



This is an extract from the book «Fraud and Corruption – Prevention and Detection» by Nigel Iyer and Martin Samociuk (ISBN 978-0566086991). Referred to in the IIA Practice Guide «Auditing Anti-Bribery and Anti-Corruption programs», june 2014.

The Corporate Health Check

The notion of a Health Check

Fraud detection programs have been used in companies, over the past few years, with varying degrees of success. This may be because some of the tests used were unnecessarily technical or complex, or because the results were never understood, or simply because the program itself was not properly supported at the top of the organisation. Without the full support and understanding of senior management any program aimed at detecting fraud and corruption will usually fail.

In the eyes of the average employee or manager the word detection can conjure up notions of spying on the employees behind their backs and delving into their private affairs. Names like ‘Fraud Detection Program’, ‘Continuous Monitoring’, or ‘Penetration Audit’ can trigger negative associations of intrusion and a culture of fear, which can harm the credibility of the program.

Modern attitudes call for a more proactive, open and all inclusive program, hence the name ‘Corporate Health Check.’

Rather like a medical health check, the principle objective of a Corporate Health Check is to test for those indicators which are hidden below the surface in order to pro-actively identify and root out the red flags of fraud and corruption. This contrasts with and complements awareness programs, which train people to react once they spot red flags during the course of their normal work. Red flags identified in awareness sessions comprise only the visible signs of fraud and corruption at any particular moment in time. The Corporate Health Check probes much deeper looking at transactions and patterns, that is to say the actual footprint of fraud and corruption. It provides intelligence for further investigation to uncover hard evidence. The emphasis is on prevention and early detection.

A Corporate Health Check complements any internal audit program and can become a routine part of corporate life. It can be applied to an entire organisation or company, a division, a single department or subsidiary, or even to just one process within the organisation.

A properly performed Corporate Health Check will provide extremely valuable information to financial controllers, internal auditors, risk managers, corporate security, human resources and not least the executive management. However, it is important to recognise that a Corporate Health Check can only work within a climate of transparency and integrity.

Therefore, before a Corporate Health Check program is launched, it is crucial to obtain as broad a base of support as possible at the top of the company. This will help avoid resistance later on and in itself will help to contribute towards a more honest and open culture.

The sponsors of a Corporate Health Check should be the executive management, endorsed by the non-executive board, and supported by business units such as procurement, sales support, accounting, legal and human resources.

The executors of the Corporate Health Check could be Corporate Security, Corporate Internal Audit, Risk Management, Corporate Financial Controllers, or best of all, a team which combines representatives from each of these functions. The greater the buy-in to the concept of a Corporate Health Check, the greater the chance of success.

When a Corporate Health Check is carried out, expectations will vary considerably. At all stages the expected nature of the findings should be communicated clearly to all persons involved.

The importance of a broad base of management support is demonstrated by the following experiences:

Experience 1

During a Corporate Health Check, it was discovered that very substantial payments were made to an intermediary run by a person with links to organised crime, operating from the cover of a tax haven. When the findings were raised, people from the division concerned displayed outrage, stating that the person concerned was a legitimate businessman with whom they “had eaten dinner several times”. The division also tried to discredit the Corporate Health Check saying that the findings were misleading and the program was put on hold for two years until the true facts emerged.

Experience 2

A Corporate Health Check which examined the behaviour of fifty senior managers was quietly discontinued when it was discovered that over 25 percent of the managers had benefits from outside undisclosed business interests. This was on top of the fact that a number of managers were often submitting wholly inappropriate or private business expense claims.

Experience 3 (C Heading)

When indications of price fixing and cartels were discovered with the help of a Corporate Health Check of sales and marketing, management decided that the internal auditors had probably “gone too far”.

Experience 4

Three round-sum million dollar payments to a front company and numbered account should have been enough to indicate that systematic bribes (incidentally contravening the company Code of Conduct) were being paid. The Marketing Department furiously defended these payments as legitimate agency fees and dismissed the Corporate Health Check findings as “trivial”.

Although these reactions may seem a little unusual, they are typical of managers when confronted with a problem in their own territory. In other words, when the problem is ours, we often become defensive.

It is a fact that people simply don't like being watched or monitored. Therefore the Corporate Health Check has to be introduced and performed with a sensitivity and care. Sometimes a Corporate Health Check is not politically acceptable to senior management. The reasons for this can include a fear of the unknown, a dislike of intrusive testing or even a reluctance to lay their past transactions and behaviours open to scrutiny. It is the fear or chance that inappropriate transactions and behaviour will be discovered which can lead to a Corporate Health Check being delayed or even put off indefinitely.

