ICAO

Version 1
Published June 2023

ICAO STARTER PACK

Human Factors and Human Performance – Strengthening Security Culture in AVSEC

Purpose:

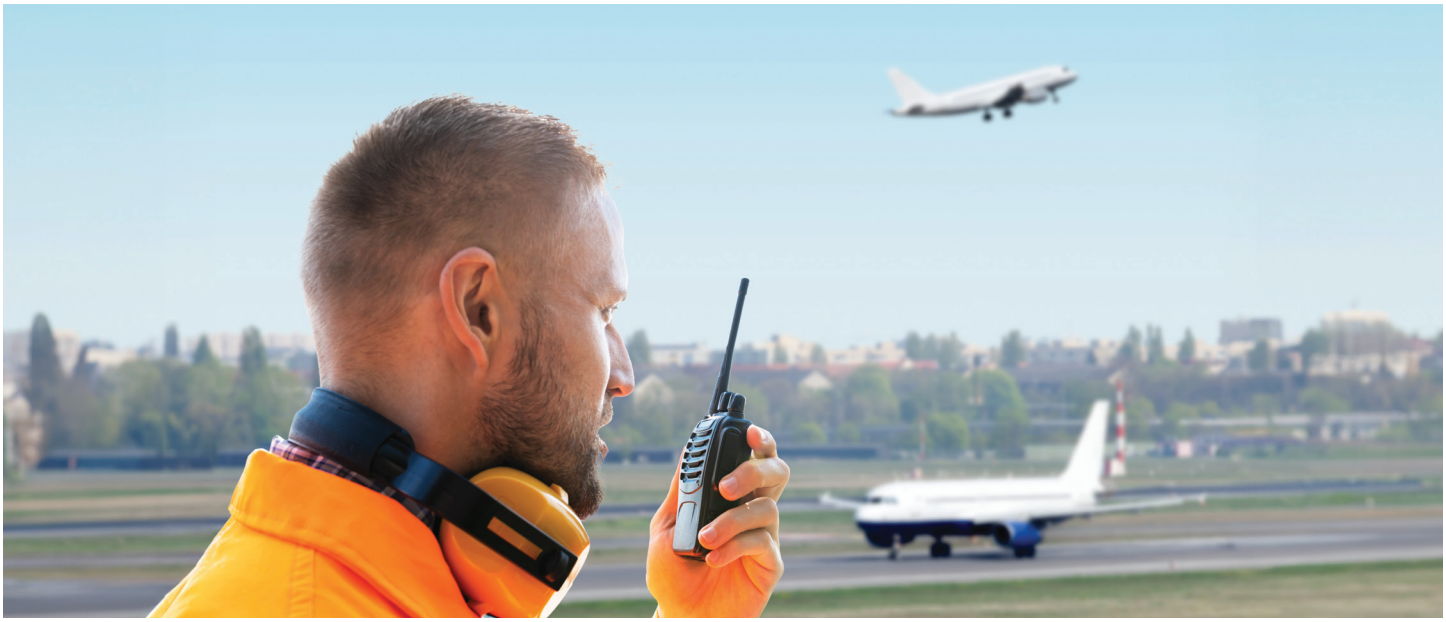
This *Starter Pack*, created by the Aviation Security Panel's Working Group on Training, is designed to supplement existing ICAO material on security culture[1] and build foundational knowledge on human factors and human performance. Considering the interconnected relationship between human factors, human performance and security culture, it aims to provide practical approaches and guidance to better understand how employees can perform at their best, thereby contributing to the effectiveness and efficiency of the aviation security system.

Evolution:

Security culture has now become an embedded concept in aviation. As the concept evolves, adding knowledge and understanding of human factors and human performance will help the aviation community to maintain and strengthen its security culture.

Audience:

The target audience for this *Starter Pack* includes managers and employees working for regulators and national appropriate authorities in security and non-security roles in the civil aviation sector. Instructors who design and deliver security culture and human factors training courses and workshops will also benefit.



