Direction de l‘Aviation Civile

Implementing a Security Culture in Luxembourg

Direction de l'Aviation Civile
Grand-Duché de Luxembourg

The following course was elaborated by the Luxembourg Directorate of Civil Aviation. Its main goal was to provide to the Luxemburgish aviation industry (Security & Deputy Security Directors/Managers – Managers Quality Control – Instructors) an AVSEC course containing the necessary information on Security Culture, Insider threat and Radicalization. Each operator/entity was informed that a certain number of points listed in the slides needed to be integrated into their Security Programme and Training Programme, before they could provide the course internally. The course contains also a summary of the 7 Modules of the Help2Protect* website. Each participant has received a copy and explanation on the *ICAO Security Culture Toolkit* which needs to be shared internally.

**Help2Protect is an Insider Threat Program funded by the European Commission.*

Test

Internal Threat

Security Culture

Documentation

Legal Basis

Preparation

Test

Internal Threat

Security Culture

Documentation

Legsl Basis

Preparation

Preparation of the Project

Contacts were made with:

- European Commission;
- ICAO;
- CAA IE/MT;
- DAC;
- Juridical Department;
- CoESS; and
- Operators.

Test

Internal Threat

Security Culture

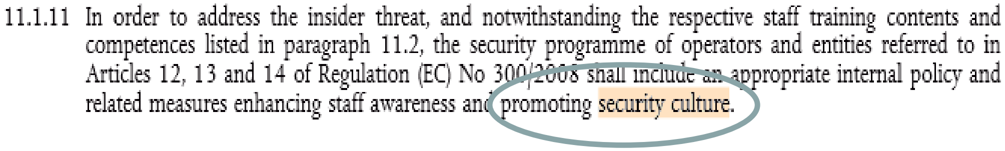
Documentation

Legal Basis

Preparation

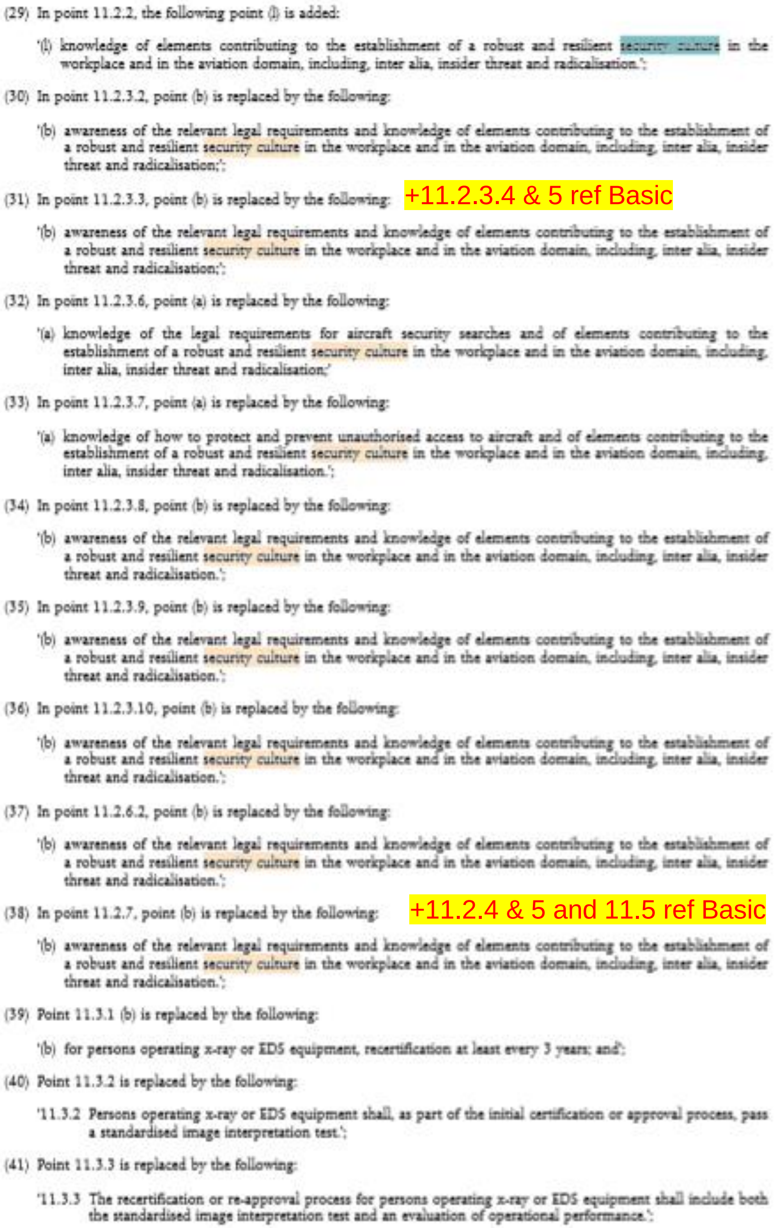
Legal basis

Regulation (EU) 2019/103



11.1.11 In order to address the insider threat, and notwithstanding the respective staff training contents and competences listed in paragraph 11.2, the security programme of operators and entities referred to in Articles 12, 13 and 14 of Regulation (EC) No 300/2008 shall include an appropriate internal policy and related measures enhancing staff awareness and promoting security culture.

ICAO doc 8973-11 chapters 8 & 9



(29) In point 11.2.2, the following point (l) is added:

'(l) knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(30) In point 11.2.3.2, point (b) is replaced by the following:

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;';

(31) In point 11.2.3.3, point (b) is replaced by the following: +11.2.3.4 & 5 ref Basic

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;';

(32) In point 11.2.3.6, point (a) is replaced by the following:

'(a) knowledge of the legal requirements for aircraft security searches and of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation;'

(33) In point 11.2.3.7, point (a) is replaced by the following:

'(a) knowledge of how to protect and prevent unauthorised access to aircraft and of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(34) In point 11.2.3.8, point (b) is replaced by the following:

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(35) In point 11.2.3.9, point (b) is replaced by the following:

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(36) In point 11.2.3.10, point (b) is replaced by the following:

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(37) In point 11.2.6.2, point (b) is replaced by the following:

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(38) In point 11.2.7, point (b) is replaced by the following: +11.2.4 & 5 and 11.5 ref Basic

'(b) awareness of the relevant legal requirements and knowledge of elements contributing to the establishment of a robust and resilient security culture in the workplace and in the aviation domain, including, inter alia, insider threat and radicalisation.';

(39) Point 11.3.1 (b) is replaced by the following:

'(b) for persons operating x-ray or EDS equipment, recertification at least every 3 years; and';

(40) Point 11.3.2 is replaced by the following:

'11.3.2 Persons operating x-ray or EDS equipment shall, as part of the initial certification or approval process, pass a standardised image interpretation test.';

(41) Point 11.3.3 is replaced by the following:

'11.3.3 The recertification or re-approval process for persons operating x-ray or EDS equipment shall include both the standardised image interpretation test and an evaluation of operational performance.';

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Test

Internal Threat

Security Culture

Documentation

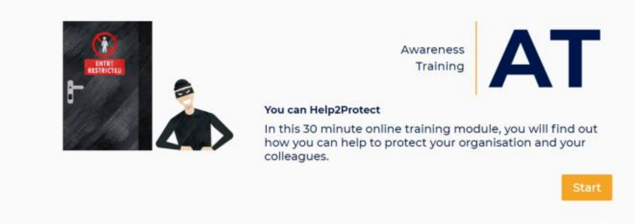
Legal Basis

Preparation

Documentation

- ❑ Regulation (EU) 2015/1998 - amendment (EU) 2019/103 (*amendment (EU) 2020/910)
- ❑ ICAO Doc 8973-11 Chapters 8 and 9 and ECAC Manual
- ❑ Magazine ECAC (2018) with articles related to Security Culture

- ❑ Help2Protect (https://help2protect.info/module/)



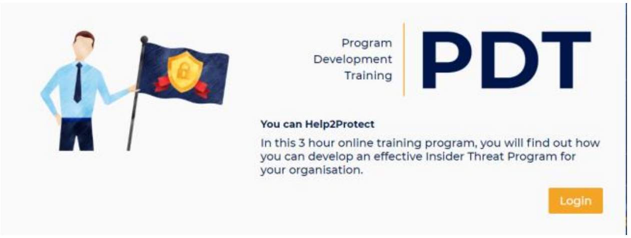
Awareness Training **AT**

You can Help2Protect

In this 30 minute online training module, you will find out how you can help to protect your organisation and your colleagues.

Start

- ❑ Help2Protect 7 Modules in relation with internal threats – Security Culture



Program Development Training **PDT**

You can Help2Protect

In this 3 hour online training program, you will find out how you can develop an effective Insider Threat Program for your organisation.

Login

https://app.help2protect.info/Account/Login

- ❑ Documents related to cyber criminality
- ❑ Security Programmes of certain operators

*Commission Implementing Regulation (EU) 2020/910 of 30 June 2020 amending Implementing Regulations (EU) 2015/1998, (EU) 2019/103 and (EU) 2019/1583 as regards the re-designation of airlines, operators and entities providing security controls for cargo and mail arriving from third countries, as well as the postponement of certain regulatory requirements in the area of cybersecurity, background check, explosive detection systems equipment standards, and explosive trace detection equipment, because of the COVID-19 pandemic

Test

Internal Threat

~~IM~~POSSIBLE

Security Culture

Documentation

Legal Basis

Preparation

Positive message

Who is concerned and what is it ?

Who?

Everyone should be involved. It goes from top to bottom.

What?

Security culture is an organizational culture that encourages optimal security performance.

There are resemblances with the safety culture which is far more regulated.

Security Culture Model

- Our security culture model is an important element in a broader security framework.
- The model consists of several dimensions: behaviors (attitudes), cognition (learning), communication, compliance, norms and responsibilities.
- Each dimension is observed separately and measured from low risk to high risk.

How to improve Security Culture ?

In order to be able to improve culture (e.g., to make it stronger or more positive), we need to know what we mean by the concept of security culture, that is, what human or organizational aspects we are talking about.

Only then will we know what makes a security culture strong or positive in the first place. Once it is defined, we can measure it. Using the results, we discover what mechanisms can be used to influence the security culture and the magnitude of its impact.

DAC / guidelines

DAC as a regulator will provide guidelines in the National Aviation Security Program (NASP) for stakeholders on how to:

- ❑ Implement a security culture and internal threat program;
- ❑ Promote staff awareness training; and
- ❑ Create an anonymous and confidential reporting system.

Implementation of a reporting system

➢ The DAC, entities and operators that play a role in security shall implement a security culture reporting system by:

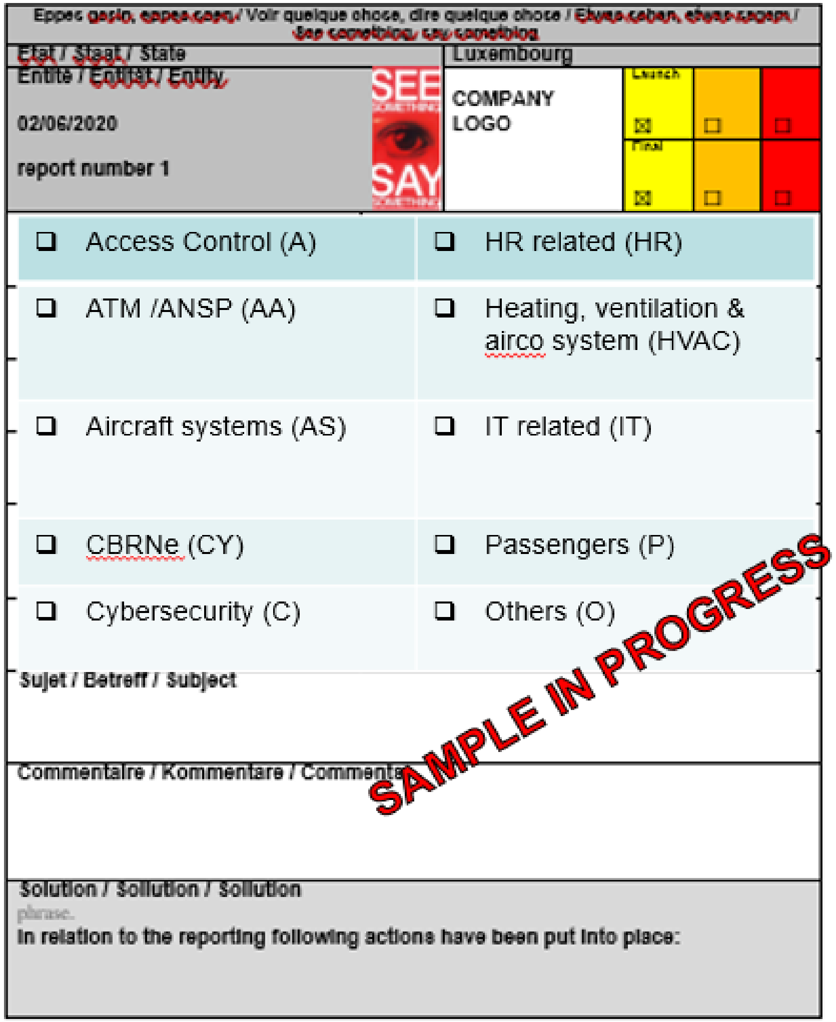
❑ Establishing a system to ensure the confidentiality of reporting persons (by which personal data is not collected and/or stored). When personal data is collected, it should only be used for clarification and more information about the reported event, either to provide feedback to the person who reported it;

❑ Identify an independent organization or person responsible for managing, maintaining and ensuring the confidentiality of data collections, as well as analyzing and tracking reports;

❑ Provide appropriate training and awareness about how the culture reporting system works, its benefits and the rights, responsibilities and duties of individuals in relation to events; and

❑ Implement an incentive program to encourage staff to report events. Such a program should also encourage staff to provide feedback on security measures to improve the system as a whole and achieve greater security performance.

