HUIS VOOR
KLOKKENLUIDERS

KNOWLEDGE & PREVENTION

Brochure ‘Risk-sensitive roles’

August 2026

1. FOCUS ON INTEGRITY RISKS IN THE WORKPLACE

1.1 INTEGRITY RISKS AND THE IMPACT OF VIOLATIONS

Every organisation is at risk of an integrity violation. The possible consequences of integrity violations vary widely and may include financial, material and/or reputational harm. Integrity violations can also harm the employees involved. Across the organisation, integrity violations can lead to reduced trust among employees, customers, patients or other stakeholders in the organisation and its integrity.

The consequences of a violation can be serious, which is why organisations have a major responsibility to promote integrity across the board and to help prevent violations as much as possible. In this way, they protect both their own organisation and their employees and others involved. It is important for an employer to keep sight of broader measures that concern all employees and the entire organisation, such as a reporting procedure, code of conduct and the deployment of confidential advisers. In addition, employers must also pay attention to the individual. After all, every integrity violation can ultimately be traced back to an act or omission by one or more individuals, even when those individuals are acting as part of a larger collective.

What is an integrity violation?
Integrity violations can take serious forms. An integrity violation is a failure to act in accordance with the applicable moral values, norms and related rules within an organisation. An integrity violation is referred to as wrongdoing when the public interest is at stake. The public interest is at stake when the violation goes beyond one or more individual interests and when it is also part of a pattern or structural in nature, or when the act or omission is serious or extensive in terms of scope. Every case of wrongdoing is an integrity violation. The reverse is not always true. Integrity violations are often associated with fraud or corruption. However, an integrity violation is not limited to misuse of financial or other resources. Examples also include using business contacts for private purposes or providing information or other benefits that have value, such as granting a permit. Any of these types of integrity violations may occur. The level of risk depends largely on the role and the resources or powers assigned to an employee.

1.2 PROCESSES VERSUS THE INDIVIDUAL

This brochure focuses on risk management in the field of integrity. Identifying and assessing risks at **process level** is the most common approach in this area. We take individual employees as the starting point and look at integrity risks at **role level**. By focusing integrity policy on employees, the employer fulfils its responsibility to practice good employment.[1] This enables employers to take more targeted control measures and strengthen the resilience of both the organisation and employees against integrity risks.

[1] Section 7:611 of the Dutch Civil Code.
The employer and the employee must behave as befits a reasonable and fair employer and a reasonable and fair employee.

The impact of an employee’s integrity violation depends, among other things, on the extent to which that employee can cause harm in their role. After all, embezzlement by an employee who is authorised to manage a company’s business accounts can potentially cause more financial damage than embezzlement by an employee who has no direct access to business accounts.

It is difficult to predict whether an employee will misuse their powers or the resources made available to them by the employer in the future. The intention is not for employers to regard all employees as untrustworthy from the outset or to approach them with suspicion. This can negatively impact the organisational culture. However, it is often possible to identify vulnerabilities that increase the risk of an integrity violation. Sometimes these vulnerabilities lie within the organisation itself, such as neglecting the four-eyes principle, or applying it incorrectly. At other times, they stem from personal employee issues, for example when the employee has financial problems. It is in the interests of both the organisation and the employee for the employer to identify, acknowledge and address these vulnerabilities as much as possible. The next chapter uses an action plan to explain how employers can do this.

2. A ROLE-LEVEL ANALYSIS

THE ACTION PLAN

To make employees more resilient to integrity risks, it is important to make them aware of the possible integrity risks associated with the work they perform. Widespread organisational and individual awareness of role-specific integrity risks helps both management and employees to anticipate more easily and take measures to avoid or reduce risks. In the rest of this publication, we use an example – see the blue box on the next page – to go through various steps that help to identify integrity risks at role level. We do this in a number of steps:

1. Identifying the **different role types** within an organisation;
2. Mapping, for each role type, which **tasks** and **powers** are susceptible to misuse by the employees, or by one or more third parties;
3. Identifying the **vulnerabilities** that may increase this risk;
4. Identifying existing measures that reduce this risk;
5. Determining which **measures** still need to be taken to reduce the risk.

