Duty of Care Maturity Model

How to improve your safety and security risk management processes.

This model is intended to serve as a learning tool for Swiss NGOs to understand and improve their maturity in safety and security risk management related to Duty of Care (DoC) processes. The concept of DoC is based on Article 328 of the Swiss Code of Obligations and uses key processes identified through best practice examples of European NGOs. The model does not intend to set DoC standards and should not be seen as a DoC compliance self-assessment tool.

Duty of information

Collecting, collating, analysing, sharing, informing, understanding

Duty of prevention

Anticipating, planning, providing guidelines

Duty of monitoring

Reviewing, checking compliance, learning

Duty of intervention

Responding, supporting, caring, protecting, ensuring compliance

eisf

In collaboration with the working group of the Swiss Security Network
EISF | cinfo

cinfo

Duty of information

Collecting, collating, analysing, sharing, informing, understanding

Maturity level	Initial	Structured	Defined	Measured	Optimised
Processes	**Ad hoc and reactive implementation of DoC processes due to a lack of awareness of obligations.**	**DoC obligations are acknowledged and identified resulting in processes being documented and therefore repeatable. Implementation needs improvement.**	**DoC obligations are defined and integrated into related management processes thereby ensuring they are consistently followed.**	**DoC compliance is quantitatively managed in accordance with agreed-upon metrics.**	**DoC processes are consciously reviewed for continuous improvement at an organisation-wide level.**
Recruitment	Security and safety information is fed into the recruitment of new staff members on an ad hoc or reactive basis.	Safety and security **information feeds into recruitment** based on the risk levels of locations and roles. **Risk assessments** for the context and candidate are carried out. Prospective candidates are provided with safety and security information relevant to the context and candidate.	Safety and security information and risk assessement are **documented** and **systematically** fed into the recruitment process based on risk levels for locations and roles. **Consent** on security is included in the employment contract. Security training needs are assessed and fed into training methods. This includes: – Carrying out a risk assessment before recruitment and again upon selection of a final candidate. – Providing security information to prospective candidates before recruitment. Security and safety input into the recruitment process can include, for example: – Information on personal risk profiles. – Security and safety information in the job description and recruitment advertisement. – Security and safety questions in the interview questionnaire.	Recruitment is **monitored** in order to **assess** the level of security and safety information provided during recruitment. **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	Improvement is achieved through learnings from: – internal and external incidents – other organisational processes (e.g., risk assessments) – staff consultation (recruiters and recruited) – expert review – peer learning/community of practice **Feedback** from recruited staff is systematically obtained and fed back to recruitment.
Induction / Onboarding	Some form of induction received by most staff. This induction is more or less informal.	New staff **receives essential information** and documentation after recruitment and prior to deployment. This includes: – key policy documents related to duty of care – relevant procedures – code of conduct	A **systematic** and **compulsory** induction of new staff is part of the onboarding after starting their function / before deployment. As part of the induction staff receive specific briefings to ensure their understanding of: – key policies and/or regulations (e.g. Code of conduct, security, insurance, sexual harassment, mobbing, whistleblowing) – related procedures including local security plans – roles and responsibilities concerning duty of care as required – other key briefings related to the role The nature and content of the briefings are **defined** in accordance with the work country's risk level.	Induction is documented through: – Attendance of staff to their induction briefings. – The provision of key documents. – Roles and responsibilities are communicated and clarified. **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	Improvement is achieved through **learnings** from: – internal and external incidents – risk assessment – staff consultation (recruiters and recruited) – expert review – peer learning/community of practice Feedback from staffs' induction is systematically obtained and fed back to the induction process.
Training	There are some opportunities for staff to develop their personal capacity based on their interests in relation to their job.	Training options are **available** to staff pertaining to: – personal safety and security – their role as managers (SSRM and crisis management) Key competencies relating to duty of care are identified in organisational documentation.	Staff are required to complete **training as per identified needs,** carried out by experts on key competencies in relation to: – personal safety and security – their role as managers (SSRM and crisis management) – organisation-specific safety and security plans and procedures The process ensures that training needs are assessed and satisfied based on: – staff members' personal risk profile – the work country's risk level	Personal staff development is **documented** and failure to obtain identified key competencies within a specified period is **recorded,** and **redress measures** are taken.	Feedback on training is regulary obtained from: – trainers – trainees – experts – peers/community of practice This information is used to inform policy and future training. Identified key competencies relating to duty of care are regularly **re-assessed** and adapted to changing risks.

