



WHISTLEBLOWERS
AUTHORITY



INTEGRITY IN PRACTICE

The confidential integrity adviser



Introduction 4

1 What is a confidential integrity adviser? 5

- 1.1 Confidential integrity advisers in a nutshell 5
- 1.2 In which domains do confidential integrity advisers work? 5

2 The purpose of confidential integrity advisers 8

- 2.1 Importance for employers 8
- 2.2 Importance for employees 10

3 Who can be a confidential integrity adviser? 12

- 3.1 Make it easy 12
- 3.2 Personal background 12
- 3.3 Senior – junior officers 12
- 3.4 Centralised – decentralised 12
- 3.5 Full-time – part-time 13
- 3.6 Internal – external 14
- 3.7 Multiple confidential integrity advisers 14

4 What does a confidential integrity adviser do? 15

- 4.1 Organisational fit 15
- 4.2 Support function 15
- 4.3 Information function 17
- 4.4 Signal function 18

5 Confidentiality and anonymity 20

- 5.1 Core element of the job 20
- 5.2 Limits of confidentiality 20
- 5.3 Anonymous & confidential reporting 23

6 What do confidential integrity advisers require? 27

- 6.1 Start with policy 27
- 6.2 Appointment 28
- 6.3 Facilities 29
- 6.4 Formal agreements 30

7 What are confidential integrity advisers asked? 32

- 7.1 Professionalisation 32
- 7.2 Attitude 32
- 7.3 Knowledge 33
- 7.4 Competences 33

8	Link with OHS and integrity policy	35
	8.1 Embedding confidential work	35
	8.2 Cooperation within the organisation	37
	Literature	40
	Colophon	41
	Appendices	42



Dutch Whistleblowers Authority

The Dutch Whistleblowers Authority (DWA) is for people who want to report work-related wrongdoing in the government or in business. Employees looking for advice on how to deal with a suspicion of work-related wrongdoing can also contact the DWA, and the same applies to employees suffering negative consequences after submitting a report. The DWA investigates potential malpractice, as well as how those who have reported wrongdoing are treated. In addition, the DWA provides support to organisations looking to boost their integrity by preventing future incidents and learning from past reports. This shows whistleblowers that their actions meant something and helps prevent future wrongdoing.

The confidential adviser in practice

By appointing a confidential integrity adviser (CIA), organisations reinforce their integrity, both preventively and correctively, and make their internal reporting process safer, easier and more effective. Ultimately, this will benefit the entire organisation. There are various types of confidential advisers. Employees can turn to the 'confidential harassment adviser' for a solution to issues such as bullying, intimidation and discrimination. The 'confidential integrity adviser', on the other hand, can play a role in dealing with and preventing suspected integrity violations or wrongdoing. Because these two roles are usually merged into one, this brochure will address both, and refer to this role as 'confidential integrity adviser (CIA)'.

Practical guide

This brochure serves as a practical guide for setting up a sound confidential integrity position and addresses all relevant aspects of this position, including organisational aspects such as selection and recruitment, appointments and the workplace, as well as elements such as profile, tasks and responsibilities. Paying attention to all these aspects will make it easier for CIAs to do their job. This brochure contains the most up-to-date knowledge based on research, expert sessions and surveys carried out by the DWA in the public and private sector, as well as scientific literature and expert insight.

Who is this brochure for?

This brochure is intended for everyone involved in confidentiality work in their organisation. If you are an integrity professional, compliance officer, manager, Human Resource Manager or (future) CIA, this brochure will be useful for you. The details of your role in the organisation will always differ from one case to another: a one-size-fits-all approach is just not possible. This brochure aims to inspire both management and CIAs and serves as a practical guide on the various options with regard to the selection process, defining the tasks of a CIA, and positioning the CIA within an organisation. If you have any questions about confidential work, please feel free to contact the Dutch Whistleblowers Authority.

1

What is a confidential integrity adviser?

CIA's in a nutshell

- Confidential point of contact for employees.
- For complaints and undesirable behaviour (OHS).
- For integrity and reporting wrongdoing (whistleblowing).
- Recommendation: combined confidentiality role.

1.1

CIA's in a nutshell

A CIA is a confidential point of contact for employees. Anyone in the organisation struggling with or worrying about a particular matter can turn to a CIA to talk about it in private. This system only works if employees have the courage to speak to a CIA, which requires the CIA to have an autonomous position within the organisation and to act confidentially and carefully.¹

There are two types of confidential advisers. People can turn to the 'confidential harassment adviser' for a solution to issues such as bullying, intimidation and discrimination. A second type of confidential adviser is currently emerging due to the increase in whistleblowing schemes. This 'confidential integrity adviser' plays a role in dealing with and preventing suspected integrity violations or wrongdoing. Because these two roles are nowadays usually merged into one, this brochure will deal with the combined position, and refer to this role as 'confidential integrity adviser (CIA)'.

Organisations preferably have multiple CIA's at their disposal, both internally and externally. An internal CIA is an employee within the organisation, who carries out confidential work in addition to his or her primary duties. An external CIA is a professional contracted by the organisation. This dual structure allows employees to pick an adviser they can trust and who suits the issue they are dealing with.



If you have any questions about confidential work, please feel free to contact the Dutch Whistleblowers Authority. Visit www.huisvoorklokkenuiders.nl for more information.

1.2

In which domains do CIA's work?

First of all, CIA's deal with undesirable behaviour, including discrimination, (sexual) intimidation, aggressive behaviour and violence, bullying and harassment. These types of behaviour are also known as 'social integrity violations'. Undesirable behaviour is characterised by its personal nature: the complainant and complaint often coincide.

¹ Verweij (2018).

The person making the complaint has been treated wrongly and has a direct, personal interest in stopping undesirable behaviour. With respect to this type of complaint, CIAs will focus mainly on the complainant's interests and provide support. The complainant is in charge of what happens, with the CIA supporting the complainant in making his or her own decisions, during a meeting between all those involved or during a complaints procedure, for instance. Furthermore, a CIA can provide general advice to an organisation looking to improve psychosocial safety in the workplace.

Secondly, CIAs work with integrity violations and wrongdoings (possibly harming the public interest). Examples of integrity violations include fraud, theft, undesirable ancillary activities and abuse of power. In some cases, integrity violations are carried out by an individual, but the problem can also be more serious, e.g. when several people (or even management) are involved, or when it affects major parts of the organisation or the organisation as a whole and harms customers, civilians or employees. In this case, the organisation's continuity may be jeopardised. These violations are called wrongdoing. If the violations are so serious that they jeopardise the interests of society, they are regarded a wrongdoing that harms the public interest.² Such wrongdoings fall under the Dutch Whistleblowers Authority Act.



When employees of a slaughterhouse misappropriate company assets, for instance, they are committing an integrity violation. This, however, does not constitute a wrongdoing that harms the public interest. However, what if the problem is structural, management is involved, or it concerns major sums of money? Or, even worse, if employees – due to worsening culture and poor supervision – start tampering with the meat, creating a danger to public health? In that case, society's interests are jeopardised to such an extent that the violations can be considered a wrongdoing that harms the public interest.

A key difference between these two domains is the party affected by the problem. In the case of undesirable behaviour, the person reporting the complaint is directly affected in being the victim of undesirable behaviour. In case of integrity violations and wrongdoing, the organisation (or even society) is affected by the problem. Typically, the person reporting wrongdoing will not be a victim, but rather a witness or bystander. The CIA must then support the person reporting wrongdoing and help them take the right steps. To make sure this happens, it is important that the reporting threshold be kept as low as possible, which can be done by protecting the reporter's identity if necessary, for instance. In a more general sense, though, CIAs also serve to protect and promote the integrity of an organisation by identifying worrying developments in the organisation's structure and culture, for instance, and advising the employer accordingly. This will allow the organisation to prevent violations and wrongdoing.

It is up to the CIA to carefully examine and assess each and every specific situation that is brought to their attention. For instance, the person reporting wrongdoing will

² Article 1d, Dutch Whistleblowers Authority Act.

often be personally affected by the problem they report. Unfortunately, the efforts of people reporting wrongdoing (that harms the public interest) are not always appreciated and they might suffer negative consequences. Anyone looking to report wrongdoing is forced to consider the personal consequences he or she may encounter and must therefore seek to protect him- or herself as much as possible. The CIA has an important advisory role to play.

In some cases, undesirable behaviour and integrity violations may coincide, as intimidation and abuse of power can go hand in hand. People who are intimidated by others are personally affected, but abuse of power is also undesirable from an organisational point of view. Large-scale forms of intimidation may even lead to (social) wrongdoing, which can make it difficult, or even impossible, to distinguish between the various categories.

Recommendation: combined role

In practice, 90% of all CIAs combine the domains of undesirable behaviour and integrity violations. This is recommended by the Dutch Whistleblowers Authority. The combined role has a number of major advantages. It can be difficult for employees, for instance, to distinguish between undesirable behaviour and integrity violations, as problems can belong to both domains at once, especially when the person reporting the problem is personally affected. In that case, having a single, expert point of contact can be more accessible and more effective. On top of that, it offers CIAs more opportunities to develop and maintain their expertise. It is also cheaper, more efficient and easier to communicate for employers.³

If both domains are combined, CIAs must be extra careful. They will have to assess whether an issue constitutes a complaint or an integrity violation, as that choice will determine the follow-up process. Various legal regimes will be called upon, including several rights that employees can then claim. For a CIA, the combined role is more complex and more demanding, which also makes this position more challenging and primarily suitable for highly educated individuals.

Asking a CIA involved in one of the two domains to add the other ‘on the side’ means taking a major risk, as broadening the scope of the role to include the other domain requires new knowledge and skills, repositioning the CIA within the organisation, and additional facilities. Both the organisation and the CIA in question must be aware of this.



For some of the current CIAs involved in one of the two domains, it could possibly be best to stick to one for the time being. Naturally, that also depends on your own, specific situation. The Dutch Whistleblowers Authority does recommend that organisations look for CIAs who can handle the combined role when appointing a new employee.

³ Dutch Whistleblowers Authority, *The Confidential Integrity Adviser, Current Status and Future Prospects in the Netherlands*.

2

The purpose of confidential integrity advisers

Importance for employers

- **Laws and legislation (OHS, Whistleblowers Act).**
- **Incidents are inevitable, rapid intervention prevents escalation.**
- **Positive effects: financial, reputation, quality.**

Interest for employees

- **Sound employeeship.**
- **Safety and protection.**

2.1 Importance for employer

Research has shown that many employers in the Netherlands already have a CIA.⁴ However, that also means that not all employees in the country have access to a CIA, which they should. It has also been shown that the domains of undesirable behaviour and integrity are not always combined, so there is still plenty of work to be done for employers.⁵ Although this may seem like a major expense, it is in employers' own best interests to invest in these important advisers.

Laws and legislation

Having a CIA is essential for sound employership. Even though appointing a CIA is not set out as a formal requirement in the Whistleblowers Authority Act or the Working Conditions Act, CIAs are gradually becoming crucial for organisations. The Inspectorate SZW, for instance, considers CIAs to be an essential element in an organisation's OHS policy, which is required by law.⁶

The Whistleblowers Authority Act does require that employers with 50 or more employees set up a reporting procedure that gives employees access to a confidential adviser. The Whistleblowers Authority believes that the CIA is the right person for this important role and considers him or her to be an indispensable integrity facility that employers simply must include in their organisation. Although CIAs are currently not a formal requirement, they are indispensable to organisations. It must be said that employers in various sectors are obligated to appoint a CIA due to sector-specific codes and agreements and industry- or company-specific collective labour agreements.



No organisation is too small to appoint a CIA. Even in organisations with fewer than 50 employees, CIAs can have a major effect!

⁴ Dutch Whistleblowers Authority, *Reporting procedures and integrity measures implemented by Dutch employers*

⁵ Dutch Whistleblowers Authority, *The Confidential Integrity Adviser: Current Status and Future Prospects in the Netherlands*

⁶ Ministry of Social Affairs and Employment (2018), p. 5

Quick action

In all organisations, it is possible for something to go wrong. Unfortunately, the risk of integrity violations is typically severely underestimated: they are more common than management usually realise. Research shows that in 2014, at least 1 in 5 employees had had suspicions of wrongdoing (that harms the public interest) in the past two years: 28.8% in the public sector and 21.5% in the private sector.⁷



The more severe the wrongdoing, the more difficult it will be to remedy. However, most problems do not simply crop up from one day to the next: they often start as minor incidents, which snowball when the organisation fails to tackle them. Moreover, wrongdoing is contagious. And the longer a particular problem persists, the greater the chance that the media will set their sights on it.

Long-term, large-scale integrity violations have the potential to wreak havoc. Financially speaking, it leads to expenses incurred for investigations, ad-hoc measures, fines and damages. Besides, it will damage an organisation's reputation among its customers, citizens and other stakeholders, and in particular among its own employees, who will become demoralised and scared, start to put in less effort, call in sick or look for another employer. It is therefore worthwhile to intervene quickly and nip any problems in the bud.

Employee reports can be a valuable tool in identifying and solving problems quickly, which is why it is important to make reporting problems as safe and easy as possible.⁸ Employees will not have the courage to report wrongdoing (that harms the public interest) until they can clearly see that the organisation handles their reports properly. First and foremost, this means that reporters must never suffer negative consequences as a result of their actions. Organisations should seek to create an atmosphere in which reports of wrongdoing are applauded and welcomed, rather than perceived as a threat. Respond quickly and adequately to each and every report. It is important to realise, though, that this does not only make demands on your reporting procedure, but also on how carefully your organisation handles the follow-up process.

For an effective reporting system that employees feel comfortable with, the role played by a CIA is absolutely crucial.⁹ A good CIA minimises report dropout and improves the quality of reports that are made, allowing employers to tackle problems quicker and better.

Positive effects

Reports may have a negative connotation, but empirical research has shown that organisations that respond well to reports of problems within the organisation are more successful and more profitable.¹⁰ This is not surprising. After all, organisations that

⁷ Maas et. al. (2014)

⁸ See Dutch Whistleblowers Authority, *Integrity in Practice - The Reporting Procedure* for more information about improving your reporting system.

⁹ De Graaf (2015)

¹⁰ Stubben & Welch (2018)

have employees who feel invited to report problems can learn from their mistakes. This not only prevents unnecessary expenses and damages, but also helps create a workplace where people trust each other, are more comfortable with each other and do a better job.