The Importance of Human Factors and Human Performance in AVSEC

Our employees continue to provide critical mitigation against acts of unlawful interference and threats to aviation, either directly through their job role and use of their specialized skills and competencies, or indirectly through contributing to a strong and effective security culture. Human factors and human performance considerations are therefore critical to the design of security processes, procedures and systems. The goal should be to reduce human error, to support the motivation and performance of the employees, and to make it easy to "do the right thing", for example, reporting security concerns and displaying positive security behaviours.

The growing use of security equipment and new technologies also makes human factors and human performance more critical. The more automated security processes are, the more employees risk losing their traditional security skills (as they are no longer using them) and instead occupy monitoring roles, which can make the system vulnerable to errors[2]. While many security processes are facilitated through technical equipment, or are even automated, the final decision about whether an object, a person or a situation is safe and secure is, in many cases, still made by a human and not a machine.

ICAO Definitions

Annex 17 – *Aviation Security* uses the following definition for **Human Factors principles**:

Principles which apply to design, certification, training, operations and maintenance and which seek safe interface between the human and other system components by proper consideration to human performance.

Annex 17 – *Aviation Security* provides a definition for **Human performance** in the context of aviation:

Human capabilities and limitations which have an impact on the safety, security and efficiency of aeronautical operations.

ICAO's Five Principles

ICAO identifies five principles[3] according to which human performance is influenced:

- **Capabilities and limitations:** People's performance is shaped by their capabilities and limitations;
- **Interpretation and sense-making:** People interpret situations differently and perform in ways that make sense to them;
- **Adaptation to changing demands:** People adapt to meet the demands of a complex and dynamic work environment;
- **Risk assessment and trade-offs:** People assess risks and make trade-offs; and
- **Interaction with people, technology and environment:** People's performance is influenced by working with other people, technologies, and environments.

A short ICAO film illustrating these five principles is available at: www.icao.tv/videos/human-performance

ICAO Resources

The ***Manual on Human Performance (HP) for Regulators*** (Doc 10151) provides guidance to regulators on human performance principles in the safety environment, such as motivation, managing change, and job design. Much of this ICAO guidance is equally applicable in the security domain.

Hindsight: Understanding employees and their actions

Everyone takes action or makes decisions based on what seems right at the time (the logic of the situation). In an aviation security setting, this could be a security officer at their checkpoint or a senior manager making strategic security decisions.

Our performance is based on our knowledge and understanding of the situation, and our level of concentration. This "*local rationality principle*"[4] makes it more difficult for employees to take actions that do not make sense to them. This is important because if employees do not understand threats to aviation, how security equipment works or know why they are asked to perform security tasks, then employees will have greater difficulty adequately performing such tasks.

It is also important to recognize that security actions that may not appear to make sense, or seem logical only in hindsight, may reflect an employee's understanding of a given situation at that time. Therefore, it is important to carefully consider whether the situation could reoccur if the original context is still present for other employees.

There is also a tendency among employees towards complacency; the belief that a security incident will never happen to them or their organization. This can be a major problem when attempting to convince employees or senior leaders of the need to look at human factors, to recognize risks and to implement security improvements, rather than merely paying "lip-service" to security and security culture.

The link between motivation and performance

High employee motivation plays a critical role in the maintenance of a positive security culture and in the effective implementation of aviation security measures. Motivation drives performance, alongside individual capabilities, the working environment and levels of accountability. Just as certain factors help motivate employees and increase job satisfaction, other factors have the opposite effect and low motivation can have negative security and performance outcomes.

Employee performance relies on motivation, which can be defined as follows[5]:

