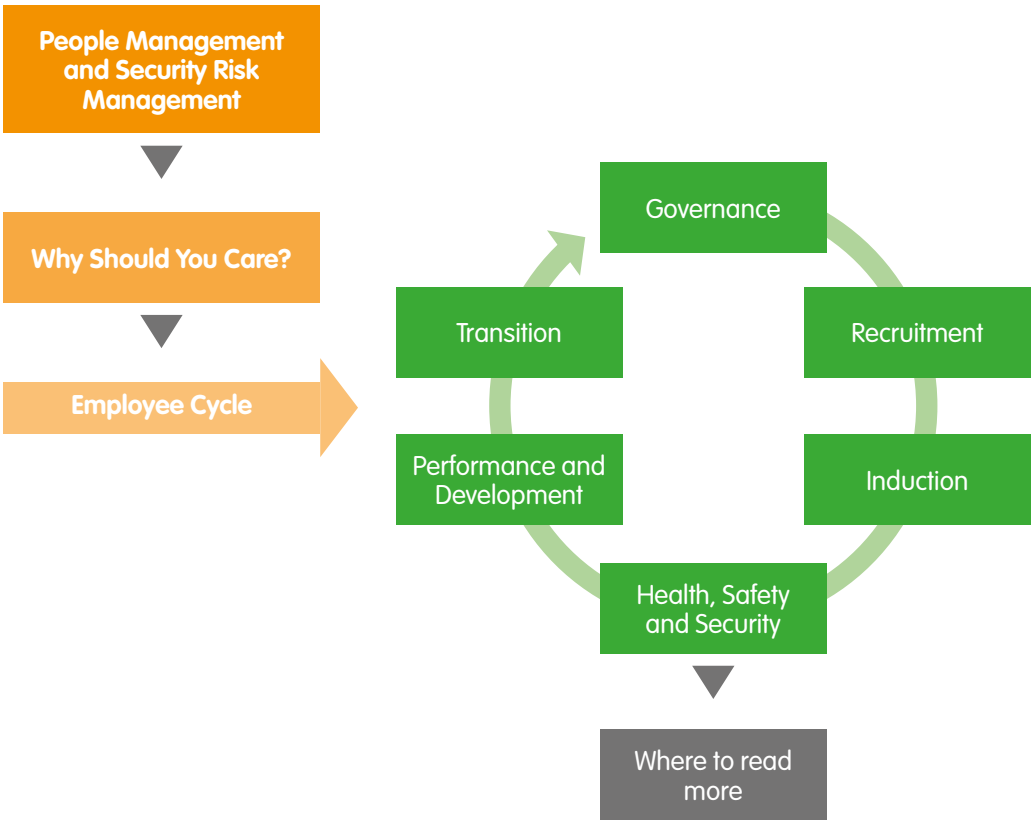
12 People management



People management and security risk management

Good people management could be described as getting the best results from an employee in a healthy and safe way. People are our most valuable resource and if we believe happy, secure and motivated employees are more likely to be engaged, committed and productive, it makes good business sense to support employees well and to provide them with a healthy and safe working environment.

People management is a broad and complex subject that carries legal and ethical responsibilities for an organisation to ensure the physical and psychological health of an employee before, during and after the period of employment. Organisations have many legal and ethical 'duty of care' obligations and are expected to go above and beyond the legal minimum when working in high-risk environments.

Those in leadership positions – trustees, directors and managers – must invest time and resources in people management practices, and ensure technical specialists within human resources and security provide the necessary advice at the right time and in the right way.

People and security risk management – why should you care?

People management has a direct impact on security risk management, for example:

1. **Recruitment** – employing the wrong people can create security risks. A lack of skills and competencies can lead to poor performance and decision-making; poor behaviours can lead to personal and programme risks; and failure to consider the implications of the ethnic mix in some regions can create issues between staff and negative perceptions in the local community.
2. **Induction** – preparing people appropriately has a direct impact on how well and quickly staff settle into their new role, team life and the environment, thereby reducing the risk of security incidents.
3. **Office closure and contract termination** – a clear and transparent process on office closure and when contracts come to an end should be implemented some time before the notice period begins. Failure to do so can have serious security implications.
4. **Stress management** – risky and high-pressured situations are more likely to lead to a highly stressed workforce, which can impact behaviours, relationships and the ability to make good security-related decisions.
5. **Employment policy and practice** – employees are more likely to feel valued and protected when employment policies (e.g. reward, performance and conduct) are clear and consistently applied. Disgruntled and dissatisfied staff are a source of security threats to the organisation, staff and programmes.

