FANC

FEDERAL AGENCY FOR
NUCLEAR CONTROL

AFTERCARE

Internal and external staff

April 2024

FANC AFCN

FEDERAAL AGENTSCHAP VOOR NUCLEAIRE CONTROLE

AGENCE FÉDÉRALE DE CONTRÔLE NUCLÉAIRE

Aftercare for internal and external staff

Contents

1. Introduction

This document is the conclusion of the "Aftercare for internal and external staff" project, part of the insider threat programme. Nuclear operators and nuclear transport companies working in the nuclear and radiological sectors must take account of insider threats and draw up a programme to counter them.

The aim of this project was to develop guidelines for preventive measures against an insider adversary.

In the nuclear sector, there are currently clear regulations governing screening (security clearances/security certificates/access authorisations[1]). Anyone with access to sensitive areas or information in nuclear facilities or nuclear transport companies will have undergone a screening process. However, screening is only a snapshot, a photograph of a person's situation at a given moment in time, with the aim of assessing that person's future behaviour. In addition to screening, it is therefore important to include measures to monitor a person's reliability. The person can therefore be monitored as part of a trustworthiness programme.

The focus will be on the employee's life cycle. The aim is to give an overview of the possible actions that nuclear facilities or nuclear transport companies can take, as well as to indicate where the boundary lies with what can currently be done legally and what is not possible as part of the verification/monitoring of a person's reliability. It is up to the nuclear facilities or nuclear transport companies to implement the measures they deem necessary within their facility, and to decide to whom these measures will apply. Responsibility for implementing the measures lies with the industry. The FANC also draws attention to the need for prior consultation with the social partners, and for any necessary adjustments to the work regulations.

The first meeting in March 2021 focused on this project's objective, as well as some fundamental principles to be respected.

The second meeting, held in February 2022, took a closer look at the fundamental principles of a good Security Culture.

The third meeting, held in December 2022, provided an overview of practical measures that could be taken over the course of the employee life cycle.

At the fourth meeting in June 2023, we focused on measures that could be taken to monitor staff while working in the organisation, as well as the various partners likely to hold information.

In the fifth part, in November 2023, we examined how this information can be further monitored and processed.

At the final meeting in March 2024, everything was consolidated into a single document, with the emphasis on continuous improvement.

This is a guideline to provide support. However, it is always up to the organisation to decide which measures are implemented and how.

[1] No longer applicable with the change of legislation of 5/05/2024 of the Royal Decree of 17/10/2011 on security certificates for the nuclear sector and on rules on access to security zones, nuclear material or nuclear documents under specific circumstances

2. What are insider threats, and why are they threats?

The threat of internal staff (insider) intentionally committing (or attempting to commit) an unauthorised action, targeting or using nuclear or other radioactive materials, or associated facilities, transport companies or activities, is very present.

For the definition of insider threats, we refer to the IAEA Nuclear Security Series no. 8-G (Rev1). An 'insider' is considered to be: "*An individual with authorised access to nuclear material, associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorised acts involving or directed at nuclear material, other radioactive material, or associated activities*".

More specifically, an 'insider' has "**access**", "**authority**" and "**knowledge**", and this individual can constitute a threat as soon as they intend to commit or facilitate an unauthorised act.

To protect against the insider threat, a combination of preventive and protective measures must be taken within an organisation:

- Preventive measures (before an act): to minimise the number of possible insider threats and to reduce the possibility of an unauthorised act by an insider;
- Protective measures (after an act): measures to resolve the situation after an act by an insider and to mitigate the severity of the act.

Ideally, preventive measures should be sufficient to prevent all attempts at potential insider acts, but unfortunately there is no way of obtaining a complete overview of the behavioural indicators that predict insider acts. Again, we are witnessing human behaviour here, which remains difficult to predict. However, studies have shown that an insider's act also contains indicators that are visible beforehand. These are the indicators we need to work on to implement preventive measures. Although it is also necessary to take protective measures for those cases where prevention has been impossible or ineffective.

Insider threats were also included in the Design Basis Threat analysis where the actual threat is described in greater detail. However, an insider's motivation can vary considerably, for example: money, ideology, revenge, ego, coercion, or a combination of these factors. It is also highly individual. The challenge is to notice that a person is beginning to develop, or has developed, this motivation to effectively identify the threat and act against it.

3. Trustworthiness programme

A. General

A trustworthiness programme examines undesirable or suspicious behaviour or characteristics to determine whether someone could be a threat. In such a programme, it must be possible to provide guarantees that the persons concerned are trustworthy as far as they do not present an unreasonable risk to the health, safety and security of the organisation and other members of staff.

This is very difficult, as an insider's intention may not be visible, and the behavioural patterns of a person representing a threat may differ considerably or have another cause. However,

research has shown that a number of behaviours or characteristics may be an indicator of a greater likelihood that an individual will undertake an intentional unauthorised act. These are internal, external, and contextual factors that drive a person towards intentional unauthorised acts in order to provoke a reaction.

Some of these behaviours include, but are not limited to, the following:

- Anger management problems
- Association or sympathy with criminal or terrorist groups
- Difficulty accepting comments or criticism
- Conflict behaviour
- Job dissatisfaction
- Non-acceptance of authority
- Drug or alcohol abuse
- Social isolation
- Financial problems
- Reluctance to follow rules and procedures
- …

A trustworthiness programme has several components. This is a process for collecting information about a specific person, analysing the information against specified criteria and determining whether the reliability of a person can be sufficiently assured. However, a person's behaviour and reliability can also change over time. Consequently, it is imperative that adequate reliability assessments are also carried out throughout the person's career.

This concerns the monitoring of individuals in addition to the legal verifications provided for by legislation. Behaviour can change over time. The role of the Security Officer is to monitor the behaviour of persons for whom an investigation has been requested (Art. 13/1, par. 1, b. Law of 11 December 1998 [concerning classification and security clearances, security certificates and security advices]). However, the Security Officer cannot monitor all staff. Mechanisms must be put in place to enable them to access the information, and a framework must be created within the organisation to ensure that this information is monitored. This will need to be defined in procedures, along with the positions of the people who will handle this information (e.g. HR). In the case of investigation into people in the recruitment phase, or people who are not required to undergo a legal verification, the HR department has a role to play.

B. Basic principles

Overview:

1. Management must set an example, and the principles must also be supported by management.
2. A sustained security culture within the organisation is the foundation: staff must see security as their own responsibility, and so notice and pass on any indications of changes in people's behaviour.
3. Staff should not be seen as a permanent threat, but as a possible means of dealing with a threat.