Duty of information

Collecting, collating, analysing, sharing, informing, understanding

Maturity level	Initial	Structured	Defined	Measured	Optimised
Risk assessment	Safety and security risk assessments are carried out in a reactive or ad hoc manner without a standardised template and used only at local level.	There are **policies and plans in place,** which regulate safety and security risk assessements and associated responsibilities are clarified in job descriptions. There is a **defined template** for risk assessments.	Safety and security risk assessment is **regularly updated** according to a context-specific frequency. The risk assessment includes the following outputs: – understanding of threats and hazards (including physical and psychological ones) – the vulnerability of staff/assets to these threats and hazards – risk level categorisation of locations and activities Findings from risk assessments are **systematically** integrated into other management processes beyond security management, e.g. project cycle management, country strategy development, acquisition.	Safety and security risk assessment otputs are **documented.** A system is in place to monitor that risk assessments are done/updated as prescribed. **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	The safety and security risk assessment is regularly **reviewed** and **improved** by the management board with regards to: – how it compares with peers – its adequacy for the organisation (activities, means) **Feedback** from risk assessment is systematically obtained and used for impovement of induction
Pre-departure briefings for travellers	Briefings are received upon request.	Pre-departure briefings are **documented** in policies and security plans, and reflect the risk level of the location or role. A standard briefing template is provided.	**All travelling staff receive pre-departure briefings** by the designated person in accordance with the risk level of the location and role. This information includes: – safety and security risks (including personal risks due to profile) – safety and security risk treatment measures – staff safety and security roles and responsibilities (procedures to follow) – staff right to withdraw (informed consent)	The provision of the briefing to travelling staff is **registered,** e.g. by staff acknowledging understanding of the content of the briefing in writing. Failure to obtain briefings in accordance with agreed-upon procedures is responded to in accordance with **consistently-applied, documented and transparent disciplinary procedures.**	Information in briefings is **regularly updated** using information received from: – peer learning/community of practice – risk assessments – post-deployment de-briefings – expert reviews **Feedback** from pre-departure briefings is systematically obtained and fed back to the induction process.

Duty of prevention

Anticipating, planning, providing guidelines

Maturity level	Initial	Structured	Defined	Measured	Optimised
Processes	**Ad hoc and reactive implementation of DoC processes due to a lack of awareness of obligations.**	**DoC obligations are acknowledged and identified resulting in processes being documented and therefore repeatable. Implementation needs improvement.**	**DoC obligations are defined and integrated into related management processes thereby ensuring they are consistently followed.**	**DoC compliance is quantitatively managed in accordance with agreed-upon metrics.**	**DoC processes are consciously reviewed for continuous improvement at an organisation-wide level.**
Risk treatment	Safety and security risk treatment is carried out in response to incidents rather than on the basis of proactive risk assessments.	Safety and security risk treatment measures are **identified** and **documented** in policy and plans.	Organisational risk threshold is identified. Safety and security risk treatment measures are **systematically implemented** based on the security risk assessment, including: – prevention – mitigation – equipment – training, etc.	Implementation of safety and security risk treatment measures is documented and monitored against an agreed organisational risk threshold (as documented in policy). Non-compliance is responded to via consistently-applied, documented and transparent disciplinary procedures.	The effectiveness of safety and security risk treatment measures is regularly reviewed and improved. Through learnings from: – internal and external incidents – other organisational processes (e.g., risk assessments) – staff feedback – expert review – peer learning/community of practice
Pre-departure measures for travellers	There is no consistency in whether travellers receive medical (physical and mental) support before travel or not.	Pre-departure measures are identified and **documented** based on risk assessment for destination and role. All staff are informed.	Prior to departure travelling staff **confirm** to the designated person they implemented pre-depature measures. These measures include: – health checks (mental and physical) – vaccinations – medication – personal safety and security competence – country risk-specific information	Completion of pre-departure measures is documented and **registered.** **Failure** to complete all pre-departure measures is addressed in accordance with consistently-applied, documented and transparent disciplinary procedures.	Improvement is achieved through learnings from reviews, which include: – post-deployment de-briefings – other organisational processes (e.g., risk assessments) – peer learning – expert review
Insuring against risks	The organisation does not have comprehensive insurance coverage in place.	Required personal insurance coverage is identified and **documented** based on risk assessment of locations and roles. Required organisational insurance coverage is identified and documented based on risk assessment of locations and roles.	**Systematic** procedures are in place to ensure that all staff are insured against: – health risks (as required) – liability risks (as required) The management takes systematic decisions on organisational insurance coverage based on identified risks.	Insurance coverage is monitored by experts. Provision of insurance information to staff is **registered.** **Failure** to obtain insurance coverage as prescribed in policy and plans is responded to in accordance with consistently-applied, documented and transparent disciplinary procedures. (under- and overcoverage to be checked)	Insurance policies and providers are assessed. **Improvement** is achieved through learnings from: – internal and external incidents – risk assessements – staff consultation – expert reviews – peer learning/community of practice

