

Training on the handling of (suspected) integrity violations for NGO Federatie members: a summary report

By Emily Marr and Sylvia Borren, Governance & Integrity International

This report

This report provides a summary of the training delivered to NGO Federatie members on 12/13 October and 19/20 October by Governance & Integrity International. The training was delivered online over 4 half day sessions, with approximately 24 participants. The training focused on the process of handling reports of integrity violations, as well as how to manage communication around such cases.

This report will not repeat the full discussions that took place within the training but will summarise the main points and principles identified. The Integrity System Guide (Handreiking Integriteit) should be seen as an accompanying document to this report. The report will also identify some of the key areas of concern expressed by the participants. In the annex, a template job description is provided for an integrity officer and for a person of trust (vertrouwenspersoon).

PART 1

Introduction to the integrity system and focus on the repressive apparatus

The integrity system contains 2 pillars: the moral learning process and the compliance practice. Each of these pillars is broken down into two components. In the moral learning process, this includes moral judgement and moresprudence. In the compliance practice this includes the preventive cycle and the repressive mechanism (also sometimes referred to as enforcement).

Moral learning process	Compliance practice
Moral judgment	Preventive Cycle
Moresprudence	Repressive mechanism

The training focused on the repressive mechanism. Please refer to the Integrity System Guide for a more detailed explanation of the 4 components.

The integrity officer (or unit, for larger organisations), is responsible for implementing and managing the integrity system, and reports directly to the highest manager. See Annex for a description of this function.

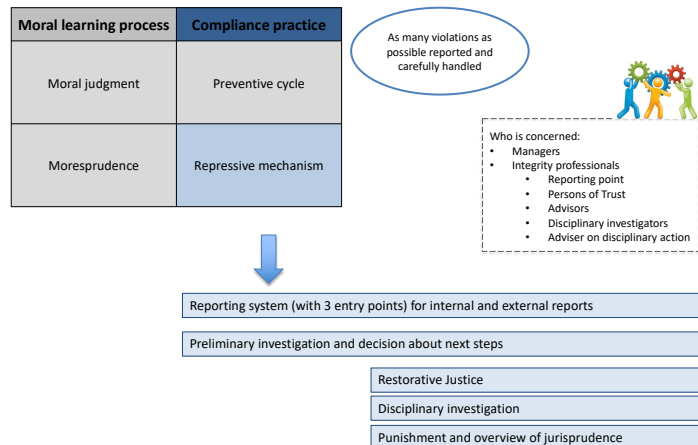
Components of repression: reporting procedure, preliminary assessment, investigation, sanctions and/or other measures, plus roles and responsibilities

The repressive mechanism contains several parts. At the core of the repressive mechanism is the Code of Conduct. The Code defines and describes the behaviours expected of staff by their employer as well as what considered unacceptable behaviour. The code not only expresses the values of the organisation, but is the place where the organisation defines what it considers to be a violation of integrity. We typically identify 4 categories of integrity violation in a Code of Conduct:

- Professional (culpable negligence)
- Interpersonal violations (harassment, sexual harassment, discrimination etc.)
- Misuse of power (corruption, partiality or failing to prevent the semblance thereof)
- Financial (fraud, theft, wastage, misuse of organisational resources etc.)

Although we create these clear categories, we cannot always expect cases to fit neatly into one box. It might often be the case that cases involve a combination of violations.

The repressive mechanism is designed to enforce the Code of Conduct. The repressive mechanism has a preventive effect in that it acts as a deterrent for wrongdoing. It is also the means by which violations of integrity, as defined by the code, can be detected and sufficiently handled by the organisation. The goal of the repressive mechanism is to ensure that as many violations as possible are reported and carefully handled.