Reporting



Eppes gesin, eppes soen / Voir quelque chose, dire quelque chose / Etwas sehen, etwas sagen / See something, say something

Etat / Staat / State	Luxembourg			
Entite / Entität / Entity 02/06/2020 report number 1	COMPANY LOGO	Launch ☒	☐	☐
		Final ☒	☐	☐

SEE SOMETHING
SAY SOMETHING

❑ Access Control (A)	❑ HR related (HR)
❑ ATM /ANSP (AA)	❑ Heating, ventilation & airco system (HVAC)
❑ Aircraft systems (AS)	❑ IT related (IT)
❑ CBRNe (CY)	❑ Passengers (P)
❑ Cybersecurity (C)	❑ Others (O)

Sujet / Betreff / Subject

Commentaire / Kommentare / Comments

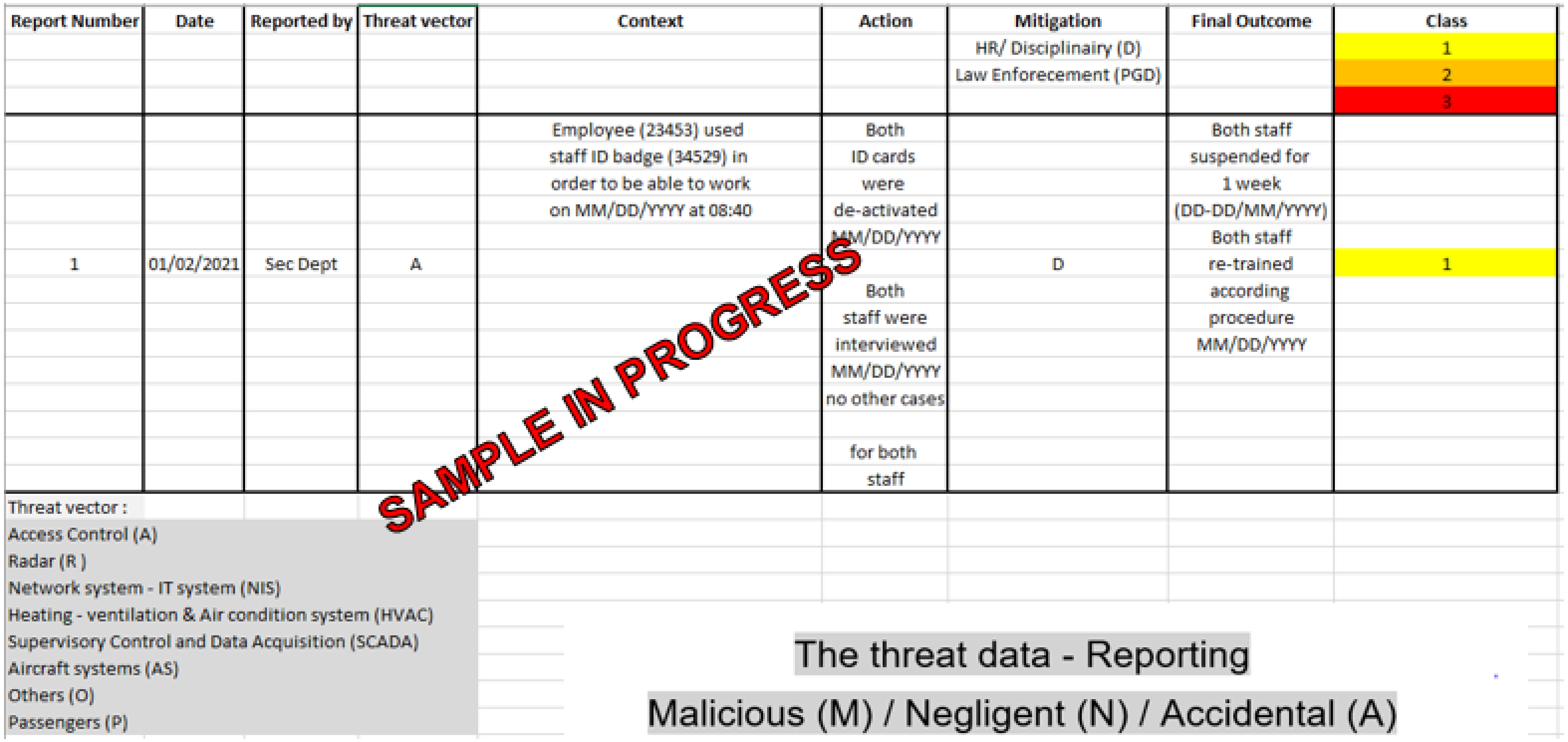
Solution / Sollution / Sollution

phrase.

In relation to the reporting following actions have been put into place:

SAMPLE IN PROGRESS

Reporting



Report Number	Date	Reported by	Threat vector	Context	Action	Mitigation	Final Outcome	Class
						HR/ Disciplinairy (D)		1
						Law Enforecement (PGD)		2
								3
1	01/02/2021	Sec Dept	A	Employee (23453) used staff ID badge (34529) in order to be able to work on MM/DD/YYYY at 08:40	Both ID cards were de-activated MM/DD/YYYY Both staff were interviewed MM/DD/YYYY no other cases for both staff	D	Both staff suspended for 1 week (DD-DD/MM/YYYY) Both staff re-trained according procedure MM/DD/YYYY	1

Threat vector :
Access Control (A)
Radar (R)
Network system - IT system (NIS)
Heating - ventilation & Air condition system (HVAC)
Supervisory Control and Data Acquisition (SCADA)
Aircraft systems (AS)
Others (O)
Passengers (P)

The threat data - Reporting

Malicious (M) / Negligent (N) / Accidental (A)

How to construct an efficient Security Culture ?

- Recognizing that effective security is critical to business success;
- Establishing an appreciation of positive security practices among employees (thank you – feedback);
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or burdensome expense.

Conformity

Adoption of security compliance in organizations involves:

- Implementation of effective and balanced information security measures and mechanisms;
- Compliance with legal and security requirements and needs of organizations;
- Maintaining both employees' and stakeholders' confidence and trust in the security.

DAC Strategy

- Enhance Security Culture – Insider Threat in the Security Awareness Training (SATP);
- Provide guidelines for the stakeholders on what to do.
- Besides our air carrier operators, the Regulated agents, Known consignors and Known Suppliers also DAC/ALSA needs to introduce a security culture reporting system for security occurrences, drawing from the experience gained from the establishment and implementation of just culture systems in safety.
- Ensure that an insider threat dedicated programme, awareness and reporting is put in place by operators.
- Assess who is the competent authority for the implementation and follow-up of the reporting system(s). (for insider threat)
- Reference: Regulation (EU) 2020/910 COMMISSION Article 2, second sentence, of the Regulation (EU) 2019/103, "31 December 2020" is replaced by "31 December 2021".

As a result, the DAC will not start with quality control monitoring activities in this area as of the year 2022.

Course contents (positive)

1.Goal of the training : What is an effective Security Culture and what are its advantages ?

Security Culture: ''*Security culture is an organizational culture that encourages optimal security performance. Organizational culture is commonly understood to be a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of organizations and are reflected by the actions and behaviors of all entities and personnel within those organizations. Security culture cannot be considered in isolation from the organizational culture as a whole."*

Avantages :

"a) continuously improve security, encompassing the effectiveness and efficiency of security in mitigating risks;

b) encourage awareness of and alertness to security risks by all personnel and the role that they personally play in identifying, eliminating or reducing those risks. Encourage familiarity with security issues, procedures and response mechanisms (e.g. whom to call in case of suspicious activity);

c) allow the necessary time and make the necessary efforts to comply with security measures, even when under pressure;

d) promote willingness to accept responsibility, be pro-active and make decisions autonomously in the event of security occurrences (which include incidents, deficiencies and breaches);

e) challenge other personnel in case of irregularities and accept being challenged;

f) immediately report occurrences or any suspicious activity that might be security-related;

g) foster critical thinking regarding security and interest in identifying potential security vulnerabilities, deviation from applicable procedures, and solutions; and

h) handle sensitive aviation security information appropriately"

Course contents (positive)

2. Integrate also the internal threat and radicalisation in the course

Definition Internal Threat : Any individual with inside knowledge or access has the potential to harm the organization and its people.
(this definition takes in consideration theft, fraud, espionage, workspace violence, sabotage, other criminal activities)
Note : Explain the 3 types of internal threat (malicious, negligent, accidental).
Note : Encourage the participants of the course to consult the web site.
https://help2protect.info/module/ in order to improve their knowledge on insider threat.
Definition Radicalisation : the phenomenon of people embracing opinions, views and ideas, which can led to an act of (Insider Threat) terrorism.

Course contents (positive)

3. Striking stories and messages (Cover at least 3 stories, one from each to demonstrate the difference).

4. Discuss the ICAO Security Culture Toolkit that should be available to all staff.

5. Rules of behavior (how do I behave, what I should do).

6. Explain how your entity could be the target of an internal threat.

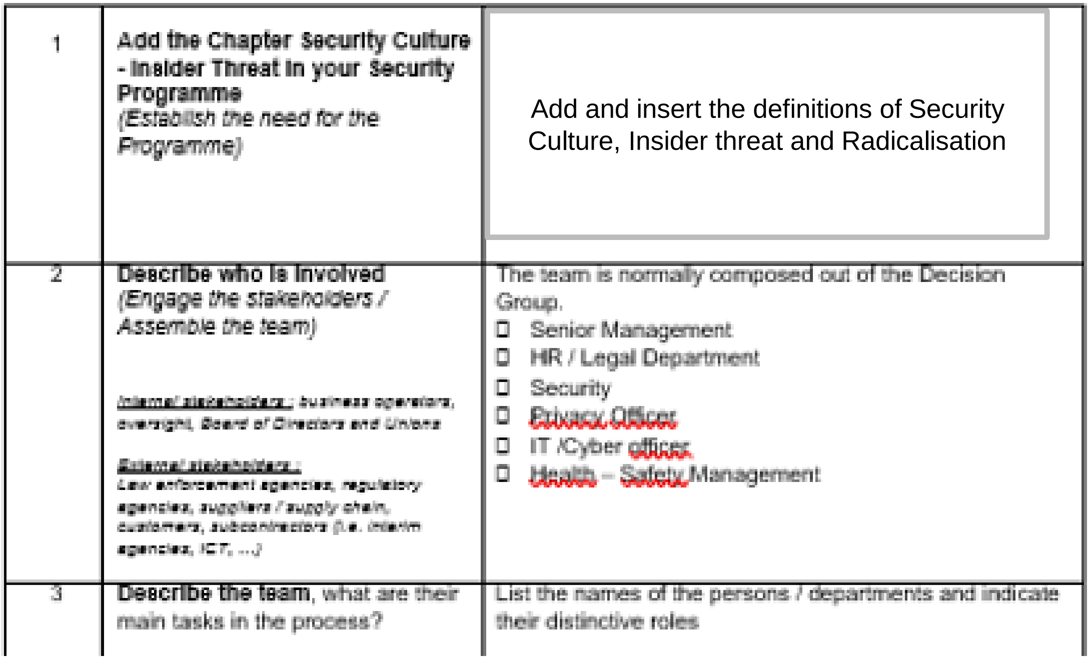
7. Explain the red flags for internal threats.