Tip!
You should preferably critically review roles and actions on a periodic basis. Some risks are situation-specific and context-dependent. Changes in an employee's personal life may also make them more vulnerable in the performance of their role compared to the moment they were appointed. In addition, a change in role, internal processes or certain developments in society, for example, may prompt a reassessment of risks. An effective approach is to speak with employees at least once a year about whether anything has changed in their personal circumstances or work-related activities. Discuss with employees how this change affects their work.

STEP 1: IDENTIFYING ROLES

To complete these steps, it is important to consult job profiles, where available. If no job profile is available, for example, job vacancy texts describing the duties can be consulted. This reflects the role as it appears on paper. It is then important to check whether this corresponds to the reality in practice. This can be done by speaking to several people in the department and gaining insight into the internal relationships between roles, and the external relationships with stakeholders outside the organisation. This creates a picture of what an employee is expected to do and what the role actually involves. This is an important starting point for determining whether the organisation's interests are sufficiently protected and whether the employer is also protecting the employee sufficiently from the perspective of good employment practices.

Examples in this brochure
This document uses the example of a sales representative who sells products and services to potential new customers on behalf of a company. In the example, the activities of this representative always relate to one **work area** and one **risk**, so that the example remains clear. The table is completed further at each step, accompanied by an explanation. When you start working on the analysis yourself, you will identify various **work areas**, **risks** and **measures** for each role. After all, the representative we use in the example might have a broader range of tasks that relate to various work areas. Initially, given the high level of contact with customers, it is natural to think of risks related to corruption and the exchange of gifts. But also consider their role in financial administration: the representative is in contact with the finance department where it involves matters such as the handling of invoices. Expense claims can also be a risk area, especially when the representative often travels alone. Various risks and measures apply in this area. A non-exhaustive list of examples of work areas, tasks, powers, vulnerabilities and measures can be found in the appendix.

STEP 2: IDENTIFY HIGH-RISK TASKS AND POWERS

To determine which tasks and powers associated with a role are risk-sensitive, it is important to consider whether performing, exercising, not performing or not exercising a task or power represents a certain value in economic transactions or for certain groups in society. This is because such tasks and powers are more susceptible to various forms of misuse.

An employee who has access to an organisation's financial resources, for example when making payments on behalf of the organisation, may be tempted to misuse this power and may also be an attractive target for third parties, for example in phishing attempts. The value of this particular employee's power can easily be determined from the volume of the money flows. That value is more difficult to express when it concerns an employee who manages databases containing sensitive data. Even something seemingly simple, such as issuing passports, can create an integrity risk because of the value that an authentic passport represents to criminals. Organisations must be alert to roles that involve working with customer data, such as addresses and citizen service numbers (BSNs), or with business-sensitive data or competitively sensitive information.

When considering high-risk tasks and powers, we should not only look outwards. Powers over other staff can also pose a risk. For example, this occurs when an employee's role allows them to grant authorisations to other colleagues, or when a manager has the power to hire new colleagues.

Every role in an organisation may therefore involve different integrity risks. In the example used in this brochure – see the blue box above – the role of 'sales representative' involves both an internal and an external integrity risk. In the table, you first see the **work area** to which the role belongs, the specific **situation** in which integrity risks may arise and the possible **risk** associated with that situation.

Role name: sales representative **Tasks**: selling products and services, identifying potential customers and sales markets in the Netherlands and abroad.		
Work area	Situation	Possible risk
Contact with third parties	**Employee is responsible for contact with and onboarding of new customers**	**Employee accepts a dishonest customer as a result of manipulation**

Explanation: In this table, we focus on the risks that exist in the sales representative's contacts with customers. In this example, the representative is responsible for customer retention and new client onboarding. Many organisations have an acceptance policy for new customers. One reason for this is to gain insight into the supply chain, to ensure you do not inadvertently contribute or associate with wrongdoing through that chain, for example. Other reasons include verifying that a new customer has the ability to meet long-term obligations, that they share the values to which the organisation is committed and that a new customer actually exists. In the example, one of the risks identified is that the representative is tempted or persuaded to accept customers who do not fit within the organisation's acceptance policy. Another risk is that the representative offers existing customers an overly favourable rate that does not fit within the organisation's policy. An overly close relationship with the customer, or certain benefits promised by the customer, could tempt the representative to do so.