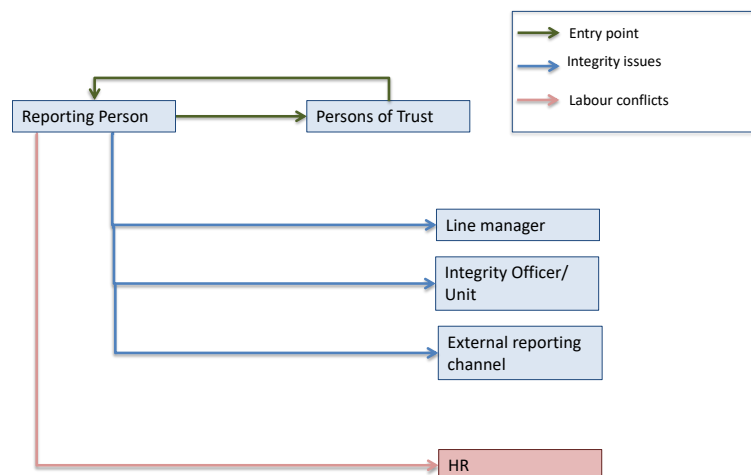


Note: a low number of reports does not a good indicator. Very often, it is an indication that the integrity system is not functioning as it should, and that the organisation is therefore not aware of the violations that might (and most likely are) happening.

The repressive mechanism begins with the reporting procedure. This is the procedure by which individuals (employees, partners, programme participants, members of the public) can report a suspected integrity violation. Here we aim to make the threshold for reporting as low as possible. This means we provide 3 reporting points:

- Through the management line
- Through the Integrity Officer
- Through an external reporting channel

When reports are made to either the management line or the external reporting point, those reports are transferred back to the integrity officer for handling. We advise 3 reporting channels so that reporting persons have options to choose from, but we limit this to 3 and not more because if we create too many channels, it can be confusing for people to know where to go with their concerns, and makes possible that reports simply get lost in the confusion.



Here we identify the key role of the Person of Trust (Vertrouwenspersoon, see Annex for a description of this function). This person has a very important and special role in the system. They provide the entry point. This is a person to whom you can go to discuss your concerns or suspicions and to receive advice about which options are available to you in the integrity system for reporting this suspicion. Should you proceed with a formal report, the Person of Trust can accompany you through the process to provide support and help you understand

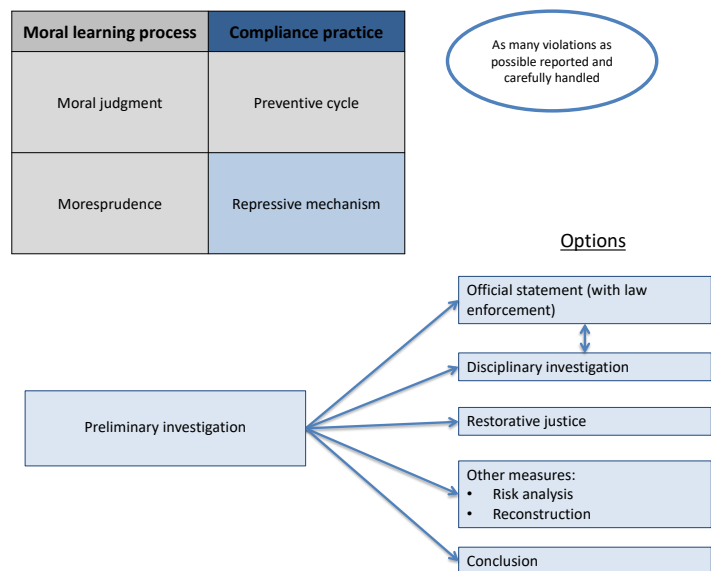
what to expect. (A person of trust may also support an accused person through the process in a similar way. But of course a person of trust cannot serve both parties in a case.)

The Person of Trust must be a separate role from the Integrity Officer. This is because we need to offer people the opportunity to discuss a concern in full confidence with someone who understands the integrity system, but to retain the option to walk away without making a formal report. The Person of Trust may not take an action in those instances (unless legally obligated to do so). Their role is to listen, to think through the case together and to explain the options available. An Integrity Officer cannot fulfil this position. If the Integrity Officer receives a report, they are obligated to take (some) action.

The Person of Trust is a vital position in maintaining the low threshold for reporting. Historically (or traditionally) the role has focused on Interpersonal Violations. However, it is necessary for the integrity system to be centralized and deal with all integrity violations in one place, rather than in silos. Therefore, we advise that persons of trust should be trained to deal with concerns about all four categories of integrity violations.