8. Explain the reporting procedures (+ add example) where it is and who to send it to.

9. Final word - resume key points.

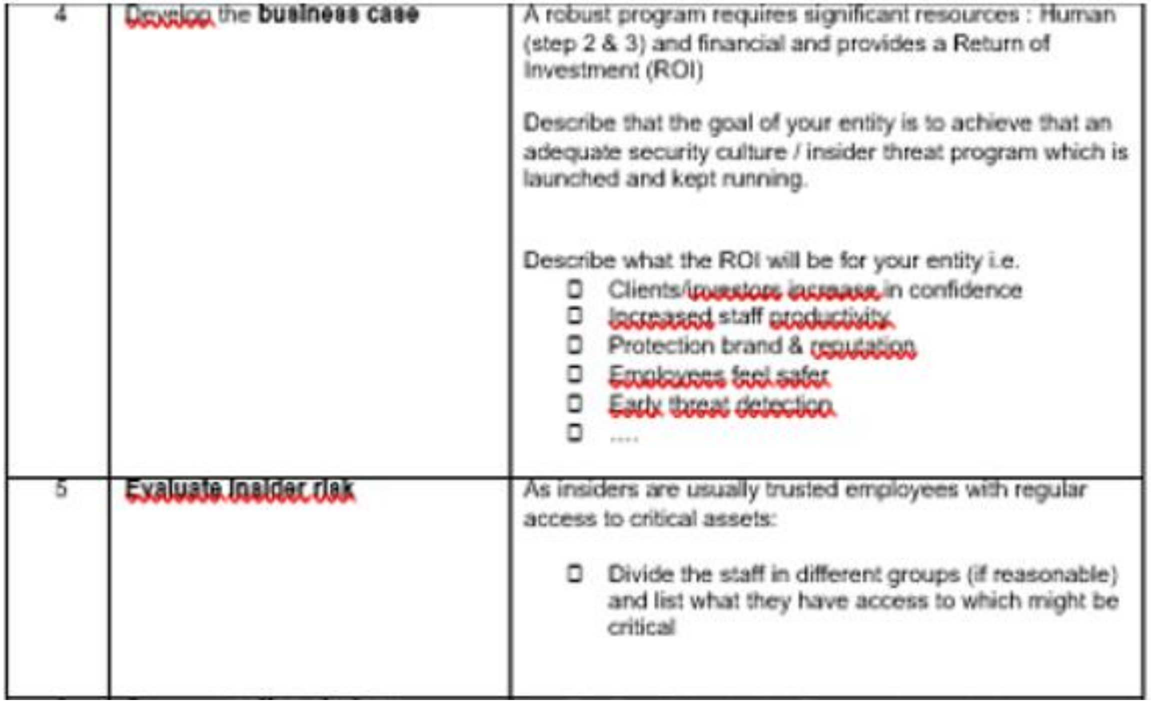
10. Questions (course evaluation form) + Keep attendance list of participants.

Security Programme



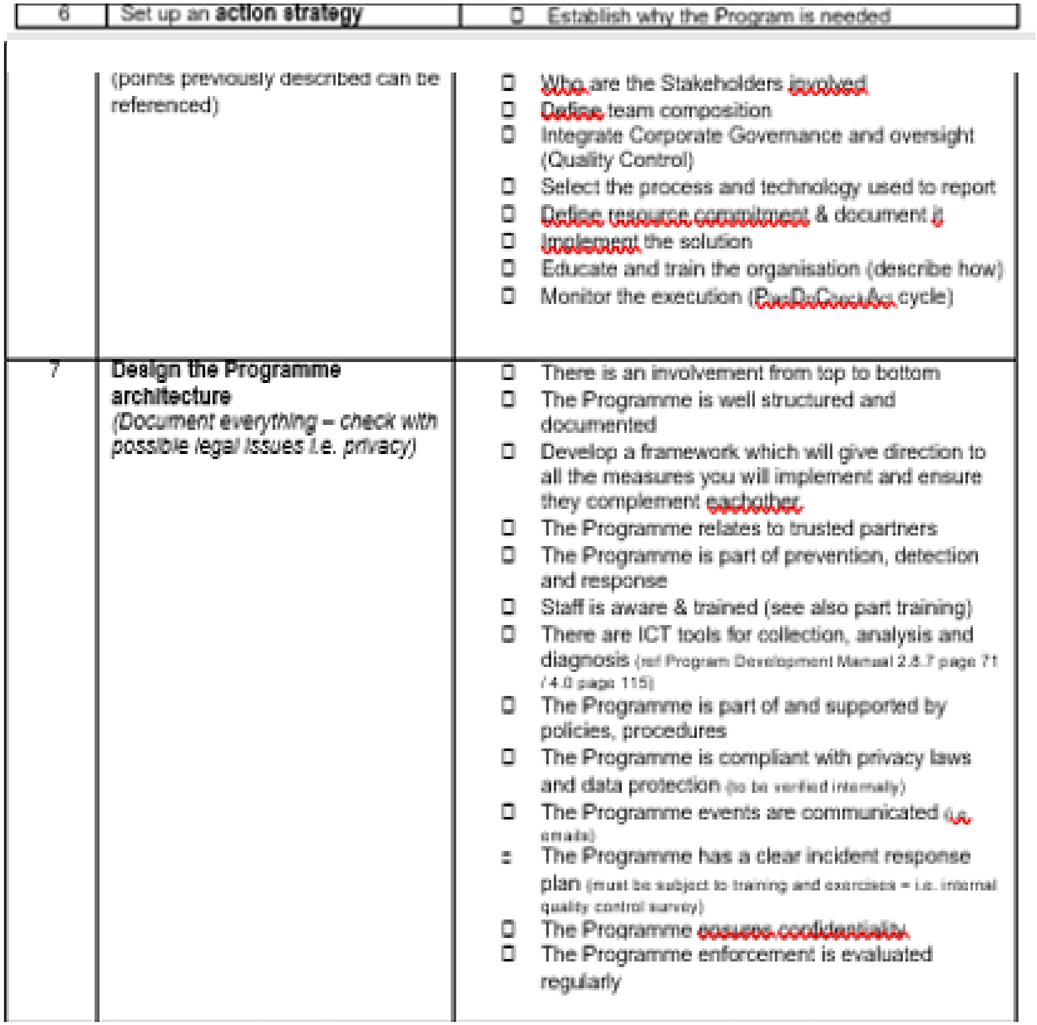
1	**Add the Chapter Security Culture - Insider Threat in your Security Programme** *(Establish the need for the Programme)*	Add and insert the definitions of Security Culture, Insider threat and Radicalisation
2	**Describe who is involved** *(Engage the stakeholders / Assemble the team)* *Internal stakeholders : business operators, oversight, Board of Directors and Unions* *External stakeholders : Law enforcement agencies, regulatory agencies, suppliers / supply chain, customers, subcontractors (i.e. interim agencies, ICT, ...)*	The team is normally composed out of the Decision Group. □ Senior Management □ HR / Legal Department □ Security □ Privacy Officer □ IT /Cyber officer □ Health – Safety Management
3	**Describe the team**, what are their main tasks in the process?	List the names of the persons / departments and indicate their distinctive roles

Security Programme



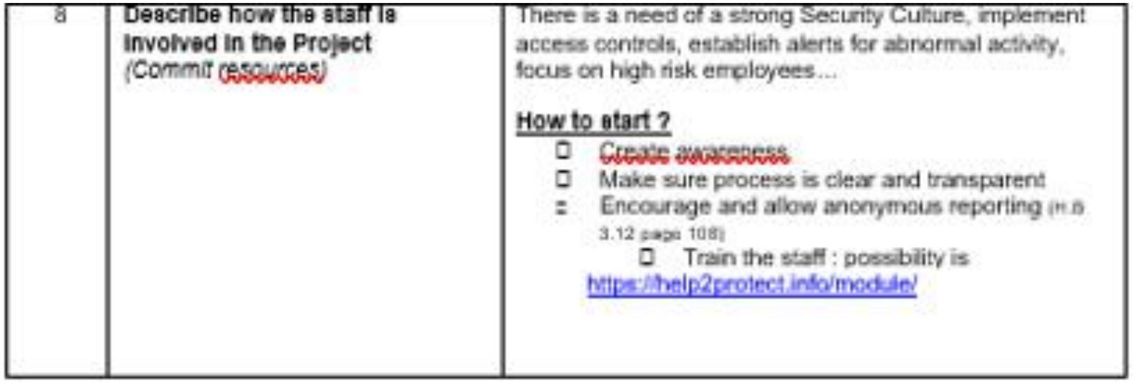
4	Develop the **business case**	A robust program requires significant resources : Human (step 2 & 3) and financial and provides a Return of Investment (ROI) Describe that the goal of your entity is to achieve that an adequate security culture / insider threat program which is launched and kept running. Describe what the ROI will be for your entity i.e. □ Clients/investors increase in confidence □ Increased staff productivity □ Protection brand & reputation □ Employees feel safer □ Early threat detection □ .....
5	**Evaluate Insider risk**	As insiders are usually trusted employees with regular access to critical assets: □ Divide the staff in different groups (if reasonable) and list what they have access to which might be critical

Security Programme

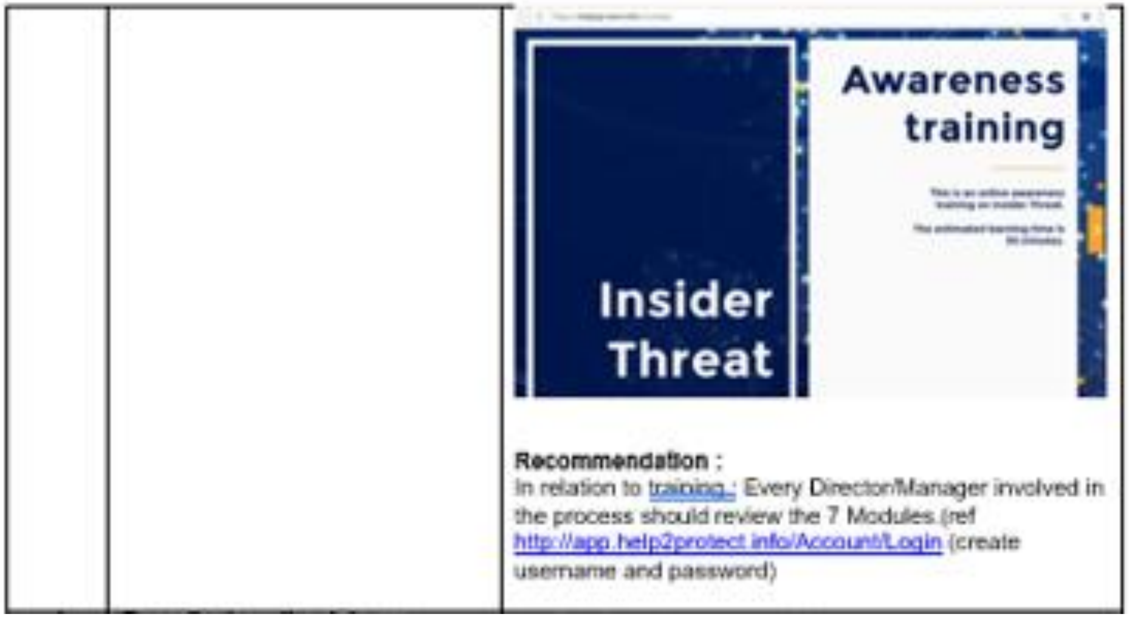


6	Set up an **action strategy** (points previously described can be referenced)	□ Establish why the Program is needed □ Who are the Stakeholders involved □ Define team composition □ Integrate Corporate Governance and oversight (Quality Control) □ Select the process and technology used to report □ Define resource commitment & document it □ Implement the solution □ Educate and train the organisation (describe how) □ Monitor the execution (PlanDoCheckAct cycle)
7	**Design the Programme architecture** *(Document everything – check with possible legal issues i.e. privacy)*	□ There is an involvement from top to bottom □ The Programme is well structured and documented □ Develop a framework which will give direction to all the measures you will implement and ensure they complement eachother. □ The Programme relates to trusted partners □ The Programme is part of prevention, detection and response □ Staff is aware & trained (see also part training) □ There are ICT tools for collection, analysis and diagnosis (ref Program Development Manual 2.8.7 page 71 / 4.0 page 115) □ The Programme is part of and supported by policies, procedures □ The Programme is compliant with privacy laws and data protection (to be verified internally) □ The Programme events are communicated (i.e. emails) □ The Programme has a clear incident response plan (must be subject to training and exercises = i.e. internal quality control survey) □ The Programme ensures confidentiality □ The Programme enforcement is evaluated regularly

