

Fraud & Corruption Resistance Profile

The Framework – Public Version



MANAGING RISK

DNV - PROVIDING TRUST AND CONFIDENCE

DNV is an independent and autonomous foundation working to safeguard life, property and the environment. We are a knowledge-based company and our prime assets are the creativity, knowledge and expertise of our people. Helping companies to manage risk is our business. DNV is recognised as one of the leading and most respected management system certification bodies in the world. We hold 80 accreditations in different countries and have issued more than 50,000 management system certificates worldwide.

Fraud & Corruption Resistance Profile
The Framework – Public Version

October 2006

Authors:

Knut Anderssen	(DNV)
Nigel Iyer	(HIBIS)
Veronica Morino	(HIBIS)
Peter Wieland	(DNV)

Introduction

The fact that corruption constitutes a major obstacle to democracy and the rule of law has been known for some time. Empirical research estimates that an average organisation loses about 5% of its total annual revenue to fraud and abuse committed by its own employees. Thus, fraud and corruption are major risks for all organisations.

Recent cases of organisations involved in fraud and corruption show a substantial financial loss, both directly due to the fraud and subsequent investigation expenses and fines as well as indirectly due to reputation damage. No surprise that the fight against fraud and corruption has become a popular and focal topic within Corporate Social Responsibility (CSR) these days and this has been supported by both sides, the corporations and society at large.

Anti-corruption has been integrated as 10th principle into the UN Global Compact. Anti-fraud measures are being strengthened in many organisations following major corporate financial fraud scandals mainly in the US and the subsequent Sarbanes-Oxley Act of 2002.

As more and more organisations put in place systems to assess and manage risks of fraud and corruption, one question remains: how can we measure the effectiveness of these systems to prevent fraud and corruption, and how can we rate how resistant an organisation actually is?

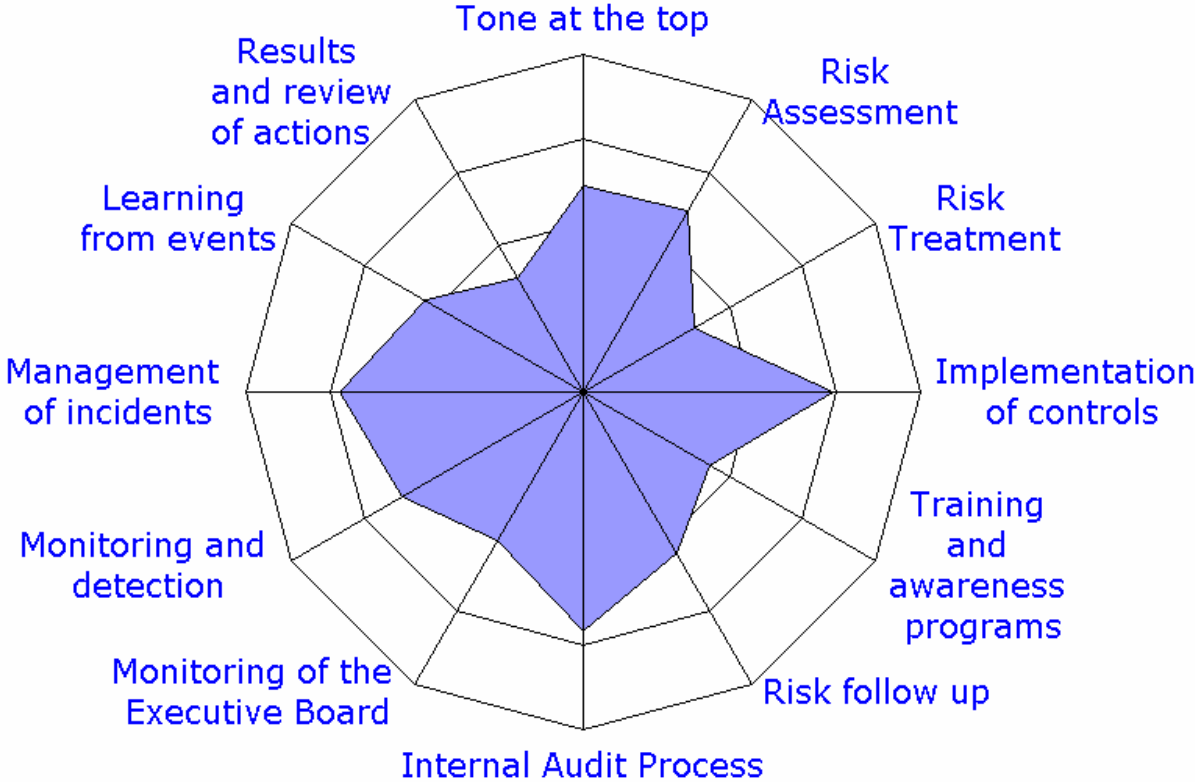
This framework explains how organisations typically integrate and implement guidelines and best practices on how to fight fraud and corruption (e.g. the OECD Business Approaches to Combating Corrupt Practices or Transparency International's Business Principles for Countering Bribery) throughout their business processes. It is the baseline for DNV's rating system to measure the resistance of organisations to fraud and corruption.