4. The basis of a "human reliability programme" is good human resource management: to ensure that employees do not turn against the organisation, they need to be satisfied with their working environment.
5. People need to be deployed in the right place: not only technical skills, but also personality traits need to be taken into account (e.g. resistance to stress).
6. A 'graded approach' should be applied: do not deploy all resources across everyone, but according to access, authority, hierarchical position, and knowledge. It is important to analyse which positions can cause the most damage.
7. A clear overview must make it possible to determine, for example, which behaviours are detectable, to clearly define these behaviours (also to avoid suspicion), criteria to ensure a person's reliability, and also the possible reactions and who takes what decision (further investigation by the NSA, possible complaint to the police, temporary change of position, dismissal, etc.) and how to act quickly (in some cases, direct action is required).
8. Privacy rules: the privacy rules applicable in Belgium must be taken into account. The trustworthiness programme must be balanced with human rights. A good description of the programme and possible measures is a good start.

4. Security culture

A. General

An integral "security culture" is an important element in the 'Aftercare' context. This should be integrated into the overall corporate culture, so that it becomes a habit for everyone, as is currently the case with the safety culture.

If we look at the definitions of a "culture", we can conclude that it concerns the ideas, habits, and values of a specific group. This means that security rules and principles must be widely known and used, so that it becomes second nature for people to react. The overall aim is for internal and external staff to voluntarily and consciously consider security as their responsibility.

Staff values and loyalty to the organisation (nuclear operator or nuclear transport company) are important aspects in the context of insider threat. It can be assumed that people who are loyal to their organisation and have good morals within that organisation are less of a threat, as they are less likely to take action to harm that organisation. A 'no blame' culture that encourages dialogue is therefore very important.

It is important that everyone in the company is kept up to date with the security measures and procedures and is aware of the existence of the insider threat, and of the possible consequences. Good management of the various procedures and how to react to situations is therefore one of the measures against unwitting insider threat (abuse of someone's access, without the person being aware of it). Training and practice of these procedures and rules are also necessary.

Insider threat training must also be presented with the necessary nuances. Everyone should be aware of the threat and the possible consequences, but the aim is not to distrust everyone and see everyone as a threat. Within this threat, however, it is important to be aware of staff

behaviour and that changes to this behaviour or any suspicious behaviour are noticed so that this can be monitored. Also, a change in behaviour is not the standard proof of a possible insider threat. The person may be facing other problems or challenges, so reporting such behaviour can also lead to the necessary help and support for the person. This should be considered as a whole. Thanks to reporting, we can try to provide the person with the support they need, whether or not they have actually started to become an insider threat. Reporting must become second nature, and as far as possible, without the need to impose sanctions, to enable self-reporting as well (without this being a licence to break rules).

Therefore, it is also important that measures can be taken as soon as possible when someone is observed as a possible insider threat. Without any action being taken, everything can still be avoided, and the person can still adjust their behaviour. It is important for direct colleagues to be able to discuss such behavioural changes or misconduct among themselves, and to be able to report it. This is part of the "security culture". It is also important to be aware of report follow-up, so it can be ensured that the information will be properly processed and consulted. The aim is to prevent a situation where people dare not report anything for fear of sanctions.

B. Interface with 'IAEA Nuclear Security Series No. 7 Nuclear Security Culture: Implementing Guide'

If we look at the IAEA's security culture guidelines, we find the following diagram:

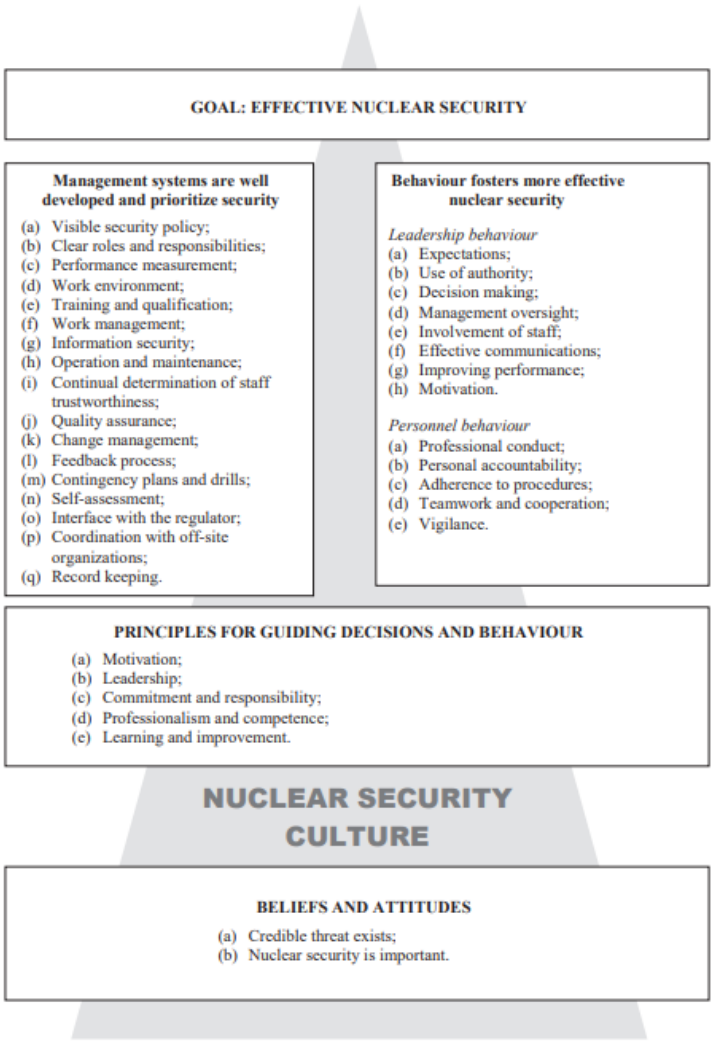

FIG. 2. Characteristics of nuclear security culture.

It is clear that certain aspects have a direct impact on the notion of "Aftercare", particularly:

- Clear roles and responsibilities: the role of all members of the organisation must be explained, as well as the role of follow-up on the information communicated;
- Work environment: when a person works in a good environment and feels loyal to an organisation, they are less likely to pose a threat to the organisation;
- Training: awareness and advice must be provided on insider threats and aftercare;
- Continuous monitoring of reliability: all members of an organisation should follow up on each other's behaviour. If there is any doubt or change in behaviour, this should be reported for further investigation;

- Leadership behaviour: management must set an example to reinforce the security culture (this topic is developed further in section C);
- Staff behaviour: the organisation is supported by its staff. It is therefore important that everyone knows what behaviour is expected of them, and that they see the organisation's security as their responsibility, to ensure that procedures are followed. The boundary between behaviour that is considered acceptable and behaviour that is considered unacceptable must be determined;
- Beliefs and behaviours: this remains the foundation of the entire security culture.

The security culture must therefore be embedded in the organisation, and everyone's role and responsibility must be assumed. It is also important that this subject is not just supported by the security department, but also and above all demonstrated by the organisation's management. They must ensure that there are sufficient resources (human and financial) and arrangements made to encourage this security culture. Sufficient procedures and structures must therefore be put in place, but it is also necessary to ensure that there is training and follow-up of the information communicated.