Whilst reading this module, it is worth noting:

- The employee should have the competence and tools to do the role well.
- The working environment should be one where an employee feels healthy and safe.
- Employees should know their health, safety and security responsibilities, understand the risks, and accept any residual risk they face when undertaking their role, knowing that there has been appropriate analysis and care taken by the organisation.
- Employees should have the option to say no if they are concerned about the risks they are being asked to take to carry out their role.

The employee cycle and good people management

Ensuring your people management standards remain high and meet your duty of care obligations involves everybody in the organisation, starting with the most senior, and including every level of staff.

The employee cycle is a good way to identify the practices in people management which carry an obligation or risk. The best solution for good people management integrates security risk management with all stages of the employee cycle.

Using the employee cycle can also assist in understanding who owns or is responsible for the different practices in the organisation. In most cases, there is more than one person involved or a body or group that is responsible e.g. a risk management group (sometimes known as a health and safety committee).

Governance

The first stage of the employee cycle is governance, i.e. the structures and policies that your organisation is built upon. An organisation's health, safety and security culture relies heavily on having robust systems and practices in place. The key ones are often the basic ones. Employees are more likely to feel valued when policy and practice are clear and applied consistently. If practice is poorly aligned, or poorly implemented, this will adversely impact your employees and increase the risk to their health, safety and security. Key practices and the minimum levels of provision for each are outlined below.

Robust practices are ones which are value-centred, of a high standard, sustainable, accessible, relevant, known, used, monitored and evaluated.

Practice	Minimum levels of provision
Mission, goals, values	Clarity on the mission, goals and values provides vision and clear expectations. The mission demonstrates why the organisation exists and how it would like to change the world for the better. The mission is needed to motivate staff. The goals ensure that employees are working towards the same purpose. The values show how the organisation will do its work and the kinds of employees needed to do it. Everything should come back to this: the big picture.
Organisational risk threshold	The risk threshold identifies what the board/senior management of an organisation considers to be an acceptable level of risk for the organisation. The threshold may be different for different types of activities (e.g. saving lives vs. development). The risk threshold forms the basis for all security risk management policies and plans throughout the organisation. It also enables individual staff to check their own acceptable risk threshold against that of the organisation.
Organisational strategy and structure	A strategy gives direction by providing a picture of the work to be done, by whom, where and by when. The organisational structure outlines who is who in the organisation. It is used for job descriptions, grading and job titles, and shows the numbers for reporting lines. It aids recruitment, induction and general management and communication across the organisation.
Contract of employment and employee handbook	Legal, clear and accessible contracts and handbooks with consistent principles of employment practice are required for all defined categories of staff, including short-term contracts often used during an early humanitarian response stage. For local contracts, make sure to seek local legal advice. The employee handbook is a reference tool for managers and employees that contains useful information about the organisation, the terms and conditions of employment, and outlines the organisation's policies.

Practice	Minimum levels of provision
Pay and benefits	Pay and benefits (including allowances) should be applied using consistent principles, aligned with local practice and adaptable for an early humanitarian response stage. Employees should be consulted on changes to their pay and benefits. Variations for different staff types – international, re-located, national, volunteer, etc. – must be clearly defined. Actions concerning benefits include: **Leave** – monitor annual leave and carryover, national holidays, rest and recuperation (R&R), sick leave and maternity/paternity leave. Support sickness absences appropriately and conduct 'return to work' meetings. **Retirement** – provide details of an optional retirement scheme. **Insurance** – provide a summary of medical, travel and death in service provision with annual reviews and records of cases.
Working hours	Working hours and compensation for overtime, with adaptable working patterns for when staff initially respond to a sudden onset emergency.