CIA's have a positive effect on organisations. They are an investment that yields financial profits and an improved reputation, both internally and externally.

CIA's can also be valuable in situations where employees have doubts about what they are allowed to do or should do. Sometimes, employees may struggle with complicated issues which their teams simply do not have the time or space to discuss. In other situations, employees may not feel safe enough to raise these questions. Besides, many integrity schemes are unknown and difficult to understand.¹¹ The CIA can help employees make the right decisions, acting as a source of information and a sounding board. After all, an ounce of prevention is worth a pound of cure!

In an ideal situation, all integrity issues should be up for discussion.¹² If an organisation offers its employees the opportunity to discuss dilemmas among each other and everyone feels they can speak out about each other's behaviour, they will not have to resort to a reporting procedure in the first place. In such an organisation, violations will be less frequent and those violations that do occur will be detected at an earlier stage. For that reason alone, it can be valuable to give employees plenty of practice with such a system and culture.¹³ A CIA can also make an additional positive contribution by giving training sessions and providing information.

2.2

Importance for employees

It is important for employees that they have access to good confidential integrity advisers. Everyone wants their organisation to be safe and pleasant to work for, and CIA's play a key role in ensuring that this is the case. A CIA is also necessary to ensure sound employership, offering a listening ear to every employee with concerns about a particular matter.

Sound employership

Organisations expect their people to be good employees.¹⁴ They are supposed to contribute to the integrity and proper functioning of the organisation, which naturally means that no employee should engage in wrongdoing (that harms the public interest) but also that they should identify problems and wrongdoing (that harms the public interest) if at all possible. After all, that will help an organisation ward off any further disaster.

Sound employership is also linked to a condition included in the Dutch Whistleblowers Authority Act, which states that employees must first report suspected wrongdoing internally, unless this cannot reasonably be required. Some organisations even

¹¹ De Graaf et. al. (2013), p. 7 and p. 68

¹² Dutch Whistleblowers Authority, *Integrity in Practice: Working on culture*, p. 6

¹³ Karssing (2018), p.285 ff.

¹⁴ Dutch Civil Code, Article 7:611

include mandatory reporting in their reporting procedure, which lets them attach legal consequences to a failure to report wrongdoing. In practice, however, mandatory reporting has little effect on employees when deciding whether or not to report suspected wrongdoing.

Sound employeeship must be facilitated by means of sound employership, however. A CIA makes it easier to report difficult issues, thus supporting sound employeeship.

Safety and protection

A CIA increases employee safety, which, in turn, increases their willingness to report. For an employee, this sense of safety plays a greater part in their decision whether to report issues than mandatory reporting and expectations of sound employeeship.



For employees, the main reasons not to report suspected wrongdoing (that harms the public interest) are:

- A perceived lack of safety.
- Fear of negative consequences.
- The expectation that nothing will come of the report.
- Lack of confidence in the reporting point.¹⁵

CIA's provide a sense of safety because they give employees the chance to discuss matters confidentially. Employees remain in charge of the process,¹⁶ while CIA's give them the space they need to address their dilemmas and concerns. A session with a CIA need not even lead to direct action: in some cases, the conversation alone can provide the relief employees are looking for. Undesirable behaviour and suspected wrongdoing can place a heavy (mental) burden on employees, but having a listening ear to talk to can be perceived as a source of support.

Should an employee decide to take action, CIA's can increase the chance of a positive outcome. Reporting and complaints procedures are often long, complicated and emotionally draining. With a CIA to provide good advice, employees run less risk of suffering negative consequences and are more likely to make the right decision.

The manager is often the first person to receive a report

Many employees first turn to their direct manager when they suspect (that harms the public interest), research shows.¹⁷ At the same time, it appears that managers are rarely prepared for this through training or information sessions, which means that they too can benefit from the knowledge of a CIA. The latter can inform them about the reporting procedure and the dynamics of reporting, the formal steps and informal options, allowing the organisation to quickly imbue any concerned employee with a sense of safety!

¹⁵ Dutch Whistleblowers Authority, *The Confidential Integrity Adviser: Current Status and Future Prospects in the Netherlands*, p. 22

¹⁶ There are limits to the confidentiality of a confidential integrity adviser. For more information, see chapter 5.

¹⁷ De Graaf et. al. (2013), De Graaf (2015), Ethisphere (2018), CEB Compliance & Ethics Leadership Council (2013)

3

Who can be a Confidential Integrity Adviser?

Recommendations:

- As low-threshold as possible.
- Multiple confidential integrity advisers.
- Internal and external.
- Avoid unwanted role combinations.
- Mirror the organisation.

Take the following aspects into consideration:

- High – low.
- Central – decentralised.
- Full-time – part-time.

3.1

Make it easy

Employees often find it difficult to get in touch with a CIA. Make it easier for them by making the CIA as accessible as possible. It is important that the CIA is easy to reach and that employees know they can rely on him/her. To make this happen, the background and position of the CIA are of key importance, as there are a number of roles that cannot be combined with confidential work. It can be wise to take the following considerations into account.

3.2

Personal background

When it comes to confidential work, it is important that employees feel they can connect to the person they are talking to, which means the personal background of a CIA can be very important. It is therefore best to mirror your CIA to the population and structure of the organisation. Provide a good mix of backgrounds, so that all employees are able to identify with someone.

3.3

High – low officials

In order to give both higher-up and lower-down employees a place to go, it is important that internal CIAs come from several different layers and that external CIAs are capable of working with employees from different levels. If employees have someone to talk to who is at the same level as they are, this can be of particular benefit to the sounding board aspect of the CIAs. Make sure that higher-ups also have someone to turn to, whilst watching out not to position a CIA too high up in the organisation. Finally, it is not advisable to only appoint managers as CIAs.

3.4

Central – decentralised

It is important that CIAs are 'nearby', especially in large organisations, as this benefits their visibility and accessibility. Make sure to appoint CIAs in plenty of business units. Preferably, local CIAs are to be supported by an experienced, central CIA, who can

serve as a sounding board, organise training sessions and intervision meetings, and coordinate reports from various business units. If necessary, an integrity officer or compliance officer can also take up this coordinating role.



Internal CIAs typically do not have a full-time appointment. Make sure that employees always have someone to turn to with whom they do not have a direct working relationship. If the CIA is a colleague from the same business unit or a manager in the same hierarchy, this may be a problem, especially for employees looking to submit a complaint or report about their own working environment. If internal CIAs come from various departments, this can make them more accessible.

3.5

Full-time – part-time

Organisations will also have to make a decision as to whether to appoint CIAs in a full-time or part-time position. Will they be 100% committed to this role, or is it just something they are doing ‘on the side’? Internal CIAs typically have a part-time position, which gives them the great advantage of knowing exactly what is going on in the organisation. At the same time, this can put them too close to the organisation to stay at a professional distance. Part-time CIAs will also gain less experience, of course, which means that intervision sessions and training courses are extra important for them.

Undesirable role combinations

Some roles do not combine well with confidential work, because dual roles can make it unclear for employees who they are actually speaking to. In some cases, this can make adequate confidentiality impossible. The Dutch Whistleblowers Authority recommends not combining the following roles with confidential work:

- Most senior executive.
- Member of the Board of Directors, Supervisory Board.
- Member of the Works Council.
- HR officer, legal affairs.
- Compliance officer, integrity officer.
- Reporting centre, internal investigator.

An undesirable role combination can occur if the CIA is also the manager responsible for the employee or business unit involved in a report, for instance. Combining a CIA role with a role in the supervisory board or participation council is also inadvisable, as this may give the person in question access to information that can be connected to their confidential work. Finally, CIAs must never be involved in a report in additional roles, such as in the investigation, the subsequent legal process or potential disciplinary measures.

3.6

Internal – external

Internal CIAs are employed by the organisation and their confidential work often sits side by side with their primary duties. An external CIA is a professional contracted by the organisation. The key advantage of external CIAs is that they are not part of the organisation, which may give employees reason to believe that external CIAs are more autonomous and less vulnerable to pressure from management. External CIAs also tend to have more knowledge and experience, which they can use to support internal CIAs and management. Disadvantages of external CIAs are that employees will not be as familiar with them and that they may not be as aware of what is going on in the organisation.



The Dutch Whistleblowers Authority recommends appointing both internal and external CIAs, as this allows employees to decide who they want to talk to.

3.7

Multiple CIAs

It is strongly recommend to appoint multiple CIAs, as this gives employees the opportunity to approach someone they trust, making the reporting process easier and more accessible. However, it is also in the interest of the CIAs themselves, as it gives them the space to refer matters that are too closely linked to them to a colleague. Besides, it allows for intervision, consultation and assistance in difficult cases. Finally, appointing several CIAs has practical benefits, making it easier to find a substitute if one CIA calls in sick or goes on holiday.

4

What do CIAs do?

Core functions of a CIA

- **Support function: supporting, guiding, informing and advising the potential reporter and other individuals involved in a report.**
- **Information function: informing employees and managers about the role played by a CIA, acting as a source of information on integrity issues.**
- **Signal function: issuing regular reports on conversations, identifying trends and areas of interest, and advising the employer and Works Council on integrity risks.**

4.1

Organisational fit

Confidential work has to be tailor-made: the best way to structure it differs from one organisation to the next. Generally speaking, CIAs have three core functions: the support function, information function and signal function. Together, these three functions can serve as a guideline to setting up a specific structure for confidential work in an organisation.¹⁸

4.2

Support function

The CIA is there to give advice and provide support to employees who are experiencing undesirable behaviour, suspect an integrity violation or wrongdoing (that harms the public interest), or are suffering negative consequences after reporting a problem. The CIA can also support employees who are suspected of having conducted an integrity violation or who are involved in a report in some other way, e.g. as a witness.

In most cases, the CIA is there to support the reporter and guide them through the reporting process. This process consists of three distinct phases: the pre-phase, the reporting phase and the post-phase.

Pre-phase

In the pre-phase, a CIA offers a listening ear to employees and provides information about the relevant reporting procedures, regulations, investigation procedures and processes. They also explain the nature of their confidential position in greater detail and tell employees what they can expect. In the first session, a CIA must also address the limits of confidentiality (see ch. 5. Confidentiality and anonymity).

In this phase, the CIA will discuss the informal and formal steps that an employee can take, depending on:

- The nature of the integrity violation.
- The goal of the person reporting the violation.
- Available evidence of the violation.
- The possibilities and risks associated with the various options.

¹⁸ CIAs associated with the National Association of Confidential Integrity Advisers (LVV) must adhere to the LVV function profiles.



CIA's must refer an employee if necessary, such as when the issue goes above and beyond their expertise or professional duties. CIA's can refer employees to professional care providers, legal advisers, external agencies or the advisory department of the Dutch Whistleblowers Authority.

Aid: collecting relevant information for a report

In order to enable the organisation to carry out the best possible investigation, CIA's can use the following questions as an aid:

- Is the report specific and detailed enough?
- Are the contents of the report coherent, unambiguous and in line with other known facts?
- Are there any other reports that may be linked to this report?
- Does the report contain verifiable elements, such as names of employees, dates, locations or specific events?
- How does the reporter get their information?
- Did the reporter witness the violation?
- Are there any documents that support the report?

Reporting phase

In the reporting phase, the CIA guides the reporter through the process of formalising their report. They can assist the reporter in drafting the report, ensuring that it meets formal requirements, and in following the prescribed procedures.

Proper reporting can be complicated, but that is what the legal protection enjoyed by the person reporting a problem depends on. Reporting procedures are often drawn up in difficult legal language, and in some cases there will be several different reporting centres to choose from. The format of a report may also be important. Furthermore, it must be clear to the employer that the report in question is a whistleblower's report. Unfortunately, reports are not always recognised as such, leading the employer to think that the employee in question is 'simply' warning them. It is important that the CIA provide sound advice on this matter.

Confidential adviser as a conduit

The CIA can act as a conduit for the report (see ch. 5. Confidentiality and Anonymity for more information). In this case, they will act as an intermediary, interfacing between the organisation and the employee in all communications. Only the CIA will be aware of the identity of the reporter and will never make this information public. Please note: In some cases, it may be impossible to protect an identity or legally required to break confidentiality. For more information, see ch. 5. Confidentiality and anonymity.

The CIA supports the reporter and guides them through the investigation carried out in response to the report. CIA's are not to provide psychological care, but simply of-

fering a 'listening ear' can be tremendously helpful. Even if the CIA is not closely involved in the investigation, they can still explain what will happen.



It is important that reporters be informed properly and on time. Unfortunately, this is not always the case. Reporters are regularly kept in the dark for long periods of time, which in and of itself can already be very unpleasant. Employers should always keep the reporter informed of procedural developments via the CIA.

CIA's can also provide guidance and support to the person suspected of a violation ('the suspect'), or to other witnesses and colleagues, as they may also be affected by the report. It goes without saying that a CIA who is providing support to the reporter is to refer the suspect to one of their colleagues.

Post-phase

In the post-phase, the CIA provides aftercare. It can be both thoughtful and professionally diligent to check how the reporter is doing after the report. This is especially important because the reporter may only start to suffer negative consequences at a later stage. If this is the case, the CIA will provide support once more and aid the employee in reporting the negative consequences they are suffering, if applicable.

4.3

Information function

The second function of a CIA is to provide information about their role and about integrity issues. This lays the foundation for employee trust and makes it easier for employees to seek out the CIA. The employer and CIA must work together to ensure that employees are properly informed.

CIA role

CIA's can only be effective if employees know who they are and where to find them. Often, however, employees are not as familiar with CIA's as they should be, which is why it is very important to inform them about the role played by a CIA.

Make sure that employees know that there is a CIA in the company, who it is, how and where he or she can be reached and which problems they can help with. It is up to the employer to communicate this information actively and repeatedly, but the CIA must also play an active role. Some CIA's, for instance, ask to be invited to work meetings for an opportunity to introduce themselves.



Tip! Link up with existing infrastructure. Include information about CIA's in the on-boarding package for new employees, set up a link on the intranet and introduce the CIA during introductory courses, or invite them to regular work meetings once a year. Supervisors can also mention the CIA during performance reviews.

More than reports

Employees often do not realise that they can also turn to a CIA with questions that they are struggling with, as well as dilemmas and integrity issues. Moreover, CIAs will be well informed about the organisation's policy with regard to integrity and undesirable behaviour, which means they can help employees make the right decisions by sharing information and talking to them. In other words: the CIA can do more than just provide advice in the context of reports of undesirable behaviour and integrity violations.