The security culture should also be regularly assessed to enable continuous improvement. Here too, there are IAEA guidelines on the self-assessment of security culture (NSS no. 28-T), which can support this assessment.

C. The role of management in security culture

The security culture must be supported by everyone. Information must be passed on from the bottom to the top and it must also be reported throughout the organisation if certain measures are not effective, so that they can be adapted. It is also important to include a "top-down" approach, otherwise this process will not be successful. It is therefore not the sole responsibility of the security department, but also of senior management and all the other departments who must also play a role in this.

Management must take security into account and adjust their behaviour accordingly, so that everyone in the organisation provides the topic sufficient consideration. Given their hierarchical position, they themselves need to maintain an overview of the reliability of the organisation's staff, both internal and external.

It is essential to have a management system with clear responsibilities, roles, and procedures to support this. A guideline of behaviours and expectations will make continuous monitoring of staff reliability more effective. In practical terms, this can also give a clearer picture of the behaviours and characteristics to be monitored (see Appendix A), such as professional behaviour, personal responsibility, following procedures, teamwork, cooperation, caution, etc.

D. Practical measures that can be taken

Below is an overview of measures that can be taken in the context of the security culture to support this topic:

- Training + training sessions: when joining the organisation, with the necessary refresher courses. This should also be provided for external staff:
    - What are insider threats?
    - Possible motivations

  - Everyone's role in this area – everyone's responsibility
  - Supporting colleagues and responding to any problems they may have
  - Measures taken to this end: restricted access, division of tasks, two-person rule, etc.
  - Possible impact
  - Thanks to early identification: the person can be offered help, with no consequences for the person or the environment.
- Campaigns to raise awareness
  - Wearing a badge
  - Cyber aspects → Kept up to date
  - Reporting
  - ...
- External:
  - Cooperation between security officers
  - Include in contracts that it is essential to pay attention to this
  - Include training
- General HR policy: focus on staff morale and have a good policy
  - The right people in the right place, not only in terms of knowledge, but also personality traits in relation to the position.
  - Good working environment
- Assessment of security culture: periodic assessment of the various aspects of the security culture

5. Trustworthiness staff monitoring

A. General

It is preferable for these measures to be taken as part of a graded approach. This involves an analysis of who has access to what (equipment, documents, and areas) and what knowledge they possess in the course of their duties (risk profiling). On this basis, it is possible to determine which people need to be monitored more than others.

This analysis can be carried out on the basis of positions and specific accesses linked to these positions. As a second step, measures can be increased or extended if a person has already held several positions and therefore has a higher level of knowledge requiring special attention. The aim is to link measures to the risk and the impact of the consequences of a deliberate act.

The aim of a trustworthiness programme is to determine whether a person is reliable and to monitor staff for changes in behaviour, but it can also have a deterrent effect (when staff are aware that behavioural changes will be observed). It is preferable to carry out the trustworthiness determination at the time of recruitment, during professional activities and at the end of these activities. This involves a combination of different measures depending on the situation. The nuclear sector is already subject to a government screening procedure. This document lists additional measures that could be taken. We need to continue examining, by organisation, which measures can be supported and implemented (and how).

B. Respecting privacy

These additional measures, over and above existing legal screenings, can only be implemented for specific and explicit purposes, in this case to protect against insider threats. The employer has a legitimate interest in carrying out certain verifications. In this respect, they must inform the employees or the applicant (in the case of pre-employment) sufficiently about all aspects of the ancillary measures (objectives, retention periods, possible actions, etc.). Documentation of these processes (see section C) is already an important part of the application process and should always be communicated.

For each measure, it is important to specify the purpose and therefore to have an overview of the data processed. As soon as the employee is no longer employed by the organisation, data processing must cease.

These measures must always take account of the principle of proportionality and, as we have already mentioned on several occasions, we follow the principles of a graded approach.

During this process, care must be taken to ensure that profiling is only carried out[2] in the exceptional cases provided for by the law on the protection of privacy. During analysis, human intervention will always be necessary.

In this process it is important to respect the requirements of privacy legislation.

C. Documentation

It is important to specify who is responsible for the trustworthiness programme. Under the legislation applying to the nuclear sector, it is the responsibility of the security officer to monitor persons in possession of a security clearance/certificate. However, the security officer must be supported by the organisation in this endeavour, otherwise it cannot be done effectively. To this end, the security officer may collaborate with the security department, HR, the direct line management and anyone else in the organisation who has any relevant input.

It is important that all processes, responsibilities, actions, and reports are well documented. The greatest possible openness to the various processes and activities will help build confidence in the programme. When working together in this way, it is important to determine in advance who has access to what information and where it is stored, so that everyone is kept informed.

Staff must therefore be adequately trained and provided with all the information they need to take additional measures if necessary.

A programme like this should be assessed regularly to identify challenges and difficulties, and to ensure that everything is implemented as effectively as possible.

[2] Any automated processing of personal data consisting in assessing, with the aid of personal data, certain personal aspects of a natural person, in particular with a view to analysing or predicting the work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements of this person.

The measures described in this document concern the collection of information. We will then continue the project with suggestions for communicating information, data analysis and possible actions.

It is important to ensure that all additional measures are the same for everyone, i.e. that they are linked to certain positions (graded approach). The measures adopted should be sufficiently detailed in the work regulations, the contract, and the privacy statement. However, it is the responsibility of the nuclear operator or nuclear transport company to determine which measures can be taken as part of their trustworthiness programme, and thus be developed within the organisation.

D. Practical measures to be taken

Pre-employment actions:

- Background check:
    - Verification of identity: possibly using special equipment to check identity cards;
    - Examination of the employee's professional history[3]: ask them to complete a document listing previous employers and their contact details, as well as their authorisation to verify the data;
    - Open-source verification/social media: data can be consulted, but care should be taken with any further processing of this data;
    - Request for criminal record: the basic document can be consulted and examined. It cannot be processed further;
    - Financial audit: an extract from the CKP (Centrale voor Kredieten aan Particulieren) and ENR (Enregistrement non régis) files can be requested. This is additional information, however, as it cannot be used specifically to exclude someone. A person's property is protected by the Anti-Discrimination Law of 10 May 2007[4].

    ➔ Industry example: only a checklist validating consultation of the above information would be kept, while documents containing personal data would be destroyed.
- Investigation by a private detective; to be determined in advance which specific positions this concerns, and what information is relevant;
- Verification of the person's skills and behaviour, to ensure that they are in line with the job, possibly by means of a personalised assessment or an in-depth interview on the skills sought;

[3] DPA's position: The applicant gives their agreement by signing a declaration whose scope they clearly understand, and which contains at least the following statements:

1. Their identity and that of the organisations or persons the employer wishes to consult;
2. The nature of the data requested;
3. The reasons for data collection;
4. The period during which the consent will be used.