Security implications

Humanitarian organisations should aim to link their values to the core humanitarian principles. These principles, particularly those of neutrality and impartiality, can help organisations gain local acceptance and safe access to insecure environments. Employees who do not follow these principles or their organisation's values can place themselves and the organisation at risk.

A weak organisational structure can result in a lack of clarity on where security responsibility lies within the organisation, including what the decision-making structure is during a critical incident, e.g. a staff abduction.

Transparency on grade, pay and allowances for all categories of staff reduces concerns and complaints. A lack of clarity on contractual stipulations, e.g. early termination, can lead to disgruntled employees retaliating and compromising the security of other employees, the organisation and programmes. Clear disciplinary procedures must be in place to deal with employees who pose a threat to their colleagues.

Recruitment

Risky environments require employees with specific skills and experience. An organisation should never underestimate the importance of the recruitment process and the risks associated with hiring the wrong person. Recruiting the wrong person can be very costly and unproductive, and employees who do not fit the role are likely to be unhappy and underperform, which will have a direct impact on programme implementation, their manager's time, team morale and security. A risk assessment of the role should be completed before the recruitment process starts, to understand the essential requirements of the role, and to ensure that suitable candidates are encouraged to apply.

Managers should be fully immersed in the recruitment of their teams.

Identifying a candidate's strengths and areas for development, and assessing them against essential values, skills and competencies is a crucial part of the process. The manager, in liaison with human resources and security, should undertake risk assessments to determine the risks that need mitigating for the particular applicant in the specific role. For high-risk roles or roles in high-risk contexts, mandatory health and safety interventions should be identified. The recruitment process should inform the content of an induction.

See Module 3 – Risk assessment tool

Practice	Minimum levels of provision
Recruitment	A clear job description and well-managed recruitment process using competency-based techniques with diversity at the heart. References and background checks are verified, and risk assessments are undertaken both for the role and the applicant, including health and resilience assessments. Managers are fully trained in the recruitment process. Where the manager does not speak the local language, steps must be taken to ensure that job applicants are not 'pre-screened' by local staff to avoid the risk that one section of the local community is given an unfair advantage.
Equality and diversity	An equality and diversity policy must be in place and employees should understand its principles and apply them in their work and behaviour. Discrimination characteristics should be outlined and strong sanctions set in place for any breach of policy. While discrimination in recruitment based on ethnicity, gender or sexuality is morally and legally unacceptable, in many environments the ability of an organisation to operate may be affected by the characteristics of an individual and these risks must be considered as part of the role risk assessment.

Security implications

The manager, in liaison with security and human resources, must carry out a robust risk assessment for all roles during the recruitment phase; this is in order to understand the risks inherent in the role itself and to help identify the type of candidates that should be recruited.

Once applicants have been identified, a risk assessment for the individual in the specific role should be completed. This is to assess the impact their skills, experience, age, gender, sexual identity, disability or ethnicity could have on their personal safety and security, whilst at the same time ensuring compliance with equal opportunity legislation.

Ethnicity, in particular, of both national and international staff, may have serious implications for the perception of your organisation and the risks both individuals and the organisation face.

The manager's aim is to recruit the most qualified person and ensure mitigating measures are in place to enable the individual to work in an environment with the lowest security risk possible. Understanding the diversity of your staff will help you develop better security systems and confidential, accessible resources to support their safety.

It is extremely important to dedicate time to verifying background checks and references for new recruits during the recruitment phase, especially for organisations that work with vulnerable people, e.g. children, and where a breach of the code of conduct can result in serious reputational and security risks for the employee and the organisation.

Induction

Preparing an employee for their assignment is one of the single most important things an organisation can do. It is not reasonable to send an employee to a high-risk environment without substantial preparation. Leaving an ill-equipped employee to make decisions that could jeopardise their personal security (and the security of others) is an abdication of responsibility and duty of care. Three areas, in particular, require attention:

1. Employees should be informed of the organisational security policies and procedures:
   - They should understand the acceptable level of risk for the organisation, and the policies which govern the security culture.
   - They should have confidence in the organisation's systems to manage their safety, security and well-being.

