Security Risk Management Toolkit: People Management

READY to go Mobile Guide

Learn how to integrate best practices in security risk management into all key stages of the employee cycle.

Security Risk Management Planning

Note to Learners

The information in this guide is for educational purposes only; it is not intended to be a substitute for professional or specialist security advice. Any reliance you place on such information is therefore at your own risk and the European Interagency Security Forum (EISF) will have no responsibility or liability under any circumstances.

Why is People Management a Security Priority for Every Organization?

People are our most valuable resource. Good people management can be described as getting the best results from an employee in a healthy and safe way. People management is a broad and complex subject that carries legal and ethical responsibilities for an organization. Organizations are responsible for ensuring the physical and psychological health of employees before, during, and after the period of employment, especially in high-risk working environments.

Organizations have many legal and ethical 'duty of care' responsibilities and are expected to go above and beyond the minimum legal obligations when working in high-risk environments.

Senior management and those in leadership positions, such as trustees, directors, and managers, must invest time and resources in people management practices. They must ensure that technical specialists within human resources and security provide the necessary advice at the right time and in the right way.

Employees should have the competence and tools to perform their roles well.

All employees should feel healthy and safe in their working environment.

Employees should be aware of their health, safety, and security responsibilities, understand potential risks, and accept any residual risk they may face in their role (knowing that the organization has developed mitigation measures to address such risks).

Employees should have the option to say no to certain tasks if they are uncomfortable with the security risks involved.

People Management and Security Risk Management

People management has a direct impact on security risk management.

Recruitment

Employing the right people for the right roles is essential to minimize security risks:

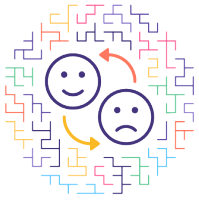
- A lack of skills and competencies can lead to poor performance and decision-making.
- Poor behavior can lead to personal and program risks.
- Failure to consider the implications of the ethnic diversity in some regions can create issues between staff and negative perceptions in the local community.

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.

Employment Policy and Practice

Employees are more likely to feel valued and protected when employment policies regarding reward, performance, and conduct are clear and consistently applied. Disgruntled and dissatisfied staff can be a source of security threats to an organization, its programs, and staff.



Stress Management

Risky and high-pressured situations are more likely to lead to a highly stressed workforce, which can impact behaviors, relationships, and the ability to make good security-related decisions.

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.

The Employee Cycle and Good People Management

Ensuring people management standards remain high and meet duty of care obligations should involve senior management and all levels of staff in your organization. The employee cycle is a good way to identify the practices in people management which carry an obligation or risk. Good people management should integrate security risk management in 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 your organization. In most organizations, this is the role of a 'Risk Management Group' or 'Health and Safety Committee'.

Governance (policies, systems, contracts)

- Mission, goals, and values
- Organizational strategy and structure
- Organizational risk threshold
- Pay and benefits
- Legal contracts and employee handbook (employment policy)

Recruitment

- Clearly defined roles
- Risk assessment of roles, tasks, and people
- Competency-based recruitment
- Verified references and background checks

Induction

- Preparation for the role and environment
- Contextual security briefings and training
- Informed consent

Health, Safety, and Security

- Clearly communicated risk management strategy
- Health and safety policies and practice
- Local security plans and crisis response policy
- Monitoring and evaluation of security practices and incidents
- Security training, briefings, and debriefings

Performance and Development

- Supervision, support, and feedback on performance
- Health and wellbeing support (managing work-related stress)
- Channels and reporting systems for employees to raise concerns
- Management of working hours and rest/recuperation
- Learning and development

Transition

- Handover and exit interviews
- Termination of contracts
- Grievance and disciplinary procedures
- Learning reviews and knowledge management

Governance

How Governance Impacts Security Risk Management

The first stage of the employee cycle is governance, which represents the structures and policies that your organization is built upon. Your organization's health, safety, and security culture rely heavily on having **robust systems and practices** in place. Employees are more likely to feel valued when policies and practices are clear and applied consistently. Uneven policy implementation will increase risks to employees' health, safety, and security. Follow these tips on building a strong and secure governance model for your organization and its employees.

Robust Systems and Practices
Robust practices are ones that are value-centered, of a high standard, sustainable, accessible, relevant, known, used, monitored, and evaluated.

Mission, Goals, and Values

Develop a clear mission, goals, and values that will provide vision and clear expectations for your organization and its employees.

- **The mission** demonstrates why your organization exists and how it would like to change the world for the better. The mission is also needed to motivate staff.
- **The goals** ensure that employees are working towards the same purpose.
- **The values** show how your organization will do its work and the type of employees needed to do it.