Motivation + **Capability**
- Knowledge
- Skill
- Proficiency

+ **Accountability**
- Structure
- Process
- Policies

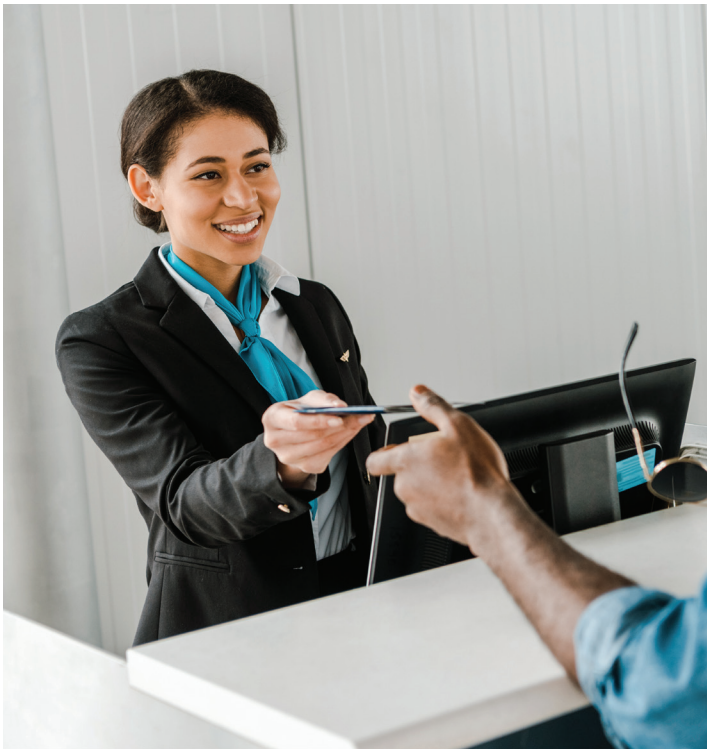
= **Performance**

How to assess and improve employee motivation

To improve employee motivation and strengthen security culture, an assessment of current levels of motivation is recommended. This will help identify specific areas or aspects of security and motivation where development is needed.

To help gather reliable and valid feedback on motivation, the following tools and methods can be considered:

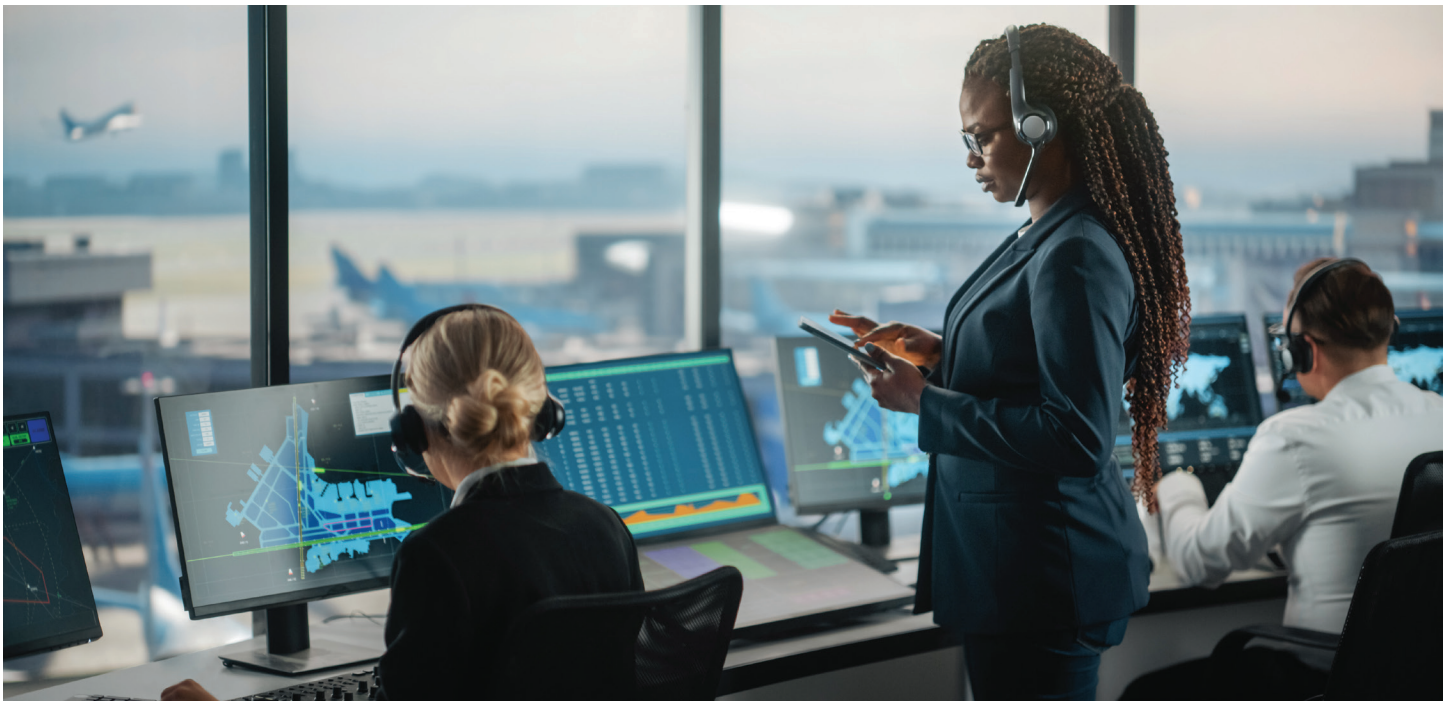
- Employees surveys and interviews;
- Focus groups involving stakeholders and customers who interact with employees;
- Observations of employee performance; and
- A combination of the above methods.