Active information

CIAs can play an active role in providing information about integrity and undesirable behaviour through workshops, presentations, blogs or training sessions. Make sure to make clear agreements with the integrity coordinator or compliance officer!

It is also important that managers are not forgotten, as they play a crucial role in encouraging and maintaining a safe working environment. Naturally, managers can also be faced by questions and dilemmas, which means that they too could have a need for confidential advice. On top of that, employees may choose to report wrongdoing (that harms the public interest) to their manager, in which case it will be very helpful if the CIA has already taught them how to handle a report.

4.4

Signal function

The third function of the CIA is the signal function, which goes hand in hand with their special perspective on the organisation. CIAs can boost integrity and safety within an organisation by talking to employees and by identifying trends, risks and developments well in advance.



A CIA is to provide solicited and unsolicited advice to the organisation, both regularly and when the situation demands it, about the atmosphere, work climate and behaviour within the organisation. This offers managers, compliance officers, integrity professionals and the Works Council the opportunity to take action when necessary.

CIAs should also have regular contact with their mandator or functional manager within the organisation (see 6.2.2 Assessment & accountability) to talk about the integrity policy and its development, as well as the CIA's findings with regard to atmosphere, the work climate and behaviour within the organisation. When possible, the CIA should provide specific suggestions for improvement or consult with people in the organisation on developing such suggestions. Employers must give their CIAs the space to respect the confidentiality of their conversations with employees.

Naturally, the CIA is not the only person in the organisation with a signal function, as other officers may also play a role in picking up on worrying trends and developments at an early stage, including compliance, HR, corporate social workers, the company doctor, internal auditors and the Works Council. For a CIA, ensuring good cooperation with these colleagues can be incredibly valuable (see 7.2 Cooperation within the organisation).

Registration and annual reporting

The CIA records all confidential sessions in a secure, digital environment and must issue regular reports (annually, at least) about their findings, though this does not include sharing information about specific cases. In any event, the CIA must report about the number of conversations, the topics discussed and possible themes, trends and signals associated with these topics while taking care to ensure that everyone involved remains anonymous. This report is to be submitted to management and the Works Council.

If the organisation also has a compliance officer or integrity officer, the CIA report can be integrated into a broader evaluation of the integrity policy, which may assess the culture within the organisation and the effectiveness of the body of integrity measures.

Organisations are legally obligated to inform the Works Council about the proper functioning of the internal reporting procedure on an annual basis (Works Council Act 31b). In this case, 'no news' definitely does not automatically mean 'good news'. After all, low report incidence may be a bad sign that indicates employees are not familiar with the CIA or do not trust him or her enough. Possibly, employees may not feel safe enough to report problems, or may be unconvinced that something will be done with their reports.

Some organisations expect the CIA to draw up a broader integrity report, making use of other sources that can explain what is going on in the organisation in terms of integrity and integrity management. Possible sources include:

- Reports submitted to the reporting centre.
- The Risk Inventory & Evaluation (RI&E).
- Outcomes of employee and engagement studies.
- Works council reports.

5

Confidentiality and anonymity

Confidentiality:

- **Core element of the job: offers protection, increases willingness to report.**
- **Also required for other parties involved in the process: reporting centre, internal investigator, reporter.**
- **There are limits to confidentiality: be sure to make clear agreements about this.**

Limits to confidentiality

- **In case of mandatory reporting for certain crimes.**
- **In case of serious organisational or public importance.**

Anonymous and confidential reporting:

- **Anonymous reporting has disadvantages for the reporter and the organisation.**
- **CIA's can act as a conduit for reports.**
- **Unless the reporter and report coincide (in case of complaint or retaliation).**

5.1

Core element of the job

Confidentiality is the core element of the CIA's job. Employees must be able to rely on the fact that they can discuss integrity issues and suspected wrongdoing (that harms the public interest) with the CIA in confidence, trusting that this information and the role they played in reporting it will not be leaked to the organisation.

CIA's must operate based on the core principle of dealing confidentially with all information shared with them. This includes the identity of the employee who decides to turn to the CIA, as well as the contents of the report. This confidentiality will encourage employees to communicate their questions, dilemmas and suspicions, in addition to making it easier and safer to talk about them. On top of that, confidentiality can protect an employee against negative consequences.

It is up to the CIA to carefully maintain confidentiality, which can be difficult. Managers may be very interested in the finer details of the conversations between CIA's and employees and could even pressure CIA's to share such details. Remember to stay firm! Furthermore, IT facilities and reports must be well-secured and, where necessary, anonymised. It is easy to make mistakes, which is why CIA's must remain careful and discreet at all times.

5.2

Limits to confidentiality

CIA's cannot offer absolute confidentiality, as they are unable or not allowed to maintain confidentiality in the following cases:

- In case of mandatory reporting for certain crimes.
- In case of matters of serious organisational or public importance.

In all cases, CIAs must treat all information shared with them with great care, ensuring that they can respect confidentiality as much as possible. This requires assessing and, where possible, categorising information they receive. The organisation must also take steps to protect confidentiality during internal investigations.



Confidentiality is paramount to the CIA. Breaching confidentiality is reserved for exceptional situations and is always done with due care after consulting with another CIA. The reporter will always be informed in advance, unless this cannot reasonably be expected of the CIA.

Mandatory reporting

Some integrity violations and forms of wrongdoing (that harms the public interest) are so severe that every employee is obligated to report this to the competent authority and/or to report it to judicial authorities. The CIA must also abide by these rules.

Article 160 of the Dutch Code of Criminal Procedure (WvSv) states that everybody is obligated to report severe crimes that may jeopardise the safety of the state or the general safety of persons or goods, such as rape, murder and manslaughter. Moreover, an additional duty to report applies to civil servants, as per Article 162 of the Dutch Code of Criminal Procedure, which also obligates them to report corruption, embezzlement and abuse of power, for instance. An extensive flow chart can be found in the appendix to this brochure, along with a list of common ex-officio crimes.¹⁹

As such, CIAs are obligated to report severe crimes and ex-officio crimes (for civil servants). In this case, the CIA must initially inform the employee in question, after which the employee must submit a report to the most senior management of his or her organisation, who must then report it to the legal authorities. Should an employee decide not to act, the CIA will be obligated to inform the organisation, taking care not to disclose the identity of the employee in question if possible.

Usually, the organisation will report the crime to the legal authorities, possibly after carrying out an internal investigation first, as this is an element of responsible employership. The reporter (employee or CIA) may assume that this will be done. The organisation can use its reporting procedure to specify what employees can count on after submitting a report, and how long they will have to wait before they are told whether or not the organisation will be reporting the matter to the legal authorities. For civil servants, the competent authority must inform the reporter of what will be done with the report (of the ex-officio crime) within no more than 12 weeks. If the reporter believes the competent authority is wrong not to report the matter to the legal authorities, it is up to this person to report the matter.

¹⁹ See appendix 2 for a flow chart and a list of crimes in office

No statutory privilege: make internal agreements with regard to privilege

The CIA has no statutory privilege, which is a witness's right to refuse to answer questions asked by a judge. Unlike doctors, lawyers and pastors, professional secrecy does not apply to CIAs. If a CIA is asked questions about what was discussed with the reporter or the identity of the reporter²⁰ in (pre-)legal or complaints procedures, they are obligated to disclose this information. However, organisations can make internal agreements with regard to privilege with the CIA that clearly specify which information must be disclosed.

Serious organisational or public importance

Confidentiality is the core principle underlying the relationship between the CIA and the reporter. In exceptional circumstances, however, the CIA may decide to breach this confidentiality, based on an estimation of the severity of the situation and the plausibility of the suspicion. This can happen in matters of life or death, for instance. In this context, appeals are made to the CIA's conscience, which is a difficult, subjective measure.

We recommend that a CIA first consults with a fellow CIA before breaching confidentiality, as doing so will also have consequences for other CIAs and future reports. Preferably, clear agreements with regard to breaching confidentiality must be made between the employer and the CIA in advance. This is in everyone's interests, from employees to reporters, and from the organisation to the CIA.

Confidentiality during and after internal investigations

During the entire reporting process, the ensuing internal investigation and the conclusion thereof, it is important for everyone involved in the process to treat the identity of the reporter as confidentially as possible. After all, this is required by law.²¹ On top of that, employees who decide to speak up about a particular issue often end up in a vulnerable position. Confidentiality can protect them from negative consequences.

Proper investigation procedures are based on the principle of confidentiality: the identity of the reporter (and of the suspect in question) is only shared with those people who need the information to properly carry out the investigation. The same applies after the investigation has been completed: only those people responsible for taking follow-up actions (disciplinary or corrective measures) will receive the confidential information they need to carry out their duties.

²⁰ This applies to CIAs who are members of the LVV, for instance, as they are covered by the general complaints procedure of the LVV.

²¹ Dutch Whistleblowers Authority Act, art. 2d.



Everyone involved in a report or internal investigation is expected to act discreetly and confidentially. This applies to the CIA, internal investigators, and all other people involved. Importantly, this includes the reporter! After all, breaching confidentiality will not just put the reporter in a vulnerable position, but also see the reporter lose their legal protection if their lack of discretion and confidentiality means that the internal reporting procedure was not followed correctly. It is important that CIAs point this out to employees reporting an issue.

Not all organisations are well prepared for reports and internal investigations. It is important that both the reporter and the CIA have faith that the organisation will address and handle reports properly, confidentially and effectively. CIAs must base any advice they give to a potential reporter on their confidence in the organisation, and the same applies to deciding whether or not to breach confidentiality. CIAs who do not have faith in the organisation will be less inclined to take such a step, as it will put them at risk and potentially jeopardise the employee who came to them with the report in the first place.



It is highly recommended that employers develop and establish an investigation protocol in advance. Identify which officers are involved in such a procedure, determine their roles and decide which information they will need. This increases the chance that reports will be handled carefully and confidentially.

Provide sound information about the limits to confidentiality

Many employees believe that CIAs can offer absolute confidentiality. Although this is a core principle underlying the job of a CIA, it is not always possible. If employees are not told about these limits until they come to the CIA, this will be detrimental to the process. In some cases, this may even cause employees to lose faith in the process, which is why it is best to pro-actively communicate the limits to confidentiality well in advance. This can be done through presentations and information on the intranet, for instance, but it remains important for CIAs to mention it explicitly during the first session.

5.3

Anonymous and confidential reporting

CIAs will frequently have to deal with the concepts of anonymity and confidentiality: these are not the same. In case of an anonymous report, the identity of the person behind the report is unknown to the CIA. In case of a confidential report, the CIA may be aware of the identity of the reporter, but he or she will keep the identity from the rest of the organisation.

Some employees prefer anonymous reporting, though this is usually not in the best interest of the organisation. However, CIAs can still keep the identity of the reporter a secret and act as a conduit for the report. This is called confidential reporting.

Anonymous reporting

In case of an anonymous report, no one knows who the reporter is. People who choose to stay anonymous are generally afraid of the consequences that the report may have. That fear can be justified, as reporters may suffer retaliation. At the same time, however, true anonymous reporting is difficult, as reports can often be traced back to a source with the help of internet data associated with a report or the mere fact that the topic of the report could only be known by a small number of people.²² Moreover, employers cannot protect a reporter against negative consequences if they do not know the identity of the reporter.

In practice, anonymous reporting often hampers the investigation, as direct contact between the reporter and the investigators can help the latter judge the merits of a report. What exactly did the reporter witness? How long has this been going on? Did they witness it themselves, or were they told by someone else? Are there witnesses? Is there anyone else involved? It is often necessary to ask these questions in order to determine whether a report is specific enough to merit an investigation. Anonymous reports often fail to lead to internal investigations, because they preclude verification.

It is possible for employers to offer their employees the opportunity of anonymous reporting while still allowing for communication with the reporter, such as through a website or call centre operated by a third party. This medium can allow the reporter and the organisation to communicate with one another without forcing the reporter to disclose his or her identity. In this case, the internal reporting procedure must specify carefully how and when this can be done.

Make sure that reporters later have a way to prove that it was them who reported the matter and that they followed internal procedures in doing so! After all, there is always a chance that the identity of the reporter is made public despite everything. In that case, it is important that the reporter has written evidence of the report in order to ensure legal protection.



The Dutch Whistleblowers Authority does not allow anonymous reports of wrongdoing (that harms the public interest): the identity of the whistleblower must always be known before an investigation can be started. The DWA can, however, provide advice to people who wish to remain anonymous. Visit www.huisvoorklokkenluiders.nl for more information on how to get in touch with the DWA.

²² One of the options is submitting a report to the Foundation for Anonymous Crime Reporting (Stichting Meld Misdaad Anoniem), an independent reporting centre that allows reporters to share information about serious crime, as well as fraud and corruption.

Confidential reporting through the CIA

As mentioned before, employees can sometimes report issues confidentially through the CIA, who then acts as a conduit for the report and interfaces between the organisation and employee. In that case, the CIA will protect the identity of the reporter.



Confidential reporting via the CIA is the starting point, but there are limits to confidentiality. If the CIA has a duty to report or experiences a crisis of conscience, he or she may breach confidentiality. In addition, the identity of the reporter/complainant must also be shared when the reporter and the report coincide (in case of a complaint or report of retaliation).

Confidential reporting offers a clear advantage to reporters, in that their identity will only be known to the CIA. The organisation and internal investigators will then turn to the CIA with a wide range of questions about the report, who will have to make sure that he or she does not inadvertently give up the identity of the reporter.

Example: identity discovered by accident

Protecting the identity of a reporter can be difficult. Suppose the CIA is asked when the reporter first became suspicious and shares the fact that it was in a certain meeting on a particular date. That can be too much information! If that meeting was only attended by a small number of people, it will not be difficult to discover the identity of the reporter. Constant vigilance is required if the reporter is to rely on the professionalism and expertise of the CIA!

Reporter and report coincide

In some cases, the identity of the reporter cannot be separated from the core details of the report, as is the case with complaints about undesirable behaviour and reports about retaliation. After all, the issue at hand is directly linked to the reporter: the reporter and the report coincide.

Naturally, employees can turn to a CIA to discuss the matter in confidence, who can then offer a listening ear and practical advice. If the employee wishes to submit a formal report, however, the CIA will not be able to keep the employee's identity from the investigators, as it would be impossible for them to investigate the merits of a particular report or complaint without this information. In case of complaints and reports about retaliation, CIAs cannot act as a conduit.