2. Employees must be aware of the risks to their own personal security:
   - They should fully understand the context in which they are working (how the society around them functions and communicates) and how their own behaviour can affect their vulnerability.
   - They should know what is expected of them (e.g. mitigation measures) during and outside normal working hours, and should behave accordingly.
3. Staff should be aware of how stress affects their personal behaviour:
   - People can often release stress in damaging ways, such as excessive drinking and promiscuity.
   - Organisations must provide the learning ground for managers and employees to be aware of and to manage their stress, and consistently enforce sanctions against employees who put themselves and others at risk.

Practice	Minimum levels of provision
Induction	An induction programme, led by the manager for each employee, includes information and training on: the mission, goals, behaviours, structure and reporting lines; strategy; team/ programme mandate; key relationships; the role; handover; contextual health, safety and security; probation objectives; key policy and practice.
Informed consent	Informed consent means: the staff member has agreed and signed a document which states that the security risks that come with the role and context have been fully explained, and the staff member has understood them; they understand the provisions the organisation is making to manage the risks in the context; they understand what is expected of them; and they are comfortable with the residual risk that remains after the organisation has put in place mitigating measures. The informed consent process should also include discussion of individual vulnerabilities.

Informed consent is a process to ensure staff engagement and understanding – it is NOT a legal waiver.

Security implications

An ill-prepared employee can make erroneous security decisions that are based on a weak understanding of the local security context. Staff who have accepted a posting without being aware of operational or personal restrictions (such as an early evening curfew) are more likely to break security procedures, put themselves and their programme at risk, and be demotivated and dissatisfied with the organisation. This contributes to a higher staff turnover.

Handover and a good induction, with appropriate support from line management, is essential for all new employees, and even more so when the role carries responsibility for making decisions about staff health and safety in a high-risk environment. For example, one of the key areas of concern in a legal case heard in Norway in 2015 (Dennis vs Norwegian Refugee Council) was the newly appointed country director's lack of knowledge about the local security context.

Health, Safety and Security

The extent to which organisations see staff as central to their mission is often reflected in the policies and practices that relate to staff health, safety and wellbeing. The health and safety of employees is a prime responsibility of any organisation and must be managed appropriately at all levels. Employers must take all 'reasonable steps' to prevent 'reasonably foreseeable' physical and psychiatric injury to their employees.

Preparation for the role, including training on self-care, psychological first aid, hostile environment awareness, and security and stress management, goes a long way towards keeping employees fit and healthy and able to respond to a crisis or security incident. Training and capacity building should not be overlooked – they are a priority.

The key questions below will help you test the robustness of your organisation's health, safety and security policies and practices.

Health

- Are employees physically and mentally resilient enough to carry out their roles? Are they aware of their stress triggers?
- Does the organisation have critical incident procedures, along with a sexual violence policy, and a team qualified to respond to such incidents?
- Does the organisation offer a confidential advice service, with referral to appropriate counselling or treatment services?

Assumptions are often made about the mental resilience of employees. Experienced international employees are often the first choice for high-risk postings. Do you continually assess their levels of resilience and know how to support them appropriately? It is also important to remember that employees from the local community are as likely to be traumatised by severe events as any other members of the local population they are helping.

▶ *See Module 11 – Medical support and evacuation*

Safety

- Has a health and safety assessment been carried out for each location and reviewed regularly?
- Are accidents reported and is medical support available, including psycho-social support?
- Are trained First Aiders present in the office, and are staff aware of how to contact them?

An employer must make the place of work as safe as possible and provide a safe system of work. If a place of work becomes temporarily unsafe, the employer must consider taking further reasonable steps to reduce the danger, including the possibility of ceasing the work activity altogether.

- *See Module 9 – Travel safety: airports, vehicles and other means of transport*
- *See EISF guide 'Office Opening: A guide for non-governmental organisations'*
- *See EISF guide 'Office Closure'*

Security

- Does the organisation have a security risk management framework and local security plan in place to identify, mitigate and manage security risks, as well as respond to security incidents if they occur?
- Does your organisation have a positive culture of security, i.e. do all staff understand and commit to following security guidance in order to keep themselves, their colleagues and their operations safe?