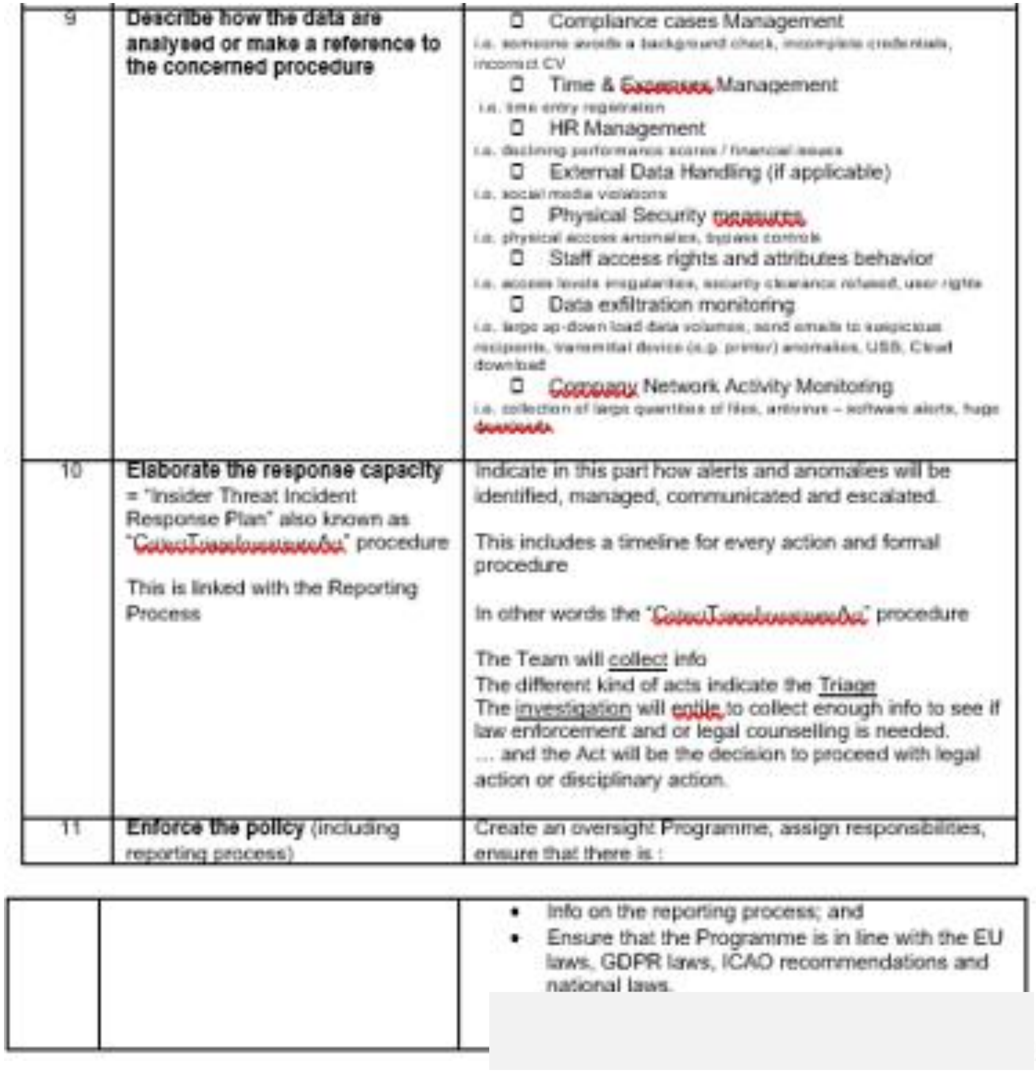
Security Programme



8	**Describe how the staff is involved in the Project** (Commit resources)	There is a need of a strong Security Culture, implement access controls, establish alerts for abnormal activity, focus on high risk employees… **How to start ?** □ Create awareness □ Make sure process is clear and transparent ▪ Encourage and allow anonymous reporting (H.5 3.12 page 108) □ Train the staff : possibility is https://help2protect.info/module/



		Recommendation : In relation to training : Every Direction/Manager involved in the process should review the 7 Modules (ref http://app.help2protect.info/Account/Login (create username and password)



9	**Describe how the data are analysed or make a reference to the concerned procedure**	□ Compliance cases Management i.e. someone avoids a background check, incomplete credentials, incorrect CV □ Time & Expenses Management i.e. time entry registration □ HR Management i.e. declining performance scores / financial issues □ External Data Handling (if applicable) i.e. social media violations □ Physical Security measures i.e. physical access anomalies, bypass controls □ Staff access rights and attributes behavior i.e. access levels irregularities, security clearance refused, user rights □ Data exfiltration monitoring i.e. large up-down load data volumes, send emails to suspicious recipients, transmittal device (e.g. printer) anomalies, USB, Cloud download □ Company Network Activity Monitoring i.e. collection of large quantities of files, antivirus – software alerts, huge downloads
10	**Elaborate the response capacity** = "Insider Threat Incident Response Plan" also known as "CollectTriageInvestigateAct" procedure This is linked with the Reporting Process	Indicate in this part how alerts and anomalies will be identified, managed, communicated and escalated. This includes a timeline for every action and formal procedure In other words the "CollectTriageInvestigateAct" procedure The Team will collect info The different kind of acts indicate the Triage The investigation will entile to collect enough info to see if law enforcement and or legal counselling is needed. … and the Act will be the decision to proceed with legal action or disciplinary action.
11	**Enforce the policy** (including reporting process)	Create an oversight Programme, assign responsibilities, ensure that there is :
		- Info on the reporting process; and - Ensure that the Programme is in line with the EU laws, GDPR laws, ICAO recommendations and national laws.

End part 1

Questions ?

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Test

Insider Threat & Radicalization

Security Culture

Documentation

Legal Basis

Preparation

Reference Help2Protect (compressed version of the 7 Modules)

Module 1 : The ROI of the Programme

- Why should every organization have an internal threat program and what is the Return on Investment (ROI) ?

- It's not “ if " it's a question of “ when "

- What is the internal threat?

Any individual with inside knowledge or access has the potential to harm the organization and its people.

- The threat does not always come from employees .... Other organizations may have access to your desktops and data.

What incidents involving internal threats go unnoticed?

- Lend badges to colleagues.
- Illegal copying of information to personal devices.
- Share passwords.
- Authorization of visitors without airport ID cards or without escort.

Different kind of Insiders

- Malicious : Ego, personal advantage, money, political or religious belief.
- Negligent : Employees who are aware of security policies and procedures but decide to bypass them.
- Accidental : Employees who are aware of security policies and procedures but accidentally bypass them.

Average cost of an Insider Threat

- The average cost of an insider incident is 350,000 euros
- Well-built internal threat program bring return on investment (ROI)

Conclusion Module 1

- Any individual with insider knowledge or access has the potential to harm the organization and its people

- All organizations are vulnerable to insider threats

- A well-built and implemented insider Threat Program provides real and immediate Return on Investment (ROI)

Module 2 : The Internal Threat

- We learn more about the person’s predispositions and motivations and what are the indicators of radicalization.
- Threats are on the rise (economic crises, digitalization, etc.)
- People are hard to find (trust), they know what is most vulnerable to the organization.

Example (Daallo Airlines flight 159 - bomb hidden in a laptop).

The CRIME model

- Compromise : an outsider coerces an employee to conduct an attack.
- Revenge : The employee feels wronged by the organization and conducts the attack to ‘get even’….
- Ideology : The employee supports ideals, which are contrary to those supported by the organization or by society in general.
- Money : The employee conducts the attack for financial gain.
- Ego : The employee likes the excitement of it and/or thinks (s)he can be smarter than the organization’s security

The path to insider threat, radicalization, terrorism

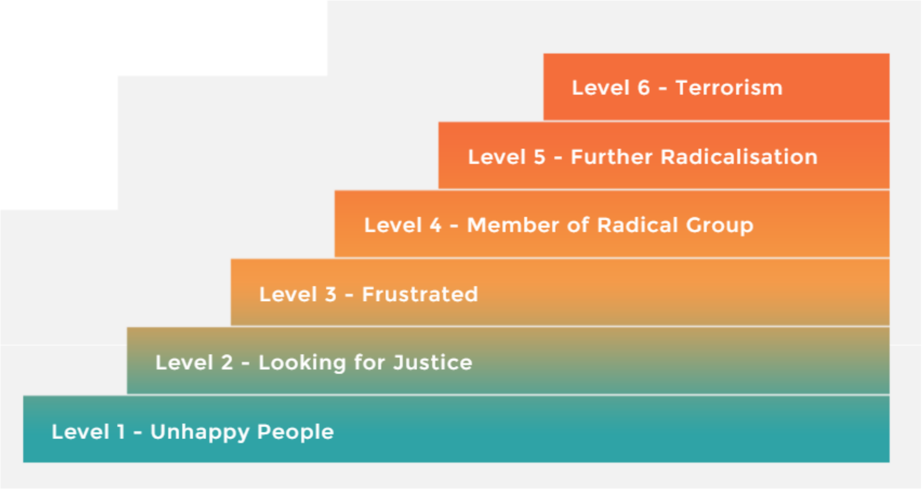
- There is a path the employee takes before becoming a threat.
- Employee makes individual decisions and displays a number of observable behaviors.
- By matching observable behaviors to phases, those investigating can get an idea where the employee stands at a certain period.

3 stages of the route

- Most employees do not join an organization with the intent to become an internal threat.
- After being hired, the employee experiences some kind of significant life change.
- The employee then takes a series of actions, which lead to a threat.

Violent radicalization

- We speak of violent radicalization when people embrace opinions, views and ideas, which can lead to acts of (Insider Threat) terrorism.
- Indicators : unusual visitors, office or work premises used as a suspicious meeting area, unusual activities at strange hours, unusual garbage disposal, misuse of company cars, cars/vans used as observation vehicles, overdue parked cars in parking lots, unusual lifestyle, cash related crimes…
- 'The stairway to terrorism' and these indicators show some insight into this process.



Level 6 - Terrorism

Level 5 - Further Radicalisation

Level 4 - Member of Radical Group

Level 3 - Frustrated

Level 2 - Looking for Justice

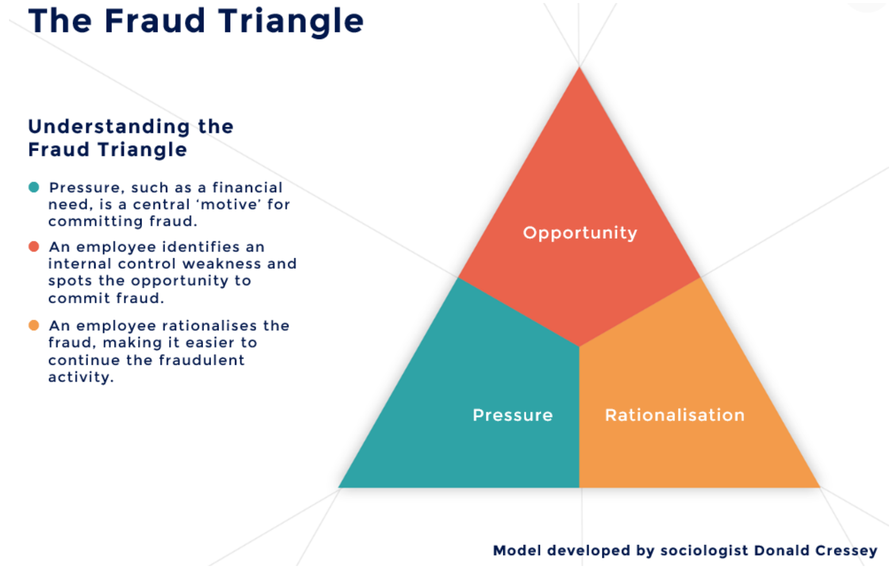
Level 1 - Unhappy People

Conclusion Module 2

- Insiders are hard to find and can hide in plain sight.
- Insiders are trusted and are supposed, or entitled to have access to sensitive assets.
- They are aware of what is most vulnerable to the organization, and they know many of the security controls.
- Not only is the keeping of confidential data a serious issue, but companies must also have a solid process to thoroughly check and revoke all (online) credentials after an employee leaves. This will prevent them from accessing information or areas to which they no longer have access!

- Insider incidents are on the rise….
- Challenging intruders, or those with access is not enough (action required)
- Who are the insiders ? (mainly people you trust, know the weaknesses of an organization)

The 5 models of insider threat

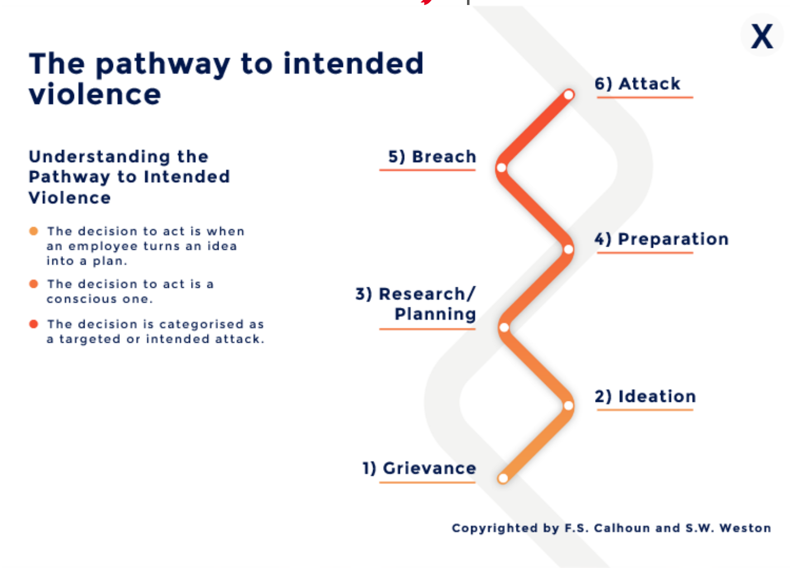


The Fraud Triangle

Understanding the Fraud Triangle

- Pressure, such as a financial need, is a central 'motive' for committing fraud.
- An employee identifies an internal control weakness and spots the opportunity to commit fraud.
- An employee rationalises the fraud, making it easier to continue the fraudulent activity.