Distinction between ‘complaint’ and ‘report about retaliation’

Employees who decide to report wrongdoing (that harms the public interest) are legally protected against the negative consequences reporters may suffer as a result, including dismissal or involuntary transfer. Employers are not allowed to disadvantage the employee in question and must ensure that other employees do not do so either, such as by bullying, ignoring or intimidating them. This protection against retaliation is not limited to a certain period of time, but in some cases it can be difficult to distinguish retaliation from undesirable behaviour. Make sure to clearly specify the difference between complaints and retaliation!



It may happen that CIAs are in contact with several employees about the same problem at the same time. If none of these employees is willing to report, the CIA might still opt to inform management of the issue at hand, though they must be careful to thoroughly anonymise such a report!

In case of integrity violations and wrongdoing (that harms the public interest) in businesses, CIAs are generally speaking able to offer a greater degree of confidentiality, as these reports do not, in principle, concern the reporter. This allows the CIA to act as a conduit for the report, thus protecting the reporter’s identity. It will, however, benefit the thoroughness of the investigation if the investigators can communicate directly with the reporter. In such a situation, it is best if the organisation continues to protect the identity of the reporter.

6

What do CIAs require?

Preconditions for an effective confidential position:

- Define policy with regard to confidential work.
- Integrate CIA into broader policy.

Preconditions for confidential work:

- **Employment:** appointment, accountability, assessment, termination.
- **Facilities:** consultation room, ICT, access to information, time, resources, training.
- **Formal agreements:** confidentiality, internal privilege, legal protection, reporting paths.

6.1

Start with policy

CIAs can make a major contribution to an organisation, but they will not be able to do so if there is no connection between them and other measures that promote safety and integrity. The confidential position is not an isolated one: it must be linked to an organisation's OHS and integrity policy. The Code of Conduct, reporting procedure, investigation protocol and RI&E, for instance, must all refer to the role of the CIA. For more information, see ch. 8. Link with OHS and integrity policy.

Before an organisation can start with confidential work, they must have policy in place, and before an organisation appoints a CIA, they must ensure they have the right infrastructure, requiring a deliberate, well-considered approach.



Establish policy with regard to confidential work. What is expected from a CIA? Which facilities do they have at their disposal? What conditions apply to confidential work? Good policy allows CIAs to operate more effectively, more accessibly, and more reliably, in addition to protecting the CIAs themselves!

This brochure has already addressed a number of key policy decisions: Should an organisation opt for internal or external CIAs, or both? Should an organisation appoint a single CIA for both domains – undesirable behaviour and integrity – or divide these tasks between several CIAs? What functions does a CIA have in an organisation?

This chapter will discuss a number of other preconditions for an effective confidential position, such as clarity with regard to how CIAs are appointed and assessed. CIAs also have to have a number of practical facilities at their disposal, such as a suitable consultation room, IT resources and access to information. Finally, there must be clear agreements in place with regard to confidentiality, privilege and legal protection.

6.2

Appointment

Confidential work is not something an employee can just 'do on the side'. After all, a good CIA must have certain qualities (see ch. 7. What is asked of a CIA?). It is therefore in everyone's interest to pay careful attention to these qualities during the recruitment and selection of a new CIA. Moreover, confidential work within an organisation can be vulnerable. When appointing a CIA, make sure to pay attention to the following factors.

Application process and appointment

'Being a good listener' is not a sound reason for asking an employee to become a CIA. Naturally, it is a precondition for being good at the job, but other qualities are also required. It is therefore wise to set out a formal application procedure for a new CIA.

This has the added benefit of clearly demonstrating that the organisation takes confidential work seriously. In addition, it provides clarity about the tasks, knowledge and qualities required of the CIA. The application procedure and the preparation it requires will help both the organisation and the candidates reflect on the requirements of the job.



For future CIAs, it can be worthwhile to ask about an organisation's policy during the application process. How does the organisation define confidential work and what is its purpose? Is there an integrity policy? Which (protective) formal agreements are included in the policy?

Assessment and accountability

CIAs can speak to employees autonomously and confidentially, but this does not change the fact they have to account for their actions to a mandator or manager. This is also part of professional confidential work. When a CIA is appointed, it must be made clear who they are to report to, whether that be a mandator or a functional manager.

CIAs can turn to their functional management for consultation, guidance and assessment, which is to take place on a regular basis, following the job description and other agreements made at the start of the contract. Furthermore, the functional manager is responsible for enabling the CIA to do his or her work properly by giving them access to the required facilities and specifying the required scopes and agreements.



Please note: The role of the functional manager can lead to (apparent) dual roles, especially if this person is the general director or someone in HR or the legal department. Preferably, the functional manager should be a central CIA, an integrity officer or a compliance officer, but it should in any case be made clear that the CIA can work autonomously and confidentially.

For internal CIAs, it is possible that their functional manager is not the same person as their 'regular' hierarchical manager. Make sure that their hierarchical manager is also well informed about the confidential work done by the employee in question, as they have to take additional roles, such as CIA, into consideration when assessing the employee's regular work. Practical agreements must be made about how much time will be spent on which of the employee's activities.

Clearly specify a mandator for confidential work within the organisation. Employees with complaints about the CIA are to report to this person, rather than the CIA's hierarchical manager. It is also important to find the right point of contact for all other integrity professionals.

Termination

The position of a CIA can be vulnerable, as they often have access to sensitive information due to their conversations with employees. Reports can lead to resistance and commotion within an organisation, which may ultimately lead to the dismissal of the CIA. Even if nothing serious is going on behind the scenes, the termination of someone's job as a CIA can cause employees to start asking questions. As such, it is very important that this part of the confidential work in an organisation is also organised properly.

There are various reasons for which an employer may decide to terminate a CIA: their work may not be up to scratch, for instance, or they may not be able to win the trust of the organisation's employees. However, CIAs should never be dismissed for being 'difficult', which is why it is important to make clear agreements about how confidential work is to be assessed and draw up clear grounds for dismissal when appointing a CIA.



Tip! Involve the Works Council in the assessment process and the start and end of the CIA's appointment.

6.3

Facilities

The CIA needs a number of practical facilities to support his or her effectiveness. Make sure that CIAs have at least the following facilities at their disposal.

Consultation room

A suitable consultation room is absolutely essential for a CIA, as employees must be able to visit them safely, discreetly and unnoticed. The consultation room must be designed with an eye on the confidential nature and sensitivity of the conversations that take place in the room.

ICT

CIAs must have secure ICT facilities in order to record the information shared with them. It is key that no other party, including the employer, be able to view that information. It is also important to consider how employees can communicate with the CIA by e-mail and phone and how the CIA's schedule is organised. All these activities must be able to take place confidentially. Ensure that the CIA has the right tools at his or her disposal to treat information securely!

Access to information

In order to carry out their signal function properly, it can be helpful for CIAs to have access to company reports such as:

- The internal annual report on the integrity policy.
- The RI&E report and the action plan.
- Relevant reports to the Works Council and management.
- Employee surveys (engagement, well-being, integrity perception).

Time and resources

Confidential work takes time. It is important to acknowledge this in advance and to record how many hours a CIA will have for this work in a formal letter of appointment. In everyday practice, however, it can be difficult to combine confidential work with a regular job, as there will be busy days and calm days. Make sure that CIAs always have enough time to do their confidential work properly, even in busy periods. It is best to consult with the CIA's colleagues and hierarchical manager to ensure that this runs smoothly.

Organisations make a financial investment in CIAs, either by asking an internal employee to take up this duty or by contracting an external professional. Organisations must reserve funds for this investment. It is important to make a realistic estimate of the (internal) costs involved, including the costs for facilities, additional training, intervision, resources and professional literature.

Further training

Regular training is a must for CIAs. They must have sufficient budget and time at their disposal to hone their knowledge and skills and to keep these at the required level. This requires access to professional literature, as well as training sessions, workshops, conferences and intervision. Most of this can be organised internally, especially in larger organisations, but the remainder can be facilitated through the trade association of the organisation in question. This has the added advantage of promoting cross-pollination between organisations and the exchange of *best practices*, as well as maintaining a shared level of integrity within the sector.

6.3

Formal agreements

Confidential advisers must be able to assist employees in difficult situations, which can involve dilemmas, violations or even greater problems. All the while, the employee might not know whether the organisation will have an open attitude to comments or reports. Furthermore, many issues are linked to power relationships and financial interests, which means it is important that clear agreements be made between the CIA and the organisation in advance, particularly with regard to confidentiality and autonomy. This will give CIAs the protection they need to offer employees a safe place to talk, which, in turn, will make it easier for employees to approach their CIA.



When appointing a CIA, make agreements about confidentiality, internal privilege and legal protection in e.g. an employment contract or formal job description. Appendix 3 contains a model for this.

Confidentiality and internal privilege

The CIA has no statutory privilege, which means that if a judge asks them about what was discussed with the reporter or the identity of the reporter, they must disclose this information. It is therefore important to make clear agreements with regard to internal privilege: agree that the employer cannot force the CIA to disclose information about employees or their identity. Simultaneously, it is also important to make agreements about exceptions to the rule (See ch. 5. Confidentiality and anonymity).

Legal protection

CIAs are expected to act autonomously, but the fact that they also see the shadow sides of the organisation means that their recommendations or involvement will not always be appreciated. In extreme cases, it can even put the position of the CIA at risk, regardless of their internal or external status.

It is therefore important to provide CIAs with formal legal protection, similar to that enjoyed by employees reporting wrongdoing (that harms the public interest) or by members of the Works Council.²³ However, that is not all that an organisation must offer its CIAs. Only when an organisation has implemented a mature OHS and integrity policy, consisting of clear-cut integrity rules and adequate enforcement, will CIAs feel safe enough to operate freely.²⁴ In such a situation, they will not feel threatened but rather feel encouraged to share their insights.

²³ Article 21 of the Works Council Act protects the legal position of members of the Works Council (protection against disadvantage) and article 7:670 ff. of the Dutch Civil Code protect them from dismissal.

²⁴ Dutch Whistleblowers Authority, *Integrity in Practice: working on culture*, p. 8 ff.

7

What is asked of CIAs?

The Role of the CIA

- Increased professionalisation, requiring (more) expertise.
- Combines undesirable behaviour and integrity.

Requirements for CIAs:

- **Attitude:** autonomous, honest, careful, sociable, trustworthy.
- **Knowledge:** regulations and procedures, behaviour and integrity.
- **Competences:** communication, proportionality, reflection, advice.

7.1

Professionalisation

The CIA role is becoming more and more professional, with awareness of the complicated nature of this important task gradually increasing. Organisations are being asked to do more to prevent wrongdoing (that harms the public interest), violations and undesirable behaviour, which also increases the pressure on CIAs in terms of attitude, knowledge and skills.²⁵ Moreover, it is now common for the various forms of confidential work to be combined in a single role. As a result, confidential advisers who until now only used to deal with undesirable behaviour or integrity issues are faced with issues they may not be familiar with.

This chapter discusses the key requirements for CIAs. Appendix 1 includes a more detailed job profile, and Appendix 6 offers a tool for evaluating the performance of CIAs.



It is important for all CIAs to develop and maintain expert skills, As such, it is important to organise regular training and intervision sessions, whilst scheduling regular assessments and drawing up a development plan. This will allow CIAs to maintain their knowledge and skills!

7.2

Attitude

Knowledge and skills may be important for CIAs, but attitude comes first. Employees and the organisation as a whole must be able to rely on the CIA to make the right decisions in complicated situations and to give well-considered advice.

CIAs are expected to be autonomous and independent, and act as competent, reasonable professionals while carefully balancing the various interests of the organisation. The CIA must be trusted by employees, but must not lose sight of the

²⁵ Dutch Whistleblowers Authority, *The Confidential Integrity Adviser: Current Status and Future Prospects in the Netherlands*: 'CIAs must do more and be able to do more to develop and maintain expertise and quality', p. 4.

organisation's interests – they must also be trusted by the employer! After all, a lot of their work will initially be hidden from the employer.

CIA's can be expected to be sociable, empathic, accessible people, with an eye for human behaviour and relationships. Apart from that, integrity is of key importance for a CIA.

All in all, CIA's must be authoritative, independent, sensible people capable of distinguishing between different interests, operating in conflict-heavy situations, and detaching themselves from the cases they work on. They must be trusted by their colleagues, whilst maintaining a good relationship with the organisation's management.

7.3

Knowledge

Working as a confidentiality professional requires knowledge about integrity issues, ranging from undesirable behaviour to fraud, corruption, abuse of information and abuse of power. In addition, the job requires insight into and knowledge of organisational culture, and a keen eye for situations that can give rise to unethical behaviour. More specifically, the CIA must have active knowledge of the integrity-related regulations and procedures that apply within the organisation, particularly the code of conduct, reporting procedure and investigation protocol. They must also be familiar with the other agencies, reporting centres, hotlines and service providers employees can turn to, to ensure they receive the best help they can.

In order to keep this knowledge up to date, it is important that CIA's stay informed of new developments, both internally and externally, e.g. by following professional literature, attending conferences and taking part in training and intervision sessions.



Frequent intercolleague contact with other CIA's within or outside the organisation often proves to be extremely valuable, as it gives them the opportunity to discuss matters with their fellow CIA's and helps combat the feeling of loneliness that is commonly experienced in this position. Ultimately, this will benefit the CIA and the organisation.

7.4

Competences

Confidential work requires a number of competences and skills. Above all, it is important that CIA's:

- Are good listeners.
- Remain silent when they have to.
- Ask questions without judging others.
- Know how to get employees to tell a clear story.
- Provide feedback.

If the CIA wants to act as a *sparring partner*, this will also require a capacity for reflection and a sense of perspective, especially when dealing with moral issues and dilemmas. CIA's must give employees enough space to develop their own insights,

balance the various interests involved, and make their own decisions. Furthermore, they must have a good sense of proportionality, as this will allow them to help employees come up with the most effective route towards a solution, whilst minimising the impact on those involved. For instance, sometimes an informal approach with more space for dialogue can be more effective than a formal report. Naturally, this also depends on what the reporter wants to achieve.