The reporting system needs to be accessible to and trusted by those it is intended to serve. This means that if we want to make it possible for programme participants and/or community members to report, we need to make sure that there is a reporting channel available to them that is both accessible in the given context, and that is safe and trustworthy. That could involve options ranging from an email address, postal address, phone number, comment box in the community/office, or community members/leaders/persons of trust in the community themselves acting as an entry point to the reporting system. The key is to decide which tool is most likely to achieve the objective of ensuring as many violations as possible are reported. In communities where 'integrity systems' are not common practice, that will require some experimentation of adaptation to the context to find the right solutions.

Once a report is received by the integrity system, it is assessed. If it is not about an integrity violation or issue, it is diverted out of the system to the appropriate place. (Most often this is the case with labour conflicts, which should be diverted to HR.) If the report is about a possible integrity violation, the integrity officer decides whether or not a preliminary investigation is warranted. The preliminary investigation can indicate whether or not a disciplinary investigation is needed, or whether other measures might be needed. A disciplinary investigation can lead to disciplinary action (punishments or sanctions), and/or made lead to alternatives such as restorative justice, mediation etc. In the following section these stages are indicated.



Stages of handling a report

1. Assessing a report

As above, assessing the report is the first important stage. Here the Integrity Officer identifies whether the report is about an integrity violation, in which case it is to be handled by the integrity system, or if it is about something else, in which case it should be diverted to the proper place.

2. Preliminary investigation (and a protocol)

If the report is deemed to be about an integrity violation, then a preliminary investigation is conducted. It is essential that at this stage integrity officers limit themselves only to clarifying the report – we are not yet investigating. We have not yet decided whether we should investigate. Our objective is to answer a set of questions which will help us to take that decision. The following questions are a guide:

- If proven, would this behaviour constitute a violation of integrity (according to the code of conduct)?
- How severe would it be?
- How culpable would the accused person be?
- Are there sufficient options to investigate? What could the sources be?
- What would the possible outcomes of an investigation be?
- What would the damage of an investigation be?
- Does the need to investigate outweigh other concerns?

At this stage we may talk with the person who made the report to ask for clarifications. We may also review any readily available documentation that is relevant to the case. Finally we may, in certain circumstances, talk with others who are aware of the case and who have indicated that they are willing to talk. However, we must not 'interview' these people, or approach others who do not know about the case, and we must not yet actively seek evidence that is not readily available.

On the basis of a preliminary investigation, the Integrity Officer advises the decision maker (highest manager, see below), about whether or not a disciplinary investigation is needed, or whether other measures are more suitable. The decision maker decides whether to follow this advice. (If they decide not to, they must have good reason for doing so.)

A preliminary investigation is essential because it prevents organisations from conducting disciplinary investigations that are actually unnecessary.

3. Managing disciplinary investigation

If a disciplinary investigation is required, this should be carried out by a trained professional. Sometimes this can be the integrity officer. Sometimes, if cases are more complex or require specialist knowledge, it might be necessary to bring in an external investigator.

It is vital to clearly define the investigation question, the mandate of the investigators and any limitations, as well as a budget for the investigation. That is particularly true for external investigations, which can be necessary sometimes but can also be very costly. They therefore need to be carefully managed.

It is highly recommended that the organisation develops an investigation protocol, on the basis of which due process can be ensured. The protocol should indicate roles and

responsibilities, mandates, principles, and specifics about investigation options. For example:

- under what circumstances should interviews be conducted and how those are documented
- when does the accused person have the opportunity to respond
- when can other evidence such as personal communications or devices be searched and under which circumstances

The outcome of the investigation should be a written report which indicates whether or not the behaviour occurred as it was reported, and if so, whether it is considered an integrity violation. It should also make an indication of the severity of the violation, and the culpability of the person concerned.

If not conducting the investigation themselves, the integrity officer is responsible for overseeing the process.

4. Proportional punishment

Together with the outcome of the investigation, the integrity officer must provide the highest manager with advice about whether or not (proportional) punishment is necessary, and what that might be. A labour law specialist must be consulted in providing this advice, so that it is compliant with local law.

It is of the utmost importance that the punishment is proportional. Primarily, that is because the goal is to develop a just system that delivers sanctions or punishments that are appropriate.