STEP 3: RECOGNISE AND ACKNOWLEDGE VULNERABILITIES

If a role falls within one or more vulnerable work areas, it is important to identify which circumstances could lead to an increased risk of an integrity violation. These circumstances are also known as 'red flags' – factors that increase the vulnerability of a role.

Vulnerabilities can be both organisational and individual in nature. Employees who spend more than they earn and are subject to an attachment of earnings (an individual vulnerability) will consider – and, in extreme cases, may seize – every opportunity to escape their difficult financial situation. This means that undesirable options, such as committing fraud or being open to corruption, may no longer be ruled out.

The way in which work is organised also has a direct influence on employees' integrity. In particular, employees involved in vulnerable processes – for example, processes involving sensitive data or money – or employees in positions of power should know exactly what tasks they are required to perform and/or what responsibilities and powers they have in that role. Vagueness and lack of clarity can give employees considerable freedom to act without clear boundaries (an organisational vulnerability).

Some examples of possible vulnerabilities, both organisational and individual, are provided below. A more extensive list can be found in the appendix:

Vulnerabilities	
Complexity	Complex legal or tax structures, opaque production chain
Change/dynamics	Strong growth or contraction, crisis situations
Management	Management attitude and role-model behaviour, tone at the top
Employee personality traits and situation	Gambling addiction or other addiction, feeling unfairly treated
History of issues	Work backlog, integrity incidents, 'poor' culture

Role name: Sales representative Tasks: transporting goods or people, managing a vehicle, sometimes contact with customers or suppliers.			
Work area	Situation	Possible risk	Vulnerabilities
Contact with third parties	Employee is responsible for contact with and onboarding of new customers	Employee accepts a dishonest customer as a result of manipulation	**Financial bonus per referred customer**

Explanation: In the case of the representative, several vulnerabilities can be identified that could prompt them to ignore the acceptance policy. While the representative would not normally give in to demands from potential customers, for example, they might do so if there is a remuneration policy that includes incentives. For example, a financial bonus for each customer the representative introduces. This type of remuneration policy is an example of an organisational vulnerability. Also personal vulnerabilities can be identified. This can include a vulnerability in the representative's personality. People who value power and status might be more vulnerable in this regard than those who do not.

STEP 4: IDENTIFYING EXISTING MEASURES

To make the organisation and employees more resilient to integrity risks, an organisation needs to take measures. Measures may vary in scope and approach. Several measures are often already in place, sometimes without those measures being explicitly linked to the specific risks of a role. Measures may be generic, i.e. organisation-wide, or specific, meaning focused on a role. Both are important and require ongoing attention.

TYPES OF MEASURES: SCOPE

- **Generic measures** are measures aimed at the entire workforce. Examples include components of the integrity infrastructure aimed at encouraging a safe working environment in which employees experience no barriers to raising concerns and reporting suspected integrity violations.
- **Specific measures** are intended to improve the resilience of a particular work area or task, or to reduce concrete role-specific risk factors. Examples include stricter screening for employees with high-risk tasks or the introduction of the four-eyes principle for certain tasks.

TYPES OF MEASURES: APPROACH

- **Preventative measures** are intended to prevent and reduce risks.
- **Detective** controls are intended to determine whether certain risks occur.
- **Remedial** measures can be used to remedy situations in which risks materialise.

Measures must be reviewed regularly to check whether they are still sufficient. Furthermore, the measures must, of course, be practicable and applied effectively. The organisation may not immediately have a full picture of all existing measures. It is therefore important to discuss this with the relevant team, the manager and subject-matter specialists in order to be properly informed about the measures. In doing so, also take account of unwritten rules in the workplace and the culture within teams. Such aspects can also contribute to reducing risks. Once you have a good overview, the next step is to effectively tighten or update existing measures and work on appropriate measures where they are still lacking.

