White Paper

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act

Preventing the misuse of the financial system for money laundering and terrorist financing purposes and controlling integrity risks

A summary and highlights of the updated DNB guidance

by Mark Dunn, Market Planning Manager, Risk & Compliance

Released January 2014

LexisNexis®

Index

In October 2013, the Dutch Central Bank (De Nederlandsche Bank/DNB) published updated Guidance for the Anti-Money Laundering and Counter-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme/Wwft) and the Sanctions Act 1977 (Sanctiewet 1977/SW)

"New good practices have been added on some points, which have emerged from DNB's supervisory investigations."

Page 4. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

The new Guidance reflects amendments made to the Wwft which came into effect from 1st January 2013 and focuses primarily on customer due diligence and the reporting of suspicious transactions. DNB also includes best practice gathered from its recent supervisory work.

The DNB Guidance was amended to include changes made to the Wwft after the Financial Action Task Force (FATF) evaluation of the Netherlands AML (Anti-Money Laundering) regime in 2010. The intent to publish new best practice Guidance was also signalled by DNB in its *Supervisory Themes 2013*, following a series of investigations which revealed that:

"Awareness and analysis regarding integrity risks are often unsatisfactory. As a result, institutions are unable to control their integrity risks, more especially their money laundering risks, in an adequate manner."

The outcome has been an upturn in supervisory activity that reviewed banks' and other financial institutions' approaches to anti-money laundering, sanctions screening and anti-bribery & corruption.

DNB stresses that the new Guidance complements the *General Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act (Wwft) and the Sanctions Act (SW)* as published by the Dutch Ministry of Finance in February 2013 and that both guidance documents should be read in conjunction with each other.

This latest LexisNexis White Paper focuses on selected extracts from the DNB Guidance that highlight recommendations, good practices and red flags.

The full DNB Guidance document should also be consulted and can be accessed via the following link:
http://www.toezicht.dnb.nl/binaries/Leidraad%20WWFT%20SW%20October%202013%20English%20version_tcm50-223813.pdf

"In addition to solidity, integrity is a prerequisite for a sound financial system."

Page 4. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

Key regulations summary

Anti-Money Laundering and Counter-Terrorist Financing Act

(*Wet ter voorkoming van witwassen en financieren van terrorisme* /Wwft)

The Act implements the EU Third Money Laundering Directive into Dutch law.

Sanctions Act 1977

(*Sanctiewet 1977*/SW)

The Act and the regulations derived from it implement international sanctions regimes, such as the United Nations and the European Union, into Dutch law.

Financial Supervision Act

(*Wet op het financieel toezicht* /Wft)

The Act covers DNB supervisory activity, including integrity supervision of a wide range of financial and other institutions to prevent the use of the financial system for money laundering and terrorist financing purposes.

Supervision of Trust Offices Act

(*Wet toezicht trustkantoren* / Wtt)

The Act focuses on supervision of trust offices and their obligations under Wtt in relation to integrity risks and customer due diligence etc.

"The integrity of financial institutions is one of the pillars of trust and is thus a prerequisite for an institution's proper functioning."

Page 6. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act (DNB October 2013)

Regulatory framework for integrity

DNB opens the Guidance by focusing on the importance of an effective regulatory framework to ensure integrity within the sectors it supervises. The Guidance stresses requirements under the DNB Suitability Policy Rule 2012 for firms to have in place senior management that implement and maintain an integrity policy to mitigate business risks such as money laundering and terrorist financing. DNB also emphasises that it is vital firms adopt a sound ethical business culture and demonstrate ethical business conduct.

LexisNexis view

As AML, ABC and sanctions systems & controls converge, there is a tendency to overlook the importance of ensuring associated technology continues to align to business requirements and deliver a return on investment.