But secondly, it is necessary to understand the effect that disproportionate punishments have. Punishments that are seen as too light serve to discourage people from reporting to the integrity systems because they lose confidence that the system will take sufficient action. But punishments that are too heavy also have a discouraging effect – if an employee believes that their colleague will be too harshly punished for their behaviour, they will be more reluctant to report to behaviour. Neither of these are in the interests of the integrity system. G&I therefore strongly advise against ‘setting an example’ and policies of ‘zero tolerance’. (Instead we favour an approach of zero-tolerance for inaction.)

Moral learning process	Compliance practice
Moral judgment	Preventive cycle
Moresprudence	Repressive mechanism

As many violations as possible reported and carefully handled

Basics of a procedure for determining punishment

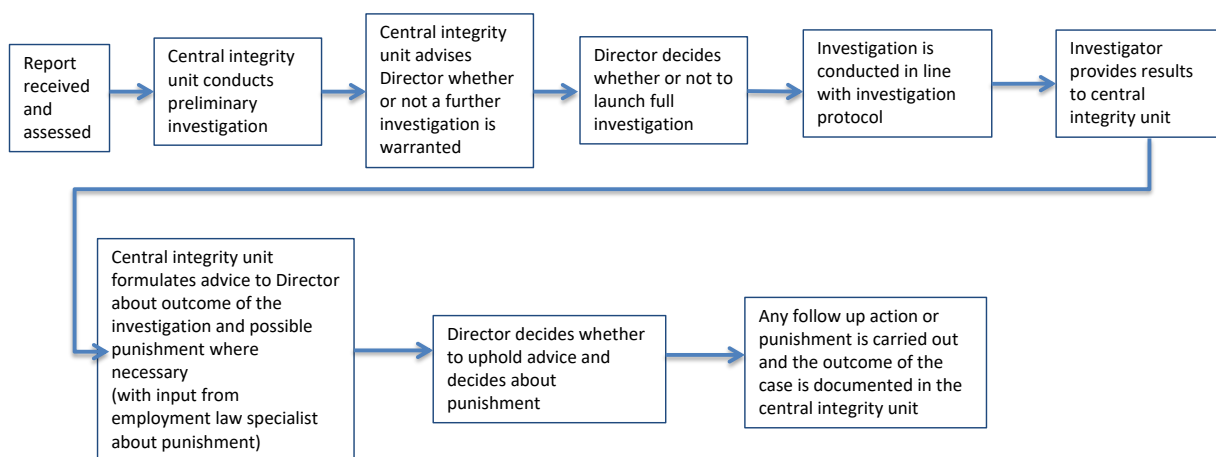
- Obligation for the person in charge to ask for (legal) advice about punishment
- Starting point: proportional disciplinary action
 - “Zero tolerance” and “setting an example” get in the way of a careful process
 - Where there is doubt between two possible disciplinary actions, the lighter of the two takes precedent
- Jurisprudence overview: ensures a careful process and prevents unjust inequality

Any sanctions or punishments should be documented so that over time the organisation can build up knowledge about disciplinary action and ensure fairness and consistency in future cases.

5. Other measures

As indicated above, it may be the case that other measures or more appropriate or necessary. These could be things like additional training or mediation, but could also involve restorative justice. This is particularly important in handling interpersonal violations, and is very often at the request of the victim/survivor. Essentially this is about acknowledging wrongdoing, taking responsibility and taking steps to 'make up for' that behaviour. This could be on the part of the perpetrator, but could equally be the organisation who acknowledges its own failings in having prevented the behaviour from happening. Restorative justice could be an alternative to or in addition to the disciplinary route. At the core of this is the notion of building a culture of justice within the organisation, where taking responsibility and doing right by the parties involved is key.

Below is a basic outline of the process for going through an investigation. This procedure should be adapted to the circumstances of the organisation. What is key is that the person with the overall responsibility for decision making is the highest manager of the organisation. This is because the procedure is rooted in the employer-employee relationship for which the highest manager is responsible.



Basic outline of the investigation procedure

PART 2

Communication when handling integrity cases

In this session of the training the group began by discussing when to believe someone, who we believe and why and which channels of communication are available to us. The group reflected on real-world examples and considered some of the main dilemmas we face in managing communication around integrity. Participants discussed the need for balance between sticking to the facts and still expressing emotion/empathy, and how displays of emotion can be genuine but can also be warning signs. We discussed the balance between transparency and privacy. We discussed the need to remain objective and aware of personal biases.