Areas to consider when assessing employee motivation

	Positive Indicators	Negative Indicators
Working environment	• Sufficient and good quality supervision (adequate and properly trained employees) • Clear security policies and Standard Operating Procedures (SOPs) • Optimal physical working conditions (including good space, temperatures, lighting, noise)	• Inadequate supervision and/or supervision not carried out properly • A lack of clear security policies and/or confusing processes • Poor physical working conditions (noisy, inadequate space, cold/hot, glare, etc.)
Organizational culture	• Employees feel supported in their role • Managers lead by example and display positive security behaviours and actions	• Employees don't feel supported • There is an "us vs. them" culture, with senior managers held to different security standards (which may be perceived as unfair)
Job Role	• Employees have an element of autonomy • Job roles include a variety of security tasks • Employees' capabilities and skills are aligned to their role • There is an established process for providing feedback to employees, so that they can understand their own security performance • Employees understand the impact (positive or negative) their work has on others and the organization • Employees understand their role in the organization and how their work relates to its overall security objectives and mission (for example, "security is everyone's responsibility".) • The working hours or shift roster allow for a work/life balance	• Employees have very little autonomy • Job roles include little variety in security tasks, with much task repetition • Employees' capabilities and skills are not matched to their roles or considered • Employees are not given feedback on their security performance • Employees are not aware of the impact (positive or negative) of their work on others and the organization • Employees see their role in isolation and don't see that security is everyone's responsibility • The working hours or shift roster have a negative impact on the work/life balance of employees

	Positive Indicators	Negative Indicators
Economic Factors	• Good job security for employees • Pay is sufficient to allow employees to support themselves and their families • Employee benefits create an attractive workplace that promotes employee retention	• Employees worry about losing their jobs • Pay is low and puts employees in a financially insecure position • The lack of benefits results in employees actively seeking employment elsewhere
Recognition and growth	• Employees have opportunities for promotion or career progression • The personal success of employees is supported by managers and leaders • Good security performance is recognized (including through an awards and recognition programme) and poor behaviour is addressed • Security roles are recognized as a profession with great responsibility • There are opportunities for professional development	• There are few promotion or career progression opportunities, and/ or they are not available to all employees • Employees are not invested in or supported • Good security performance is not routinely recognized and there is no awards and recognition programme in place. Poor behaviour is tolerated • Security roles are not recognized as a profession and there are limited opportunities for professional development.



Common human factors which can impact performance

ICAO lists over 300 human error precursors to accidents and incidents – while primarily aimed at safety, these can also impact security performance, and should be considered[6]. The most common are:

1. **Lack of communication and teamwork:** Good communication will remove barriers and support security messaging (including confirming and recording important security details and concerns). Teamwork is critical to ensuring a good security outcome and should be built into security procedures. Supervisors and team leaders should ensure that, as part of their monitoring duties, they observe team dynamics, create a positive atmosphere and address any communication issues early.