Model developed by sociologist Donald Cressey

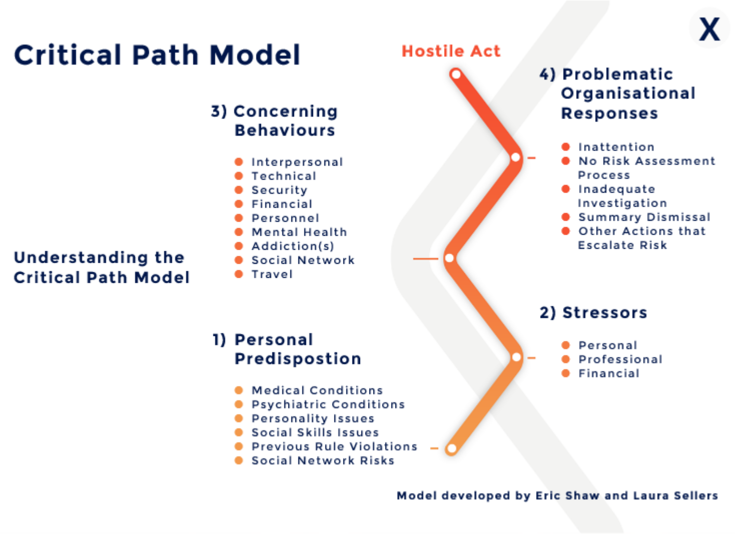


The pathway to intended violence

Understanding the Pathway to Intended Violence

- The decision to act is when an employee turns an idea into a plan.
- The decision to act is a conscious one.
- The decision is categorised as a targeted or intended attack.

Copyrighted by F.S. Calhoun and S.W. Weston



Critical Path Model

Understanding the Critical Path Model

4) Problematic Organisational Responses

- Inattention
- No Risk Assessment Process
- Inadequate Investigation
- Summary Dismissal
- Other Actions that Escalate Risk

3) Concerning Behaviours

- Interpersonal
- Technical
- Security
- Financial
- Personnel
- Mental Health
- Addiction(s)
- Social Network
- Travel

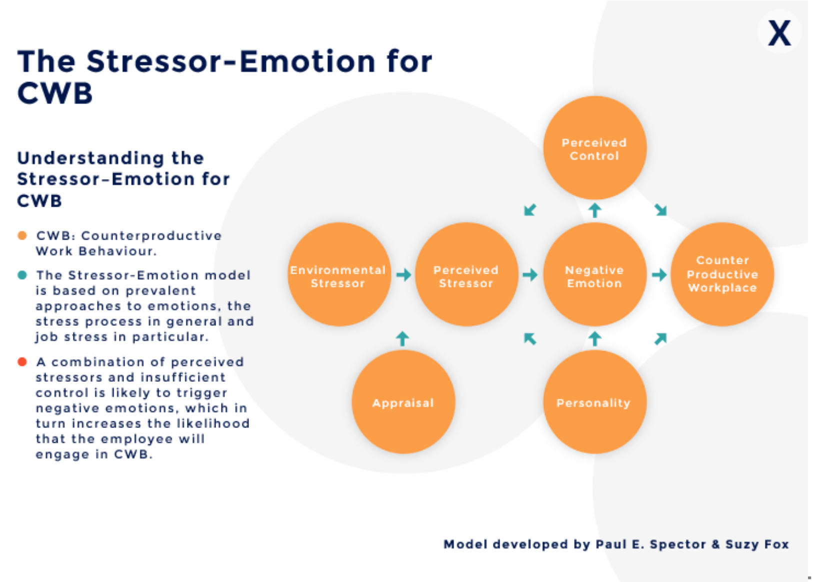
2) Stressors

- Personal
- Professional
- Financial

1) Personal Predispostion

- Medical Conditions
- Psychiatric Conditions
- Personality Issues
- Social Skills Issues
- Previous Rule Violations
- Social Network Risks

Model developed by Eric Shaw and Laura Sellers



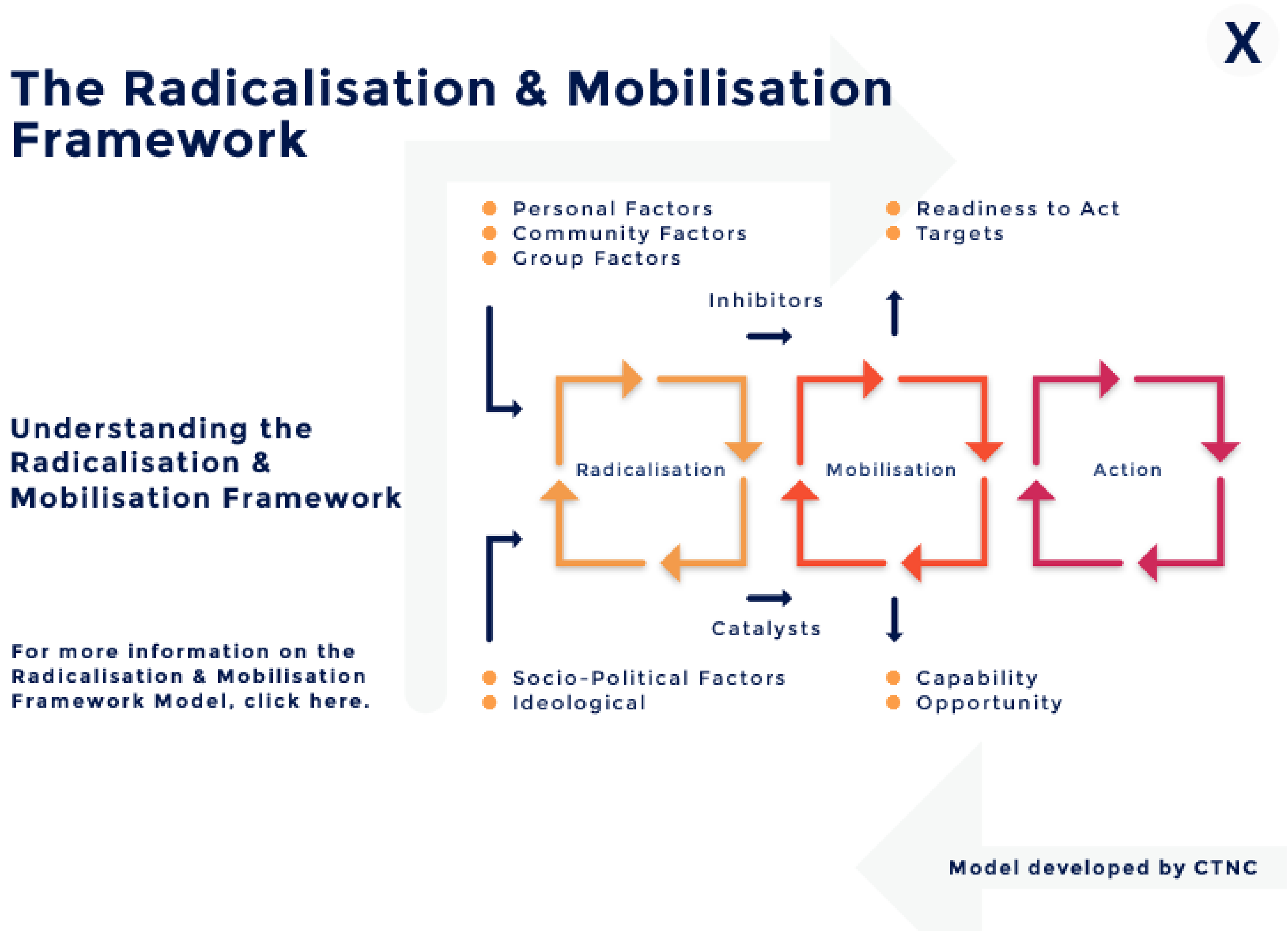
The Stressor-Emotion for CWB

Understanding the Stressor-Emotion for CWB

- CWB: Counterproductive Work Behaviour.
- The Stressor-Emotion model is based on prevalent approaches to emotions, the stress process in general and job stress in particular.
- A combination of perceived stressors and insufficient control is likely to trigger negative emotions, which in turn increases the likelihood that the employee will engage in CWB.

Model developed by Paul E. Spector & Suzy Fox

The 5 models of insider threat



X

The Radicalisation & Mobilisation Framework

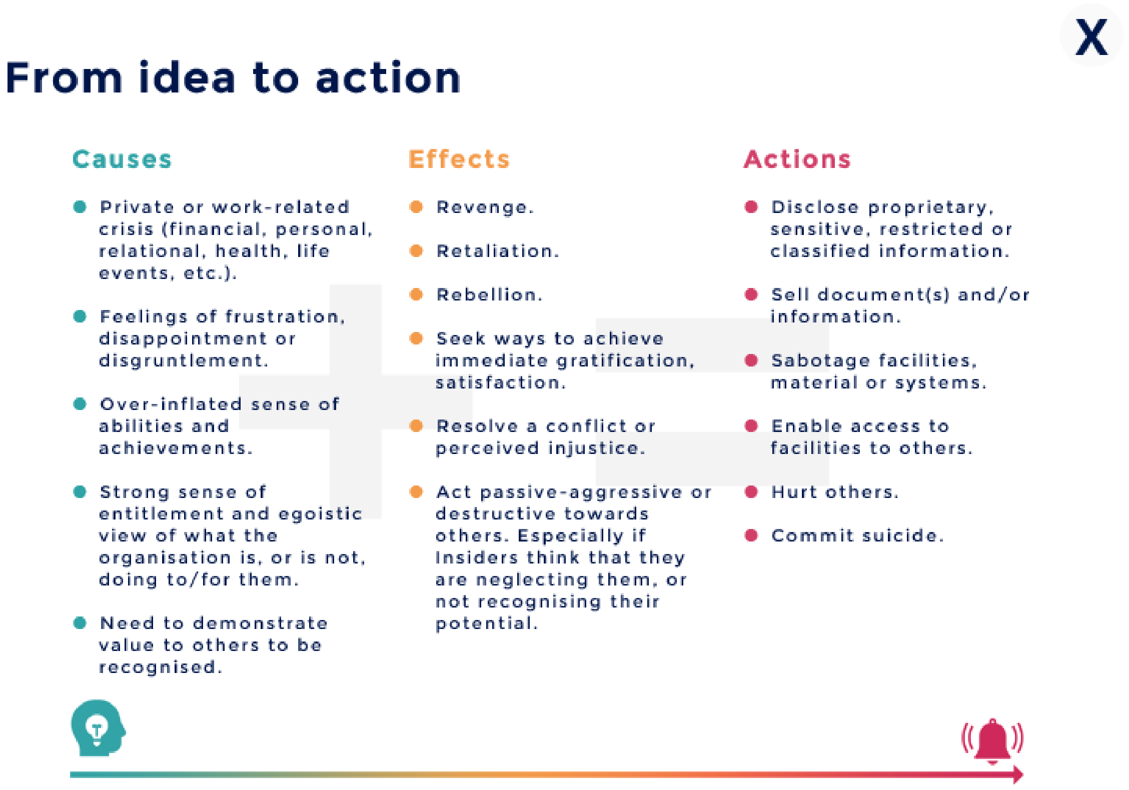
Understanding the Radicalisation & Mobilisation Framework

For more information on the Radicalisation & Mobilisation Framework Model, click here.

Model developed by CTNC

Indicators

- ➢ It is important to identify a threat in time, so threat indicators help identify insiders in time.
- ➢ There are observable behaviors



From idea to action

Causes

- Private or work-related crisis (financial, personal, relational, health, life events, etc.).
- Feelings of frustration, disappointment or disgruntlement.
- Over-inflated sense of abilities and achievements.
- Strong sense of entitlement and egoistic view of what the organisation is, or is not, doing to/for them.
- Need to demonstrate value to others to be recognised.

Effects

- Revenge.
- Retaliation.
- Rebellion.
- Seek ways to achieve immediate gratification, satisfaction.
- Resolve a conflict or perceived injustice.
- Act passive-aggressive or destructive towards others. Especially if Insiders think that they are neglecting them, or not recognising their potential.

Actions

- Disclose proprietary, sensitive, restricted or classified information.
- Sell document(s) and/or information.
- Sabotage facilities, material or systems.
- Enable access to facilities to others.
- Hurt others.
- Commit suicide.

Conclusion Module 3

- There is no single model that fully explains the variety of insider threats.
- Protecting the confidential nature of data is essential.
- Companies must have a solid process to revoke all credentials, offline and online, of employees leaving the company, with immediate effect. This will eliminate the risk of them accessing information or areas to which they are no longer entitled.

