Standards Framework

The table below presents the standards framework for Digital Criminal infiltration[1] (NDO). Text highlighted in blue is specific to criminal infiltration-related content. The remaining text consists of existing CYRA content to which the NDO is linked.

In cases where the NDO adds to existing CYRA control measures, this addition is shown in blue in the column "Criminal infiltration-Specific Control Measure". The reference in the first column then refers to the corresponding standard element in the underlying ISO 27001:2022 standard.

If the control measure does not refer to ISO 27001, the entire text is displayed in blue. In such cases, the reference in the first column corresponds to a unique NDO numbering system.

ISO reference	Control measure and initial question	Level 1 Ad hoc	Level 2 Best effort	Level 3 Defined
5.1	**Policies for information security and privacy** Does the organisation have up-to-date policies regarding information security and privacy?	Although there are some policy guidelines, actions are primarily based on common practice rather than policy. **Criminal infiltration-Specific Control Measure:** Generally recognised risks of criminal infiltration are known. A procedure has been established for reporting potential signs of criminal infiltration, the 'least privilege' principle is applied, and codes of conduct have been communicated.	The policy has not been formally approved. A high-level policy has been published with objectives and principles. Responsibilities have been assigned and processes for handling deviations and exceptions have been defined. The high-level policy has been further elaborated into subject-specific policy rules that mandate the implementation of control measures for information security and privacy. **Criminal infiltration-Specific Control Measure:** Topic-specific policies have been developed for: • Social media • BYOD (Bring Your Own Device) • Least privilege	The published overarching policy has been approved by management and communicated to staff and relevant external parties. The policy is periodically reviewed for relevance and whenever a serious incident occurs.
5.7	**Threat intelligence** Are information security threats assessed?	Potential information security threats are taken into consideration. **Criminal infiltration-Specific Control Measure:** The organisation takes into account potential threats originating from within ('insider threats'), specifically those involving the misuse of business processes and organisational information (or that of its supply chain partners).	Potential threats to the organisation's information security are monitored and lessons are learned from them. **Criminal infiltration-Specific Control Measure:** Measures have been implemented to detect or prevent unintentional and/or unauthorised access to corporate assets.	Potential threats to the organisation's information security are monitored. These threats are gathered and analysed to reduce the likelihood of such incidents or to minimise their potential impact. This process takes into account the types of attacks, attacker profiles, as well as the methods, tools, and indicators that may be used to detect an attack. **Criminal infiltration-Specific Control Measure:** The organisation has established a policy regarding the sharing of threat intelligence with other organisations.
5.9	**Inventory of information and other associated assets** Are information-related organisational assets recorded?	Some assets are included in an inventory that is kept up to date on an ad hoc basis. **Criminal infiltration-Specific Control Measure:** Assets considered relevant from an insider threat perspective, including at least those containing personal data, are listed in an overview that is updated annually.	Identified assets are assigned owners, and the inventory is kept up to date **Criminal infiltration-Specific Control Measure:** Employees are involved in identifying the criminal infiltration risks associated with the organisation's asset(s).	All assets relevant to the information lifecycle are identified and maintained in an inventory, with an owner assigned to each (category of) asset(s). The inventory is systematically kept up to date. **Criminal infiltration-Specific Control Measure:** The inventory of assets is reviewed annually based on the classification(s) of the asset(s), with criminal infiltration specifically included in the risk analysis.
5.12	**Classification of information** Does the organisation employ a classification mechanism?	Information and the assets in which it is stored or otherwise processed are (partially) classified. A classification scheme with uniquely named levels is used for this purpose. **Criminal infiltration-Specific Control Measure:** The classification scheme is linked to at least the confidentiality of information.	Information and the assets in which it is stored or otherwise processed are classified and provided with corresponding controls per classification level. Asset owners are responsible for the classification. The classification scheme includes rules for classification and criteria for re-evaluation. Classification is incorporated into organisational procedures and aligns with access security requirements.	Information is classified with regard to legal requirements, value, importance, and sensitivity to unauthorized disclosure or modification.

[1] In the Dutch context, 'undermining' or 'criminal infiltration' refers to the influence and infiltration of organised crime into legitimate sectors and institutions.

This document has been compiled with care. No rights can be derived from its contents. The information provided in the Dutch-language online CYRA self-assessment tool is leading. All content is protected by copyright and may not be copied, distributed, or otherwise used without prior written permission.

