth.

Donations, charity and sponsoring

Donations, charity and sponsoring are also prone to corruption. To build an element of objectivity into the process, it is important for financial undertakings to formulate policy designed to ensure that decisions on donations, charity and sponsoring and the nature and size of the amount are assessable and explicit. The basic question for an undertaking is to decide on the extent of its commitment. Risk-based due
diligence will furnish information about the integrity of the recipient third party. Besides reputation, integrity and any involvement of public officials, due diligence will cover persons or entities associated with the party to which the payment will be made. Due diligence of this kind will protect the financial undertaking’s own integrity.

**Good practices**

- The policy on donations, charity and sponsoring sets out clear, objective criteria, such as limits on amounts, parties that may or may not receive a donation or sponsoring, and the terms on which donations or sponsoring may be given.
- Donations and sponsoring are always recorded in sufficient detail.
- The financial undertaking is internally and externally transparent about donations and sponsoring.
- Responsibility for authorising payments of sponsorship moneys or donations is explicitly allocated to senior management, subject to application of the four-eyes principle.
- Donations and sponsoring form part of the third-party policy and the related due diligence.

**Personal networks and interests**

The risk of corruption is greater when the interests of policymakers and employees conflict with those of the undertaking. Once this risk has been identified and assessed, appropriate measures can be taken, including a description of how personal, professional and financial interests are to be dealt with. This can examine, for example, the position on:
- personal, professional and financial interests in relation to dealing with clients and other contacts;
- information, particularly confidential information;
- entering into client relationships;
- transactions in a private capacity;
- second jobs of the employee (i.e. besides the job with the undertaking).

Examples of private interests are both commercial and family interests.

By requiring its employees to adopt a proactive approach to reporting any secondary positions or high-risk positions and private interests, a financial undertaking is able to identify possible conflicts of interest. The appearance of a conflict of interest must be avoided. It is important for the records of secondary positions or high-risk positions and private interests to be kept up to date and monitored and for the registration procedure to be clear and accessible.
Good practices

- The undertaking has a policy containing explicit examples of how employees can recognise conflicts of interest.
- Employees may accept secondary positions only with the prior approval of the financial undertaking.
- The register of reported secondary positions and private interests is consulted when the undertaking enters into contracts with third parties.
- The undertaking periodically sends a request to the policymakers and employees to check whether the information they have provided about secondary positions and private interests is up to date.
- The statement of private interests and secondary positions is monitored by means of random sampling.
In 2013, DNB carried out a cross-sectoral thematic examination of the efforts of banks and insurers to prevent and combat involvement in corruption. In carrying out this thematic examination, DNB first set about identifying the nature, scope and causes of the corruption risk in Dutch financial undertakings. For this purpose, DNB consulted its partners in the prevention and combating of financial and economic crime (such as the Fiscal Intelligence and Investigative Service (FIOD) and the Public Prosecution Service) and above all the financial undertakings themselves. By means of questionnaires, interviews and roundtable sessions with representatives of the banking and insurance sector, DNB obtained information about key risk indicators and controls. This resulted in an extensive internal assessment framework on the basis of which the efforts of financial undertakings to prevent corruption can be assessed by DNB. In the second phase of the thematic examination, DNB used this assessment framework to perform examinations at a selection of 13 banks and insurers.

The assessment framework was organised along the following lines:

<table>
<thead>
<tr>
<th>Organisation and culture</th>
<th>‘Tone at the top’</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Human resources</td>
</tr>
<tr>
<td></td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td>Awareness</td>
</tr>
<tr>
<td></td>
<td>Incident reporting</td>
</tr>
<tr>
<td></td>
<td>‘Gifts, hospitality &amp; entertainment’</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>‘Governance’</th>
<th>Duties, responsibilities and management information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Systematic risk assessment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>‘Third parties’</th>
<th>‘Third party’ policy (general)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Political donations, charity and sponsoring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network (conflicts of interest)</th>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secondary positions</td>
</tr>
<tr>
<td></td>
<td>Private interests</td>
</tr>
</tbody>
</table>
The examinations are based on the principle that ethical business practices require undertakings to prevent situations in which either the undertaking or its employees become involved in conflicts of interest and/or breaches of the law and/or acts that are contrary to socially accepted standards, as a result of which trust in the undertaking or in the financial markets may be damaged (Section 3:10 Wft). In addition, the financial undertaking is required to pursue an adequate policy that safeguards sound business practices geared to the nature, scope, risks and complexity of the activities of the undertaking (Section 3:17 Wft). As part of the sound and ethical operations, undertakings must identify and systematically assess the risk of corruption and take measures to control it.

The examinations deal with the anti-corruption procedures and measures incorporated into the business processes of the undertakings. They focus on organisational and personal integrity risks and, as regards relational integrity risks, on relations with third parties. Third parties are taken to mean all contacts of the financial undertaking, with the exception of clients. The relational integrity risk in respect of clients therefore falls outside the scope of these good practices (on this subject see the DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act issued in October 2013, which are intended to support the efforts of banks and insurers to combat money laundering).