Module 4 : The Approach

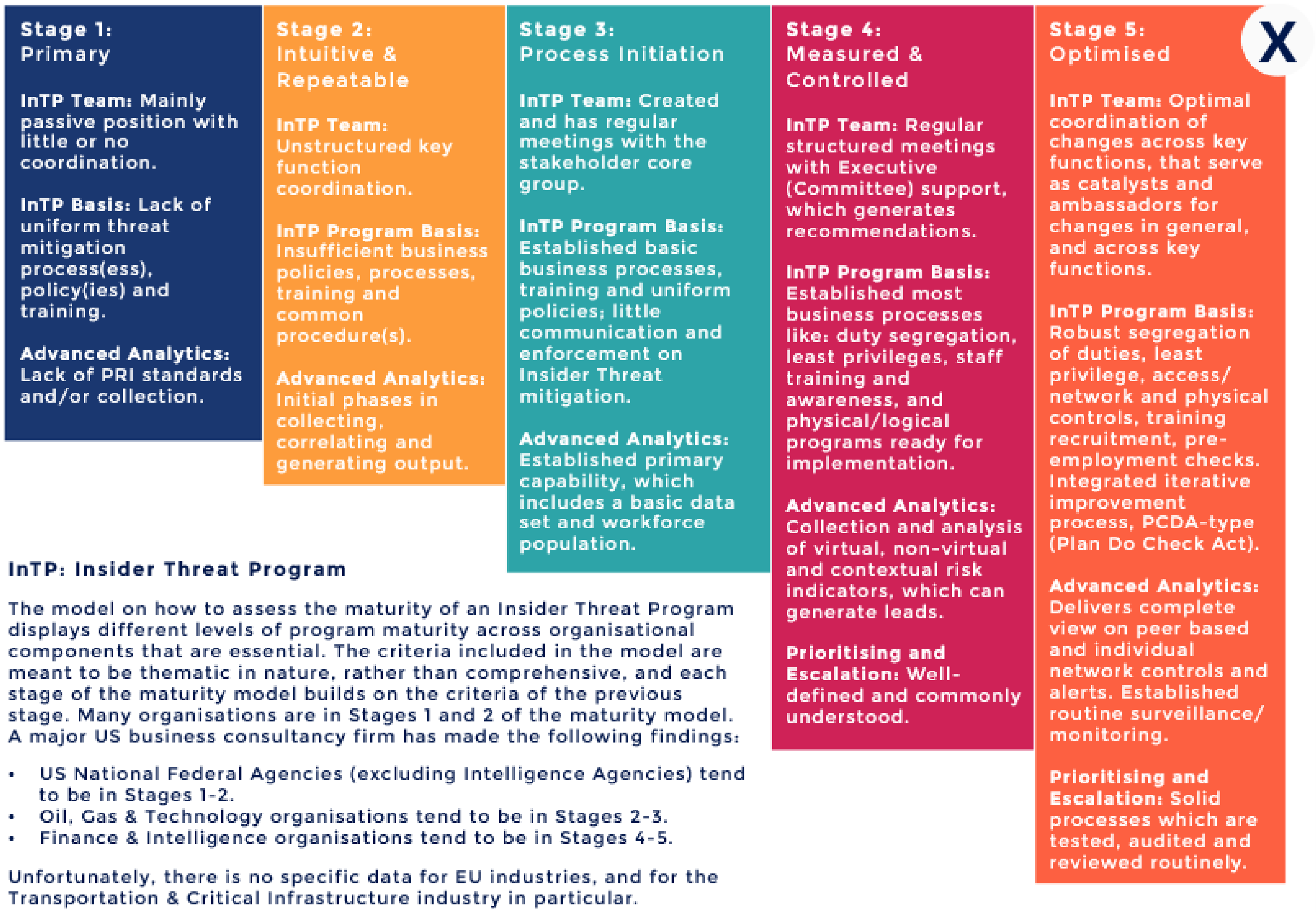
- Challenges of building an effective Insider Threat Programme.

- Explore the process of building an effective Insider Threat Programme.

Before building a Programme….

- What are our critical points, those that, if compromised, would have the most impact on the business?
- Do these points correspond to the priorities of our business continuity plan?
- What measures are in place to protect us?
- How do I identify internal and external threats?
- Who are the potential insiders that are putting our business at risk?
- How likely are they to act effectively?
- What is the impact on our business?
- What is the probability of (serious) damage?
- How will you react once a critical threat is detected?
- If we lost sensitive data, how would we react and minimize risk (GDPR)?

The 5 stages to build an Insider Threat Programme



Stage 1: Primary

InTP Team: Mainly passive position with little or no coordination.

InTP Basis: Lack of uniform threat mitigation process(ess), policy(ies) and training.

Advanced Analytics: Lack of PRI standards and/or collection.

Stage 2: Intuitive & Repeatable

InTP Team: Unstructured key function coordination.

InTP Program Basis: Insufficient business policies, processes, training and common procedure(s).

Advanced Analytics: Initial phases in collecting, correlating and generating output.

Stage 3: Process Initiation

InTP Team: Created and has regular meetings with the stakeholder core group.

InTP Program Basis: Established basic business processes, training and uniform policies; little communication and enforcement on Insider Threat mitigation.

Advanced Analytics: Established primary capability, which includes a basic data set and workforce population.

Stage 4: Measured & Controlled

InTP Team: Regular structured meetings with Executive (Committee) support, which generates recommendations.

InTP Program Basis: Established most business processes like: duty segregation, least privileges, staff training and awareness, and physical/logical programs ready for implementation.

Advanced Analytics: Collection and analysis of virtual, non-virtual and contextual risk indicators, which can generate leads.

Prioritising and Escalation: Well-defined and commonly understood.

Stage 5: Optimised

InTP Team: Optimal coordination of changes across key functions, that serve as catalysts and ambassadors for changes in general, and across key functions.

InTP Program Basis: Robust segregation of duties, least privilege, access/ network and physical controls, training recruitment, pre-employment checks. Integrated iterative improvement process, PCDA-type (Plan Do Check Act).

Advanced Analytics: Delivers complete view on peer based and individual network controls and alerts. Established routine surveillance/ monitoring.

Prioritising and Escalation: Solid processes which are tested, audited and reviewed routinely.

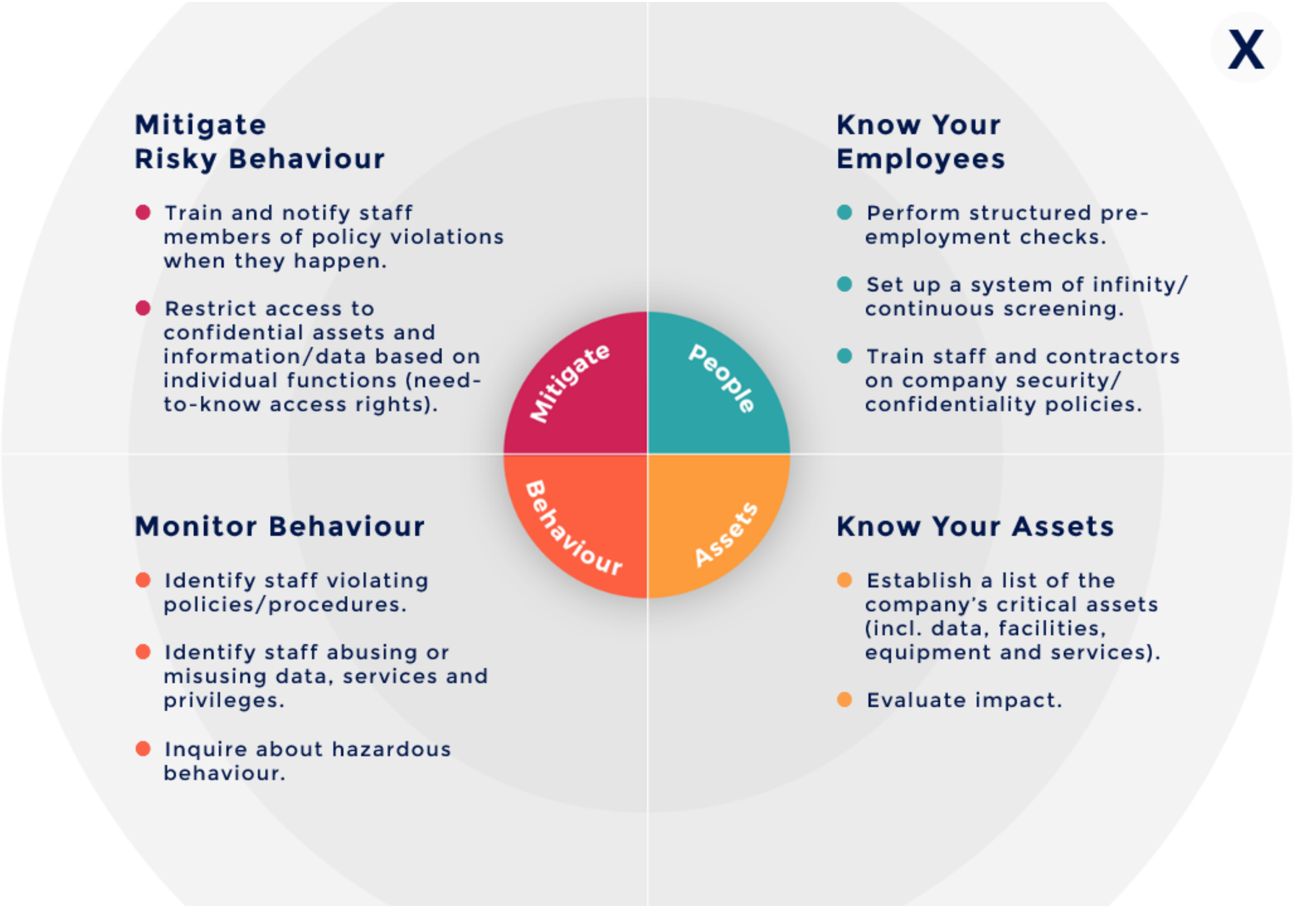
InTP: Insider Threat Program

The model on how to assess the maturity of an Insider Threat Program displays different levels of program maturity across organisational components that are essential. The criteria included in the model are meant to be thematic in nature, rather than comprehensive, and each stage of the maturity model builds on the criteria of the previous stage. Many organisations are in Stages 1 and 2 of the maturity model. A major US business consultancy firm has made the following findings:

- US National Federal Agencies (excluding Intelligence Agencies) tend to be in Stages 1-2.
- Oil, Gas & Technology organisations tend to be in Stages 2-3.
- Finance & Intelligence organisations tend to be in Stages 4-5.

Unfortunately, there is no specific data for EU industries, and for the Transportation & Critical Infrastructure industry in particular.

How to manage the Insider Threat effectively?



Mitigate Risky Behaviour

- Train and notify staff members of policy violations when they happen.
- Restrict access to confidential assets and information/data based on individual functions (need-to-know access rights).

Know Your Employees

- Perform structured pre-employment checks.
- Set up a system of infinity/continuous screening.
- Train staff and contractors on company security/confidentiality policies.

Monitor Behaviour

- Identify staff violating policies/procedures.
- Identify staff abusing or misusing data, services and privileges.
- Inquire about hazardous behaviour.

Know Your Assets

- Establish a list of the company's critical assets (incl. data, facilities, equipment and services).
- Evaluate impact.

Sharing information is key, as an alarm signal in one department cannot be known in another department….