The ability of persons trying to undermine the program should not be underestimated. Typical counter-arguments to performing a Corporate Health Check include:

- 'the Corporate Health Check infringes on Human Rights and Data Protection Legislation. We want our people to believe that they can be trusted so we don't want to spy on them'
- 'fraud and corruption is a next generation issue, not something we have to deal with now'
- 'we have an awareness program so why do we need to do more'
- 'we already have auditors so why do we need a Corporate Health Check?'

It is important to anticipate these objections and the reasons for them. The fear factor and the perceived intrusiveness can be addressed fairly easily. A Corporate Health Check should always be a non-intrusive and non-disruptive process where the subject is involved throughout the process. In addition the Corporate Health Check should comply with data protection or human rights legislation, as well as be in full compliance with company policies and employee relations agreements. Furthermore, legislation will vary considerably from jurisdiction to jurisdiction. Therefore it is advisable either to begin the Corporate Health Check in areas which clearly have no relation to individuals or to take appropriate legal advice at the start.

Setting aims and objectives

The aim of a Corporate Health Check is to identify symptoms of fraud and corruption as early as possible. The objectives also need to be clearly defined. The following are typical objectives of a Corporate Health Check:

- it should target those fraud and corruption risks which have the highest impact on the business and provide warnings of ongoing fraud and corruption as early as possible
- tests should be repeatable across the organisation and provide results which are consistent, comparable, easy to classify and act upon
- specially trained persons within the company should perform the Corporate Health Check
- it should be integrated within the work of the Internal Audit, Corporate Security or Risk Management functions
- it should not lead to, or raise, any false alarms.
- it should avoid contentious data protection issues by focussing on data which cannot be classified as personal data
- it should be equally applicable to the whole organisation, a division, a single department or subsidiary, or to one process within the organisation.

How a Corporate Health Check works

The five steps below summarize how a corporate health check is done:

- understand the risks of fraud and corruption, document them in a Fraud and Corruption Profile and then identify what sort of footprint would be left behind if the method was used
- decide where to collect data and information and build a model
- select which tests to apply, run the tests, summarise the results in the form of a diagnostic report
- interpret and understand the diagnostics report and run further tests if deemed necessary
- perform preliminary research into the findings, evaluate and decided on next steps.

Just as with any form of health check, a wide range of equipment, tools and techniques can be used. However it is wise to be selective as the more tools used the greater the volume of information generated, not to mention the cost. If you have a good idea what you are looking

for, the scope and extent of the Corporate Health Check can be much narrower. A well developed Fraud and Corruption Profile is the key to knowing what to test for.

A Corporate Health Check provides the insider's view of the extent of fraud and corruption in the company. It is true to say that raised awareness together with the health check will still probably not uncover every instance of actual fraud and corruption. However interpretations of the results combined with the use of a well developed Fraud and Corruption Profile makes it much easier to target those areas where the company is most exposed. Fraud and corruption is often a function of the culture of an organisation. If it is in one area it is likely to be in others. Therefore it is also not necessary to look absolutely everywhere. Unethical behaviour in one area of the business often leaves it's footprint in another area.

Where to use the Corporate Health Check

The Corporate Health Check can be used for example to identify:

- signs of procurement fraud and relationships with potentially unsuitable business partners
- unusual payments to front companies and offshore destinations
- symptoms of overspending
- signs of repeat fraud
- collective customer arrangements and other unhealthy customer relationships and potential employee conflicts of interests
- deliberate misstatements.

Because many of the tests used are in fact a way of testing the culture within the business, a well designed Corporate Health Check will often also identify problems related to management's investment and divestments strategy and other inappropriate business behaviours.

A typical template is provided at Appendix VII showing how a Corporate Health Check can be designed and constructed, by focussing on the major risks and developing key tests. For illustration purposes we have also provided some examples of the findings.

A number of international companies have already used Corporate Health Checks as a way of improving their testing for the symptoms of fraud and corruption. One of the lessons learnt has

been that rather than using too many tests, more time should be spent in interpreting and classifying the results. Also, it is important to hold back from investigating red flags as they are uncovered. Often a Health Check will throw up a large number of symptoms which can, if not properly analysed and interpreted, be easily misinterpreted. It is only by clearly defining, then grouping and analysing the symptoms can the problems be properly diagnosed. Those companies which have been doing this are now becoming more and more self-sufficient and are able to perform several health checks a year with very impressive results.