If a reference person is mentioned in the CV, this may be considered as consent from the applicant. In any case, the employer cannot systematically verify the information provided by the applicant with third parties. If there are obvious gaps in a CV, the employer should first ask the applicant about these obvious "gaps" in their educational and professional history. Only if the applicant's explanation on the subject is not sufficient can the prospective employer consider collecting data from other persons or organisations, provided the applicant has been informed beforehand and has given their consent.

[4] 10 MAY 2007 – Law combating certain forms of discrimination

- Documented analytical review process (including as an "awareness ex ante" component): request authorisation to undergo a trustworthiness check and indicate that investigations will be carried out and that there will be ongoing monitoring of the person's behaviour (it is advisable to include this in the employment contract);
- Positive screening (security certificate/access authorisation/security clearance) required for the contract;
- Training for recruiters on insider threats and recognising signs of suspicious behaviour;
- Documentation of the recruitment process to increase transparency;
- Documentation of decisions made during the recruitment process;
- A recruitment panel made up of various members of the organisation; and
- A clear and consistent list of convictions and behaviours (if possible) that are not acceptable in terms of responsibilities.

→ Industry example: set up a separate department (or call in a private detective) that consults/requests certain information in order to draw up a security notice. This allows a degree of independence from HR departments, and this advice can be used to continue working within the recruitment process. Criminal records, for example, can then be handled separately.

Employment:

- Transparency:
  - Possession of a clear "code of conduct": provide a brief and clear overview, not just a set of rules;
  - Overview of all measures taken as part of the insider threat project: increase transparency;
  - A well-known system for reporting information about yourself and others;
  - Clear procedures concerning the measures taken and investigations launched when information is obtained = administrative investigation + rights that the person can assert themselves;
- Different mechanisms for reporting;
- Create an open culture of support ('no blame' culture);
- Permanent tutoring/coaching/mediator system to ensure direct and continuous monitoring of training and follow-up;
- Mandatory annual security briefings: basic briefing on security clearances and how to handle information, possible consequences in the event of misuse, aspects of security culture, Insider Threats;
- Training employees and management to identify red flags, a reporting culture resulting from training in the detection and reporting of alarm signals in their context, and definition of the means of reporting, including through the use of POC's (Persons of Contact): the aim is to inform employees that they can support their colleagues and voice their concerns.
- Creation of an 'insider threat mitigation' team: management, security (security officer), IT, HR, legal department;
- Concrete monitoring system for systematic forwarding of changes internally and to the NSA: change of address, change of family situation, travel abroad, etc.;

- Ongoing recurring meetings with each member of staff, accompanied by an analysis of their fiduciary functioning, based on the following elements:
    - Checklist;
    - Standard questionnaire based on objective criteria.
- Monitoring of people's digital behaviour (access to areas, documents, browsing behaviours, etc.);
- Systematic request for criminal records every X years: the basic document can be consulted and examined; it cannot be processed further (to be provided for in the work regulations + justification required);
- Possibility of meetings based on information obtained: information declared (by the person themselves or through another person);
- Recurring meeting with an identified team to discuss individuals/incidents, if necessary: based on general statistics and whether certain individuals have been the subject of recurring reports. Including general information held by HR (pay particular attention to any conflict of interest);
- Appeal procedure in the event of disagreement with management;
- Clarity as to the possibility of meeting trusted persons;
- Clarity on the possibilities of psychosocial analysis;
- Systems for picking up signals received through trusted persons and additional analyses;
- Restriction of employees' access for specific reasons that must be clearly defined;
- Systems and access audit;
- Four-eyes principle;
- Alarm systems on access systems;
- Secure access to connected digital systems;
- Allocation of specific roles and responsibilities;
- In specific, documented cases, we can work with a private detective.

Measures in case of doubt or long-term absence:

- Access restriction (on a general basis, which must be documented);
- Forward additional information to the NSA and request further investigation;
- Additional measures (additional trustworthiness meeting, etc.).

Post-employment/upon termination:

- A clear off-boarding plan;
- Documentation of a dismissal procedure;
- Denial of access, both physical and digital (in this respect, a distinction must also be made in the procedure between forced and voluntary termination of the employment contract);
- Return of all the organisation's work equipment (badges, IT equipment, etc.);
- Confidentiality clause/contract.

6. Human Reliability Programme

A. Personnel policy

Employees must be supported in their work. This includes implementing a personnel policy that enables people to be heard and listened to, by creating solid, staff-oriented human relationships.

To this end, the necessary resources should be put in place to pick up the staff's aspirations or complaints, and then action should be taken wherever possible. Everyone in the organisation must be able to pass on comments about the way they work, about their colleagues and about the hierarchy. The necessary terms and conditions in this regard are laid down in legislation on personnel policy.

The methods for being heard must be adequately explained. The aim is to ensure that these are accessible, and that information is easily communicated, so that the methods can be circulated. This will also support reporting possibilities/methods.

Staff members need to feel good about their organisation in order to reduce the likelihood of acts aimed at harming the organisation. This starts with a good human resources policy and a culture of support. As part of measures to combat insider threats, it helps to deploy employees in the right place, not only with the required knowledge, but also in the right environment for them.

B. Collecting information to monitor behavioural changes

Periodic assessments

Periodic assessment of all employees is a method of regularly monitoring a person's well-being, how they feel at work and how well they are performing their tasks. This gives an N + 1 the opportunity to have regular and, preferably, quality contact with colleagues, and to clarify certain actions or behaviours where necessary. This also makes it possible to measure any changes in behaviour, which can then be linked to specific circumstances that may or may not explain these changes. As these are notified via reports, this measure is also designed to combat subjectivity and arbitrariness.

These assessments must be documented, and the frequent reminders of the process must be shared so that the staff member is aware of it. This will enable the individual to assess their own actions in the workplace and, if necessary, indicate whether anything can be changed.

Regular interviews lead to better detection of changes in behaviours or reactions. Indeed, these changes may be less noticeable in the normal course of things, given that the focus is often on the result of the work.

Periodic assessments can also be carried out on data provided by the individual themselves. For example, a social media inspection is carried out during recruitment.

Contact with the person concerned

In addition to periodic consultations and assessments, it should always be possible to consult a person if there is any doubt about certain actions or behaviours. The organisation must ensure that the corporate culture allows for this and include it in its processes.

Regular registration

In addition to the information provided by the person themselves, it is always useful to have monitoring systems in place to report anomalies. These mainly concern access logs or access attempts. Needless to say, self-reporting systems facilitate this process.

Reports

Data received via a notification mechanism must be monitored.

HR communicates changes to the SO

The Security Officer (SO) is obliged to notify the National Security Authority (NSA) of any changes in a person's living situation if they are in possession of security clearance. By default, these changes must already have been forwarded to HR for the staff file (taking into account the maximum retention period). Setting up a system whereby this data is forwarded to the security officer via human resources can facilitate this process. This can ensure that these changes are systematically communicated to the NSA. Below are a few examples:

- Changes in marital status
- Changes of address

Communication between HR and the SO ensures that data is entered in the right place. The data to be forwarded should be defined in sufficient detail.