With the growing convergence of AML, ABC and sanctions regime compliance, firms should take a more holistic approach to tackling the risk of financial crime and make sure there is commitment from the top. Current examples of good practice illustrate where firms have proactively aligned their business structures to best meet the increasing challenges of evolving legislation and industry guidance whose purpose is to reduce financial crime. As senior management recognises the risks of non-compliance and the associated impacts on business reputation and the balance sheet, firms are increasingly centralising their approach and the resources deployed to mitigate such risks. Once in place, firms continue to regularly monitor their risk exposure to ensure systems & controls remain effective and are aligned to changing business requirements, incoming legislation and regulators' expectations.

In this rapidly changing environment, it is critical firms ensure that the technology used to tackle such evolving risks continues to meet expectations. Through consultation and review, LexisNexis has helped firms successfully implement AML, ABC and sanctions systems & controls to ensure firms' clients and third-party agents are efficiently screened and monitored.

DNB recommendations, good practices and red flags

Selected extracts from the DNB Guidance that highlight recommendations, good practices and red flags:

As a minimum, the control framework for integrity risks comprises the following:

- Systematic assessment of integrity risks.
- Formulation of a strategy.
- Adoption of an adequate policy aimed at risk control and integrity of action.
- Translation and implementation of the policy principles into procedures and measures.
- Systematic testing and assessment of the adequacy of the control environment.

Page 6. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

"The principal goal remains that the institution should know who it is doing business with and for what purpose the business relationship is used."

Page 7. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act (DNB October 2013)

Know your customer: customer due diligence (CDD)

DNB stresses the importance of undertaking customer due diligence to help maintain the integrity of business operations and to comply with obligations and goals under Wft, Wtt and Wwft. Knowing who firms are doing business with and for whom transactions are being executed is critical to mitigate the risks of money laundering, terrorist financing and other financial crime.

LexisNexis view

Having in place effective anti-money laundering systems & controls is long considered a prerequisite for banks and other financial services firms operating within the Netherlands and associated regulated markets.

With an EU Fourth Money Laundering Directive on the horizon and ongoing enforcement in this area, it is critical that firms have in place effective AML procedures that are both proportionate to their business risk profile and regularly reviewed to reflect changing compliance standards. DNB has made it very clear that supervision of banks' integrity controls will continue to be a key focus:

"DNB devotes more attention to the integrity risks at institutions that arise from involvement in money-laundering and financing of terrorism, and violation of international sanctions."

Against this backdrop of ongoing supervisory scrutiny and global enforcement activity, it is essential firms do not neglect the technology services they have in place to help mitigate such risks. Screening, due diligence and monitoring services should not only reflect firms' changing risks but should also deliver business process efficiencies as budgetary constraints on compliance resources continue to bite.

LexisNexis regularly helps firms review their AML, ABC and sanctions systems & controls to ensure clients and third-party due diligence checks are delivered in a timely and cost-efficient manner.

DNB recommendations, good practices and red flags

Selected extracts from the DNB Guidance that highlight recommendations, good practices and red flags:

An institution's CDD policy incorporates procedures, processes and measures in relation to:

- The identification and verification of the identity of customers;
- The acceptance and risk assessment of customers;
- The monitoring of customers, accounts and transactions.

Page 7. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

Identification and verification of the customer:

Customer identification: the process whereby the customer's data and information are collected with the objective to 'know your customer'. The data allow an adequate and robust risk assessment to be made of the customer.

Verification: the process whereby the accuracy of customer-submitted and other data is checked using a reliable and independent source, e.g. in the form of original and valid identity documents and possibly supported by further investigation.

Customer acceptance: the process whereby, based on the identification, verification of identity and knowledge of the nature and background of a customer, a decision is taken about whether or not to enter into a relationship with the customer.

Page 14. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

A customer due diligence procedure is carried for all customers, including existing customers, if:

- there are indications that the customer is involved in money laundering or terrorist financing;
- the institution doubts the reliability of information obtained previously from the customer;
- the risk of an existing customer's involvement in money laundering or terrorist financing gives cause to do so.
- there is a heightened risk of money laundering or terrorist financing due to the country where the customer lives;
- a one-off electronic money transfer is effected

Page 16. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

When is the customer due diligence reviewed?