Organizational Risk Threshold

Define your organization's risk threshold that:

- Identifies what the board/senior management considers to be an acceptable level of risk for the organization.
- May be different for specific types of activities (saving lives vs. development).
- Forms the basis for all security risk management policies and plans throughout the organization.
- Enables employees to check their own acceptable risk threshold against that of the organization.

Organizational Strategy and Structure

- Develop a comprehensive organizational strategy that provides direction and defines the work to be done, by whom, where, and by when.
- Establish an organizational structure that:
  - Outlines who is who in the organization.
  - Shows the reporting lines.
  - Is used for job descriptions, grading, and job titles.
  - Facilitates recruitment, induction, general management, and communication across the organization.
- Set up a strong organizational structure that clearly defines security responsibilities within the organization and the decision-making process during a critical incident (staff abduction).

Contract of Employment and Employee Handbook

- Develop organizational contracts and handbooks that are legal, clear, and accessible with consistent principles of employment practice for all defined categories of staff, including short-term employee contracts.
- Be transparent on grade, pay, and allowances for all categories of staff to reduce concerns and complaints.
- Avoid lack of clarity on contractual stipulations, for example, early termination, that can lead to disgruntled employees retaliating and compromising the security of other employees, the organization, and its programs.
- Seek local legal advice when setting up local contracts.
- Create an employee handbook that provides managers and employees with useful information about the organization, including organizational policies and terms and conditions of employment.

Pay and Benefits

Apply pay and benefits (including allowances) using consistent principles that are aligned with local practice and adaptable for an early humanitarian response stage. This includes:

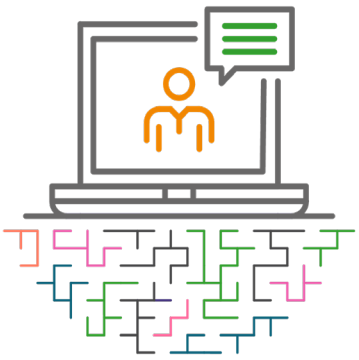
- Consulting employees on changes to their pay and benefits.
- Clearly defining variations for different staff types (international, re-located, national, volunteer).
- Taking direct action regarding benefits such as:
    - **Leave:** Monitor annual leave and carryover, national holidays, rest and recuperation (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 provisions with annual reviews and records of cases.

Working Hours

Establish appropriate working hours and compensation for overtime with adaptable working patterns for when staff initially respond to a sudden-onset emergency.

Disciplinary Procedures

Define clear disciplinary procedures to deal with employees who pose a threat to other colleagues. This should include provisions related to safeguarding, harassment, bullying, and other internal threats.



Recruitment

How Recruitment Impacts Security Risk Management

Risky environments require employees with specific skills and experience. An organization should never underestimate the importance of the recruitment process and the risks associated with hiring the wrong person. Employees who do not fit the role are likely to be unhappy and underperform which will have a direct impact on program implementation, their manager's time, team morale, and security.

Follow these tips on developing a sound and secure recruitment process.

Risk Assessment

- Complete a risk assessment of the role before the recruitment process starts. This is done by the manager in liaison with security and human resources. The purpose of the risk assessment is to:
  - Understand the essential requirements of the role.
  - Ensure that suitable candidates are encouraged to apply.
  - Identify the risks inherent to the role itself.
  - Determine the risks that need mitigating for the particular applicant in the specific role.
  - Define mandatory health and safety interventions for high-risk roles or roles in high-risk contexts.
- Complete an individual risk assessment for the specific role once applicants have been identified. This will assess the impact their skills, experience, age, gender, sexual identity, disability, or ethnicity could have on their personal safety and security, while also ensuring compliance with equal opportunity legislation.

Recruitment

- Develop a clear job description and well-managed recruitment process using competency-based techniques with diversity at the heart.
- Verify references and conduct solid background checks. This is especially important for humanitarian organizations working with vulnerable populations (including children) and the reputational and security risks associated with a breach of the code of conduct.
- The recruitment process should inform about the content of an induction.

Involvement of Managers

- Fully train managers in the recruitment process.
- Involve managers in the recruitment of their teams. If the manager does not speak the local language, ensure that job applicants are not 'prescreened' only by local staff to avoid the risk that one section of the local community is given an unfair advantage.
- Encourage managers to recruit the most qualified person and set up mitigating measures that enable the person to work in an environment with the lowest security risk possible.