Duty of monitoring

Reviewing, checking compliance, learning

Maturity level	Initial	Structured	Defined	Measured	Optimised
Processes	**Ad hoc and reactive implementation of DoC processes due to a lack of awareness of obligations.**	**DoC obligations are acknowledged and identified resulting in processes being documented and therefore repeatable. Implementation needs improvement.**	**DoC obligations are defined and integrated into related management processes thereby ensuring they are consistently followed.**	**DoC compliance is quantitatively managed in accordance with agreed-upon metrics.**	**DoC processes are consciously reviewed for continuous improvement at an organisation-wide level.**
Auditing	The auditing of safety and security risk management in the organisation is ad hoc, reactive and not according to organisation-wide indicators.	Safety and security risk management auditing is **documented**.	The safety and security risk management system is regularly, **systematically and consistently audited** with regards to: – risk assessment – risk treatment – risk monitoring	Auditing is **documented** and carried out according to agreed-upon metrics. Key staff **oversee** the completion of the audit's final improvement action plan. **Failure** to do so is addressed in accordance with consistently-applied, documented and transparent disciplinary procedures.	Staff is informed about the outcome of audits. **Improvement** is achieved through **feedback** and learnings from audit outcomes, which include: – comparision of audit results with peers and staff – internal and external incidents – risk assessments
Safety and security incident information management	Safety and security incident data is captured in an inconsistent manner.	Safety and security incident data are **documented** in a **standardised** way.	Safety and security incident data is systematically: – **gathered** – **processed** – **analyzed** to support the incident response management process, risk assessment and risk treatment including crisis management. Outputs are **systematically fed back** into local, national, regional /international level organisational learning and decision-making, e.g.: – programming and reporting – safety and security procedures – advocacy/media response – HR – finance Designated staff are **systematically trained** in gathering, processing and analyzing incident information.	Safety and security incident information management is **monitored and documented.** Failure to do so is addressed in accordance with consistently-applied, documented and transparent disciplinary procedures. Underreporting of incidents is addressed through traget-oriented measures, which include: – awareness-raising – training	**Improvement** is achieved through **feedback** and learnings about information management based on: – quality and quantity of internal and external incident reporting – peer learning/community of practice – staff consultation and feedback on trainings in information management – expert reviews Learnings from incident reporting databases are regularly shared across departments and within management, where deemed appropriate.
Documentation	There is no consistent documentation of safety and security risk -related information.	Safety and security risk management related information is documented.	Decisions and actions taken in relation to safety and security risk management are **systematically documented** at organizational level. These include: – policies – plans – procedures – staff signature documenting informed consent processes and understanding staff conduct requirements outlined by policy. Documents related to safety and security risk management are **systematically archived.**	Documentation processes is monitored. **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	Documentation is **regularly reviewed** and amended. **Improvement** is achieved through learnings from: – quality and quantity of internal and external documentation – peer learning/community of practice – staff consultation and feedback on documentation – expert reviews