To properly fulfil the signal function of a CIA, candidates must have good analytical skills and writing skills, allowing them to interpret the information they have at their disposal and incorporate it into an anonymised report. CIAs must be able to pick up signals with regard to (new) risks, undesirable developments in the organisation's culture and vulnerabilities in the integrity policy, in addition to effectively communicating policy-related signals to management.

Finally, CIAs require good communication skills: they must be capable of communicating actively about their role and of informing employees as well as possible. This means that CIAs must be able to give clear presentations, make compelling contributions to employee meetings and win the trust of employees during training and information sessions.

8

Link with OHS and integrity policy

Embedding confidential work in the organisation:

- Make sure confidential work is embedded in OHS and integrity policy.
- Code of conduct, reporting procedure, investigation protocol.

Cooperation within the organisation:

- HRM: health and safety, integrity, culture.
- Legal affairs: whistleblowing, laws and legislation, enforcement.
- Compliance or integrity officer: the broader policy, integrated approach.
- Reporting centre: assessing reports, internal investigations and measures.
- Works Council: appointment, policy development and reporting.
- Upper management: informing about signals, decision-maker on reports.

8.1

Embedding confidential work

CIAs make an important contribution to integrity and safety in society. More specifically, research has shown that a soundly set up CIA position increases the willingness to report. However, it is also known that confidential advisers can only do their work properly when they are part of a broader OHS and integrity policy: they are, after all, a link in a greater chain. The importance of developing specific policy with regard to confidential advisers was discussed before, but this chapter will address the link between CIAs, policy and the other professionals involved.

OHS and integrity policy

There is no egg of Columbus that will create instant safety and integrity within an organisation. Time and time again, it has been shown that this requires a large-scale, coherent approach, including a wide range of measures. After all, we are talking about the very culture and structure of the organisation, the risks and opportunities inherent in the organisation, as well as its management and employees. Taking an integrated approach to integrity and safety pays, but it does require coordination and assurance. Without these elements, any policy will remain a loose-fitting set of measures that do not reinforce each other and might even counteract each other, or run the risk of being limited to temporary efforts that will vanish as soon as the mood in the organisation changes.

To prevent this from happening, you can establish a formal OHS and integrity policy. This is becoming common practice in more and more organisations. Such policies can include:

- The measures taken.
- The needed budget.
- The people responsible for coordination.
- The methods used to assess their performance.
- Regular modifications.

The foundation of this policy must be based on frequent risk analysis, as this allows organisations to prevent problems from arising which could have been predicted and therefore avoided. CIAs can make an important contribution to this policy, primarily due to their signal function. Conversely, it is also important to pay attention to the role played by the CIA in the documents mentioned above.

Code of conduct

Establishing a code of conduct has become common practice for governments and for many (major or listed) organisations, as it is an element of ‘good governance’. A code of conduct specifies what behaviour an organisation expects from its employees. What behaviour is encouraged, what constitutes undesirable behaviour, and what consequences will this have? Smaller organisations are less likely to have a code of conduct, despite the fact that it can be very useful to have one.²⁶ The code of conduct is an important resource for CIAs, as it serves as a guideline in assessing behaviour and providing advice about dilemmas.



The code of conduct is an important document, as employees with doubts or concerns about a certain issue will most likely consult the code of conduct first. It is therefore best to make sure that the code of conduct refers to the CIA.

Reporting procedure

Since 2016, having an internal reporting procedure has been mandatory in most organisations.²⁷ For CIAs, this is a crucial document, as it describes how employees can formally raise a particular issue, something the CIA should support them in. Increasingly, employees can take their pick from several paths when reporting an issue, with systems including various, parallel channels being considered ‘best practice’.²⁸ CIAs can examine the various options available to the potential reporter and guide them through the process. In many organisations, the reporting procedure is a difficult, highly technical document, which means that a clear reference to the CIA can be an enormous help in giving employees access to the aid and support they need.

Investigation protocol

An investigation protocol is essential for organisations looking to exercise due care in internal investigations. This protocol will provide clarity to the investigators, specifying what, when, who, and how they should investigate. This is particularly important if the organisation does not have a fixed investigation team in place, as this protocol is what will ensure a uniform, consistent approach. Apart from that, such a document will also provide clarity for the reporters and the suspects mentioned in a report. This will let them know what to expect and boost their sense of trust and safety, but of course only if the organisation complies with the protocol. The CIA must be able to explain the investigation protocol, specifying what the reporter can expect, what will happen, and which information will be shared with the reporter.

²⁶ Kaptein (2016), *Leiderschap in ethiek*, Ch. 5

²⁷ Dutch Whistleblowers Authority, *Integrity in Practice: The reporting procedure*

²⁸ Ethisphere (2018), p. 9

The investigation protocol must also describe the role played by the CIA, where necessary. Consider, for example, the situation in which the CIA acts as a conduit for a report. How exactly will the reporter and the investigators communicate in this situation?

8.2

Cooperation within organisation

The CIA position is one of several support positions within an organisation. Particularly confidential advisers combining integrity and OHS policy will have to work with colleagues from different departments. It is wise to develop good working relationships with the colleagues mentioned below (insofar as they are present in the organisation: their roles are often combined in smaller organisations). Cooperation between several support professionals will ultimately allow them to help employees the best they can, and also safeguard the integrity and safety within the organisation.

HRM

Confidential advisers who primarily deal with undesirable behaviour often have a functional relationship with the personnel officer or HR manager. Together, they can discuss the OHS policy and suggest potential amendments to this policy. Generally speaking, the integrity policy, or part of it, also falls within the scope of HR, as it affects how employees are screened, trained and educated, and remunerated, for instance, and may be linked to legal measures. Furthermore, employee culture is usually an area of attention for HR, and CIAs will want to communicate about culture with this department.



CIAs must also remember to stay in touch with the corporate social worker, as this officer will be well-informed about the organisation's work climate, in addition to potential new problems or risks. This is valuable information for CIAs!

Legal affairs

Confidential advisers who are mainly involved in integrity and whistleblowing can be closer to an organisation's legal affairs department, which is concerned with the laws and legislation that apply to the organisation. They are an important source of information for questions about laws, rules and integrity. CIAs can refer employees to this department for questions about 'what is and is not allowed', or gather information themselves. If a report has already been made, CIAs will have to exercise care in referring employees to legal affairs, as this department will often have a role to play in internal investigations or enforcement processes in response to reports. This is another area in which CIAs and legal affairs can meet.

Compliance, integrity officer or integrity agency

More and more organisations have specific departments or officers for integrity and compliance, which is generally where the relevant aspects of HRM and legal affairs meet. This officer or department is charged with drawing up and rolling out the integrity policy, which typically covers both undesirable behaviour and wrongdoings. As such, the integrity or compliance officer is usually the first point of contact and the mandator for CIAs.

Reporting centre

The reporting procedure specifies where employees can report their suspicions. This point of contact, or reporting centre, is a direct representative of the organisation, and once a report has been submitted to the centre the organisation is considered to have been formally informed.



A CIA can never double as a reporting centre! This is because this role and its nature as a direct representative of the organisation conflicts with the principles of autonomy and confidentiality that underly CIAs.

Various officers can act as a reporting centre, such as the secretary of the Board of Directors, the head of legal affairs, the head of HR, the compliance officer and the integrity officer, in addition to people in other positions. The reporting centre is typically also responsible for coordinating an investigation and will, depending on the outcome of said investigation, advise the competent authority (the direct supervisor or management) about possible follow-up, including disciplinary and corrective measures.

The CIA mainly deals with the reporting centre when working on reports and any subsequent investigation. A key responsibility of the reporting centre is to ensure that the reporter stays well-informed of progress made throughout the process, but the CIA can also play a role in this. Good contact with the reporting centre can also help CIAs exercise their signal function. When combined, the reports submitted to the reporting centre and the CIA paint a clear picture of the number and nature of issues within the organisation.

The Works Council

For the CIA to function properly, it is important that he or she is supported by the organisation's employees. This can be guaranteed by discussing the scope of this role and the appointment of a candidate to this position with the Works Council and requesting their approval. Involving the Works Council in this process reinforces the position of the CIA, which will contribute to employee trust in the CIA. As per the Works Council Act, the Works Council has the right of consent for all regulations related to working conditions, including complaints schemes and reporting procedures.²⁹ If the CIA is also part of this scheme, the role and the scope of this role will automatically be subject to the right of consent. The Works Council can also use its right of initiative to submit a proposal to appoint a CIA, or to submit specific areas for improvement with regard to current policy or the current scope of the role.³⁰

²⁹ Article 27 of the Works Council Act, paragraph 1; The approval of the Works Council shall be required for every proposed decision on the part of the entrepreneur to lay down, amend or withdraw:
j. regulations relating to complaints procedures;
m. a procedure for handling the reporting of suspected wrongdoing that harms the public interest, as referred to in Article 2, paragraph 1 of the Dutch Whistleblowers Authority Act.

³⁰ Art. 23 WOR, see also Hoekstra, Talsma & Zweegers (2016)

Upper management

Finally, it is wise for the CIA to maintain a good relationship and stay in touch with upper management, as the board is ultimately responsible for integrity and safety within the organisation. The signal function of CIAs means that they inform the board about undesirable or risky developments. Upper management receives annual reports from CIAs, of course, but direct contact is also worthwhile to help explain these reports and provide effective advice on policy.

It is up to upper management to make decisions with regard to how reports are followed up and which measures are taken. If upper management feel they can rely on the expertise and judgment of the CIA, this will increase the chance that they will take reports seriously. Again, a good working relationship will ultimately only contribute to the safety of employees who decide to submit a report.



Literature

- Dutch Whistleblowers Authority, *Integrity in practice: The reporting procedure*.
- Dutch Whistleblowers Authority, *Integrity in practice: Working on culture*.
- Dutch Whistleblowers Authority, *Reporting procedures and integrity measures implemented by Dutch employers*.
- Dutch Whistleblowers Authority, *The Confidential Integrity Adviser: Current Status and Future Prospects in the Netherlands*.
- CEB Compliance & Ethics Leadership Council (2013), *Key Insights for Compliance and Ethics Professionals*.
- De Graaf, Lasthuizen, Bogers, Ter Schegget & Struwer (2013). *Een luisterend oor. Onderzoek naar het interne meldsysteem integriteit binnen de Nederlandse overheid. (A listening ear. Research into the internal integrity reporting system within the Dutch government)* Amsterdam: VU University.
- De Graaf (2015). What works: The role of confidential integrity advisers and effective whistleblowing. *International public management journal*.
- Ethisphere (2018), *Leading Practices and Trends from the 2018 World's Most Ethical Companies*.
- Hoekstra, Talsma & Zweegers (2016), Integriteit, misstanden en de WOR. Over het drieluik Preventie, Melden & Onderzoek (Integrity, wrongdoing (that harms the public interest) and the Works Council Act. About the trinity of Prevention, Reporting and Investigation), in: Van Halem (red.), *Klokkenluiders en medezeggenschap*.
- Kaptein (2016), *Leiderschap in ethiek (Leadership in Ethics)*, VNO-NCW.
- Karssing (2018), *Als de oplossing het probleem is. Compliance met een moreel kompas. (When the solution is the problem. Compliance with a moral compass.)*
- Maas, Oostdijk, Verheij & Wesselink (2014), *Veilig misstanden melden op het werk (Safely reporting wrongdoing (that harms the public interest) at work)*, Berenschot.
- Ministerie SZW (2018), *Vertrouwenspersonen in arbeidsorganisaties, onderzoek naar de rol en positie van vertrouwenspersonen ongewenste omgangsvormen. (Confidential advisers in labour organisations, a study into the role and position of confidential advisers for undesirable behaviour.)*
- Stubben & Welch (2018), *Evidence on the Use and Efficacy of Internal Whistleblowing Systems*.

More information?

For more information, please consult the following brochures and research reports published by the Dutch Whistleblowers Authority:

Brochures from the Integrity in Practice series:

- The Reporting Procedure.
- Towards an Ethical Culture.
- The Confidential Integrity Adviser.

Exploratory studies:

- Reporting procedures and integrity provisions at employers in the Netherlands (2017).
- The Confidential Integrity Adviser: Current Status and Future Prospects in the Netherlands (2018).

Colophon

The recommendations and insights included in this publication are based on previous exploratory studies conducted by the DWA, scientific research and the experiences of expert confidential advisers. For more information, please visit www.huisvoorklokkenuiders.nl.

Authors: Lucianne Verweij, Jitse Talsma, Alain Hoekstra en Marijtje Zweegers

Editors: Ravestein & Zwart

Design: Lauwers-C

January 2019



WHISTLEBLOWERS
AUTHORITY



Appendices

- 1** Job profile: Confidential adviser 43
- 2a** The Confidential Integrity Adviser and integrity violations; a model 46
- 2b** Flow chart: mandatory reporting and ex-officio crimes 47
- 3** Template: appointing a CIA and recommended agreements 49
- 4** Flow chart: breaching confidentiality 53
- 5** Checklist: report contents 55
- 6** Checklist: CIA assessment 56
- 7** Checklist: elements to include in the annual report 59
- 8** CIA roadmap: from report to aftercare 61
- 9** Model CIA information folder 65

Functions

CIA's have three core functions:

- 1 Support function: supporting, guiding, informing and advising potential reporters and other individuals involved in a report about undesirable behaviour, integrity violations and wrongdoing (that harms the public interest).
- 2 Information function: providing information to employees about the role and duties of the CIA, source of information for integrity-related questions.
- 3 Signal function: issuing regular reports on conversations, identifying trends and areas of interest, and providing the employer and Works Council with solicited and unsolicited advice on integrity risks.

Duties

Support function

The confidential integrity adviser:

- Provides a listening ear to employees.
- Provides information about relevant policy, the relevant regulations, reporting procedures and investigation procedures drawn up by the mandator and the role played by the CIA.
- Discusses the informal and formal paths an employee can take to address unethical behaviour.
- Refers, where necessary, to professional care providers, legal advisers, occupational psychologists, the company doctor, inspection agencies, supervisory agencies, external reporting centres and hotlines, or the advisory department of the Dutch Whistleblowers Authority.
- Guides the reporter through the process of formalising their report.
- Acts as a conduit for the report, if necessary. In that case all communications between the mandator and employee will first pass through the CIA. Only the CIA will be aware of the identity of the reporter and he or she will not make this information public, unless obligated to do so.
- Supports and guides the reporter – or other people involved in the report – during the subsequent investigation. If the CIA acts as an intermediary, he or she will convey any questions that arise during the investigation to the reporter, and vice versa.
- Provides aftercare and supports employees suffering from disadvantage as a result of a report. The disadvantage suffered by an employee for reporting an issue can serve as grounds for a new report.