When a company-wide Corporate Health Check is carried out we usually see one of two following diagnoses:

- there are just a few isolated symptoms of fraud and corruption
- there are numerous incidents of fraud and corruption often at many levels in the company, or a division, touching the upper echelons.

Once the symptoms have been analysed they can then be grouped, analysed again and various treatments proposed. Treatments will include emergency fixes, longer-term changes to procedures and in some cases more in-depth investigation of certain potential problems.

An extract from a typical diagnostic report from a corporate healthcheck is provided at Appendix VIII. This was performed on external payments across over 1 million transactions over a 14 month period.

Specialist training should be provided so that internal departments can carry out Health Checks. Asking one simple question could uncover a major fraud, but only if the question is asked correctly. We believe that for external or internal audits to be more effective, auditors should receive training in how to detect specific methods of fraud.

EXAMPLE: Using some of the simplest fraud detection tests, we discovered several paid invoices. One invoice was for work done in the USA, but the company's bank account was in the Cayman Islands (and also the amount of \$49,799 seemed unusual for unspecified work). There also were strong indications that the US based supplier was in fraudulent collusion with a locally based project manager, but was skilful at hiding it from the head office.

The head office of the company paying the invoice was in Scandinavia. Internal rules stipulated that the project manager had to fax the invoice for approval. The cost centre manager at Head Office was asked why he had approved these invoices for payment. He responded:

“I have so many of these invoices to look at that, to be totally honest I don’t get the time to really look at them. I remember this one however because I thought it a bit odd that we were paying money for an American supplier into a Cayman bank. I even called an accountant that I knew in the shared service and asked him if we could actually pay these invoices to the Cayman Islands. He answered that there was no problem whatsoever and they had done it many times before. On reflection, I think he misunderstood my question...”

Statistical and trend analyses may provide an indication of where fraud and corruption is hidden. However in order to actually find it, someone has to look at the details. Complex tests require extensive interpretation of results, while thorough application of simple tests tends to consistently deliver useful results.

However as the powerful example below demonstrates, a Corporate Health Check will only work when management ceases to ignore the symptoms:

The Marketing department of an international company X, had for the past ten years been using a single supplier for all marketing and corporate events. This supply company had been incorporated by two people round about the same time as the contract commenced. On average the company had doubled its turnover every year and was now about 40 persons strong. Approximately 70 – 90% of this supplier’s turnover each year had originated from X. One year’s spend alone was around Euros 10 million.

The Marketing department resented any intrusion in its affairs by what they called ‘outsiders’ (which included the Corporate Procurement Team and Corporate Internal Audit) and for ten years managed to carry on their affairs as they liked. They were supported throughout by an Executive Director who agreed with them that marketing was such a specialised area that Corporate Procurement could not possibly understand the intricacies of choosing a supplier. Their involvement would only add to the costs.

Corporate Internal Audit noticed these indicators and conducted a Corporate Health Check on paid invoices and supporting documentation in the Accounts Payable department. It was quickly discovered that:

- *the supplier had been awarded work without any competitive tendering for over 10 years*
- *there were no contracts for what should have been provided, who should provide it and what sort of mark-ups the supplier should have made on their bought-in services*
- *pro-forma purchase orders were created based on old invoices as a way of giving the impression that a procurement process had taken place. These purchase orders were usually dated some days or weeks after the supplier's invoices*
- *the supplier submitted a large number of very vaguely specified invoices which in fact hid mark-ups of subcontractor costs (which were in excess of 200%) or in some cases, were wholly fictitious.*

This was in addition to red flags such as:

- *the staunch resistance of the Marketing department to involving the Procurement department. (Procurement department personnel were too scared to act and felt they had no channel to communicate their concerns)*
- *the fact that no projects in Marketing were put out to competitive tender*
- *the support of the Marketing department's practices by a senior member of the management team*
- *the fact that the supplier had doubled its turnover each year but still was reliant on the company for approximately 90% of its business*

However, as is often the case, people in X, including the auditors assumed that a logical explanation for all these symptoms had to exist. The fact that the situation had been ongoing for so long supported the theory that 'if something was wrong then something would have been done already'.