2. **Distraction:** Some distraction in an aviation environment, such as noise, is hard to avoid. However, employee distractions should be kept to a minimum, (for example, by limiting non-critical questions and social conversations while on duty to support the effective implementation of aviation security measures). Distractions might also be "invisible" (for example, problems at home). Good supervision is critical to spot employee distraction issues early and to determine whether the root cause is stress, fatigue, health concerns or something else..

3. **Resource limitations and fatigue:** Lack of either physical or human resources can create additional pressure on employees who must complete security tasks. Ensuring that sufficient resources are available can alleviate this pressure. Inadequate resourcing can lead to employee fatigue – although there are a range of other fatigue causes such as lack of sleep, long working hours, type of work performed and cognitive load (screeners). Work-related fatigue can be lessened through sensible shift schedules and ensuring that the length of shift is appropriate to the task.

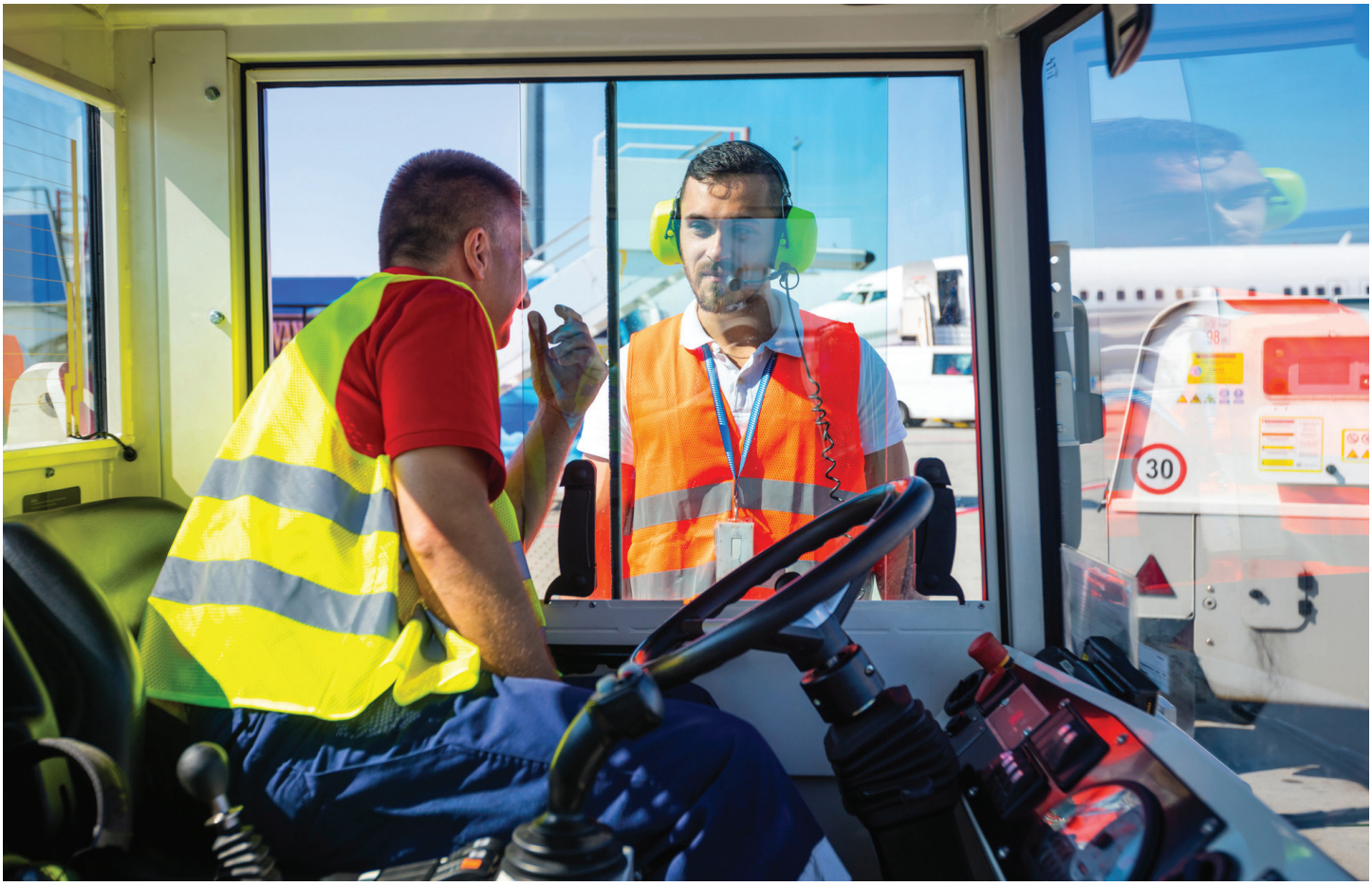
4. **Stress and pressure:** Stress commonly takes a variety of forms – including acute (real time pressure) and chronic (accumulated) stress. The symptoms of stress can include, but are not limited to, poor memory, errors of judgment and poor concentration. Assisting employees with identifying symptoms of stress at an early stage can help ensure the root cause is addressed and supports a positive security culture. Pressure can be created by the environment and lead to a "quantity over quality" mindset. Operational protocols should be designed and adapted to avoid pressure situations while empowering employees to report any tasks that incur pressure.