Information function

The confidential integrity adviser:

- Gives employees at all levels of the organisation the opportunity to reflect on integrity issues, with the intention of helping them to make the right decisions.

- Contributes to employee awareness of the potential role that CIAs can play in this process by giving presentations, organising workshops, writing blogs, using company multimedia, etc.

Signal function

The confidential integrity adviser:

- Remains watchful for signals from within the organisation that may harm safety and integrity. CIAs provide unsolicited and solicited, anonymised advice to those responsible within the organisation when their findings give cause to do so.
- Has – where appropriate – regular contact with organisation’s point of contact for integrity policy and developments of said policy, as well as the atmosphere, work climate and behaviour within the organisation.
- Provides specific suggestions for improvement or consults with people in the organisation on developing such suggestions.
- Keeps records of all confidential sessions in a secure electronic environment.
- Issues regular reports, at least once a year. Reporting frequency and scope will depend on existing forms of monitoring and reporting on the effectiveness of the organisation’s integrity policy.

Job requirements

Attitude and behaviour

The confidential integrity adviser:

- Is a sociable, empathic, accessible person with an eye for human behaviour and relationships, as well as an affinity for integrity in business.
- Seeks to maintain his or her own integrity in the job.
- Operates autonomously without a duty to consult others and acts independently.
- Acts as a competent confidential adviser, taking the greatest possible care to weigh the various interests involved in performance of his duties.
- Is capable of distinguishing between different interests, working in high-conflict situations and detaching him- or herself from the reports.
- Is trusted by employees, whilst maintaining a good relationship with the organisation’s management.
- Deals carefully and confidentially with all information at his or her disposal, including both the identity of the employees talking to him or her and the information they share.

Competences

The confidential integrity adviser:

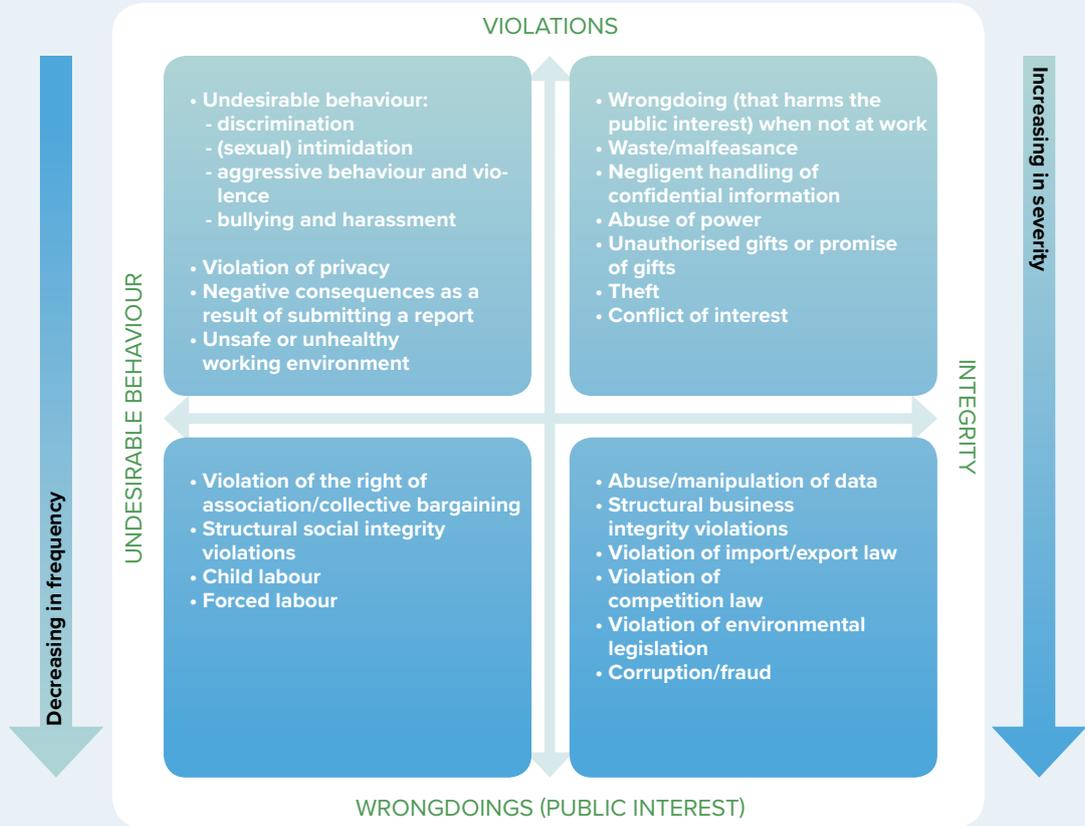
- Has good communication skills in speaking and writing and can communicate with employees at all levels within the organisation.
- Has a good sense of proportionality, as this will let him or her help employees come up with the most effective route towards a solution, whilst minimising the impact on those involved.

- Is capable of reflection and has a good sense of perspective, allowing him or her to balance between sharing relevant knowledge and giving employees enough space to let them come to their own insight with regard to which decision to make after carefully considering the various interests involved.
- Has mastered signalling and advisory skills to effectively provide policy-related advice and to discuss the desired integrity in operations with the organisation's management.
- Is capable of giving compelling, clear presentations that manage to convince the audience.
- Is capable of maintaining an open relationship with various elements in the organisation that are relevant for his or her role, based on mutual trust.

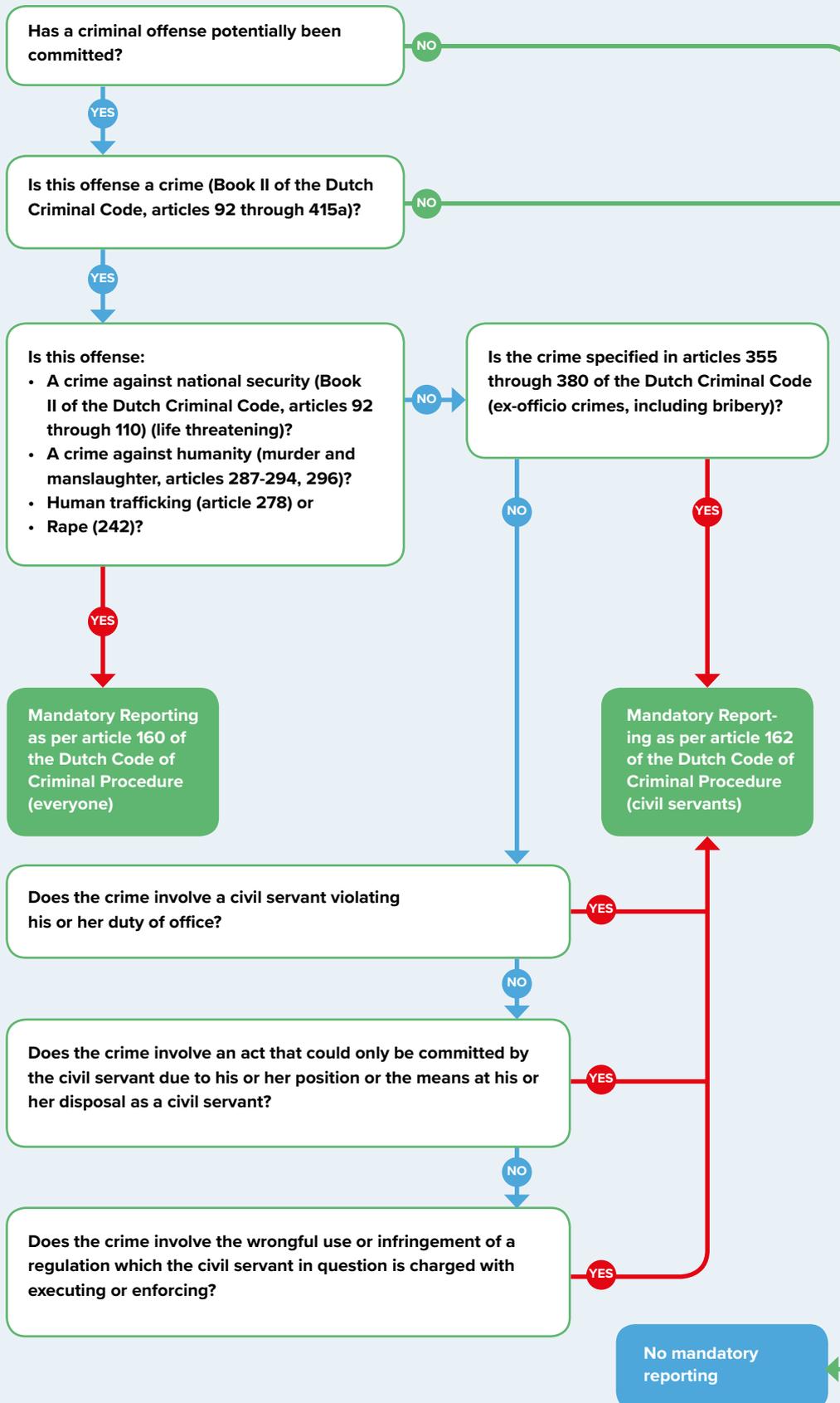
Knowledge

The confidential integrity adviser:

- Stays up to date with the organisation's internal policies, especially the code of conduct, reporting procedure and investigation protocol.
- Stays up to date with undesirable behaviour and integrity issues, such as forms of fraud, corruption, abuse of information or power, etc.
- Stays up to date with the organisation's culture, with a keen eye for situations and processes that may contribute to the emergence of integrity issues.



2b Flow chart: mandatory reporting and crimes in office



1

Ex-officio crimes:

Ex-officio crimes are included in the Dutch Criminal Code.¹ Below is a list of the most relevant ex-officio crimes.

Article	Description
---------	-------------

359	Misappropriation of funds or securities
360	Falsifying books or records
361	Spoliation of evidence
362	Accepting or asking for bribes – without violating duty
363	Accepting or asking for bribes – in violation of duty
365	Abuse of authority through coercion
366	Extortion
367	Aiding and abetting an escape
368	Failure to report unlawful deprivation of liberty
370	Unlawful entry / seizure
371	Unlawful seizure / retrieval of mail
376	Participation in contract work for or deliveries to the employer
379	Registrar performing a bigamous marriage

2

Special duty of office:

This is the case if a civil servant has committed an offense – not constituting an ex-officio crime, as referred to above – in such circumstances or in such a way that committing the offense as in violation of his or her official duty, e.g. a vice detective who is privately involved in child pornography.

3

Crime committed by virtue of position:

This is the case if the civil servant was only able to commit the crime in question – not constituting an ex-officio crime, as referred to above – because of his or her position, and the resources and/or power associated with this position. On top of that, civil servants on duty may find themselves in a position where they would not have been if not for their position. A police officer who is conducting a search for weapons, for instance, and unexpectedly finds money and pockets it, is committing an act of theft that he would not have been able to commit if not for his position (in this case by carrying out a search, which saw him gain access to the stolen good, or by making use of the power invested in him and the opportunity offered to him).

Whether or not the known facts indicate that the civil servant was only able to commit the crime thanks to the power, opportunity or means available to him or her by virtue of his or her position will have to be determined on a case-by-case basis.

¹ Section XXVIII (Articles 355-380 of the Dutch Criminal Code) of Book II of the Dutch Criminal Code, titled 'ex-officio crimes')

External CIAs are formally appointed by means of a contract.¹ For internal CIAs, a letter of appointment will suffice.

The following elements may be included in such a contract or letter of appointment:

a

An outline of the context of the role of the confidential adviser:

[Mandator] wishes, as part of the integrity policy, to appoint an [external/internal] Confidential Integrity Adviser [or plural], operating independently from [mandator], to which employees of [mandator] can turn when they need advice or a sounding board, or when they are confronted with situations in which the integrity of the organisation is at stake, for example as a result of undesirable behaviour or due to suspected integrity violations and other wrongdoing (that harms the public interest) [as specified in the code of conduct used by mandator].

[Mandator] will at all times remain responsible for following and implementing laws, legislation and the integrity policy, as referred to [above].

b

A clear job description

[Mandator] hereby tasks [name] to perform activities as a confidential adviser in accordance with the duties and powers described in the appendix to this [agreement/letter of appointment]

[for a job description, see appendix 1 to this brochure].

c

Responsibilities of the confidential adviser

[in case of an agreement] The confidential integrity adviser accepts these duties and thereby accepts full responsibility for the correct execution of this agreement and the agreed work.

The confidential integrity adviser will remain entirely independent in carrying out the agreed work. He or she will carry out the agreed activities at his or her own discretion, in careful consultation with [mandator]. [Mandator] will also provide general instructions regarding the intended purpose of the work.

The confidential integrity adviser will act as an independent point of contact for employees who are in need of confidential advice with regard to the integrity policy of [mandator] and/or are confronted with and/or have a suspicion of a violation of the integrity policy of [mandator].

¹ Confidential advisers affiliated with the LVV can use the [contract agreement approved by the Dutch Tax & Customs Administration](#). In this contract, the articles including the conditions that are important in determining whether or not the contract constitutes an employment contract have been highlighted. When using this agreement, reference must be made to its reference number. To do so, use the following text: 'This agreement is based on the contract evaluated by the Dutch Tax & Customs Administration on [date], with reference number [number]. The yellow text in the model agreement has been copied directly and has been left unchanged. In our opinion, changes made to rest of the text do not run counter to the text marked yellow.'

Availability

The confidential integrity adviser will be available for [certain amount of time, such as two days a week] to meet employees. In addition, employees will be able to reach the confidential integrity adviser by phone from [Monday to Friday, for example]. If possible, the confidential integrity adviser will talk to employees immediately, or commit himself/herself to responding within 24 hours. This may include a proposal for planning a meeting, or for scheduling a phone appointment.

Confidentiality

The confidential integrity adviser is obligated to keep secret from third parties all confidential information that he or she has obtained in the context of this [agreement/appointment] or from another source, unless obligated by law or a competent government body to disclose certain information. Information is to be considered confidential if the person providing the information has indicated it as such, or if this is evident from the nature of the information.

Conversations and other contact of any nature between the confidential integrity adviser and employees are to be considered strictly confidential.