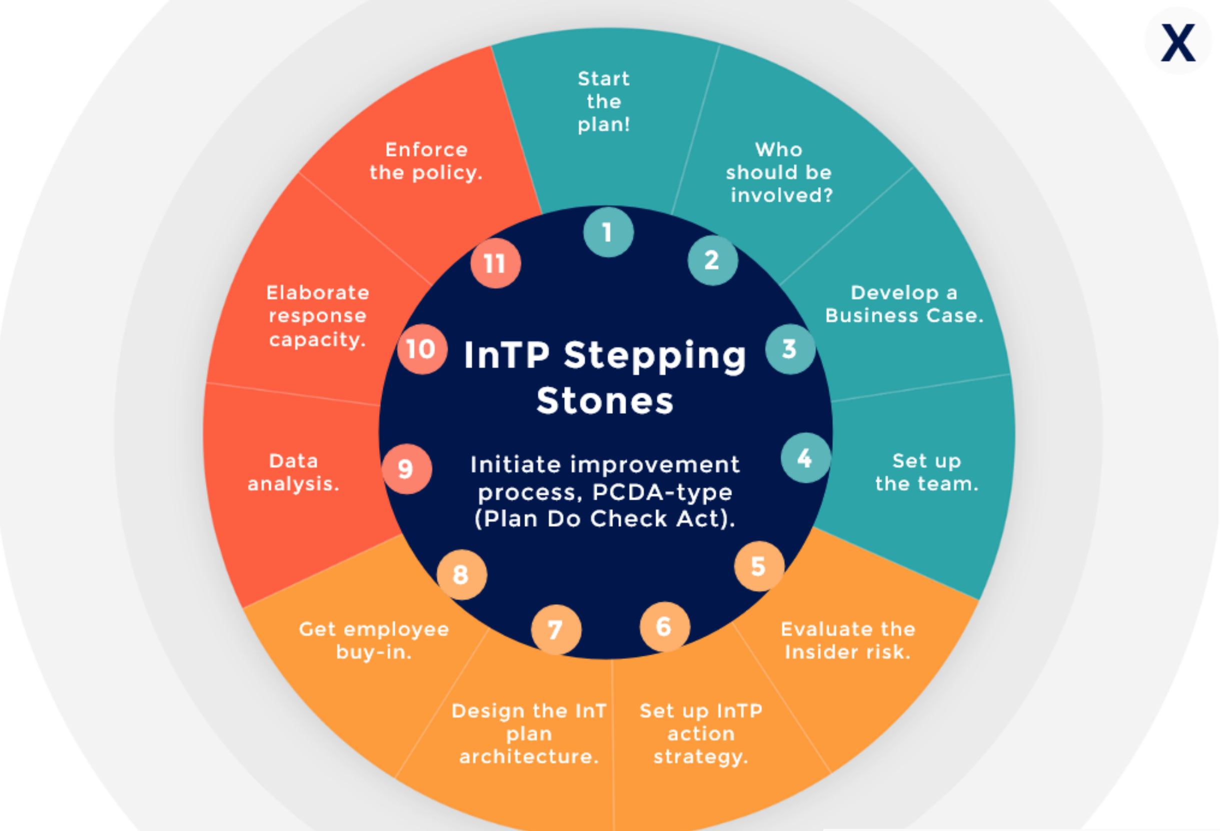
(red flag alarm)

- It's about protecting your assets, your employees and your customers.

- It will become mandatory.

- It can reduce insurance premiums.

The 11 parts that need to be covered in the Programme


X
InTP Stepping Stones
Initiate improvement process, PCDA-type (Plan Do Check Act).
1 Start the plan!
2 Who should be involved?
3 Develop a Business Case.
4 Set up the team.
5 Evaluate the Insider risk.
6 Set up InTP action strategy.
7 Design the InT plan architecture.
8 Get employee buy-in.
9 Data analysis.
10 Elaborate response capacity.
11 Enforce the policy.

This methodology includes 11 steps. Each step should be organised around five key concepts:

- **Goal**: What is the desired objective of the step?
- **Participants**: Who should be responsible for completing the objective?
- **Timeframe**: What is the time allotted for this step?
- **Justification**: Why is this step necessary?
- **Implementation**: What are the essential actions for completing the step?

Most common & annoying situations

- Ineffective termination procedures.
- Organizations are very vulnerable just before and immediately after the termination of employment.
- Consider an exit strategy for employees with in-depth knowledge of critical information.
- Lack of (pre-employment) investigations.
- Prevent previous offenders from entering the organization.
- Verification must be done periodically.

Note: Most employees become threats after being hired.

Did you know that ….

Internal threats are most frequently discovered by the IT department.

…..you might have thought it would be the Security Department.

Conclusion Module 4

- Follow the 11-step method to build your own effective Insider Threat Programme.

- Make sure you are well-informed when you start your Programme.

- Learn what others have put in place at where others did not met the expectations.

Module 5 : HR is the key to success

- Human resources are the key to a successful Internal Threat Programme.

- There are possibilities for continuous evaluation of staff.

- Post-employment awareness is just as important.

Who are most likely to become malicious ?

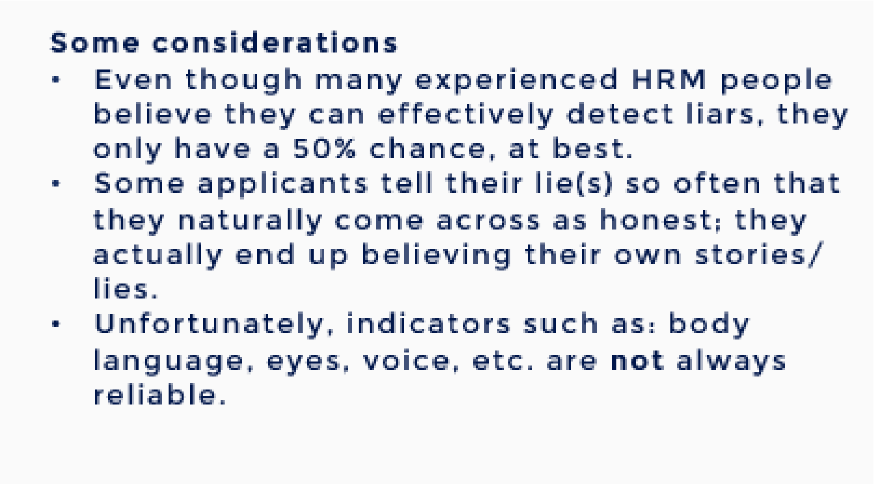
- Full-time workers

- Temporary workers, self-employed contractors and trainees.

- Guests, visitors, etc.

Honesty

- I was a Manager (in real life the person was an Assistant).
- I worked there for several years (the person hides a gap).
- I earned XX euros a year (lie on salary).
- I graduated from XYZ University.



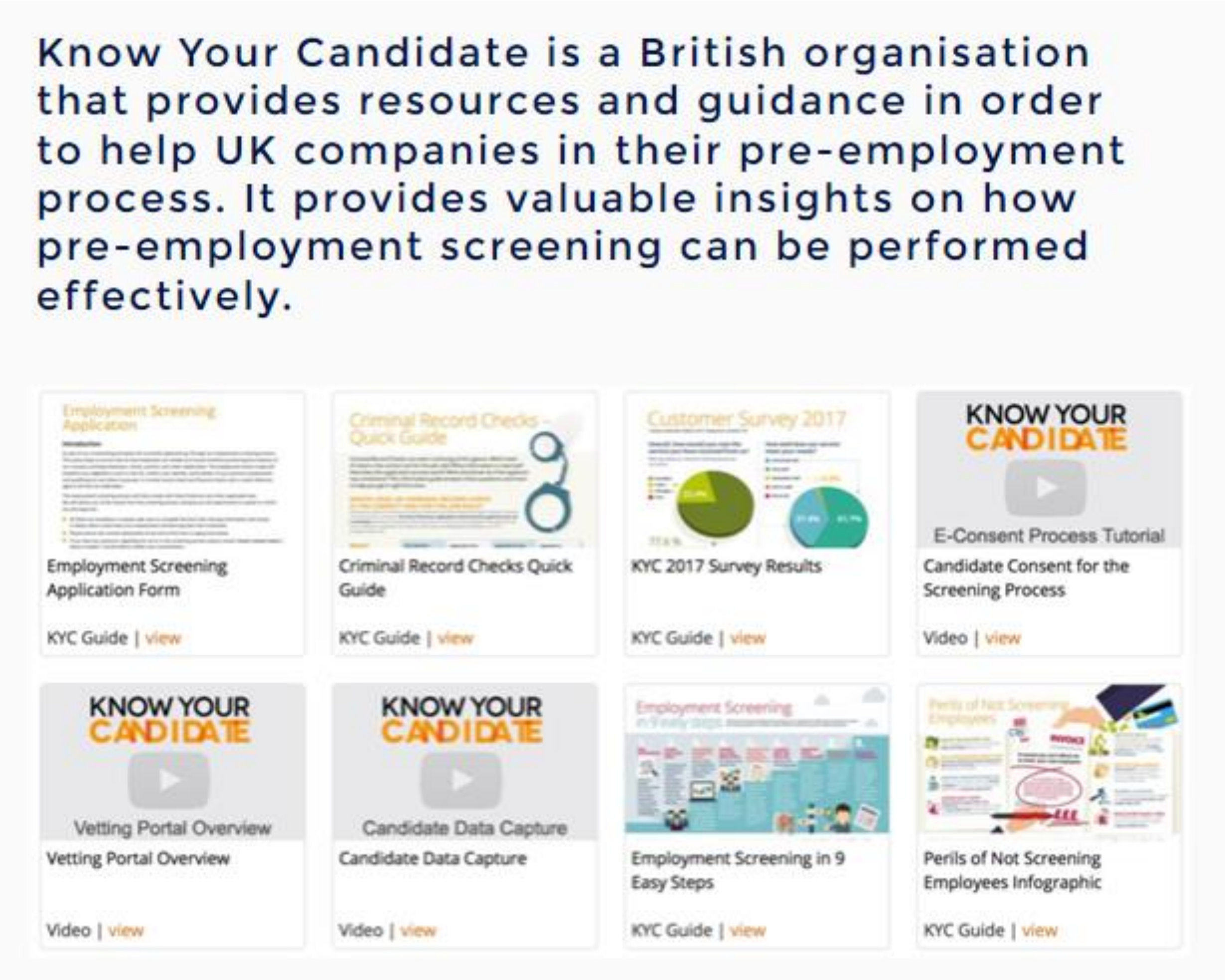
Some considerations

- Even though many experienced HRM people believe they can effectively detect liars, they only have a 50% chance, at best.
- Some applicants tell their lie(s) so often that they naturally come across as honest; they actually end up believing their own stories/ lies.
- Unfortunately, indicators such as: body language, eyes, voice, etc. are **not** always reliable.

8 reasons to develop a « safe hiring programme »

1. Safe hiring will help mitigate insider threats.
2. A bad hiring will have a negative financial impact.
3. Replacing a bad hire will have a financial impact as well, especially on management and director level.
4. Safe hiring will prevent workspace harassment and/or (verbal) violence.
5. Bad hires can upset the present workforce and/or union(s).
6. Bad hiring may lead to costly legal fees and litigation.
7. Safe hiring will prevent shareholder lawsuits / litigation (especially in litigious societies).
8. Bad hires will have a detrimental effect on the reputation (brand damage) of the organization.

Know your candidate



Know Your Candidate is a British organisation that provides resources and guidance in order to help UK companies in their pre-employment process. It provides valuable insights on how pre-employment screening can be performed effectively.

Employment Screening Application
Criminal Record Checks - Quick Guide
Customer Survey 2017
KNOW YOUR CANDIDATE
E-Consent Process Tutorial

Employment Screening Application Form

KYC Guide | view

Criminal Record Checks Quick Guide

KYC Guide | view

KYC 2017 Survey Results

KYC Guide | view

Candidate Consent for the Screening Process

Video | view

Vetting Portal Overview

Video | view

Candidate Data Capture

Video | view

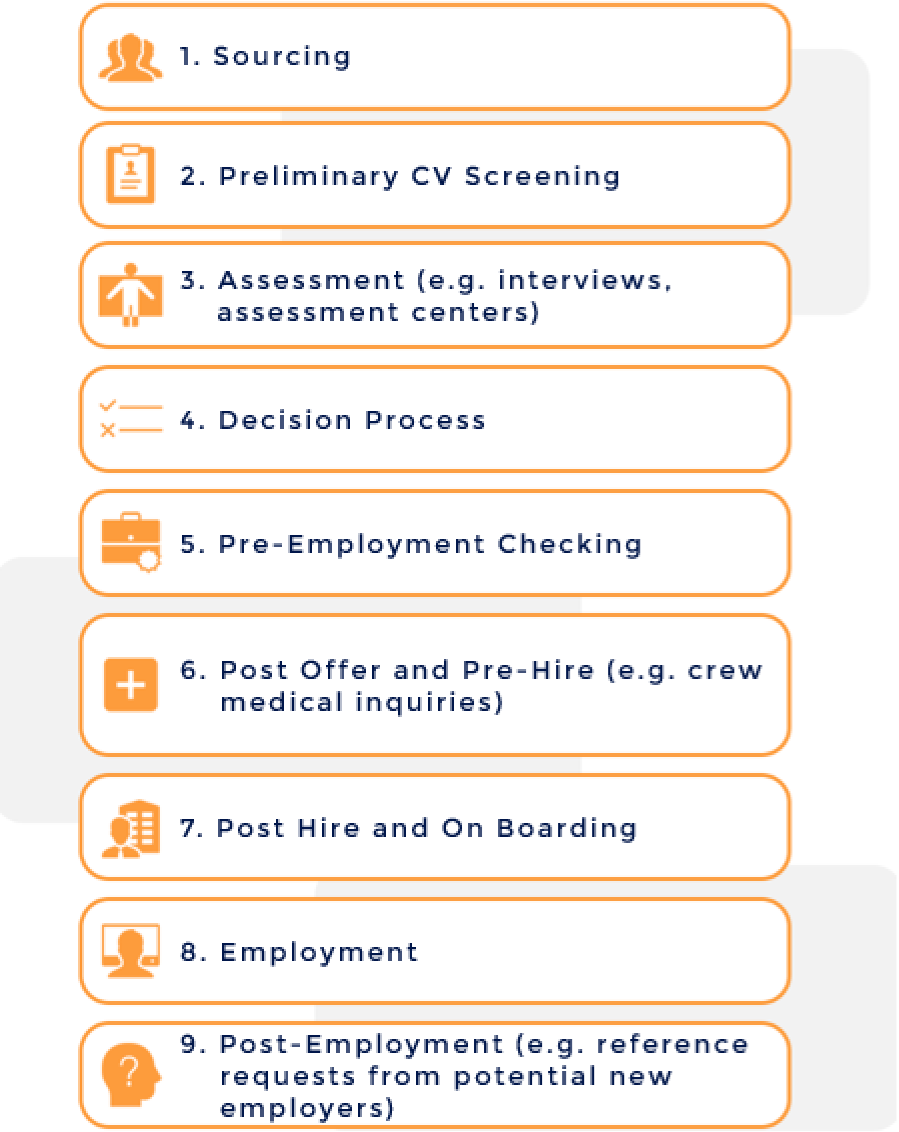
Employment Screening in 9 Easy Steps

KYC Guide | view

Perils of Not Screening Employees Infographic

KYC Guide | view

Recruitment phases



1. Sourcing
2. Preliminary CV Screening
3. Assessment (e.g. interviews, assessment centers)
4. Decision Process
5. Pre-Employment Checking
6. Post Offer and Pre-Hire (e.g. crew medical inquiries)
7. Post Hire and On Boarding
8. Employment
9. Post-Employment (e.g. reference requests from potential new employers)

Infinity screening (follow-up)

- Persons with wide access to IT or sensitive and/or proprietary information.