Equality and Diversity

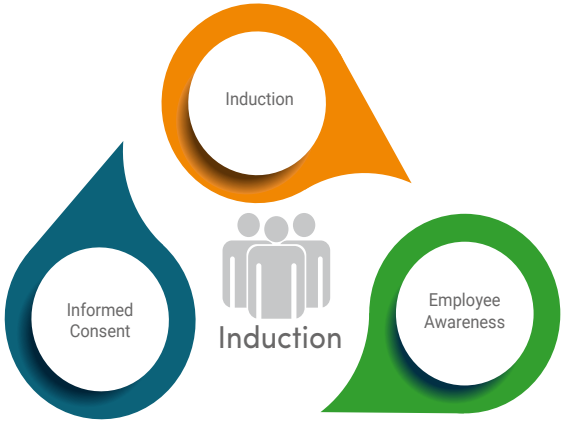
- Establish an equality and diversity policy and ensure all employees understand its principles and apply them in their work and behavior.
- Outline discrimination characteristics and define strong sanctions for any breach of policy.
- Understand the diversity of your staff to help you develop better security systems and accessible resources to support their safety.
- Identify potential security implications and risks that the ethnicity of national and international staff may have on both the individuals and the organization.
- Be aware that while discrimination in recruitment is morally and legally unacceptable, it is important to consider how an individual's ethnicity, gender, and/or sexuality may affect or impact the security of the individual, the organization, and its programs.

Induction

How Induction Impacts Security Risk Management

Effectively preparing an employee for their assignment, especially in high-risk environments, is the most important responsibility of any organization and a critical factor of duty of care. Unprepared employees who do not understand risks or the local security context can make poor decisions that could jeopardize their personal security and the security of others. Staff who are unaware of operational or personal restrictions are more likely to break security procedures, put themselves and their program at risk, and be demotivated and dissatisfied with the organization. This, in turn, will contribute to higher staff turnover.

Follow these tips on how to effectively incorporate security risk management into the induction of new employees.



Induction

A good induction and handover process are essential for all new employees, especially if they will be responsible for making decisions about staff health and safety in a high-risk environment. Management is responsible for leading each new employee through a comprehensive induction program that provides essential information and training on the following:

- The organization's mission, goals, strategy, behaviors structure, and reporting line
- Code of conduct, policies, and practice
- Team/program mandate
- Key relationships
- Role and responsibilities
- Handover
- Contextual health, safety, and security
- Probation objectives

Employee Awareness

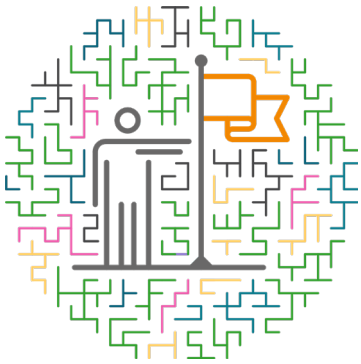
Employees should be informed and fully aware of the following:

- The acceptable level of risk for the organization, and the policies which govern the security culture.
- Organizational security procedures and systems to manage their safety, security, and wellbeing.
- Risks to their own personal safety.
- The context in which they are working and how their own behavior can affect their vulnerability and the vulnerability of those around them.
- Behavioral expectations (mitigation measures) during and outside normal working hours.
- How stress affects their personal behavior and how to manage it effectively.
- The impacts and risks of releasing stress in damaging ways (excessive drinking, drug use, promiscuity).
- Disciplinary measures that will be enforced against employees who put themselves and others at risk.

Informed Consent

Informed consent is the process in which employees are briefed on their role, their individual vulnerabilities, and fully understand and accept the risks involved in taking the job. Informed consent is not a legal waiver but must be formalized with a signed document stating that employees:

- Have been thoroughly briefed and understand the security risks associated with their role and the context.
- Understand the provisions the organization is making to manage the risks in the context.
- Understand what is expected of them.
- Are comfortable with any residual risks in their role knowing that the organization has developed mitigation measures.



Health, Safety, and Security

How Health, Safety, and Security Impacts Security Risk Management

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. Overworked staff members are more likely to make poor security decisions which can have serious consequences and risks for both individuals and the organization. Ensuring the health, safety, and wellbeing of employees is a prime responsibility of any organization. Relevant measures include training staff on how to identify and manage stress to mitigate associated security risks. The more employees understand why health, safety, and security procedures are in place, the more likely they will follow them.

Follow these tips on how to effectively incorporate security risk management into the health, safety, and security of employees.

Health

Ask these key questions to determine if your organization promotes a healthy working environment for its employees and partners:

- Do you continually assess employees' levels of resilience and know how to support them appropriately?
- Are your employees physically and mentally resilient enough to carry out their roles?
- Are employees aware of their stress triggers?
- Do you have critical incident procedures and a sexual violence policy? Do you have a team qualified to respond to such incidents?
- Do you offer a confidential advice service with referral to appropriate counseling or treatment services?
- Are you aware that employees from the local community are as likely to be traumatized by severe events as other members of the local population they are helping? What procedures are in place to protect their physical and mental health?
- Are stress-reduction measures, such as leave and rest and recuperation (R&R), applied consistently across the organization so staff feel comfortable and know when to use them when needed?