- *See Module 1 – Security risk management planning process*
- *See Module 6 – Security plan*

Practice	Minimum levels of provision
Health, safety and security	Policy and training on staying healthy, safe and secure should be in place for each location and closely aligned with stress management, personal resilience, physical and psychological health, and security risk management practices. Clear reporting of accidents, illnesses or critical incidents is key. Managers are trained to closely monitor the health of their team, using supportive conversations, informal briefs and debriefs, and spotting early signs of stress to prevent cumulative stress and burnout within their team. For senior managers who are remotely managed, a system for peer support should be considered. The organisation should continually review its health and safety practices to ensure they are relevant and provide the appropriate staff safety measures. Key stakeholders should learn from situations that are a risk to staff, programming and the organisation.

Security implications

An individual's knowledge, behaviour and attitude impact their vulnerability and exposure to risk. The more employees understand why health, safety and security procedures are in place, the more likely it is that they will follow them. For example, staff are less likely to obtain recommended vaccinations if they do not know or understand the risks of falling ill while travelling.

Road traffic accidents are one of the most serious threats to aid worker safety in the field. Ensuring drivers are trained on how to drive safely and that travellers are wearing seatbelts can significantly reduce the likelihood and impact of road traffic accidents.

Staff responding to a humanitarian crisis, especially during a fast onset emergency, are more susceptible to high levels of stress due to working longer hours in a highly pressured environment. Putting in place measures to prevent and deal with staff stress, as well as training staff on how to identify and manage stress, improves the wellbeing of staff and their decision-making. Overworked and highly stressed individuals are more likely to make poor security decisions.

Any stress reduction measures, such as R&R, must be applied consistently, otherwise staff may feel peer pressure to ignore them, even when they are needed.

See EISF guide 'Security Audits'

Performance and Development

The ability to achieve the work set out in the organisation's strategy is reliant on the employee being able to do their role in a healthy, safe and secure way. Adequate supervision and instruction must be provided to employees. Setting clear expectations with a focus on impact and providing the necessary support will help employees succeed. Through frequent two-way communication, formal and informal, the manager can listen to staff concerns and determine if performance is good and, if not, use relevant policy and practice in a consistent way to manage poor performance, grievances and misconduct.

Can't versus won't: poor performance is managed in either of two ways – a capability policy is used when the employee does not have the skills or competencies to do the work; the disciplinary policy is used when the employee will not do the work.

The frequent communication between the manager and employee should include conversations about personal development for their current and future roles. Actively supporting employees in their current activities and their career goals is more likely to motivate and enhance performance and effectiveness.

Practice	Minimum levels of provision
Performance management	Adequate supervision and instruction must be provided. Job descriptions and objectives must be clear. Frequent manager communication and feedback should take place with good performance rewarded and poor performance managed through either capability or disciplinary policies. Monitoring of security risk management should be specifically included in the performance review process for all staff who have any security responsibilities.
Grievance and disciplinary procedures	A trusted channel to raise informal and formal concerns and complaints should be in place. Grievance and discipline policy outlines a fair and consistent way to manage, monitor and learn from cases.
Whistleblowing	Whistleblowing is an anonymous way to raise a serious complaint or concern and for legitimate cases to be investigated in a confidential way.
Learning and development for the employee	Regular discussions on behaviours, development and career goals should take place.

Security should be part of every employee's performance review process.

Security implications

One of the greatest threats organisations face is from disgruntled staff. Employees who feel they have been unfairly treated can respond in a number of ways: theft, physical and verbal abuse, death threats, and 'bad-mouthing' individuals or the organisation to external stakeholders such as beneficiaries, elders and government officials, and to the media. These reactions can have serious security implications for staff, programmes and the organisation.

Performance management relies on a good employee-manager relationship. A poor relationship can erode trust and have serious implications for security if, for example, a manager's security recommendations are ignored or if an employee makes decisions which could place them and their colleagues at risk, without consulting their manager.