- Persons with access to cash, accounting, etc.

- Persons in sensitive positions with access to confidential information, such as customer lists, operational information, financial information, etc.

- Persons who can make (large) financial decisions.

- Any current or former employee / contractor with a grievance, and who might have access to a weapon (e.g. ex-military, law enforcement, security staff, etc.)

Risks during employment

Predictable risks

A staff member may have access to cash or assets, and while the need for internal controls might be well known, specific controls may need to be implemented.

Unpredictable risks

A staff member may develop financial issues, undergo stressful periods, have addiction issues, such as gambling, alcohol or drugs.
A superior may suggest, encourage, imply or order someone to perform acts of questionable honesty.

Hidden risks

A person with a political agenda gets a job to secretly pursue a goal that is detrimental to the employer’s interests.

Social network control

Employees can share content that conflicts with the organization's ethics.

Employees can be motivated to become an internal threat.

Take into account ethical, legal, discriminatory, confidentiality and accuracy issues.

How to proceed well ?

- Perform checks behind an ethics wall (neutral person).

- Have documented training on discrimination.

- Establish standard practices to show that decisions are made objectively.

- Consider showing negative elements to the applicant first.

When a staff member leaves …..

Scenarios you want to avoid

1. Access to restricted areas
2. Keep the computer soft-/hardware
3. Access to data or administration software

Pay attention to the people who are leaving your organization

- Plan an exit conversation.
- Use checklists.
- Change the password.
- Delete accounts on the last day.

Conclusion Module 5

- Make sure that our screening process is solid in order to avoid bad hires.
- You should have a continuous (infinity) evaluation in place for employees.
- Awareness does not stop after a staff member starts his/her job.
- Make sure that your exit procedures are solid for staff who are leaving your organization.

Change does not happen overnight..... So there is a need to define a strategy.

Management needs to be involved to create broad support.

Consider adapting an image to the program to help mark the message.

The strategy should include training and awareness.

Do not overdo communications, which could lead to a certain fatigue.

Protect yourself. Protect your family. Protect your community.
Vaccinate.
CONGRATS! WITH THAT LAST TEXT YOU'VE ACHIEVED STALKER STATUS.
THATSNOTCOOL.COM
TELL 'EM TO BACK OFF. SEND A CALLOUT CARD.
BE PROTECTED
WEAR YOUR SEATBELT

Do not forget privacy

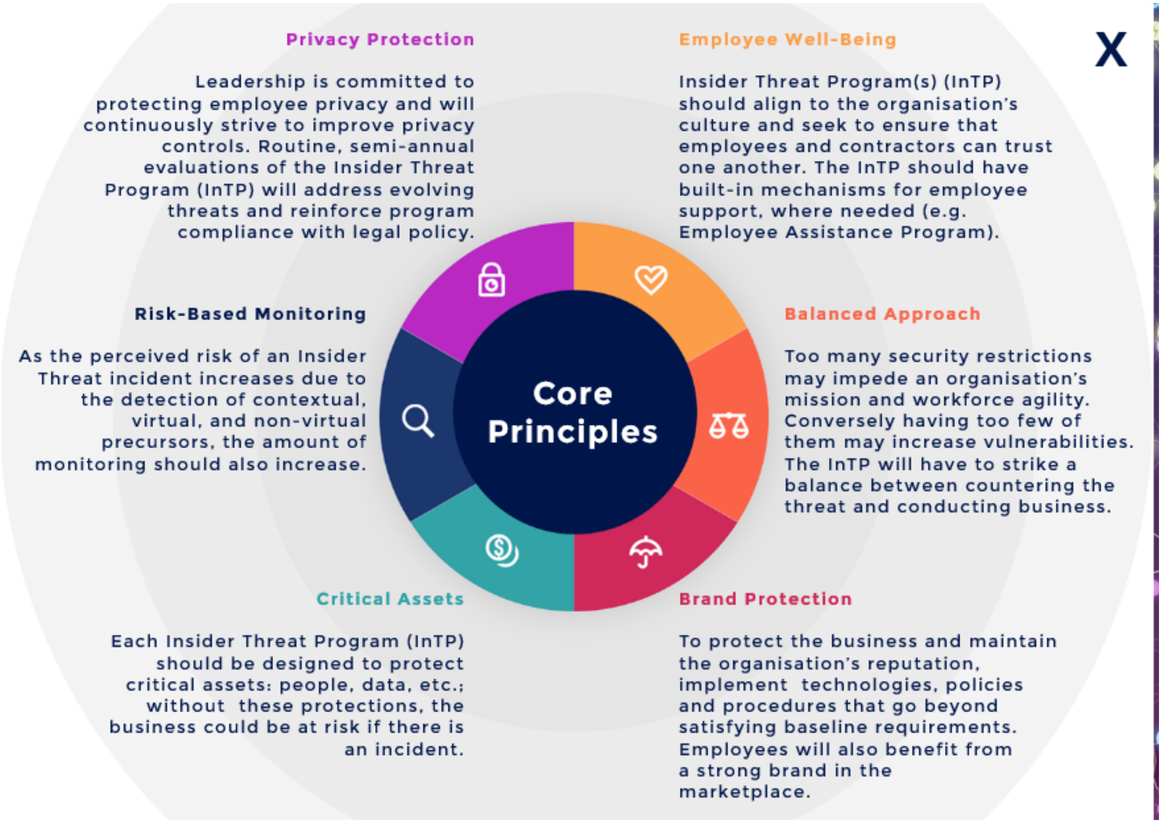
When communicating, it is important to:

Properly present the program to the staff.

To create absolute transparency of purpose and objectives. to have a common strategy for departments.

Constant coordination with the legal department (GDPR).

Involve unions from the early stages.



Privacy Protection

Leadership is committed to protecting employee privacy and will continuously strive to improve privacy controls. Routine, semi-annual evaluations of the Insider Threat Program (InTP) will address evolving threats and reinforce program compliance with legal policy.

Employee Well-Being

Insider Threat Program(s) (InTP) should align to the organisation's culture and seek to ensure that employees and contractors can trust one another. The InTP should have built-in mechanisms for employee support, where needed (e.g. Employee Assistance Program).

Risk-Based Monitoring

As the perceived risk of an Insider Threat incident increases due to the detection of contextual, virtual, and non-virtual precursors, the amount of monitoring should also increase.

Balanced Approach

Too many security restrictions may impede an organisation's mission and workforce agility. Conversely having too few of them may increase vulnerabilities. The InTP will have to strike a balance between countering the threat and conducting business.

Critical Assets

Each Insider Threat Program (InTP) should be designed to protect critical assets: people, data, etc.; without these protections, the business could be at risk if there is an incident.

Brand Protection

To protect the business and maintain the organisation's reputation, implement technologies, policies and procedures that go beyond satisfying baseline requirements. Employees will also benefit from a strong brand in the marketplace.

Recurrent training

-Internal Threat definition
-The scope of the program.
-Stories and powerful messages.
-Explanation of 3 types of (insider) threats.
-Behavior rules.
-How to know if you are being targeted (spam, etc.).
-Red threat flags (internal).
-Notification procedures - reports

Assess training. Provide direct feedback.
Workplace Climate Surveys/Studies

- ❖ Fun and positive.
- ❖ Short messages reinforce the impact.
- ❖ Simple and professional materials.
- ❖ Post on intranet / website....

Conclusion Module 6

- The training program should be positive.

- Use the agenda & tips in this module to make the training more impactful

- Evaluation should be part of your program.

Module 7 – Best practices – first interview

Human resources are the first line of defense.

Feedback: There is a feedback where departments discuss who they are hiring, how the selection process went and how it relates to the current operations.
This has proven to be very valuable and has made the whole process much more efficient.

Training: Investment in training is important (profiling).
It is important that staff is more aware of what they see, feel and hear.

Management: Management was open to the concept of a program

Problems encountered :
It is difficult for employees to see their colleagues as potential threats (colleagues and friends)

Staff find it difficult to report on their colleagues. It's like denouncing someone.

Direction: Try not to let emotions lead this process. You have to stick to the facts.

Module 7 – Best practices – second interview

What made you open your eyes: The program was launched after a malicious act. A malicious person had infiltrated the company with the intention of bringing money/drugs into an aircraft. A security expert has been hired. The results have strengthened safety rules and regulations.
Focus on staff awareness.

Internal regulations: The program included stricter (pre-employment) screening. (add selection for contractors, trainees and temporary workers)

Awareness: Everyone understands the situation, it is easy to explain and staff are more vigilant.

Legal restrictions: Beware there are limitations (legal department) - criminal records can be falsified.

The contribution of management is important: start small (evolution and not revolution).

Clear communication is the key. It's not a “witch hunt” or “Big Brother” is watching scenario. It's about protecting the company

.

Module 7 – Best practices – third interview

Success: The first step was to create an independent security service with clear objectives, procedures and agreements. The key was to follow internal threats.
All staff have received awareness training.

Everyone had the opportunity to share their observations via an internal - confidential channel.
There is also a strict selection of staff during the time it works (someone has posted explicit photos and comments on the net).
It is important to detect but also to act quickly (you can't rely on accidental discoveries but on a pro-active approach.

In most cases the actions are cleared up. When they do not, other measures are taken.

How much does it cost and what was the positive? A good program is expensive, but management's clear position ensures that there is no confusion or discussion of procedures.

We learned: We learned along the way that we need to be careful about how we handle reports and certain situations. Therefore, treat every observation, report and situation on this subject with care and professionalism.

Tip: All employees should be informed of the program.

Conclusion Module 7

(Pre-employment) Checks should be part of your Insider Threat Programme, but the screening should not stop here (infinity screening).

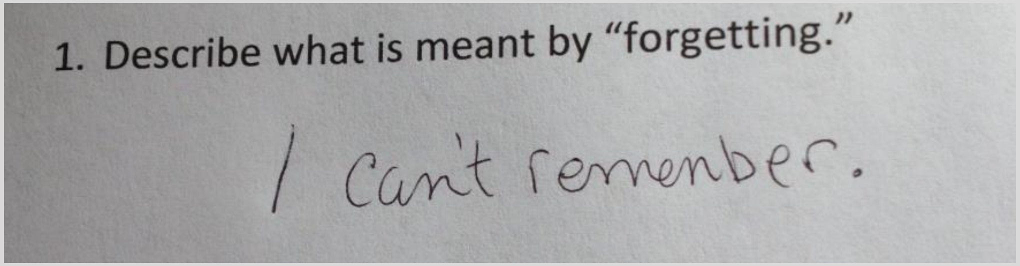
Employees need to be made aware of the Insider Threat.

Commitment from upper managment is key for a programme against Insider Threats.

Questions ?

Statistics 2018

- In 2018, 99% of organizations reported feeling vulnerable to internal attacks
- Most entities mentioned they were unprepared
- 51% of companies had a concern about the internal threat
- 47% had concerns about a malicious person
- We are not equipped to deal with minor accidental threats (not to mention malicious or terrorist attacks)
- 50% had the intention to develop a program, 14% did not have a program in place
- 50% of employees who left or lost their jobs kept confidential company data ...
- 40% of staff had the intention to use the collected information in their next job.
- In the United States, 5% of airport ID cards had disappeared (Example 2500 out of 50,000)
- 33% of staff who took part in “a course” told that the content did not inspire them
- 85% of candidates lied on their CV



1. Describe what is meant by "forgetting."

I can't remember.

Test
Menace Interne
Culture Sûreté
Documentation
Base Légale
Contact