Safety

Ask these key questions to determine if your organization promotes a safe working environment for its employees and partners:

- Has a health and safety assessment been carried out for each location and reviewed regularly?
- Are accidents reported and is medical support available, including psychosocial support?
- Are trained First Aid responders present in the office? Do staff know how to contact them?
- If the work environment becomes temporarily unsafe, do you have a reasonable action plan to reduce the danger and prevent the possibility of ceasing the work activity altogether?

Security

Ask these key questions to determine if your organization promotes a secure working environment for its employees and partners:

- Do you 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?
- Do you have clear reporting of accidents, illnesses, or critical incidents?
- Do you have a positive culture of security?
- Do all staff understand and commit to following security guidance to keep themselves, their colleagues, and their operations safe?

Training, Support, and Policies

Ask these key questions to determine if your organization provides adequate training, support, and policies on health, safety, and security for its employees and partners:

- Do you continually review health and safety practices to ensure they are relevant and provide the appropriate staff safety measures?
- Are staff prepared for their role and trained on self-care, psychological first aid, hostile environment awareness, and security and stress management so they can respond to a crisis or security incident?
- Are staff trained on how to safely travel and work in new locations?
- Are drivers working for the organization trained on how to drive safely?
- Do staff members who are remotely managed have a peer support system?
- Are managers trained to closely monitor the health of their team and to identify early signs of stress?
- Do managers know how to use supportive conversations and informal briefs/debriefs?

Performance and Development

How Performance and Development Impacts Security Risk Management

Your organization's ability to achieve strategic goals relies on its employees' capacity to perform their role in a healthy, safe, and secure way. Many factors contribute to performance management including the quality of the employee-manager relationship. A relationship lacking trust can have serious security implications and lead to poor decision-making that could place staff at risk.

Employees who feel they have been unfairly treated may respond in a number of ways that can have broader security implications. This might involve theft, physical and verbal abuse, death threats, or 'badmouthing' individuals or the organization to external stakeholders such as partners, beneficiaries, government officials, and the media.

Follow these tips on how to effectively incorporate security risk management into the performance and development of employees in your organization.

Performance Management

- Provide adequate supervision and instruction.
- Develop clear job descriptions and objectives.
- Set clear expectations with a focus on impact and provide the necessary support.
- Encourage frequent two-way communication (formal and informal) where the manager can listen to staff concerns and provide feedback on performance. Managers should consistently apply relevant policies and practices to manage performance issues, grievances, and misconduct.
- Ensure managers and employees develop a personal development plan for their current and future roles.
- Actively support employees in achieving their goals to maintain their motivation.
- Include the monitoring of security risk management in the performance review process for all staff who have any security responsibilities.

Employee-manager Relationships

- Establish efficient and trusted communication channels that allow employees to feel safe to voice their concerns.
- Encourage staff to speak up if they personally do not feel comfortable with the risks involved in their work.
- Ensure that frontline staff are able to share information up the management line to prevent incidents from occurring. They often have a better understanding of the local security context.

Grievance and Disciplinary Procedures

- Establish a trusted channel to raise informal and formal concerns and complaints.
- Set up a grievance and discipline policy that outlines a fair and consistent way to manage, monitor, and learn from cases.

Whistleblowing

- Allow for whistleblowing as an anonymous way to raise serious complaints or concerns.
- Develop a process to investigate legitimate cases in a confidential way.

Learning and Development

- Managers and employees should have regular discussions on behaviors, development, and career goals.
- Offer learning and development opportunities to all staff and encourage engagement.

Transition

How Transition Impacts Security Risk Management

All employees leave an organization 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 organization. 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, 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 and teams may have to do.

Follow these tips on how to effectively incorporate security risk management into employee transition and the handover process.

Information Sharing

Take these actions to ensure that an employee 'leaves well' and will become an ambassador for your organization:

- Have clear and transparent discussions with staff, particularly national staff, on the future of the project/office to better prepare them for the transition and an effective handover.
- Encourage managers to start discussions about their departure before the notice period begins.

Pre-departure Actions

- Establish measures to support staff transition, especially if your organization is obliged to let staff go due to loss of funding or for other reasons outside of the organization's control.
- Allow for flexible working options to give employees time for job searching.
- Offer learning opportunities to help staff update their skills to support a smooth transition and consequently reduce security risks.

Handover and Exit Interviews

- Conduct a comprehensive exit interview to collect key information and knowledge from departing employees. Ask questions about work-life balance, values, development, quality of briefings/debriefings, and the reasons for leaving.
- Conduct an effective handover process to ensure that a new employee will succeed in the role and to reduce risks to their own and others' health, safety, and security.
- Be aware of multiple leavers from one team. This may indicate there is a more serious issue and action must be taken.

Organizational Learning

- Learn from a departing employee so your organization can better develop and manage its institutional knowledge.
- Carry out regular security assessments and apply what was learned from the results. Crisis management exercises are key for senior management.