ISO reference	Control measure and initial question	Level 1 Ad hoc	Level 2 Best effort	Level 3 Defined
NDO 1	**Screening** Are personnel background checks carried out?	Personnel, including full-time, part-time, and temporary staff, are screened on an ad hoc basis. Staff selection is conducted based on a four-eyes principle. Open-source screening (including social media) is part of the recruitment process and is communicated, among other ways, in the job advertisement. The organisation has identified the criminal infiltration risks relevant to each job category within the organisation.	A recruitment process for (IT) personnel has been established and implemented, incorporating organisational requirements. Background verification may take place but is not formalised. When personnel are hired through service providers, screening requirements are included in documented agreements between the organisation and the providers. A process for periodic screening has been established, which includes checks on the use of open sources and changes in personal circumstances as part of assessing the risk of criminal infiltration.	The background of all candidates for employment is checked prior to their start date and subsequently reviewed at regular intervals. The level of screening is proportionate to the organisation's requirements, the classification of the information to which access is granted, and the identified risks. Screening also takes into account the risk of criminal infiltration. A formal procedure is in place for the appointment of new staff, in which declared references, training and qualifications from at least the past five years are verified.
6.3	**Information security awareness, education and training** Is staff knowledge maintained and updated?	Training and education occur on an ad-hoc basis. There is little to no personal certification. **Criminal infiltration-Specific Control Measure:** The organisation reminds staff every six months of the facility for reporting possible (criminal infiltration) indicators and their obligation to report such suspicious activities. The organisation provides examples of potential indicators. Additionally, the organisation maintains a system for receiving updates on developments related to criminal infiltration risks.	There are processes in place concerning certification, training, and education for staff, and personal development plans are maintained. **Criminal infiltration-Specific Control Measure:** (Subject-specific) policies and procedures are included in an annual awareness programme on criminal infiltration and the associated current risks.	All employees of the organisation and, where relevant, contractors receive appropriate awareness education and training, as well as regular updates on the organisation's policies and procedures, insofar as these are relevant to their role. **Criminal infiltration-Specific Control Measure:** An annual specialised awareness training on criminal infiltration is provided to facilitate early detection of (current) criminal infiltration activities. The organisation measures the extent to which staff are aware of the possibility to report such indicators. The topic of criminal infiltration is periodically and explicitly discussed in interactions with suppliers.
NDO 2	**Reporting Centre for Criminal Infiltration** Is a reporting centre for subversive crime being used?	The organisation has a mechanism for reporting signals that may indicate criminal infiltration. Employees are informed about this mechanism during the onboarding process.	All staff are periodically reminded that they can report signs that may indicate subversive activity via the reporting mechanism chosen by the organisation. Those who submit a report always receive a response, to a greater or lesser extent, regarding the information they have provided.	The functioning of the mechanism for reporting signs that may indicate subversive activity is evaluated annually and staff are informed about the findings.
8.1	**'User endpoint devices'** Is user equipment (laptop, PC, tablet, smartphone) functioning as part of the workplace protected?	There is no formal policy outlining what users may or may not do when using (mobile) information systems. System registration is handled on an ad hoc basis, and employees may use personal devices for work purposes without any governing policy. **Criminal infiltration-Specific Control Measure:** The organisation informs staff about the risks of mixing personal and business information in the context of subversive activity.	Responsibilities regarding systems used by end-users are documented and, in principle, known by the end-users. There is no need for active monitoring. The organisation has policies and a methodology in place that determine which systems have access to its information. However, there is no structured (remote) management of these systems. **Criminal infiltration-Specific Control Measure:** The organisation sets out agreements regarding the use of personal and business accounts.	Users are aware of procedures and requirements when using information systems, including shutting down when not in use and conduct in public spaces. Where applicable, there is controlled policy for BYOD (Bring Your Own Device). The status of systems (e.g., regarding patches and encryption) is recorded, and software installation on workstations is managed by the organization. There is technical and organizational control over all end-user equipment. **Criminal infiltration-Specific Control Measure:** User endpoint devices are, where possible, linked to personal accounts and are aligned with the threat assessment of criminal infiltration-specific risks.

ISO reference	Control measure and initial question	Level 1 Ad hoc	Level 2 Best effort	Level 3 Defined
8.15	**Logging** Are log files utilised?	Log files are not actively used. When logs are generated, this usually happens unconsciously ('default settings'), and they are rarely or never actively reviewed. **Criminal infiltration-Specific Control Measure:** The organisation has activated the default settings for log generation where possible.	There is a policy defining which activities must be logged. Access to log files is restricted to (system) administrators. Access to personal data is recorded where possible. **Criminal infiltration-Specific Control Measure:** Changes are logged, including: • the connection and disconnection of devices; • successful and failed login attempts	Log files are purposefully generated and protected. Regular reviews are carried out to detect and report deviations from normal use/functioning. Log files are considered potential evidence, with administrator access and file integrity being controlled. Technical or organisational measures prevent or compensate for manipulation. It is recorded who accessed which personal data and what modifications, if any, were made. A procedure is in place to ensure that personal data in log files is erased or anonymised as specified in the retention schedule. **Criminal infiltration-Specific Control Measure:** Login settings are reviewed annually to assess their effectiveness in detecting insider threats.

With the exception of the exact font and colour scheme, the above normative framework is verbatim included in the tool, which is used by both the organisation and the auditors when working with the NDO.