The Fraud & Corruption Resistance Profile (FCRP) is an assessment system for measuring the resistance (or resilience) of an organisation, corporation or entity to the effects and impact (on profitability, long-term value, reputation and internal culture) of Fraud and Corruption. We use the following definitions:

Fraud: "An intentional act by one or more individuals amongst management, those charged with governance, employees, or third parties involving the use of deception to obtain an unjust or illegal advantage". (International Standards on Auditing ISA 240)

Corruption: "The abuse of entrusted power for private gain" (UN Global Compact, Transparency International)

The Fraud and Corruption Resistance Profile (or assessment) has been developed by DNV using a 12-element model as shown in the Kiviat chart below:



This framework documents each of the 12 elements. The purpose of this framework is to provide all interested parties with a basic understanding of the elements of DNV's Fraud and Corruption Resistance Profile to enable them to an appropriate preparation for an assessment.

Content

Introduction 3

The Framework of Elements 5

The Concept of Risk..... 8

Sources of requirements 9

Glossary..... 11

The Framework of Elements

1. Tone at the Top

The "Tone at the Top" refers to the crucial role played by the Board and senior management in establishing and communicating policy, taking actions that demonstrate interest and commitment to the stated policies, and the personal example they set. This element evaluates the tone at the top in regards to the prevention of fraud and corruption. Has the message "Fraud and Corruption will not be tolerated" been communicated? Are management actions consistent with the message? Management's demonstration of their commitment to prevention needs to be visible to all employees, credible, embedded in the organisational culture and visible to external parties. The purpose of this element is to evaluate the degree and effectiveness of senior management's commitment to preventing fraud and corruption. The "Tone at the Top" forms the foundation on which the other elements are built.

2. Fraud and Corruption Risk Assessment

A thorough understanding of fraud and corruption risk across the organisation is a pre-requisite for effective prevention. The assessment involves the systematic identification and ranking of those fraud and corruption methods and risks which can and do affect the organisation at all levels. Fraud and corruption risk assessment involves looking at how resistant the controls are to specific methods of fraud and corruption. The purpose of this element is to evaluate the extent to which the organisation's ability to resist fraud and corruption has been assessed.

3. Fraud and Corruption Risk Treatment

Once fraud and corruption opportunities have been assessed, effective and mitigating measures have to be put in place by all levels of management, from the top down. Treatment in the form of a strategic plan, and management responses will lead to a reduced risk of fraud and corruption as well as a significantly increased chance of early detection. The purpose of this element is to measure the degree and effectiveness of mitigating measures.

4. Implementation of controls

The implementation of internal control measures should correspond to the specific fraud and corruption risks which have been identified and documented. In addition certain fundamental controls such as screening of employees, channels for reporting of malpractice and protection of assets need to be working effectively. Unnecessary or redundant controls should be identified and eliminated. The nature and purpose behind corporate governance regulations needs to be recognised by management and properly embedded within the organisation. The purpose of this element is to measure the degree and evaluate the effectiveness of how the anti-fraud and corruption controls have been implemented.