The group then focused on thinking about how to communicate about a case when everything goes as it should (the case is reported internally through the proper channels, is handled properly etc.). Based on the presentation by the trainers and the ideas and inputs of

the participants, it was possible to establish some key principles for communication by the integrity system:

- Consider the various stakeholders (audiences) and their profile, choose the right channels to reach them and understand what their interest is in the situation (what is necessary for them to know, as opposed to what they want to know)
- Communicate on a need-to-know basis
- Select spokespersons and channel all communication
- Identify the key message
- Balance transparency and honesty with the need to protect the privacy of the parties involved (including the accused)
- Focus on meta-communication
 - o tell about your values, your integrity system
 - o Strength/weaknesses, track record (History/culture: #Metoo and BLM?)
 - o Where a particular process is up to, i.e. is it under investigation?
 - o What you can and cannot share, and why
 - o What you will share later
- Consider Internal pressures (managing gossip, judgements),
- Consider external pressures (journalists, supporters, donors)
- Provide facts and figures, but do not avoid emotion - express empathy where appropriate and necessary
- Be consistent
- Communicate in a timely manner, do not rush to communicate before you have the necessary information, but do not be too slow as you risk losing control

The participants made the distinction between internal and external communication and recognized that some groups require more detailed information than others (e.g. board, managers etc. as opposed to all staff).

They also recognized that their colleagues might be concerned about the effect that such cases may have on them personally or on their work, and that there would be a need to provide careful reassurance whilst not over-promising or over-sharing.

Audiences would be asked to respect the ongoing process of handling the report, and to allow time for this work to be completed. They would be informed at various stages in the process.

The group also quickly recognized that the accused persons also have rights in terms of privacy that need to be protected, especially (but not only) when it is not yet known that there was any wrongdoing.

Lastly the group discussed whether or not to 'get ahead' by making a press statement even before an incident had reached the media's attention. In some instance this can be the right decision.

The group also discussed some common mistakes that can be made:

- Pride that your org. has had no reports/complaints/violations (actually a warning sign that the organisation is not in control)
- When there is a complaint, initial disbelief, denial, not taking action quickly, sweeping it under the carpet, whitewashing...
- Acceptance of 'a mistake', expressing much guilt, not time taken for investigation
- Apologies about 'bad apples', not taking organisational responsibility
- Optimism about the level of your integrity system, also in the field (But is it a paper tiger, but how well known/acted on are policies?)

- Protecting the organisation by belittling the complaint, or jumping to severe sanctions quickly, blaming victim/survivor/whistleblower etc.

In the second part of the of this session, the group focused on communication when handling cases where the system has failed (i.e. where there has been an information leak, or a case comes to light via the media rather than through the internal channels). Using case studies in which only preliminary information about the case was known, the group considered how they would handle the crisis both internally and externally. They discussed how they would organise themselves and the process as well as the communication.

The following are some of the key considerations about organizing in a crisis:

- The first thing is to organise a 'crisis team', usually under responsibility of the director, with a number of different 'competences' in the room. Don't forget someone to take notes of decisions/actions to be taken.
- The first question will be about the preliminary investigation: can the story be true, how can you find out? Is external investigation needed?
- But simultaneously you will have to decide what message the director should give, internally and externally. List the various audiences who need to know, and what they must/can be told. (Meta communication). Do you approach the media/social media yourselves?
- Decisions to be made: who follows the media? How often do you meet as crisis team? Who organises internally? How much time is needed to manage this crisis? What 'regular work' has to be put on hold?

Participants clearly acknowledge the need to move quickly whilst also being careful to sequence their communication. They identified the need to communicate internally first, then to donors and then to the media. Depending on the severity of the situation, this would likely be done in quick succession but nonetheless in precise order.

In cases where the incident has been shared on social media, participants noted the need for careful consideration before reacting directly on that platform.

Participants discussed the need to first establish if there was any prior knowledge about the situation within the organisation before issuing any statements to this effect. Claiming not to have known can be very damaging if it later appears that the organisation had prior knowledge (even if the spokesperson did not).

Participants also raised the possibility of bringing in external communication expertise for particularly severe crises. They also discussed the need to assess the risks to the organisation, so that those risks could be mitigated as far as possible.