Verification of information

It is obviously important to verify all information collected to ensure that there are no false accusations of suspicious behaviour. Verification depends on the information itself. The processes that could be put in place include an interview with the person or verification of data with other sources.

Contact with SO's

Given the number of subcontractors, active communication with the companies' SO's is also a source of information. These SO's have the same employee monitoring obligations. Experience shows that this does not always go smoothly. However, a good relationship with the various SO's and the exchange of information may also call into question any doubts about subcontractors' employees.

C. Internal platform

It may be useful for the organisation to create an internal platform to bring partners together to further discuss potential red flags. This platform will enable measures to be taken based on the outcome of the discussions. This platform can meet periodically to draw attention to potential risks, or on an ad hoc basis for urgent cases.

The partners involved are human resources, security, and well-being at work. Depending on the case, the N + 1 as well as the DPP or other specific individuals may be heard.

This organisation must be sufficiently well known and documented. The framework in which they work must take account of applicable privacy legislation. It is also important to weigh up potential interests (the principle of caution in security).

On this platform, actions and red flags from specific individuals can be discussed. This enables data from different departments to be brought together. For example:

- Notification reports
- Access registration (physical, digital)
- Data from periodic assessments
- Data available to HR
- ...

Please note that the data shared here must be relevant to determining whether or not an individual represents a potential insider threat. It is important to clearly define the criteria on which a case will be based. Where necessary, the list of red flags may also be taken into consideration.

It is important to unambiguously take this analysis and its conclusions into account. This indicates that the analysis has been carried out correctly and objectively. This can be added to the individual's own staff file.

D. Providing support

Any problems or challenges an employee faces outside of the workplace are, of course, not the employer's responsibility. However, if this could have an impact on their work or reliability, then this would be an element to be taken into consideration and to which the employer must pay attention.

It would be interesting to have an overview of the organisations providing support in this area within the region. Initially, this information is intended to support the employee.

In some cases, these organisations can assist with the interpretation of suspicious signals. This can also help foster cooperation or contact with the person concerned.

E. Additional investigation by the NSA

In case of serious doubt, a further investigation may be requested. To do this, the security officer must contact the NSA. This option is left to the discretion of the SO. Then it is the responsibility of the NSA to decide whether the information is sufficient.

F. Clear communication

The most important aspect of this process, and of monitoring a person's reliability, is the communication that surrounds it.

Firstly, the processes and procedures within this framework must be well documented. Secondly, this must be communicated to all members of the organisation.

If specific cases are in progress, there must be sufficient communication on this subject with the person concerned or the person who made the declaration. In this communication, the reliability of the data and the privacy of the people concerned are taken into account. If necessary, and depending on the case, simply providing a notification that something has been done is sufficient. However, this must always be taken into consideration to enable future reports.

7. Notification mechanisms

A. What are the types of notifications?

It is particularly important to try to detect signs of behavioural change as early as possible. These are signs emitted by employees with access to the nuclear site or transport company (permanent employees and employees of permanent or non-permanent subcontractors). Everyone in the organisation needs to be aware of this and involved in collecting and sharing these signs, explicitly for the purpose of helping the organisation and the individual concerned. This involves peer observation of situations that seem out of the ordinary. Generally, the process that leads a person to become an insider threat follows certain phases that can be observed externally, even if they are several snapshots.

Notification method

In this respect, it can help to ensure that certain cases are automatically reported: for example, attempts to consult documents without authorisation, or access to certain areas at unusual times. It is important, however, that everyone in the organisation is alert to these signs, and able to pass on information easily if there is the slightest doubt. It is advisable to implement accessible systems and clear processes on how to manage these doubts and this information. It should be made clear that these signs will be followed up, and the person concerned should be supported rather than punished (see also the law on 'whistleblowers'[5]). However, the organisation must be open to this.

In this respect, it is advisable to provide various options for filing a notification of these elements, including the possibility of forwarding data anonymously. Adequate levels of system security and data protection must be taken into account to guarantee the integrity of the data (also considering legislation on classification and categorisation, if necessary). Below are some possible options:

- Online form;
- Permanent email address;
- Paper form in a box (boxes in several locations, emptied regularly);
- Fixed times to talk about yourself and the service;
- Trusted persons;
- Line managers.

It is a good idea to determine what information you wish to receive in such a notification, so that you are in a position to review it. For example, in the case of an online form, you can make it mandatory (without requiring the reporter to identify themselves). Below are some examples of mandatory data:

- The name of the person concerned who is the subject of a declaration;
- Observed behaviour;
- When the behaviour was observed;
- Where the behaviour was observed;
- The reason why the person who observed the incident has doubts;
- …

[5] 8 DECEMBER 2022. - Law on reporting channels and protection of whistleblowers reporting integrity violations in the federal public sector and the integrated police

These basic elements will enable you to carry out further research in-house, or even pass on this information to a higher level. If the elements provided are not sufficient to get started, you may wonder whether you need to go any further. Care must be taken to ensure that inadequate information is not supplemented by assumptions.

Information to the reporter

It is important to examine what information can be passed on to the reporter (taking into account the possibility that the reporter is anonymous or does not wish to be contacted about the issue). An automated message or an overview of the next steps can contribute to effective and relevant communication, as well as maintaining trust.

In addition, it is possible to indicate that the information will be followed up in a way that will have no impact on the reporter. If it subsequently transpires that the allegations are false, the reporter can of course be contacted to inform them of the situation and, if desirable and possible, take other measures under the employment contract (unjustified reports may be considered as serious misconduct, fraud, etc.).

Employees of nuclear facilities and carriers need to be reminded that observing and detecting individuals who could potentially become or be an insider threat as early as possible enables us to react and design an individualised monitoring procedure that takes a positive approach.

B. Bringing information together

Internal platform

The best way to receive the notifications themselves is on a central point/platform. The aim is to ensure that all reports can be processed in the same way, and that all additional information channels are clear. It is advisable to open a case for each incoming notification, precisely to treat all notifications in the same way and have an overview of what is being done.

It is best to start by examining the notion of 'independence'. If a member of the team responsible for handling the report is too closely linked to the reporter or the person concerned, it is important to check whether this person can continue to be part of the internal investigation. Therefore, it is easier to define a small group of different departments that make up the platform.

Furthermore, to ensure that this mechanism remains flexible, it is preferable for this platform to meet only at the request of one of its members, when an individual case needs to be examined. The rest of the time, the platform can be "dormant".

However, to ensure smooth operation, it is necessary to identify one person who will be responsible for coordinating and supporting the various measures taken by the platform, as well as monitoring the situation.

Summarising messages or signs

Before opening an investigation, it is important to check whether the notification is admissible. Questions that may be asked:

- Anonymity: can we verify this notification effectively?
- Connection: is the reporter close to the person concerned so that the report may really be genuine OR does the report have a direct positive effect on the reporter?
- Information: is there enough information, or is it possible to obtain or search for further information?