5. Training and awareness programs

Training programs should be practical in nature, cover a wide spectrum of risks and apply to all employees. Training should be assured for third parties, when their activities are closely integrated. The training should be held at regular intervals and structured to encourage feedback and sharing of information and

best practices. The purpose of this element is to measure the degree and evaluate the effectiveness of the organisation's fraud and corruption training and awareness programs.

6. Risk follow-up

A system ensuring the follow-up of fraud and corruption risks should be in place. Risks should be reviewed regularly, and at a management level appropriate to the risk level. Fraud risks should be re-evaluated whenever major changes to underlying products or processes occur. The system also should include a mechanism allowing line managers to report their concerns when changes or other circumstances increase fraud risks dangerously.

When measuring the degree and effectiveness of fraud and corruption risk follow up, the following three sub elements are considered.

7. Internal Audit Process

Large organisations should include an internal audit function that continuously evaluates the effectiveness of the organisation's system of internal controls. (In small organisations this function might be performed by top management.) The internal audit function should report to the Board or to top management, in order to ensure its independence from the areas under review. Internal audit should have clear mandate, be staffed by appropriately experienced and qualified personnel, and spend a proportion of its time evaluating measures taken to reduce the risk of fraud and corruption. Sub elements used in the evaluation of the internal audit function include the following.

8. Monitoring of the Executive Board

The Board of Directors has primary responsibility for setting the fraud and corruption risk management strategy. The Board may assign an Audit Committee to be responsible for actively overseeing the effectiveness of implementation of that strategy. The Audit Committee or the full Board should also arrange and review an annual fraud and corruption risk assessment covering the Board of Directors and senior management. The purpose of this element is to measure and evaluate the degree of monitoring of the executive board and senior management.

9. Monitoring and detection

Proactive fraud and corruption detection is a key element in the risk management strategy, either to prevent illicit activity succeeding in the first place or to catch it in its infancy. Tests and triggers, which assist in the early detection of the symptoms of fraud and corruption, should be embedded into the organisation's communication policies as well as procedures and systems. The purpose of this element is to measure the degree and effectiveness of the monitoring and detection processes.

10. Management of incidents

Management of incidents involves the methodical investigation and examination of incidents of potential fraud and corruption as well as the actions taken to remedy the problems observed. This should also include identifying and treating the root causes of problems and not just the symptoms. The purpose of this element is to measure and evaluate the degree and effectiveness of

managements systems and practices for managing incidents of potential fraud and corruption.

11. Learning from events

All recognised incidents of fraud and corruption provide the organisation and its management with opportunities for improving controls. By evaluating how and why incidents of fraud and corruption occurred the organisation can learn what controls are required to prevent them recurring. The purpose of this element is to assess the extent and effectiveness of the systems for recording and follow-up of incidents, feedback to key support functions as well as the methods of dissemination of information and experiences.

12. Results and Review of Action.

All stakeholders including owners, audit committees, non-executive directors, regulators, financial institutions, governments and non-governmental organisations have different requirements and interest in respect of the prevention, management and reporting of fraud and corruption. The purpose of this element is to measure the quality, extent, effectiveness and consistency of the reporting of fraud and corruption related risks, incidents and follow up actions to the stakeholders.

The Concept of Risk

A fundamental understanding of the risk concept is at the heart of this element and many of the following. Risk in itself is not bad, and failure is a part of learning. Advancement cannot be achieved without taking risks, but we must balance risks against opportunities; control our appetite.

The components of the concepts are: A) Threats (hazards), B) Probabilities (likelihoods), C) Consequences (impacts/ outcomes). Often, the effectiveness of resistance to events (risk control) is a component embedded in B) and C).

For each characteristic threat (A) risks are imagined as measured figures calculated from its components B) and C).

An objective of using the risk concept is to speculate on and predict future events and to plan and organise preventive actions against these.

There is a wealth of reference standards for risk management, and there are numerous useful tools for risk assessment. The best risk management practice for the organisation and processes at hand is to hit a healthy balance between simplicity, capability and effectiveness.