Five years later, another Corporate Health Check of the Accounts Payable area was performed. Once more, major red flags and a number of other ones cropped up. However, this time the new CFO set about trying to understand why the situation had endured so out of control and why his policies and procedures were being ignored. Probably most importantly, before taking

action he managed to quantify what cost-savings could be made by doing things the way he had expected things to be done.

Six months after the second Corporate Health Check was performed the end result could be summarised as follows:

- *a substantial refund was obtained from the supplier*
- *new procurement experts were brought into to work alongside the Marketing department and after a competitive tendering process new suppliers were identified*
- *it was estimated that cost-savings in the future were in the region of 30 – 50%*
- *several organisational changes were made*
- *the case caused a number of waves in the organisation and the example was taken up repeatedly in training and awareness workshops as an illustration as to how bad things can get if the organisation does not recognise the risks of fraud and corruption.*

The above case example illustrates how important it is to recognise the importance of not just identifying the symptoms but also understanding what they are telling us and acting upon them.

Getting started

Before getting started on Corporate Health Checks we should provide a word of caution. The person doing the tests should be able to think creatively as well as able to use analysis software. Otherwise the output may be so huge as to be useless. Many financial institutions, for example, have successfully implemented automated fraud detection software using artificial intelligence and neural network technology to detect suspicious credit card transactions. Some organisations have attempted to mirror this for detection of corporate fraud in procurement systems, by installing specialist data mining software. The software alone has then produced many hundreds of red flags which cannot possibly be followed up in the time available to the auditor.

The flaw lies not in the software itself, but in the approach that is applied. Experience has shown that only up to 20% of fraud detection time should be spent using the computer and doing data-analysis. The rest of the time requires:

- the person implementing the detection program should first think like a fraudster in order to understand what frauds are most likely, and then should develop a Fraud Profile which is endorsed by senior management. A healthy suspicious mind is needed
- the person should think before using a computer – automated fraud detection software is generally a poor substitute for thinking
- looking for the simple tests – then the results usually are understandable
- understanding what ‘footprints’ would be left behind
- dedication to following things through and attention to those sorts of details which management usually does not have time to deal with
- spending time evaluating and researching existing findings which is much more important than producing hundreds of new findings.

When something looks like a fraud – evidence should be obtained by examining the details. No assumptions or gut-feel decisions should be made. Pitfalls which can and should be avoided include:

- relying too much on the computer to do the work and not using enough intellect and judgement in interpreting the results; the degree of automation can be gradually increased as time goes by and experience is gained
- creating a wall of opposition by delving at an early stage into sensitive areas, such as senior manager’s lifestyles and personal interests in companies; this can be dealt with later if and when it becomes a problem
- over-reacting to individual symptoms raised by the Corporate Health Check and then going out into the organisation and demanding explanations (or worse still making accusations) before reviewing all symptoms first
- when looking at symptoms, assuming that there must be a logical explanation without actually looking for that explanation (humans have a natural tendency to believe or hope for the best).

We suggest that you approach getting started with Corporate Health Checks along the following lines:

- use the initial time to go through the methodology, review your objectives then develop a framework for how the Corporate Health Check Program will be piloted and then rolled out
- decide which internal people will become your Corporate Health Check experts and what basic skills they should acquire. Broadly speaking the following skills are necessary:
 - an understanding of the methodology itself
 - how to define and collect the required data
 - how to conduct data analysis, using fast international desktop research such as metasearching, and various online databases to quickly sift through and prioritise the findings
- begin by looking at payments and purchasing moving into receipts and sales. This targets the money flows from and to the company and opens up many potential areas of abuse. In this way you can also steer clear of any contentious personal data issues
- prototype the Corporate Health Check System on one region, department or country and then refine improve and move to the next target
- review, refine and rollout the system. Parts of the computerised testing of transactions can now be automated.

Summary of Key Points

- investing in monitoring and detection can lead to a significant reduction in losses from fraud and corruption
- all employees should receive fraud awareness training
- the Fraud and Corruption Awareness program should have the backing of the CEO and Board
- training should be interactive, interesting, and based on real life cases studies
- employees should be trained to spot red flags including changes in behaviour, in transactions, systems and corporate activities. This training should link into Human Resource awareness sessions on the symptoms of depression and other mental illness, and on follow up actions

- a program to carry out Corporate Health Checks should be approved by the Board and Audit Committee
- Corporate Health Checks should be carried out by trained company employees and overseen by a senior manager who is sensitive to the political, ethical and legal issues which may arise, but possessing enough determination not to be put off by resistance from the top.