They acknowledged the need to be transparent and not hide from the situation. They expressed a strong desire to focus on meta-communication, but also discussed the possibility of reaching out to the persons concerned (those who had reported to the press/on social media) to demonstrate willingness to engage them in the process.

Participants also acknowledged the need to take into account any planned communications campaigns that might coincide with the ongoing crisis management as it may not be the appropriate time to continue with them.

Regarding communication in these crisis-type situations, the following considerations are useful: Internal communication – explain and trust your integrity system

- Internal unrest – could more (old cases) emerge?
- Tensions between board, executive level management
- Investigative journalism from the outside – how to react?

- Investigation is expanding, the clock is ticking
- How to manage donors?
- What is, and what is not your role as integrity officer.
- Does the type of integrity violation make a difference? How?

The final stage of the training included a discussion about the various types or categories of violations, and in what ways communication needs would vary depending on the type of violation.

Conclusion of the training

Participants expressed an appreciation for the practical elements of the training and had gained insight into each stage of the process. Many suggested that they now had greater appreciation for the complexity of managing integrity in practice.

Participants also shared their desire to think further about how to ensure that reports about violations actually reach the reporting channels. In general terms, if the system is installed correctly and is communicated well to those it aims to serve, the number of reports naturally increases. When the system is used correctly and proves itself to be consistent and trustworthy, this again increases the confidence of people to report. In cases where the system is implemented but reports do not increase, it is often an indication that something is not being done correctly or there is a blockage in the system. A careful analysis can help to uncover the reasons for this and correct them.

Participants also discussed the need to think about how to implement their integrity systems in locations where the idea of an integrity system is not common practice. This may take time and will likely require learning from one another's experiences in order to develop some best practices.

Finally, the participants and the trainers all agreed that a learning community (or community of practice) could be an extremely useful follow-up to this training. Such a forum would allow participants to share more of their own struggles and dilemmas and to find solutions, learning from one another and from experts where needed.

Annex 1 – Sample job description for an integrity officer

XXXXX is working towards building an integrity system that protects and supports the organisation and its employees, and is in line with the best practices in the field. To do so means installing a moral learning process, through which employees are supported in taking difficult decisions in their daily work, and to develop a decent practice of compliance. Compliance here refers not only to external laws and regulations, but to internal rules laid out in the code of conduct and related policies as well.

The integrity officer will play a key role in implementing the code of conduct and its related set of preventive policies, and in ensuring the correct use of the protocols and procedures for handling (suspected) violations. The overall responsibility for the integrity system lies with the highest operational management. The direct line management of the work of the Integrity Officer is therefore the responsibility of the director. The integrity officer plays an important role in advising and supporting the director as well as senior and middle management.

The integrity officer has a championing, initiating and supervisory role with regard to integrity. This person does not have one single function, lawyers, investigators or risk analysts. If the integrity officer does not have these competencies themselves, they will work together with specialists to ensure that the integrity system runs effectively.

TASKS

1 Managing the preventative component of the compliance practice

- Distribute and make available the code of conduct and related set of policies to all staff
- Conduct regular *integrity audits* to ensure that code of conduct and related set of policies are in place and used
- Implement the preventative cycle
 - o *Mapping, prioritising, planning annually (see planning and reporting below)*
 - o Conduct analyses to identify vulnerable processes and areas of increased risk
 - o Work together with relevant colleagues to (re)design vulnerable processes to mitigate risk, beginning with those considered high risk.
 - o Provide advice and timely deployment of integrity instruments, or outsourcing thereof when necessary (such as training, or risk analysis)
- Systematically review code of conduct and related set of policies, periodically (every 2 years), and update where necessary.
- Be the central point of contact and information for questions about prevention mechanisms, including the code of conduct and related set of policies
- Acts as a central point of information for internal and global external regulatory data to ensure the most stringent rules apply to our policies
- Together with relevant colleagues (learning and development, HR, etc.) develop and deliver trainings to staff where needed. These trainings can be delivered by internal or external parties, depending on the specialist skills and knowledge available

2 Managing the repressive component of the compliance practice

Reporting

- Be the point of contact for reports of suspected breaches of integrity (along with managers and persons of trust)

- Refer reporters to other contact points e.g. Management or person of trust where appropriate
- Ensure that the reporting procedure is followed as outlined in the protocol for handling (suspected) violations of integrity
- Set up and centrally manage the anonymous overview of reports of (suspected) integrity violations.