If there is insufficient information to go any further, it may be decided not to proceed with an investigation. This will also be linked to the outcome of the risk assessment determining whether or not to pursue an investigation.

The information received must be as objective as possible. This is a difficult exercise, as people are invited to report their observations, so that the report received can reflect a person's feeling, or a situation that is felt to be illegal. The aim is to make the complaint as objective as possible and to determine what it concerns. Defining complaint categories can make this task easier. Some examples:

- Behavioural change
- Not following the rules
- Dispute
- ...

Requesting basic information

Once it has been decided that the notification will be examined further, it may be useful to obtain some basic data for a more in-depth internal investigation, for example:

- HR data;
- Any complaints against the person;
- Personal assessment.

The use of a fixed model (template or model) for handling complaints can promote objectivity.

In the case of subcontracting, this information must, where appropriate, be requested from the security officer of the company by which the person is employed. The security officer should also be involved in the investigation, as they are the individual authorised to conduct an internal investigation into the people employed in their organisation.

C. Internal investigation

A security officer has the power to conduct an internal investigation to ensure the aftercare of the screening (Art. 13/1 b of the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations). As part of an internal investigation, it is important to take into account the risk the person may pose to the organisation, on the one hand, and the information available on the person concerned, on the other. The actions to be taken and the investigation of the person concerned must be proportionate to the damage they may cause.

As soon as an investigation is underway, of course, it is essential to gather the information needed to make an informed decision. Several actions can be taken in this regard:

- Interview with the person concerned and the person who reported the incident: it is important to hear from both parties;
- Recording of the data on the activities;
- Interviews with colleagues;
- Observation of the individual;
- Open-source verification;
- ...

This investigation should be as well-documented as possible, to serve as a basis for any possible action. In this regard, the need to respect privacy (access to information, retention of this information, etc.) must be taken into account. The investigation will be proportional to the risk the person may represent to the organisation. This internal investigation may involve the collection of the individual's personal data, in the general interest of the organisation and the legal competence of the security officer, but it must always be examined in the light of the principle of proportionality.

The information collected must be analysed by the internal investigators to determine whether the person represents a genuine threat to the organisation.

D. Measures

At the start of, or during the investigation

Depending on the risk that the individual poses to the organisation, it may be decided to take certain preventive measures right from the start of the investigation:

- Restricting access;
- Additional support;
- ...

If it is decided to take such measures, it is best to communicate this clearly to the person concerned. It is important to know that such actions may cause a person to distance themselves or diminish a person's trust in their organisation. It is therefore essential to ensure communication is as open as possible in this respect. In this case, it is advisable to talk to the person concerned, so that the report can also be discussed by mutual agreement, and the person concerned has the opportunity to explain their point of view.

This decision can also be taken during the course of the investigation if, over time, the analysis indicates that the risk to the organisation appears to be higher.

Proportionality must be taken into account when implementing operations. Taking concrete action can also push a person towards a threat that was not there at the beginning.

Another option would be to request an additional analysis from the National Security Authority (NSA), based on information collected in advance.

After the investigation

A conclusion will be drawn at the end of the investigation: is there a potential threat for which additional measures need to be taken? Possible actions are as follows:

- Continued monitoring;
- Additional security measures: support, etc.;
- Working in another location;
- Suspension;
- Terminating the contract.

If there is no concrete threat to the organisation itself, but the person is in a situation in which they need help or support, it is important to consider what the organisation can do in this regard. The aim is to preserve the confidence of the person concerned following a possible investigation and get them back on a more positive track.

E. Internal reports (team/internal)

In the event of a substantiated report, the person concerned may be informed of the investigation. In most cases, a conversation will be scheduled with the individual. On completion of the internal investigation, a summary of the findings must be communicated to the person concerned.

Wherever possible, the notification process can be based on the existence of contact with the reporter, on the fact that everything has been examined and whether (effective) measures have been taken. Care should be taken not to share too much data about the investigation. However, if effective measures have been taken, this should be clear to all. Communication with the individual's own team, or the people with whom they work, can also provide some guidance in this respect. In this case, the interested party must work with the additional measures. It is essential to ensure that the organisation still has confidence in this person (given that they are still an employee), but that additional measures are taken temporarily to support the individual and thus help them to carry out their work in the best possible circumstances.

In this respect, it should be borne in mind that an internal investigation, whether conducted or not, may have an impact on the person concerned. The individual's trust in the organisation could be compromised. In this case, closer monitoring by the manager could be recommended. Open communication throughout the process, with the necessary respect for the person concerned, can be a significant help in this regard.

8. Continuous improvement

This employee monitoring process should be assessed regularly. The danger with such measures is that they are assumed to work, which can create complacency in a system. It is therefore recommended to set up a permanent assessment cycle through which these measures are reviewed on an ongoing basis. In particular, we can assess:

- The success of the measures (number of investigations, reports, incidents);
- The security culture;
- The level of management support for the measures;
- The effectiveness of the implementation of the graded approach;
-...

It will then be possible to determine whether additional measures can be taken, or whether less effective initiatives can be adapted.

Such an assessment provides an opportunity to raise 'awareness' and re-evaluate the success of the monitoring programme. The aim is to ensure continuous improvement in line with the organisation's evolution.

9. Conclusion

Insider threats are a genuine threat to the nuclear sector. This threat is entirely determined by the organisation's employees and the nature of the organisation. It is therefore important to monitor these people before and during employment, and after the end of their appointment. In this document, we have attempted to implement the international guidelines in this field to the Belgian situation with the help of national stakeholders. By testing these elements with people working in the field, we were able to share best practices within the sector, but also

with other sectors. Clearly, there is no one-size-fits-all solution for employee monitoring. Measures must always be targeted at a specific organisation. This is one of the reasons why it was decided to draw up an 'overview' of possible measures. The nuclear facility or carrier can choose the measures that are able to support its own organisation.