The confidential integrity adviser acknowledges that it is in the interest of [mandator] to intervene in a timely fashion in case of suspected social wrongdoing (that harms the public interest), as referred to in the Dutch Whistleblowers Authority Act, or in case of suspected crimes covered by mandatory reporting. This means that, should the confidential integrity adviser receive an anonymous report, or should the confidential integrity adviser be given permission to act as an intermediary for an employee, he or she may still share with the mandator the information at his or her disposal insofar as it can not be traced back to the source of the information, provided that the confidential integrity adviser assesses that the information he or she has received constitutes a reasonable suspicion of social wrongdoing (that harms the public interest) and respects the requirements of due care and confidentiality. This enables [mandator] to initiate an investigation and to take corrective and disciplinary measures, insofar this is necessary.

The confidential integrity adviser is also relieved from his or her duty of confidentiality in the event of any complaints, disciplinary proceedings or legal proceedings lodged against the confidential integrity adviser by [mandator] or an employee.

Training

[external confidential integrity adviser] The confidential integrity adviser will ensure that his or her professional skills and knowledge are maintained at his or her own expense.

[internal adviser] The adviser ensures that his or her professional skills and knowledge are maintained. In consultation with the client, the specific work to be carried out by the adviser, as well as the associated resources (time and budget) will be determined each year.

Responsibilities of mandator

[Mandator] will ensure that the confidential integrity adviser is adequately and regularly informed about the organisation's integrity policy and any changes made to it, including changes made to the code of conduct and related processes and procedures, the reporting procedure, the investigation protocol and possibly any other applicable integrity instruments and measures.

[Mandator] will ensure that the confidential integrity adviser is familiar with and has access to the officers who are responsible for and involved in implementing the integrity policy, including the officer/officers who serve as a reporting centre within the framework of the reporting procedure.

[Mandator] commits himself/herself to adequately announcing the appointment of the confidential integrity adviser to employees, as well as specifying what they can expect from the adviser and how he or she can be reached.

The Mandator will ensure that all required resources, as specified below, and all other data and information that are considered to be necessary for his or her duties are provided to the confidential integrity adviser properly, completely and in a timely manner.

Facilities

Mandator shall provide the confidential integrity adviser with a meeting room, in which employees will be able to talk to the confidential integrity adviser with a feeling of security and safety. When determining the location of said room, the mandator shall consider the confidential nature and sensitivity of the conversations that will take place in the room. In addition, the confidential integrity adviser must have access to a lockable archive space.

Mandator will provide the confidential integrity adviser with ICT resources on which information and notes can be recorded, which can in no way be accessed by the Mandator and which make it possible to keep encrypted records of digital information. All ICT measures and information used by the confidential integrity adviser in the performance of his or her duties are excluded from monitoring, with the exception of standard monitoring with regard to the security of electronic traffic.

Mandator is to provide the confidential integrity adviser with access to the intranet, if such a system is in place, and will make agreements with the adviser on which e-mail address and phone number employees can use to contact the adviser.

Documentation

Mandator will provide at least the following documentation to the confidential integrity adviser, immediately after publication:

- Relevant personal and company information required for the job
- Internal quarterly/(bi-)annual integrity policy report
- RI&E report
- Code of conduct
- Reporting procedure
- Investigation protocol
- Other relevant documents required for the adequate performance of the duties and responsibilities of the confidential integrity adviser, as specified in the job description in Appendix 1

Budget

Mandator will provide the confidential integrity adviser with sufficient funds to perform his or her duties properly.

e

Duration of the appointment

The appointment/agreement is entered into for a period of one year and will be tacitly continued for 1-year periods, unless the confidential integrity adviser or mandator indicate that they wish to terminate the appointment/agreement.

After the end of the agreement, the confidential integrity adviser will continue any current, unconcluded support of a reporter (or multiple reporters), unless the employee(s) in question gives/give the adviser permission to hand over the cases to another confidential integrity adviser.

f

Protection of the position of the confidential adviser

The mandator will ensure that confidential integrity advisers do not suffer any negative consequences in the performance of their other duties in the organisation as a result of their position as a confidential integrity adviser. In view of the importance the mandator attaches to having the confidential integrity adviser function independently, he or she is assigned the same dismissal protection enjoyed by WC members. Article 7: 670 of the Dutch Civil Code has been declared applicable by analogy.

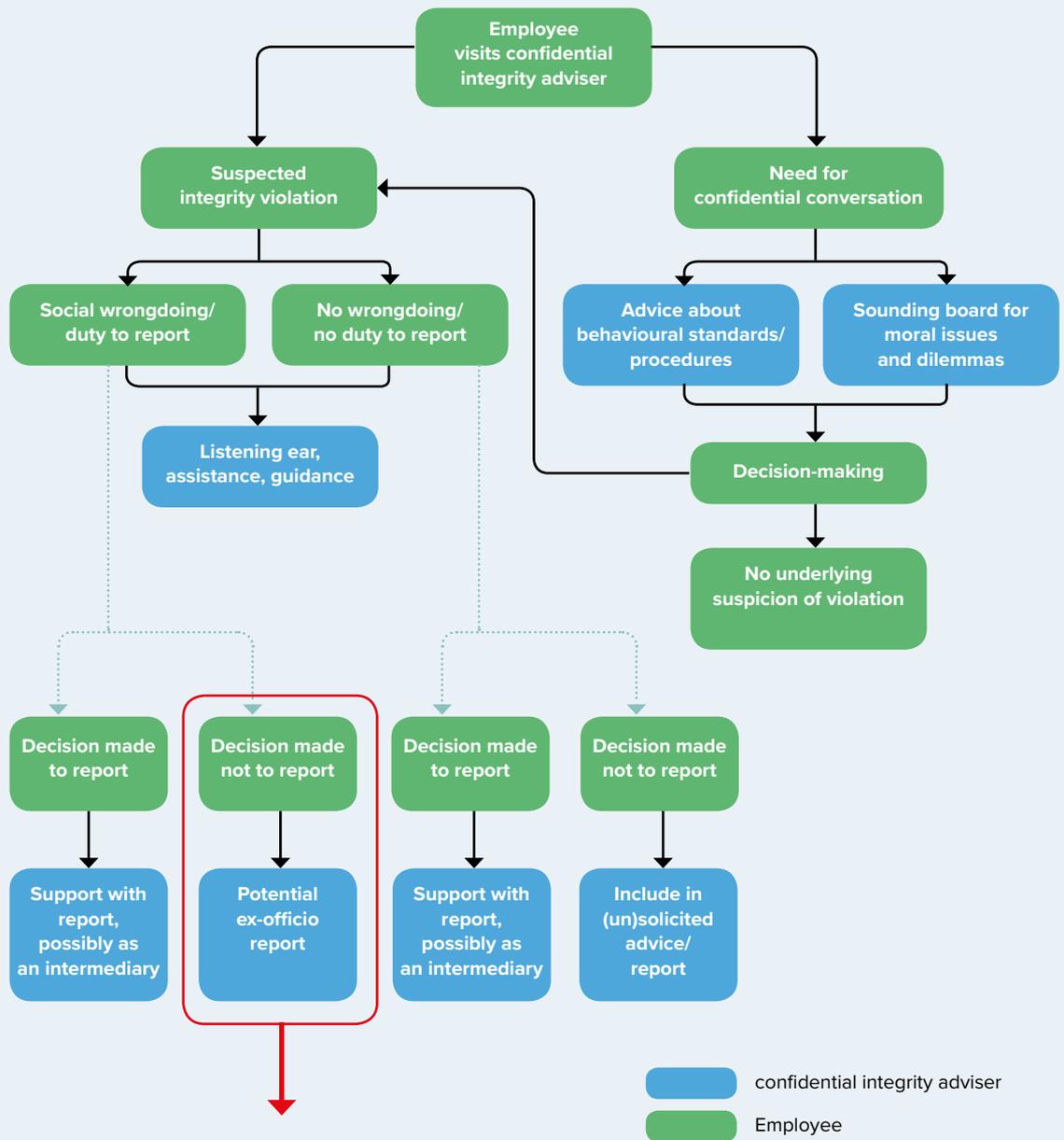
g

Reporting, consultation and evaluation with regard to performance

The confidential integrity adviser will report to [position] in carrying out his or her duties. [Position] and the confidential integrity advisor will [frequently / x times per year] schedule meetings to discuss the general state of affairs, as well as specific matters that require more attention. In addition, [position] and the confidential integrity adviser will meet [...] times per year to assess the latter's performance within the organisation.²

The confidential integrity adviser will submit a report to [position] about his or her activities, the nature and number of contacts with employees, and an evaluation thereof once a year.

² See appendix 7 for a model annual report.



An 'ex-officio report' involves the confidential integrity adviser reporting, from said office, suspected social wrongdoing (that harms the public interest) or a crime covered by a duty to report. The report will only consist of information received by the CIA and will not provide any information with regard to the source. This requires the CIA to be extra careful when making the decision. Questions that may arise include:

A

- Is the suspicion reasonable?
- Is the report specific and detailed enough?
- Are the contents of the report coherent, unambiguous and not contrary to other known facts?
- Are there multiple reports of wrongdoing (that harms the public interest) that could be linked to this report?
- Does the report contain verifiable elements, such as names of employees, dates, locations or specific events?
- How did the reporter get their information?
- Are there any documents that support the report?

B

- Does the investigation procedure guarantee that confidentiality is protected, keeping the source away from harm?
- Is the principle of confidentiality recognised as the core principle of the reporting procedure and the investigation protocol?
- Is this principle actually observed during investigations?

The more questions are answered with 'No', the more difficult it is for the CIA to guarantee due care, which may possibly result in the decision to retract the ex-officio report.

Agreements made with the employer may also have an influence: if retracting an ex-officio report conflicts with these agreements, it is important that the confidential integrity adviser discuss the obstacles keeping him or her from honouring said agreements, such as a lack of confidentiality during the investigation process that jeopardises employee interests, in order to maximise transparency.

The more comprehensive a report, the better an organisation will be able to investigate. Many organisations use a reporting protocol that includes fixed elements, which can then be checked. If this is not the case, a CIA can use the following checklist.

Checklist

- Who is or are involved in the report (as the perpetrator or victim)?
- What happened?
- Where did it take place?
- When did it take place?
- How did it take place?
- How often has it occurred?
- What is the potential scope of the event (expressed in potential damage, number of products, area size, etc.)?
- Is documentary proof or any other evidence available? (note: do not send reporters out to find evidence. This may alarm the alleged perpetrator and possibly falsify or destroy evidence)
- Who else knows about it?

It is also important that the confidential integrity adviser:

- Points out the importance of confidentiality to those involved in the report. They must not talk about the report with anybody else, for the sake of the investigation and those involved.
- Clearly asks those involved in the report to distinguish between facts, assumptions and interpretations, and assisting the reporter in making this distinction.
- Checks with the reporter that the report is complete, or whether more information could possibly be added.

Many organisations work with the following principles with regard to recording reports:

- 'Once it's in the system, it never leaves', to prevent reports from vanishing from the system for whatever reason. This means that if a reporter decides he or she wants to retract the report, this will often not be possible.
- 'Report – Record – Validate'; it is not up to the confidential adviser to validate whether suspicions actually have merit. Confidential integrity advisers are not qualified to do so. It is up to the organisation to validate a report, more specifically trained investigation experts. This will typically take place after the report is entered into the system, for the sake of completeness and due care.

CIA evaluation checklist. Apart from using this checklist, the mandator and CIA may also make specific agreements with regard to particular objectives, such as a given number of presentations in a given amount of time.

In addition to their own experiences, the following sources can be useful for evaluation purposes:

- Assessments completed by reporters after completion of the guidance and assistance process.
- Evaluations with officers and professionals who frequently consult with the confidential integrity adviser, such as WC, HR, legal affairs, the OHS service or the company doctor.
- Responses to specific questions in employee surveys.
- Complaints or other comments, both positive and negative, with regard to the performance of the CIA, made to a CIA or their hierarchical manager.
- Output: reports, written advice, presentations/workshops/training sessions (and participant evaluations thereof).

Functions

The three functions of the confidential adviser:

- 1 Support function: supporting, guiding, informing and advising potential reporters and other individuals involved in a report about undesirable behaviour, integrity violations and wrongdoing (that harms the public interest).
- 2 Information function: providing information to employees about the role and duties of the CIA, a source of information for integrity-related questions.
- 3 Signal function: issuing regular reports on conversations, identifying trends and areas of interest, and providing the employer and Works Council with solicited and unsolicited advice on integrity risks.

Duties

Support function

Is the confidential adviser able to:

- Actively listen to and gain the trust of the employees who turn to him or her?
- Provide information about relevant policy, the relevant regulations, reporting procedures and investigation procedures drawn up by the mandator and the role played by the CIA? Does he or she have sufficient active knowledge of the contents of this policy?
- Provide clarity with regard to the informal and formal paths an employee can take to address undesirable and unethical behaviour, whilst leaving the employee in question in control?

- Referring employees to appropriate professional counselors, legal advisers, or the advisory department of the Dutch Whistleblowers Authority in a timely fashion when he or she is confronted with problems that exceed his or her expertise or job description, or which require others to be involved?
- Guide employees through the process of formalising a report, potentially acting as an intermediary?
- Support the reporter – or other people involved in the report – in such a way that their faith in the confidential integrity adviser remains unshaken?
- Pass on any questions that may arise during the investigation and the answers to these questions in a timely, accurate fashion, taking care to maintain confidentiality with regard to the identity of the reporter in the situation that the CIA acts as an intermediary?
- Provide aftercare and be alert for possible negative consequences as a result of submitting a report?

Information function

Is the confidential adviser able to:

- Give employees at all levels of the organisation the opportunity to reflect on integrity issues, with the intention of helping them make the right decisions?
- Contribute to employee awareness of what constitutes integrity in business in the workplace and the potential role that CIAs can play in this process by giving presentations, organising workshops, writing blogs, using company multimedia, etc.?

Signal function

Is the confidential adviser able to:

- Keep up with the developments within the organisation with regard to policy or culture?
- Be alert to signals from within the organisation that may detract from a safe, pleasant and ethical working environment, to identify these signals and report them to those responsible within the organisation, translating them – where necessary – into concrete suggestions for improvement?
- Maintain an open, constructive working relationship with his or her point of contact within the organisation?
- Fully and accurately record relevant information obtained during conversations in a dedicated, secure electronic environment?
- Draw up effective reports to properly inform the organisation with regard to the status of the implementation and possibly the effectiveness of the integrity policy?