For low-risk customers, a review may take place when:

- the customer requests a new service or product, or in the case of customer contact which presents an opportunity to carry out the customer due diligence procedure;
- the characteristics of the customer change (e.g. relocation to a high-risk jurisdiction);
- alerts have been received relating to incidents or transactions.

For high-risk customers, a review of the specific risks will in practice be carried out (once or several times per year) and, for example, in the case of:

- possible signs suggesting a higher risk. Examples are the manner in which accounts are used or specific transactions are effected, as viewed from the consolidated position of the customer in question.

In all cases, the employees involved are aware of the possible risks surrounding this type of high risk customers.

Page 18. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

"Within the framework of the Wwft, the Wft and the Wtt, institutions are expected to classify their customers into risk categories on the basis of the nature and level of the risk they present."

Page 8. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act (DNB October 2013)

Practical design of integrity policy: risk-based approach

DNB reminds firms of the importance of adopting a risk-based approach to AML compliance. Under the framework of the Wwft, the Wft and the Wtt, there is an expectation that firms assess their business risk and apply risk categorisation as appropriate. The risk-assessment process includes typical criteria such as sector, products & services, as well as country and geographic risk. Institutions are reminded that any risk-assessment process should remain static and be subject to regular monitoring.

LexisNexis view

Keeping the compliance team and key staff updated with changing risk indicators and regulator expectations needn't be a costly and cumbersome exercise.

The inability for a regulated firm to maintain its risk-assessment process has been highlighted by a number of recent enforcement actions in the UK and US. Regulators expect companies to be aware of changing risks in their markets and to apply a risk-assessment process that is agile enough to be amended and updated accordingly. A flexible approach to risk assessment is not only important to take account of ad hoc changes in risks related to specific countries and entities, for example, but also to be able to quickly assign risk assessment to the firm's business development strategy, new product adoption, etc. Industry best practice recommends that the risk-assessment process be reviewed at least once a year. However, as pointed out above, many firms need to ensure their risk-assessment process is flexible enough to respond to market forces.

DNB recommendations, good practices and red flags

Selected extracts from the DNB Guidance that highlight recommendations, good practices and red flags:

Possible indicators of country or geographical risk:

- Countries or geographic areas subject to sanctions, embargoes or comparable measures, for example imposed by the United Nations, the European Union or the United States.
- Countries or geographic areas identified by credible sources (e.g. the FATF, the IMF or the World Bank) as lacking an appropriate system for preventing money laundering and/or terrorist financing. The ICRG (International Cooperation Review Group) process of the FATF provides a useful tool: after each of its meetings (held in February, June and October) the FATF publishes lists of countries which in its opinion lack an adequate system for combating money laundering and terrorist financing. These lists are published on the FATF's website (http://www.fatf-gafi.org), and DNB refers to each update of these lists on its website (also see the Q&A: http://www.toezicht.dnb.nl/3/50-223306.jsp).
- Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
- Countries or geographic areas identified by credible sources as having a high level of corruption or other criminal activity.
- Countries or geographic areas characterised by political instability.
- Countries or geographic areas that are known as offshore financial centres.

Page 9. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

Possible indicators of product/service risk:

- Services identified by internationally recognised and credible sources as being higher-risk services, such as international correspondent banking services and (international) private banking activities.
- Services involving trading in and delivery of banknotes and precious metals.
- Services that inherently foster anonymity or can readily cross international borders, such as online banking and other services, stored value cards, private investment companies and trusts.
- New or innovative products or services that are not provided directly by the institution but via the institution.
- Consultancy companies where it is difficult to verify that the transaction is matched by a specific consideration in the form of a service or product.
- Business or commercial real estate activities.