Investigation

- In the event that a report is made, conduct preliminary research to determine whether or not an investigation is mandated. This may require external support depending on the severity of the case.
- Potentially conduct investigations for minor cases where it is appropriate
- Where external support is required for an investigation, supervise the process
- Provide advice on any aftercare within a team or department, following an investigation
- Ensure that all investigations are conducted in line with the protocol for handling (suspected) violations of integrity

Sanctions

- Provide advice to management on sanctions, in consultation with labour law specialists

Coordination

- Coordinate between various actors in the repressive component of the compliance practice (such as counselors, employment lawyers, HR consultants, or regulatory bodies internal or external)
- Provide solicited and unsolicited advice to directors, managers, and staff departments on integrity issues
- Act as central point of contact for questions from staff
- Ensure that staff who play a role in the governing component receive the training necessary to conduct their role effectively.

Documentation and review

- Document and securely archive all notifications and reports of (suspected) violations, including subsequent investigations and outcomes.
- Periodically review this archive to identify any (recurring) problems in the preventive component that need to be addressed

3 Organising moral learning process

- Document and archive cases
- Organise mores prudence – gathering all the cases that come out of regular moral deliberations and analyse underlying principles, repeating dilemmas and moral hazards
- Give feedback to top management on moral hazards
- Ensure that training on moral judgment is provided
- Institutionalise the practice of regular moral deliberations, including installing practical arrangements to monitor the process and where necessary assist in implementation
- Acknowledge and counter moral hazards

- Provide solicited and unsolicited advice to directors, managers, and staff departments on moral dilemmas and hazards
- Act as central point of contact for questions from organisation on moral dilemmas

4 Annual planning and reporting

- Develop multiyear integrity plans that meet the vision and ambition of the organisation
- Monitor whether agreements about integrity are met and plans are achieved
- Produce an anonymous annual review on both the preventative and governing components of the compliance practice, and on moral dilemmas and the moral learning process

POSITIONING AND RELATIONSHIPS

The integrity officer reports directly to the name of the **highest executive management**. He/She works closely together with the **highest executive management** and senior management team.

Further, the Integrity officer works together with colleagues involved in financial and legal compliance for example, the legal department, auditor, financial controller or similar. With Human Resources to develop training and on issues concerning labor law. Other important relationships will become clear during the course of the work.

In case of a report of a suspected integrity violation, the Integrity officer will work together with other members of the integrity system, including Persons of Trust, line managers, and investigators, as appropriate to the case.

Finally, the integrity officer also has a relationship with **supervising body/the board**. Although the **highest executive management** is responsible for the line management of the Integrity officer, it is necessary that the position is protected as far as possible. Therefore, the **highest executive management** can only fire the Integrity Officer with due cause and a request to do so must first be brought before the board, before action can be taken.

Likewise, the Integrity Officer first and foremost reports to the highest executive management. However if all other channels are exhausted, the integrity officer may escalate a case to board as a last resort.

COMPETENCIES

- Able to conduct (integrity) risk analysis
- Able to hold investigative interviews
- Able to facilitate moral deliberations
- Able to analyse mores prudence
- Able to write case reports in the proper manner
- Able to write clear reports
- Able to project authority
- Able to make decisions/ be decisive
- Realistic idea of what the organisation is able to do, and understands what is sensitive to the organisation

- Knowledge of governance structure
- Analytical thinking and problem solving capability
- Able to manage conflict and enforce
- Independent
- Accessible
- Networker
- Trustworthy
- Inventive
- Experience in non-profit sector, in international fields,
- Team working

NOTES ON IMPLEMENTING THIS FUNCTION

Each Integrity Officer should be evaluating their own competencies. It is not anticipated that every integrity officer has all of the specialist skills and knowledge needed to run the integrity system. It is necessary therefore to understand what skills and knowledge are available, and what is missing. It is then possible either to decide to acquire those skills and knowledge, or to seek it from an external agency. The organisation should therefore commit to the learning and development of each integrity officer.

Annex 1 – Sample description for a Person of Trust

Persons of Trust play a key role within the integrity system. It is a very important role, because they are often the first point of contact when it comes to discussing a suspected violation. It can also be a challenging role, and requires professional training and on-the-job learning.