APPENDIX A: Signs that could indicate a change in behaviour

The following characteristics may indicate that a person may more easily be exploited or become unreliable. Exhibiting any one of the following behaviours does not automatically indicate that a person will commit an insider act, but it may lead to them doing so more easily. Depending on the situation, these factors may be concerning. Moreover, the fact that a person displays one of these behaviours does not necessarily constitute grounds for in-depth investigation, but if several elements come to light, this can be reviewed, especially so when the behaviour observed is out of the ordinary for this individual. This is therefore a non-exhaustive overview of possible behaviours that should be reported:

Attendance:

- Leaves the workstation without authorisation (when authorisation is required)
- Repeated abuse of sick days or over a long period without apparent reason
- Frequently arrives to work late (when this was not a habit)
- Specific and implausible excuses for absence or lateness
- Repeated, unplanned short-term absences (with or without medical certificate)
- Absence during working hours or difficulty finding the individual
- Frequent requests to take on work on their behalf

Productivity:

- Repeatedly fails to meet deadlines and commitments without justifiable reason
- Unreliability (e.g. you cannot trust they are where they say they are, or doing what they say they are doing)
- Gives implausible excuses for poorly performed tasks
- Avoids work or does not do all the work required of them
- The work requires more effort or more time than expected
- Makes frequent mistakes, poor decisions, or errors in judgement
- Sudden and repeated bouts of absent-mindedness, which has an impact on their work
- Difficulty following instructions, lack of understanding and unwillingness to understand

Emotional stability:

- Hypersensitive to criticism
- Is resentful and acts accordingly towards colleagues, superiors and/or the organisation
- Frequent mood swings
- Quickly irritated
- Aggressive outbursts
- Increased irritability with colleagues or others
- Unusual suspicion or paranoia
- Seems anxious, nervous, or panicked
- Exceptionally energetic, hilarious, euphoric

- Appears depressed, expresses a feeling of deep despair about life, work, or society in general.
- Indecisive, lacking confidence
- Withdrawal, sudden isolation from others for no apparent reason
- Apathy, loss of motivation
- Distracted by family, financial, legal, or other stressful situations, difficulty managing the stress inherent in the situation
- Suicidal tendencies or suicide attempts

Undesirable behaviour in the workplace:
- Frequently on the defensive
- Blames others for their problems
- Frequently lies and exaggerates
- Complains about colleagues
- Threatens or intimidates colleagues
- Increased irritation with colleagues or others
- Systematically argumentative in each situation or context
- Inappropriate sexual language or behaviour
- Out-of-context or unpredictable behaviour
- Does not follow security rules or procedures
- Unreasonable behaviour and demands on others
- Indication of deceit, delinquent behaviour, or unreliability

Cognitive decline:
- Disorganised habits or work pace
- Distracted, frequently daydreaming
- Easily distracted, unable to concentrate
- Slower movements and reaction times
- Problems with short-term memory
- Unusual ideas or thoughts
- Appears to have poor judgement of applications
- Does not seem to realise that they are less able to work properly, difficulty distancing themselves
- Has trouble staying alert

Physical decline:
- Frequently looks exhausted
- Deterioration in personal hygiene
- Numerous physical complaints and illnesses
- Significant weight loss
- Appears to be weak or deteriorating in health
- Hearing problems
- Trembling
- Other signs of physical decline

Signs of alcohol or drug abuse:

- Appears high or drunk at work
- Unusual speech problems, disorientation, or lack of coordination
- Drowsiness or sleeping in the office
- Hiding drugs or alcohol in the car/at work
- Able to drink large quantities of alcohol with little effect, need for frequent alcohol consumption
- Irregular working hours
- Consecutive unexplained absences on Mondays and/or Fridays
- Repeated and unsuccessful attempts not to use drugs or alcohol
- Use of drugs or alcohol to manage stress
- Prescription drug abuse

Signs indicating a change in mental state:

- Unexplained mood swings
- Increased nervousness or anxiety
- Reduced performance or work habits
- Changes in personal hygiene
- Expression of unusual thoughts, perceptions, or expectations
- Unreliability and lies
- Attempts at self-harm, repeated need for strong, dangerous sensations
- Dissatisfaction with employer or contracting authority

Lack of respect and signs of possible aggression:

- Argumentative or abusive behaviour towards work colleagues or family, leading to arguments in the workplace or interruptions to work activities
- Tendency towards self-isolation, rejection of social interactions, lack of social support, unexplained and overt depression
- Verbal outbursts, usually drawing attention to subjects not directly related to the discussion or work
- Exploitation or mistreatment of others, usually through intimidation or abuse of power
- Disruptive behaviour for which advice or supervision from management does not seem to have an impact
- Verbal or physical threats against colleagues or family members
- Extreme or repeated statements expressing bitterness, resentment, or revenge
- Violent attacks or throwing objects at any time
- Harassment behaviour
- Extreme or recurrent violations of rules or laws
- Abuse of any kind

Signs that the person is (or is suspected to be) criminally active:

- Theft or attempted theft
- Fraud or attempted fraud
- Abuse or neglect of spouse/children
- Attempts to involve others in illegal or suspicious activities

Signs of misuse of sensitive information:

- Provides information to people who do not have access to it
- Asks questions about operations and/or projects to which the person does not have or no longer has access
- Unauthorised contact with the media
- Collects or stores sensitive materials outside of dedicated facilities
- Lax security habits (handles sensitive information over the phone, does not use the designated storage area for sensitive information, works on sensitive information at home)
- Statements or actions that demonstrate that the person believes the rules do not apply to them

Signs of abuse of IT capabilities:

- Unauthorised or unnecessary access to databases
- Unauthorised searching/browsing in computer libraries
- Unauthorised deletion of database information

Signs of financial vulnerability:

- Inability to repay debts or non-compliance with debt mediation plan
- Repeated compulsive spending
- Fails to keep proper track of the organisation's finances or property

Signs of collusion:

- Lives/spends beyond their financial means
- Large unexplained or unexpected sums of money
- Unexpected debt repayments
- Declarations of large sums of money from inheritance, wealthy relatives, gifts, investments, family businesses, etc.
- Personal assets incompatible with income

Signs of links to suspicious third parties:

- Possession and use of a foreign passport
- Encourages or glorifies aggressive actions by third parties or organisations
- Association with or sympathy for people and/or organisations that encourage this type of action

Signs that the person has been recruited:

- Contacts/has contact with people known to have contacts or potential contacts with foreign intelligence services or terrorist organisations
- Does not report foreign trips
- Does not report being approached by foreign organisations
- Does not report requests for sensitive information outside official channels
- Participates in or is invited to participate in illegal activities

Signs that the person is gathering information or letting material disappear:

- Questions about obtaining information or materials that the person does not have access to
- Requests signatures to confirm deletion of information or material without you having seen the deletion take place
- Use of unauthorised equipment in areas where sensitive information or material is stored, discussed, or processed
- Use of listening or observation equipment in sensitive or secure areas
- Takes sensitive information or material home or to other unauthorised locations
- Unauthorised access to sensitive digital information systems
- Observing a colleague trying to gain access to sensitive information or material that is not related to work duties
- Demonstrates an unusual interest in information that is beyond their current position
- Unusual interest or aptitude for security
- Deliberately gauging the reaction of the security services

Signs that a colleague has criminal intentions:

- Tries to gain access to areas containing sensitive information by regularly volunteering for tasks outside their usual responsibilities
- Excessive use of photocopiers, printers, or other devices to reproduce or transmit information that is beyond the person's competences
- Attempts to lure colleagues into situations that may put them in a compromising position
- Attempts to impose an obligation on colleagues through special treatment, favours, gifts, money, or other means

Extra info “THE BEHAVIOUR BAROMETER: An Education and Awareness Tool”: BAROMETRE_EN_CPRLV_2016-1.pdf (info-radical.org)