Page 10. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

Possible indicators of customer risk:

- Customers who conduct their business relationships or transactions (or have them conducted) under unusual circumstances, such as an unexplained geographic distance between the institution and the location of the customer, frequent and unexplained transfers of accounts to different institutions and frequent and unexplained movements of funds between accounts in various geographic locations.
- Customers where the structure or characteristics of the entity or relationship make it difficult to identify the true owner or controlling interests.
- Cash-intensive businesses, such as bureaux de change, money transfer offices, gambling halls, etc.
- Charities and other not-for-profit organisations (especially those operating on a cross-border basis) which are not subject to any form of monitoring or supervision.
- 'Gatekeepers' such as accountants, lawyers or other professionals holding accounts or acting on behalf of their customers, and where the institution relies on the gatekeeper for the supply of information.
- Use of intermediaries who are not (or not sufficiently) subject to anti-money laundering and counter-terrorist financing measures or who are not supervised.
- Customers who are designated as Politically Exposed Persons (PEPs).
- Customers who receive negative news coverage for any reason, since this negative publicity can have an impact on the institution.
- Foreign feeders: customers who are introduced to trust offices by foreign service providers, especially from countries with a (presumed) duty of secrecy.
- Several ultimate beneficial owners (UBO) of target companies between whom there is no economic relationship.
- Provision of services to companies with active branches abroad.
- UBO-UBO structures' in combination with advisory services or trading activities, possibly via a conduit company. A UBO-UBO structure is one where the UBO of the company providing the (consultancy) service or product is the same natural person as the UBO of the company that makes the payment (company receiving the service/product).

Page 10. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

"The decision to enter into a business relationship with a PEP or to conduct a transaction for a PEP should be taken or approved by persons authorised by the institution to do so."

Page 24. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act (DNB October 2013)

Politically exposed persons (PEPs) and sanctions regulations

DNB emphasises the unique risks associated with PEPs and the approach firms should take when assessing such business risks. The Guidance reminds firms that PEPs constitute a specific factor under the Wwft and that, in jurisdictions where corruption is widespread, the financial sector also faces potential reputational and other risks from bribery. Separately, the Guidance calls out firms' obligations under the Sanctions Act 1977 and the need to check EU and other lists.

LexisNexis view

Given ongoing global enforcement and severe penalties for poor sanctions controls, it is critical firms continue to review processes and remain aligned to regulators' expectations.

Few financial institutions need to be reminded of the importance of implementing and maintaining a robust sanctions screening process. And few areas in the world of financial crime have come under more scrutiny in recent years than compliance with national and international sanctions regimes. The Guidance highlights details on DNB's supervision of compliance with the Sanctions Act (SW) and its reporting procedure. The Guidance also refers to the extensive information on sanctions provided by the Ministry of Finance in an associated General Guidance document.

As for international measures to implement and maintain effective sanctions regimes, the recent FATF guidance updates current thinking in this area and summarises international best practices. Targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6) (FATF, June 2013) http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP-Fin-Sanctions-TF-R6.pdf

DNB recommendations, good practices and red flags

Selected extracts from the DNB Guidance that highlight recommendations, good practices and red flags:

Politically Exposed Persons

How should institutions deal with PEPs?

- During the acceptance process, institutions check whether the customer or the UBO of the customer is a PEP.
- This check is repeated periodically, and in the event of alerts or changes. The PEP is part of the risk assessment or forms a separate risk category. If PEPs are not accepted, this is seen as a risk category: unacceptable risk.
- Senior management decides on the acceptance of PEPs.
- Compliance is involved in the decision-making, signing off or in an advisory role in cases involving PEPs.

Page 25. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

How does an institution filter transactions against sanction lists?

- Information or fields against which checks are carried out as a minimum:
  - ordering party
  - beneficiary
  - place names
  - country
  - description
- The institution filters the SWIFT MT series and fields (including the n99 messages) that it has identified on the basis of a documented risk assessment.
- Trust offices, insurers and institutions with limited payment transactions carry out a check when making payments to third parties/beneficiaries as to whether the legal or natural person concerned appears on the sanction lists.