Without a trusted channel for raising concerns, employees may feel compelled to accept all decisions made by their managers, even if they are uncomfortable with the risks involved. Frontline staff are likely to have a better understanding of the security context but a lack of communication channels can impede information-sharing up the management line and increase the risk of a security incident occurring.

Transition

All employees leave an organisation at some point. The way an employee leaves can have an impact on the wellbeing of the individual, their colleagues and the reputation of the organisation. An employee who 'leaves well' can become an ambassador for the organisation. The more time and information an individual has to prepare for their departure, the better. Where possible, managers should start the discussions about departure before the notice period begins. It is also important to understand the reasons why staff choose to leave of their own accord.

See EISF guide 'Office Closure'

Practice	Minimum levels of provision
Pre-departure actions	Clear and transparent discussions with staff, particularly national staff, on the future of the project or office can enable employees to be better prepared for the transition and ensure that good handovers take place. Organisations should put in place measures to support staff transition, especially when the organisation is obliged to let staff go due to loss of funding or for other reasons outside of the organisation's control.
Exit interviews	Collect information and knowledge from leavers. Include questions on work-life balance, values, development, quality of briefings/debriefings and reasons for leaving. Multiple leavers from one team can indicate something more serious, and action must be taken.
Organisational learning	Learning from a leaver is a good way for an organisation to develop and manage its institutional knowledge.

Security implications

Unhappy leavers carry a security risk. Dismissals through disciplinary procedures, loss of funding, office closure and heightened security can all lead to different kinds of risks.

Disgruntled employees can disrupt project performance and relationships, and create a very unhealthy environment. In a high-risk environment, managing an employee's exit in difficult circumstances is one of the most important and complicated things a manager may have to do.

Sharing information with other employers, allowing more flexible working for job hunting and offering training opportunities (e.g. computer and English language skills) can aid staff to transition well and thereby reduce security risks.

If information is not collected from a departing employee (usually via a handover and through exit interviews), it is likely the learning will not be passed on and mistakes will be repeated. Without a good handover, there is a greater risk that a new employee will fail in their tasks and be a risk to their own and others' health, safety and security.

In order to learn and adapt, organisations need to carry out regular security assessments and apply what they learn. Crisis management exercises are also key for senior management.

When an unsuccessful programme was closing its office in Indonesia, it did not let its employees know until two days before the end of their contracts. Rumours had already circulated and employees were very upset. An office robbery took place the night before the final pay day to steal cash from the safe and take valuable items from the office. The managers believed it was best not to let employees know the exact closure date in the interests of security. However, the lack of transparency resulted in a more aggressive retaliation and compromised the security of staff. A more honest and supportive approach for the programme staff would have likely resulted in fewer incidents and greater security.

Where to read more

The CHS Alliance website (www.chsalliance.org) hosts resources which support organisations with the health, safety and wellbeing of their employees. Standard 8 of the 'Core Humanitarian Standard' outlines policies that should be in place for the security and wellbeing of staff.

Duty of Care International (http://dutyofcareinternational.co.uk/) hosts several resources including:

- The 'Human Resource Management (Roots 12)' guide published by Tearfund. This is a useful people management tool for managers, particularly where there is no human resource expertise in country.
- 'The Importance of HR Management in Supporting Staff Working in Hazardous Environments' by Roger Darby and Christine Williamson.
- 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff' by Edward Kemp and Maarten Merkelbach.

International SOS Foundation (www.internationalsosfoundation.org) provides a number of useful resources, including 'Managing the safety, health and security of mobile workers: an occupational safety and health practitioner's guide' produced jointly by International SOS Foundation and IOSH.

The EISF website (www.eisf.eu) hosts a number of relevant EISF publications that support organisations with staff care, as well as a library of further resources on staff health, safety and security.

Contents

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 85 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Acknowledgements

This module was developed by Christine Williamson. The project manager was Adelicia Fairbanks, Research Advisor at EISF.

The European Interagency Security Forum (EISF) would like to thank Rebekka Meissner and Christine Newton for sharing their expertise with us.

Suggested citation

Williamson, C. (2017) People Management. In *Security to go: a risk management toolkit for humanitarian aid agencies*. European Interagency Security Forum (EISF).

Design and artwork : www.wave.coop