Duty of intervention

Responding, supporting, caring, protecting, ensuring compliance

Maturity level	Initial	Structured	Defined	Measured	Optimised
Processes	**Ad hoc and reactive implementation of DoC processes due to a lack of awareness of obligations.**	**DoC obligations are acknowledged and identified resulting in processes being documented and therefore repeatable. Implementation needs improvement.**	**DoC obligations are defined and integrated into related management processes thereby ensuring they are consistently followed.**	**DoC compliance is quantitatively managed in accordance with agreed-upon metrics.**	**DoC processes are consciously reviewed for continuous improvement at an organisation-wide level.**
Crisis management	Management response to crises is ad hoc and reactive.	Crisis response **manuals / tools** are elaborated in a) guidelines b) policies and c) approved plan that delineate a crisis management response structure.	**Response procedures** responding and managing crises (internal and external) are documented and in accordance with prescribed **risk levels.** This process is supported by: – **regular** crisis management **training** – **pre-identified** and vetted crisis **assistance providers** – investigation procedures – identification of qualified crisis management staff – consideration of staff needs, e.g. staff with disabilities	**Monitoring** of the crisis management process implementation and preparation through: – registering crisis management training **attendance** – documentation and review of crisis management decision-making **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	Improvement is achieved through learning from crisis management experiences: – staff consultation – a lessons learned exercise – peer learning – other organisational processes (e.g., risk treatment) – a review of crisis response providers A process is in place to regularly test the crisis response management structure, through: – peer learning/community of practice – risk assessments – post-deployment de-briefings – expert reviews Feedback from crisis management responses is systematically fed back to the crisis management process.
Post-deployment/travel de-briefings	Post-deployment/travel de-briefings are ad hoc and at the discretion of line managers.	Post-deployment/travel de-briefings are **regular. Timing** is adequate, response structures defined and **availabe.**	Post-deployment/travel de-briefings are **systematically integrated** into related management processes and undertaken in accordance with prescribed risk levels through: – trip reports – face-to-face de-briefings with management and experts – provision of psycho-social support services And may be applicable for in-country and/or international travel in accordance with prescribed risk levels.	**Monitor** post-deployment/travel de-briefings: – Registering attendance at face-to-face de-briefings. **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	**Improvement** is achieved through learning from post-deployment experiences: – staff consultation – a lessons learned exercise – peer learning – other organisational processes **Feedback** from post-deployment is systematically fed back to the post-deployment process.
Complaints mechanisms	The receipt of complaints is ad hoc and linked to awareness-raising activities. Responses to complaints is reactive and unstructured and dependent on management interest and capacity.	**Mechanism** for receiving and addressing complaints is communicated and documented.	Procedures for compaints and respond from internal and external individuals are **communicated, systematic and transparent.** It requires communication about and assurance that: – **Anonymous reporting** is guaranted and accessible through a variety of reporting mechanisms, e.g. online platform, email, letterbox. – Reponse is available in operational **languages.** This process is **integrated** into related management processes, including awareness raising activities within and outside of the organisation (e.g. training, induction, etc.). There is a process in place to **protect the identity** and well-being of reporters.	**Monitoring** complaints/response mechanism in accordance with agreed-upon metrics. Have anonymised report list of complaints. **Documenting** of the security audit process or relevant staff performance reviews. **Non-compliance** with documented requirements is managed in accordance with consistently-applied, transparent and documented disciplinary procedures.	The complaint procedures as well as response to complaints are **systematically reviewed,** for example, through a regular audit by experts. A process is in place to gather feedback on the complaints mechanism and amend processes accordingly. – internal and external incidents – other organisational processes (e.g., risk assessments) – staff consultation – peer learning/community of practice. **Feedback** from reviews are systematically fed back **operational management** and code of conduct.