Luck is that not all parts of an organisation and all parts of process networks are equally threatened. But it is most important to highlight specifically those functions and activities that do allow fraud and corruption threats. The memory of the organisation will often enough tell the story of intolerable consequences of well known threats. Competent insight and weighted imagination are other valuable sources of input to risk assessments. Knowledgeable employees could be joined; records and analysis of process data could be processed in forums such as workshops. The mapping of these threats would be the backbone of the risk assessment. They are often called "Risk Registers", even if the probability component is not considered specifically.

A challenge is that the 3 components of the risk concept cannot readily be combined to give a meaningful "risk measure". "Probability" is often given as a frequency and a "Consequence" in money language or in terms of loss. A simple and common solution is to convert the frequency- and consequence measures into a "Low-Medium-High" scale of ranking. A "High/ High" risk will peak as a priority, and a "Low/ Low" may be left out.

Or may be not! That would depend on the tolerance of the organisation. It is most important that policies, objectives and goals indicate the realistic ambitions. These must be translated into the risk ranking matrix to roughly give an answer to if "Medium/ High", or other, represents a tolerable risk. It will be a health check for the fraud and corruption motivation to link ambitions against projected efforts and costs of controls.

And that was all? No, risks are dynamic! We need to assess and re-assess continually what can go wrong! Risks change with changes in markets, products, processes and personnel. Planning of assessments must take this situation into consideration by determining reviews at intervals.

Sources of requirements

Legislation and guidelines on how to prevent fraud and corruption have been improved substantially during the last decade. Rather than introducing new requirements, our rating system is built on the following framework of widely accepted conventions, principles, and guidelines in the field of preventing fraud and corruption:

- **UN Global Compact Principle on Anti-Corruption:** The Global Compact seeks to promote responsible corporate citizenship so that business can be part of the solution to the challenges of globalisation. In this way, the private sector – in partnership with other social actors – can help realize the Secretary-General's vision: a more sustainable and inclusive global economy. The 10th principle covers anti-corruption.
- **OECD Business Approaches to Combating Corrupt Practices**, anti-corruption material published on the websites of companies in UNCTAD's list of top 100 non-financial multinational enterprises which seeks to understand these companies' views of corrupt business practices as well as their anti-corruption management and reporting practices.
- **Transparency International's Business Principles for Countering Bribery** which were published by Transparency International, the global civil society organisation leading the fight against corruption. The Business Principles aim to provide a practical tool to which companies can look for a comprehensive reference to good practice to counter bribery.
- **the COSO Internal Control Framework**, a model for evaluating internal controls developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control.
- **Sarbanes-Oxley Act of 2002** introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: "To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws".
- **U.S. Foreign Corrupt Practices Act** of 1977 (FCPA) which prohibits U.S. companies, their subsidiaries, as well as their officers, directors, employees, and agents from bribing "foreign officials" and also requires U.S. companies that issue debt or equity to maintain internal accounting controls and to keep books and records that accurately reflect all transactions.

Glossary

Audit Committee: an operating committee where members are normally drawn from the Company's board of directors. Responsibilities typically include overseeing the financial reporting and monitoring internal control process.

Event: an incident or situation which occurs in a particular place during a particular interval of time. It develops from a threat and propagates through a particular set of circumstances. It generally ends with a probable negative consequence (incident).

Consequence: the outcome of an event.

Likelihood: used as a qualitative description of probability or frequency.

Probability: the extent to which an event is likely to occur.

Risk: the combination of the probability of an event and its consequence

Risk assessment: the overall process of risk identification, analysis and evaluation

Risk control: that part of risk management which involves the implementation of policies, standards, procedures and physical changes to moderate adverse (intolerable) risks.

Risk management: coordinated activities handle the culture, processes and structures that influence adverse effects (and potential opportunities).

Risk reduction: a selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both.

Risk treatment: the process of selection and implementation of appropriate options to modify intolerable risk. There are 4 sub activities: Evaluate-, select options, prepare-, implement plans

Supervisory board: a group of individuals chosen by the shareholders to promote their interests through the governance of the company and to supervise and control the executive directors and CEO.

Threat (Hazard): understood to be a source of potential harm or a situation with a potential to cause loss.

Det Norske Veritas
NO-1322 Høvik, Norway
Tel: +47 67 57 99 00
www.dnv.com