Job requirements

Attitude and behavior

Does the CIA meet the expectations set out in the job requirements with regard to attitude and behaviour?

Competences

Does the CIA possess the competences set out in the job requirements?

Knowledge

Does the CIA have active knowledge in those fields specified in the job requirements?

Workable environment

Policy and communication

The confidential integrity adviser:

- Is informed sufficiently with regard to policy and policy changes related to integrity.
- Has sufficient access to relevant officers within the organisation.
- Has been sufficiently introduced to others in the organisation, so that employees know how to contact the CIA.

Facilities

The confidential integrity adviser has:

- A suitable meeting room to talk to employees.
- Sufficient, suitable ICT support and resources.
- Internet access, and an email address and phone number that can be used by employees.

Documentation

The confidential integrity adviser receives all relevant documentation required for the job in a timely fashion.

Budget

The confidential integrity adviser has sufficient budget and resources to carry out his or her job properly.

Below are several elements that may be included in the annual report issued by a confidential integrity adviser. The depth of the report will depend on other reports issued within the organisation by e.g. the integrity or compliance officer. If there are several CIAs active within the organisation, the scope of the report will depend on the degree of coordination of reporting.

Please note that data collection and reporting must comply with the requirements of the General Data Protection Regulation (GDPR, or AVG in the Netherlands), which includes determining whether a Data Privacy Impact Assessment (DPIA) will be necessary. A DPIA is only mandatory if data processing is likely to pose a significant privacy risk for the people whose data are processed by the organisation. It is up to the person responsible for data processing to determine whether a DPIA is necessary. The DPIA, if applicable, and any other prior consultation must have been completed before data processing can begin. For more information, please visit the website of the Dutch Data Protection Authority.

1

Summary

A summary, highlighting key data and data trends, interpretation of these data and recommendations to the organisation based on the outcome.

2

Data

Possible data elements, potentially broken down by business unit, division, department, location, position, gender (of reporter or suspect):

- Number of requests for advice.
- Nature of requests for advice (requests for information or need for a sounding board).
- Contents of requests for advice.

- Number of reports/complaints
- Nature of reports/complaints.
- Settlement options chosen.

- Number of direct reports (as far as known to the confidential integrity adviser).
- Number of reports in which the CIA acts as an intermediary.
- Number of 'ex-officio' reports.

- Number of referrals.
- Nature of referrals.

- Number of information sessions.
- Nature of information sessions.
- Evaluation of information sessions.

3

Data-based analysis, interpretation and advice

- Comparisons with previous years.
- Comparisons between sites/departments/positions.
- Impact of organisation-specific events, such as a reorganisation.
- Number of completed cases versus number of pending cases.
- Number of questions/reports compared to total population.
- Outcomes of satisfaction surveys (for instance carried out after the completion of the reporting assistance process, e.g. scores/comments made by employees involved in the process).
- Benchmark data with external data (national, sector, or industry data, if available).
- Data compared to input from other relevant bodies (e.g. Works Council or OHS department), or other relevant reports (RI&E, employee satisfaction surveys, etc.).
- Recommendations to management.

4

Activities carried out by confidential adviser

Activities carried out:

- Number of activities.
- Nature of activities.
- Hours spent per activity.

- Training courses and additional training followed.
- Intervention sessions held/attended.
- Budget and expenses.

5

CIA preview

What will next year look like:

- Activities.
- Budget.

The confidential integrity adviser is there to assist and support employees suffering from undesirable behaviour, who suspect integrity violations – ranging from marginal violations to potential social wrongdoing (that harms the public interest) – or who are suspected of an integrity violation. How do you do that? In what follows, we have included a few dos and don'ts for each phase.

In the pre-phase

Introduction:

- Take your time, switch off your phone and computer or make sure they are not in view, be there for the employee(s), indicate how much time you have (if you do not have enough time at that moment, schedule an appointment right away. Make sure not to rush through a session because you do not have the time).
- Reassure people who come to you, allow them to express their emotions. This will contribute to creating an atmosphere of trust and safety, in which potential reporters will find it easier to listen to what you have to say. This, in turn, will make it easier for them to determine what they have to do and who they will need.
- Explain what you can and cannot do as a CIA and specify the limits to confidentiality. It is strongly advisable to explain the role that a CIA can play in advance, indicating what employees can expect from you. When making an appointment, for instance, you can refer to information on the intranet.

Offer a listening ear to the employee(s). What are they bringing to you, what do they want to achieve, what have they already done. This requires active listening. A good mnemonic for active listening is MORE PIES:

- Minimal Encouragers
- Open-Ended Questions.
- Reflective Mirroring
- Emotional Labelling
- Paraphrasing
- I-Messages
- Effective Pauses
- Summary

It is also important to pay attention to **non-verbal communication**. A few tips:

- Ensure that everyone's physical position in the room demonstrates equality.
- Maintain eye contact: mostly with the person speaking, but also make sure to maintain eye contact with other people present.
- Regularly nod your head: show the other that you are listening.
- Posture: stay relaxed, but open. Sit up straight/with a slight forward tilt.
- Pay attention to your facial expressions, your legs and especially your hands: they will betray your lack of interest, nervousness, etc.
- Try to control your 'tics', such as constantly scratching your nose or ear.

- Avoid leafing through documents when someone else is talking.
- Make use of the non-verbal information you receive. Generally speaking, the first session will be highly emotional and very tense.

Provide information to the employee(s). Explain:

- How important integrity is to the company in relation to its objectives, and how this translates into:
- The applicable policy, referring to rules & regulations, and the relevant reporting procedures.

This information – not just the rules, but an explanation of why they are important – can make a big difference for employees, as it can give them the feeling of shared interests. This can make it easier for potential reporters to make the right decision.

Discuss the informal and formal paths an employee can take. It is important to make sure that the employee stays in control as much as possible. One way to do that is to examine:

- The goal of the employee
- The nature of the integrity violation.
- The feasibility of the various potential paths, due to the availability or absence of evidence.
- The possibilities and risks associated with the various options, and how these risks can be reduced.

If your expertise or position does not allow you to solve the problem in question (such as issues related to performance evaluations, reorganisations, labour disputes or private issues), **refer the employee in question to another professional**. The same applies if the problem at hand requires the involvement of other people. Make sure that you know who you can refer to, but remember that the hurdle to turn to another professional can be very high. It is recommended to stay on top of things and, if the employee in question would appreciate it, to introduce them to the right professional in person.

Pay attention to the following when you end the conversation:

- Start wrapping up on time, to avoid running out of time and not being able to end the conversation properly:
 - Repeat what the employee can expect from you.
 - Indicate what you expect from the other person.
 - Make agreements about a follow-up meeting, if applicable.
 - Take the time to finish up your notes and put them in a secure place, if necessary.

During the reporting phase

- You can assist the reporter in **drafting the report**, making sure it meets the formal requirements and follows the procedures prescribed by the organisation. Note that the reporter is in charge and that you, as the CIA, should not do the work for him or her.
- If the reporter is unable to or unwilling to report, he/she could **ask you to report**, in your position as a CIA. In that case, all communications between the organisation and the employee regarding the report, and any subsequent investigation, will first

pass through the CIA, who acts as an intermediary. In principle, the identity of the reporter will remain confidential, unless you have to breach confidentiality.¹ Please note that CIAs cannot act as intermediaries for complaints about undesirable behaviour or a report of retaliation. In those cases, the report and the reporter coincide, which means the identity of the reporter is important for the ensuing investigation.

- **Support and assist the reporter** during the investigation resulting from the report. Reporting can be emotionally and mentally challenging and can have a major impact on a person's working and living environment. Support may consist of offering a listening ear, contributing ideas and providing information about the various possible procedures. Based on your active knowledge of the procedures, you can tell the reporter what they can expect at what time. If you are acting as an intermediary, you might have to convey questions that arise during the investigation to the reporter and pass on the answers to the investigators. Sometimes, theory and practice do not converge. In some cases, the investigation may not follow the timelines or methods set down in the policy, and the informer is not informed of this. You could then choose to support the reporter if he or she decides to take action in response. This involves examining alternatives with the reporter, such as submitting a report to an external authority, an inspectorate, or a supervisory agency. In case of social wrongdoing (that harms the public interest), this could lead you to the Dutch Whistleblowers Authority.
- In addition to the reporter, **other people involved** in a report may also turn to you for support, such as the person mentioned in a report, or witnesses. Being involved in a report can be emotionally and mentally challenging for them as well. Remember that you can only support these other parties if you are not already supporting the reporter. In this case, you can refer employees to one of your fellow CIAs, if possible. If this is not possible, you can point out other forms of support, such as legal assistance.

In the post-phase

- **Provide aftercare** in the period immediately following the completion of the report. Make sure to check in with the person involved, to see how they are doing. If they are suffering negative consequences as a result of the report, talk to them to determine whether this warrants a new report.
- **Make sure that the report is accurate and complete** and keep the file in a safe place. Make sure to comply with the (legal) retention period. When recording personal data, you will have to comply with the General Personal Data Regulation (GDPR, or AVG in Dutch),² which means that personal data may no longer be stored if the basis for storing them has expired. For more information, please visit the website of the Dutch Data Protection Authority.

¹ For exceptions to the rule, please refer to ch. 5 Confidentiality and anonymity.

² For CIAs who are members of the LVV, the retention periods specified in the [code of conduct](#) apply: 'The retention period of completed files is five years, after which the file must be removed from the CIA's archive and subsequently destroyed.'

- **Consider scheduling an evaluation session**, preferably of the verbal kind, with the reporter or other parties involved in the process. Ask them how they experienced the process. This will provide important input to help you determine how you are functioning as a CIA, but can also help the organisation assess the effectiveness of its policy and determine whether any changes must be made.
- In the event that reporters suffer negative consequences as a result of the report, or if reporters choose to report the matter to external authorities, this can be indicated in **unsolicited advice** to the organisation or included in the standard CIA report. This will allow the organisation to discover the gaps between policy and practice. Make sure your reports are sufficiently anonymised!

Interim termination

If you do not believe that you are the right person to assist and support someone – for whatever reason – you have the professional responsibility to stop assisting and guiding them. Should you consider this, you must first discuss it with the employee in question, unless this is not reasonably possible. Try to refer the person in question to other CIAs and/or counselors.

The following text contains elements that can be included in such a brochure, though it must be aligned to the context and house style of the organisation using it.

It is the mission of our organisation to [mission/vision], but we care about more than just our objectives: we also care about how we achieve them. This will enable us to continue to be successful. Now and in the future. That is why it is important that we behave according to the values we consider important and in line with the expectations that society has of us [core values/appropriate behaviour or code of conduct].

We are aware that acting in line with these values/our code of conduct is not always easy in the complex world we live in, which is why we believe it to be important that our employees feel free to talk about situations in which they do not know what to do or doubt the merits of a particular line of action. Talk about it with your supervisors, or with each other. If you feel that certain behaviour is not in line with what we have agreed with each other, mention it to each other. And if you find your comments falling on deaf ears, do not hesitate to report it according to our reporting procedure. This is very important to the organisation, which is why we have various people who can provide support to our employees for whatever reason.

One of those people is our confidential integrity adviser. This brochure explains the role of a CIA and what they can mean for employees.

The purpose of CIAs

Employees can turn to our CIAs if they are looking for confidential advice or a sounding board to help them decide what to do. After all, they may not be sure what to do and what is expected of them in a certain situation, but it can also be the result of a situation in which someone has experienced undesirable behaviour or has a suspicion of behaviour that is not in line with our [core values/code of conduct].

Our confidential integrity advisers are qualified professionals who can assist and advise our employees.

- If it is unclear what type of behaviour is expected in a given situation, our CIA will provide relevant information to the employee in question, or explain where they can find this information. On top of that, employees can always talk to CIAs to determine the best move in a particular situation.*
- If employees have a complaint or suspect unacceptable behaviour, they can turn to our CIAs for support in these difficult, demanding situations. The CIA will help employees make a decision on how best to deal with the situation and, if an employee decides to report a matter, will assist and support this employee during the entire reporting process. If the employee does not want his or her identity to be made public, the reporting procedure states that they can report issues anonymously or via the CIA. We have a preference for the latter, as experience has taught us that it can greatly benefit the effectiveness of the ensuing investigation to return to the original reporter with any questions that may arise. Confidentiality is one of the key principles underlying the investigation, but if employees decide that they simply are not able to report an issue themselves, reporting it via the CIA may be an acceptable alternative.*

Our CIAs

Our organisation has various internal and external confidential integrity advisers, allowing employees to turn to the CIA they trust the most.

Our CIA/CIAs can be found on [our intranet site, our contact directories/etc.] You can also find their availability there, and see how you can reach them. Employees can get in touch with the CIA [from Monday to Friday, for instance] by phone or by email. The CIA will talk to them immediately if possible, but they can also leave a message asking the CIA to contact them.

Confidentiality

Our confidential integrity advisers operate [autonomously/independently] and are, in principle, obliged to treat all information they receive with due care and confidentiality. This means that they are obliged to keep secret all confidential information they receive and that, in principle, they may not do anything with this information without prior consent from the employee in question. When acting as an intermediary for an employee, for instance, they are only allowed to report information they have received if they are given permission by the employee in question, without revealing the identity of said employee.

There are two important exceptions to this rule:

- In case of a reasonable suspicion of a violation of such severity that it may seriously harm the interests of our organisation if we do not investigate this suspicion as quickly as possible and take appropriate measures to prevent or limit further damage. This category includes reasonable suspicions of crimes which the organisation has a duty to report, as well as reasonable suspicions of so-called 'social wrongdoing (that harms the public interest)'. This includes, for instance, cases of large-scale fraud or corruption, environmental offenses, or violations that jeopardise the health & safety of society or particular individuals. In the event that an employee refuses to cooperate with any type of report of such a suspicion, we have agreed with our CIAs that they will report only the information pertaining to the nature of the suspicion in their own name, without revealing the identity or involvement of the employee in question.*
- If the CIA is legally obliged to share confidential information when asked to do so by a judge or prompted by a complaints procedure.*

Complaints

We believe that the support that our CIAs can provide to our employees is an important component of our integrity policy. In case of complaints about one of our confidential integrity advisers, please contact [position/contact information].