This function description is based on guidelines from the (Dutch) National Association for Persons of Trust (Landelijke Vereniging van Vertrouwenspersonen) and best practices in the field.

TASKS

Tasks when dealing with (suspected) integrity violations

- The Person of Trust is the contact person, sounding board and source of information for colleagues on questions of integrity and the integrity system
- handles complaints received with confidentiality and informs third parties only with the consent of the colleague who makes the complaint
- informs colleagues about the various options for handling a (suspected) integrity violation, including rules for reporting violations, both externally (legal) and internally (rules/protocols), advises about the possible reporting channels, and accompanies the individual through the reporting procedure if required
- supports colleague if he or she wishes to file a complaint
- ensures that, when requested by the reporter, a report is submitted to the right place
- where an investigation is carried out, functions as an intermediary in a confidential reporting process between the ‘reporter’ and the investigators
- makes referrals on issues that are not within his or her power and duties (e.g. employment conflicts)
- considers the possible referral of the colleague to external experts if appropriate/necessary
- provides information and increased awareness about integrity policy
- gives solicited or unsolicited advice to the board or other persons in the organisation on preventing and handling violations
- documents reports and meetings, and delivers an annual (anonymised) report to the board.

Confidentiality for Persons of Trust

In principle, discussions between colleagues and Persons of Trust must be kept confidential. The Person of Trust ensures that the confidentiality of the “reporter” and the identities of the concerned parties are protected. However, there are certain legal limits to the confidentiality that Persons of Trust can offer, and these limits depend on the legal context in the country in question. It is up to the Person of Trust to be aware of the legal limitations

with regard to confidentiality, and to discuss these up front with colleagues. (The organisation should support Persons of Trust in accessing this information.)

Workplace conflicts

Workplace conflicts (such as disagreements about promotions, employment contracts, internal vacancies or employment conditions) are the responsibility of HR. Persons of Trust must therefore be able to distinguish between workplace conflicts and other types of integrity violations, in the first instance. In such cases, Persons of Trust can act as a listening post for the employee and refer them to the relevant HR professional. The Person of Trust can exchange ideas with the employee about how to move forward with the issue. The report and type of conflict should be recorded in the annual reports.

COMPETENCIES

There is a certain level of expertise that Persons of Trust are required to have. This means an affinity with and substantial knowledge of integrity issues. Persons of Trust should be trained in these areas, alongside their regular job.

Persons of Trust must also keep themselves informed and updated about relevant regulations, such as employment law, and how to handle reports of undesirable behaviour and (suspected) integrity violations.

The following competencies and skills are important:

- has an affinity with and knowledge (acquired through training) about undesirable behaviour and integrity in general
- has strong and quick analytical skills, with an ability to initiate the right processes and follow-up actions
- is accessible and empathetic while able to keep distance
- is able to reflect on own behaviour and that of others
- is pro-active
- is well-balanced and self-assured
- is independent, and not susceptible to interference, intimidation or external pressure
- can combine courage and diplomacy
- is prepared to handle difficult situations creatively and in a tactful way
- knows the internal structure of the organisation (reporting lines and responsibilities) and the culture
- knows the integrity policies, protocols and procedures within the organisation
- has excellent oral and writing skills and can communicate adequately with colleagues in various levels and specialisms.
- has insight into own actions and how this can influence others
- has strong advisory skills (able to recognise a problem, identify the source of it, and give clear advice)
- has 'life-experience'
- can deal with confidential information
- can handle resistance

- is willing to undergo further training, peer reviews and periodic consultations with colleagues

NOTES:

- Persons of Trust agree to take on these tasks in a voluntary capacity, in addition to their regular duties. Persons of Trust must volunteer themselves to take on the role, but must not be required to do so by management.
- Persons of Trust should be accessible to everyone in the organisation. It is therefore generally advised not to select Senior Managers as Persons of Trust.
- It is recommended to have at least one male and one female Person of Trust. This is a minimum requirement, but other diversity factors could also be taken into consideration. The total number will depend on the size of the organisation.
- Persons of Trust occasionally (in complex cases) may need to take time out their normally daily role in order to fulfil their duties as a Person of Trust. Managers should be aware of this and facilitate it as much as possible.