APPENDIX B: Link to doctoral research providing an overview of measures

Title	**Exploring insider threat awareness and mitigation: more than the devil in disguise**
Author	***Reveraert, Mathias***
Abstract	Employees that steal, commit fraud, sabotage, or leak confidential information: it is every employer's nightmare. Even though every public or private organisation – big or small – is vulnerable to so-called 'insider threats', this problem is too often overlooked because organisations assume that their employees can be trusted. Indeed, employees need to be trusted with access to the organizational assets because they need it in order to do their job. Still, this access implies that insiders are largely exempted from the security obstacles that external enemies have to overcome. Despite the fact that insiders can relatively easier threaten the organization's assets, they are often overlooked as potential threat. Belgium already encountered multiple insider threat incidents. The most striking example is the nuclear reactor Doel 4 that was deliberately sabotaged by an insider. More recent examples in Belgium are Jürgen Conings and Operation Sky. To on the one hand raise awareness on the insider threat problem, and on the other hand provide organizations with mitigation measures to better secure themselves against insider threats, research was done with the support from Brussels Airport Company, Bel-V, Elia, Engie-Electrabel, the Federal Agency for Nuclear Control and G4S on the insider threat problem. The results of the first part of the research provide us with insights on the awareness gaps of Belgian organizations concerning the characteristics of the insider threat as well as the ways to mitigate it. The results of the second part of the research give useful insights on what can be considered 'red flags' of insider threats that organizations should be vigilant of, as well as with mitigation measures that organizations can use to better secure themselves against insider threats.
Language	English
Publication	Antwerp: Antwerp University, Faculty of Social Sciences, Department of Political Sciences, 2023
Full text (open access)	https://repository.uantwerpen.be/docstore/d:irua:17211

APPENDIX C: Interview Tips & Tricks[6]

If you have doubts about someone's behaviour or changes in behaviour are noticeable, often the person is not malicious; it can be useful to talk to the individual themselves in order to get an idea of the reason. It is necessary to collect information in order to conduct a threat assessment. Data can be very useful, but to gather information on the intent or motivation, information from the individual themselves is of the greatest importance.

In general, you will gather more information if you can have an informal conversation (one-on-one), but whether this is possible depends on the national legislation and your company's culture. In some cases, you may need to have the conversation in the presence of a third party. For example, it can help to have an objective view on what was discussed. In this case, it would be useful to prepare who will lead and who will observe (with a focus on how the person acts and reacts). Sometimes, the person being interviewed may ask to have counsellors (advocate, union representatives, etc.) with them.

Preparation for the meeting

°Gather the information you already have. You can use such information during the conversation, for example to substantiate or explain why you are asking a question. Make sure to differentiate facts from assumptions and hearsay.

°During the meeting, you may want to offer support and help to the person: gather information on how you could do this in a practical way.

°Make sure you know what you want out of the meeting: what information. The objective should be to "clear" the person by finding clear and innocuous explanations for suspicious elements.

°Check what kind of information you are legally authorised to ask. You may refer to regulations regarding private life, medical secrecy, anti-discrimination, etc.

°Prepare (open) questions, to obtain the necessary information. Open questions may acquire more information.

°Leave your own perception out of your preparation; try to be as objective as possible. It could be helpful to identity what your perception is in order to ensure it does not impact questions/conversation. Try to keep an open-mind and approach the meeting with good intent towards the person.

Invitation to the meeting

°Make sure you are in a place you cannot be disturbed.

°An invitation to a planned meeting can be helpful, so the person cannot pretend to be needed elsewhere – but it might make the person suspicious → depends on company culture.

[6] IMPORTANT: These tips & tricks are appropriate for usual situations, when most of the time, people are not dangerous criminals and terrorists and, therefore, must be treated with respect and care. If you have proof of or serious doubt about the fact that the person is malicious and/or dangerous, you should instead contact your security service and police in a timely manner before deciding to carry out an interview with the person. It could alert them and give them an opportunity to commit a malicious act or to flee. It could also hamper a judicial investigation.

°Putting yourself in a position where you are asking help from the person, might help the conversation: 'Could we have a meeting, because I need your help with something.'

The meeting itself

°Inform the person why you are having the meeting. You have information that needs to be clarified.

°Ask open questions.

°Talk from an "I" perspective. Avoid "you" sentences that are not perfectly factual or questions, because they can be interpreted as a judgement, and the person can feel threatened, and refuse to answer.

°Leave enough silence, so the person can answer and feels free to speak. Most people also tend to "fill the void" and give more information, even unexpectedly, when there is silence.

°Focus on the caring for the person's well-being: 'Is there something we can help you with', 'I am concerned about your well-being'.

°Create a relaxing environment, so the person does not feel threatened.

°Look at a person's body language. Try to observe.

°If you have doubts as to whether the person is lying, you can insist on the fact that it is very important that the person is truthful. Information given may be checked and if it is found that the person has lied, this could have consequences.

°If the person seems distressed, try to reassure them that you are here to help them, to clarify the situation and, if needed, find solutions suitable both for them and for the service.

°Respect the person.

°Listen to what is being said and leave enough space for the person to talk. They should be talking more than you.

°Note down all important elements. Verify with the person that you have properly understood what they said.

After the meeting

°Try to make an objective analysis.

°Write down your initial thoughts; you can analyse them later, but the first impression is often the correct one.

°Check the information provided by the person.

°If the person required help or support, act accordingly.

°If needed, contact your security service/police.

APPENDIX D: Circular CP3

The aim of this circular is to improve service and optimise the management of internal activities within the integrated police, thereby making them more transparent. The objective is to develop an internal inspection system. This also includes complaint management.

Circular CP3: Circular of 29 March 2011 CP3 on the system of internal control in the integrated police, structured into two levels. (openjustice.be)

APPENDIX E: Examples of training courses

Preventing radicalisation:

- BeFUS - Preventie van gewelddadig extremisme op https://befus.be/2020/12/25/prevention-des-extremismes-violents/?lang=nl
- Handboek Lokale preventie en veiligheid in België op https://politeia.be/nl/artikels/290193-lokale+preventie+en+veiligheid+in+belgi%C3%AB
- VVSG - Rapport Radicalisering & Polarisatie (Ledenbevraging 2022) op https://www.vvsg.be/Publiek/VVSG%20Rapport%20Ledenbevraging%20Radicalisering%20Polarisering%202022.pdf
- Community Policing and the Prevention of Radicalisation (CoPPRa) - International update 2021 at https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/collection-inspiring-practices/ran-practices/coppra_en

FANC

FEDERAL AGENCY FOR
NUCLEAR CONTROL

Rue du Marquis 1 bte 6A • Markiesstraat 1, bus 6A

1000 Brussels • Belgium

www.fanc.fgov.be
contactpoint@fanc.fgov.be
+32(0)2 289 21 11

RESPONSIBLE EDITOR
Frank Hardeman

April 2024