Role name: Sales representative Tasks: Customer acquisition and maintaining existing relationships.				
Work area	Situation	Possible risk	Vulnerabilities	Preventative measures
Contact with third parties	The employee is responsible for recruiting and accepting new customers	The employee accepts a dishonest customer as a result of manipulation	Financial bonus per referred customer	**Mandatory advice from the legal department**

Explanation: In the example, the review shows that preventative measures are already in place. One of these is mandatory advice from the legal department when a customer is onboarded. This partially limits the representative's authority.

STEP 5: IDENTIFY ADDITIONAL MEASURES

Now that you have identified which tasks and powers are susceptible to misuse, which factors may increase vulnerability to integrity risks and which measures your organisation has already taken to reduce those risks, it is important to assess whether the risks have been sufficiently avoided and/or mitigated.

Whether the identified measures are effective depends on circumstances such as their **relationship** with existing measures and the **organisational culture**. It is also important that the measures are **known** to those concerned and that they are **up to date**.

Organisations can often reduce integrity risks through small adjustments. For example, by assigning a particular control task to another officer. For example, an organisation that conducts internal checks on money flows can take additional measures by ensuring that the decision-making and control processes for expenditure do not rest with one person, but that at least two people carry out the necessary checks at different points in the process. This is an example of **segregation of duties**. For an extensive, non-exhaustive list of examples of measures, see the appendix.

When adding new measures, carefully consider whether their scope and impact are appropriate to the risks, i.e. **proportionate**, and check whether there are less intrusive measures that could achieve the same effect, i.e. whether they are **subsidiary**. You do not want to burden employees unnecessarily with checks and must guard against unnecessary infringements of employees' privacy.

In the case of the sales representative, the following additional measures could be taken, for example: mandatory screening of new customers by a department or employee other

than the representative, and the presence of two employees during crucial negotiations with the potential customer.

GETTING STARTED IN YOUR OWN ORGANISATION

The approach described above can be applied to organisations in various industries and sectors, regardless of the size of the workforce. While small organisations struggle with overlapping roles between different employees, large organisations struggle with mapping all activities related to the various roles. In that case, one option is to start, for example, with the roles within a particular department. In practice, the approach may differ on certain points, but it is important that all steps described are reflected in the organisation-specific approach.

It is also important to use the analysis as a **preventive** tool. That means preferably before there are any signals of possible integrity violations. Only then can an organisation identify risks and take action at the earliest possible stage. This allows the analysis to be used as efficiently as possible as a tool to help prevent integrity violations and wrongdoing.

Who should carry out the analysis depends on how the organisation is structured and what expertise is available. In larger organisations, it makes sense for the analysis to be carried out by an officer responsible for overseeing integrity policy, or by an employee from the Risk & Control department or a comparable department. What matters is that the people carrying out the analysis understand the various roles and processes, and that knowledge regarding assessing integrity risks is available. Setting up a small working group to bring together different areas of expertise can lead to a better analysis. Small organisations may consider engaging external expertise.

Another point to consider is designing the process in such a way that vulnerabilities within roles are examined critically and constructively. It must not become a box-ticking exercise or a copy-and-paste job. For this reason, the Authority has chosen not to provide a fully developed analysis. As described above, an appendix with examples is available for anyone looking for inspiration and examples of work areas, tasks, powers, vulnerabilities and measures.

About the Dutch Whistleblowers Authority
The Dutch Whistleblowers Authority is an organisation that focuses on all matters relating to whistleblowing and integrity. From advice to support, from investigation to prevention. Would you like to know more? Our website is a source of information for employers, employees and policymakers. You can find us at http://www.huisvoorklokkenluiders.nl.

This is a publication of the Dutch Whistleblowers Authority.

Contact details
Muzenstraat 89-91, 2511 WB The Hague
Telephone: +31 (0)88 13 31 000
E-mail: info@huisvoorklokkenluiders.nl

www.huisvoorklokkenluiders.nl