Page 37. Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act. (DNB October 2013)

Conclusion

The new DNB *Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act* provides useful insight and best practice. Read in conjunction with the *General Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act (Wwft) and the Sanctions Act (SW)*, published by the Dutch Ministry of Finance, firms have comprehensive information to help implement an effective anti-money laundering and sanctions process together with key indicators on tackling anti-bribery & corruption.

Further Reference

DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act (De Nederlandsche Bank)
http://www.toezicht.dnb.nl/binaries/Leidraad%20WWFT%20SW%20October%202013%20English%20version_tcm50-223813.pdf

General Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act (Wwft) and the Sanctions Act (SW) (Dutch Ministry of Finance)

DNB Supervisory Themes 2013
http://www.dnb.nl/en/binaries/DNB%20Supervisory%20Themes%202013_tcm47-284483.pdf

Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (Ministry of Justice)
Official UK guidance to accompany the Bribery Act 2010
http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

A Resource Guide to the U.S. Foreign Corrupt Practices Act (US DoJ and SEC)
Official guidance for the US Foreign Corrupt Practices Act
http://www.justice.gov/criminal/fraud/fcpa/guidance/

Bribery Act 2010 – Guidance on compliance (British Bankers' Association)
BBA's sector guidance to help financial services firms tackle the UK Bribery Act
http://www.bba.org.uk/media/article/bribery-act-2010-guidance-on-compliance

How LexisNexis helps organisations comply with AML CDD obligations

LexisNexis risk solutions can protect your business in a number of ways – we simplify the compliance process, we reduce the related costs and we enable an effective risk based approach based on the right information at the right time. Our fast, intuitive solutions do not require any additional IT investment or training. All searches are time and date stamped providing you with the audit trail you need for the regulator.

Manage enhanced due diligence checks on new and existing parties

Search on a company, individual or country through our online due diligence solution. Lexis Diligence® searches global news and business information, sanctions and PEPs delivering accurate and relevant matches immediately. Results can be saved, printed or put into a report to enable a decision to be made on whether to progress the relationship. Be confident that your decisions are based upon content you can trust, and save valuable time with account opening or third party due diligence checks.

Lexis Diligence is used by the world's top five banks, law firms and blue chip companies to mitigate risk every day. Achieve a competitive advantage by speeding up the client acceptance process whilst maintaining necessary controls.

Conduct ongoing screening of existing customers

Monitor customers and other third-parties through LexisNexis Bridger Insight™ XG.

Stay compliant and safeguard your organisation's reputation by regularly monitoring high risk customers in case their status changes, as per your risk-based approach.

Simply upload all the customers you need to monitor to LexisNexis Bridger Insight. You can screen as many companies and individuals as you need in one transaction. The list will be screened against our global sanctions, watch lists and PEP data and the results file returned for review. Any matches are clearly highlighted so that you can choose which alerts would merit further investigation in Lexis Diligence.

Our superior fuzzy-name matching algorithm ensures better matches saving you valuable time and money investigating irrelevant results.

Monitor high risk customers across the media

Monitor news across all key media on your high risk third parties through your own early warning system.

Fuzzy matching is not used, ensuring you only get the relevant results you need to see.

Automated monitoring enables you to anticipate and mitigate any financial and reputational risks to protect your organisation. Using a unique mix of multi-lingual data mining and sentiment analysis techniques, supplemented by our in-house analysts' expertise, LexisNexis® Analytics automatically monitors internal, online and press coverage through a single interface.

LexisNexis Analytics can also be used to monitor competitor movement, partner's reputations and key customers and suppliers, arming you with invaluable insight.

LexisNexis Amsterdam

T +31 (0)20 485 34 56
E servicedesk@lexisnexis.nl
W www.lexisnexis.nl