Duty of intervention

Responding, supporting, caring, protecting, ensuring compliance

Maturity level	Initial	Structured	Defined	Measured	Optimised
Disciplinary/sanctions procedures	The organisation becomes aware of infringements on a staff members' physical and mental wellbeing in an informal way or by chance. Perpetrators of such infringements are randomly held accountable, with some not held to account at all.	A disciplinary/sanctions process is **documented** in policy and plans. This includes: – Documenting **managers' responsibility and right** to take action to discipline or sanction staff for lack of compliance.	Disciplinary procedures **are in place** that are consistently and transparently **applied** for non-compliance with documented requirements. This process includes: – Staff and managers to have **formal opportunities** to discuss infringements against the physical and mental wellbeing of staff, e.g. in the annual appraisal process or through a whistleblowing mechanism. – Managers to know when and **how to escalate** reports on infringements to another level (both internally or externally). – Managers to be trained on **how to investigate** reports and **how to discipline** or sanction at their level. – **Supervising managers** to take action when lower level managers fail to act in accordance with provisions. It is ensured that staff who report suspected non-compliance are not dicriminated against.	The organisation **collects and analyses** data on allegations of infringements against the physical and mental wellbeing of staff. This includes how reported cases were handled by management.	The disciplinary/sanctions policy and procedures are reglularly **reviewed and amended.** Such revision can be informed by, for example: – a dedicated internal lessons learned exercise – external expert review – risk assessments followin internal or external incidents – staff consultation – peer learning/community of practice Staff and managers' awareness of their rights and obligations in relation to compliance is regularly **assessed and improved,** including procedures for investigating allegations of infringements.
Health and safety	There is no consistent process for meeting site-related health and safety regulations.	Health and safety regulations to meet reasonable standards in all the organisation's facilities, including offices, accommodation and warehouses are **documented.** Staff care support is **available and documented** in policy or regulations in all countries in the form of services (internal or external) and/or trainings.	Responsibilities for the implementation of health and safety regulations in all the organisation's facilities are clearly **defined and reflected** in job-descriptions. Site-related health and safety considerations are **integral part** of relevant management processes, e.g. project management, budgeting. Risk management is integrated into related management processes, e.g. risk assessments. Staff care measures are **put in place** and are adequate. Staff's wellbeing is systematically **assessed and acted upon** at the end of deployments or after serious incidents. Staff are **encouraged to attend** sessions or access services in a confidential manner and can do so without going through their line manager or other senior staff.	Site health and safety measures are **systematically audited** according to transparent criteria. Staff's wellbeing is **benchmarked** against acknowledged criteria, e.g. through regluar reports from the responsible for staff care or by means of a staff barometer. **Adjustments are made** on the basis of monitoring outcomes and **infringements addressed** in accordance with policy.	The health and safety process is **regularly reviewed,** and learnings used to **adapt** the process for continuous improvement. This can be informed by, for example: – analysis of incidents (internal or external) – staff consultation – expert review – peer learning/community of practice – legislative changes
Redress measures	Staff access to redress measures is ad hoc and dependent on senior management interest.	Redress measures are **documented** in policy or regulations allowing staff (or their next of kin) to ask for satisfaction of un-covered needs.	Management at the appropriate level **receive information** on un-covered needs of staff (or their next of kin) having suffered a wrong at their workplace. Such needs may be e.g.: – additional psychological support to staff or their next of kin – financial losses to staff or their next of kin – flexible return to work options – legal or administrative support The information is **formally acted** upon and the decision shared to the staff concerned (or their next of kin). The organisation has the **resources at hand** to provide redress measures, e.g. a special fund for extraordinary measures.	The concerned staff (or their next of kin) have the possibility to **appeal** decisions taken in respect to redress measures concerning them.	**Learnings** concerning systemically un-covered needs after critical incidents are gathered, for example, through information from, e.g.: – de-briefings with affected staff about the incident – wider staff consultation – expert review – peer learning/community of practice – regular reporting from the responsible for staff care The coverage of needs arising from critical incidents is periodically reviewed and improved where feasible.

Duty of intervention

Responding, supporting, caring, protecting, ensuring compliance

Maturity level	Initial	Structured	Defined	Measured	Optimised
Risk management	Safety and security risk management roles and responsibilities are not well-informed and designated reactively.	The safety and security risk management process is **documented** in policy or guidelines. The persons responsible for safety and security are **identified** and **communicated.**	Safety and security risk management is **integrated** into relevant other management processes, for example, HR processes, project management, finance management, compliance, etc. Risk owners and risk managers are **defined** and their responsiblities and tasks reflected in job-descriptions. Expertise is **sought** where needed to duly inform safety and security risk management steps (assessment, treatment, monitoring, communicating). This includes expertise on crisis management.	Safety and security risk management is periodically **audited** based on reckognised standards. Job descriptions are regularly **checked** against actual tasks and requirements.	Safety and security risk management processes and roles are regularly **reviewed and updated** in accordance with learnings from, e.g.: – staff consultation – expert review – peer learning/community of practice
Partnership arrangements	Partnership arrangements are driven by programmatic and strategic demands and do not consider safety and security considerations.	The way how safety and security risks are managed in partnership arrangements is **documented** in policy or regulations. This includes: – the way to attribute roles and responsibilities of the partners in relation to safety and security – the way to attribute roles and responsibilities of the partners in relation to crisis management	Due diligence checks on partner organisations are **carried out systematically** before entering into partnership agreements, this includes: – the partner's capacity to take care of their employees – the partner's capacity to manage crisis Written partnership arrangements specify the partners' roles and reponsibilities in relation to: – safety and security – crisis management – capacity building (where deemed appropriate) This applies in particular to consortia arrangements and to seconded staff.	Partnership arrangements are periodically **checked** for completeness in relation to: – due diligence done – contractual specifications Failure to comply with this process is brought to the attention of senior management and **remedial measures** are taken.	Due diligence processes and partnership arrangements are regularly **reviewed and assessed.** Learnings are acted upon and informed by, e.g.: – analysis of incidents (internal or external) – staff consultation – expert review – peer learning/community of practice