5. **Complacency and Habituation:** Complacency is a state of satisfaction accompanied by a lack of awareness of potential dangers – this can be brought on by a relaxation of vigilance in the face of no recent security incidents. Ensuring employees are motivated to perform their tasks in accordance with security protocols is essential. Clear career pathways and opportunities for development can be keys to maintaining this motivation. Regular communication, recurrent training and continuous system testing can also help to reduce the risk of complacency and prevent acts of unlawful interference.

6. **Lack of knowledge and awareness:** Lack of knowledge or on-the-job experience can lead to misjudgment and poor decision-making. Fading security skills can also be an issue – particularly after periods of absence. These can be mitigated through recurrent training and careful analysis of training needs. A loss of awareness ("tunnel vision") of the impact of one's work on others and on the organization can develop, but good supervision can mitigate this.

7. **Lack of assertiveness:** Assertiveness is a communication and behavioural style that allows us to express feelings, opinions, concerns, beliefs and needs in a positive and productive manner. Lack of assertiveness can lead to individuals not raising concerns – supervisors can assist with providing feedback and raising awareness.

8. **Norms and organizational culture:** Organizational culture relates to how things are done in the workplace – good and bad practices that stem from the values and culture of the organization. A positive and supportive organizational culture will allow employees to do the right thing when it comes to security and help to build a strong and effective security culture.



Constructing a checklist to assess the impact of human factors

One way to assess the impact of human factors for new, changing or existing security tasks, or following a security incident, is to use a checklist. A checklist can be designed by creating a list of relevant features – either for one specific task or generically for a range of tasks – enabling a systematic review to take place.

The table below contains examples of features that could be included in a checklist. These should be considered in the context of human capabilities.

Context:		Checklist:
Operational, Including Task Design	→	☐ Personnel selection ☐ Experience of staff ☐ Adequacy of training (initial or refresher) ☐ Occupational currency of staff ☐ Knowledge of specific processes and equipment ☐ Policies/SOPs (available and clear) ☐ Supervision (sufficiency and quality) ☐ Local operating pressures ☐ Resourcing (inadequate or adequate)
Behavioural	→	☐ Distraction and boredom ☐ Haste in completing tasks ☐ Personal problems (financial, family, or professional) ☐ Impact of fatigue ☐ Lack of confidence or overconfidence ☐ Complacency ☐ Motivation (low or high) ☐ Team cohesion ☐ Stress ☐ Impact of shift work

Context:		Checklist:
User Design	→	☐ Design and location of equipment controls ☐ Confusion of controls, switches, etc. ☐ Misread controls or screens ☐ Visual restrictions due to structure ☐ Task oversaturation (complex steps) ☐ Workspace design and configuration ☐ Effects of automation
Task Related	→	☐ Tasking information (briefing, etc.) ☐ Task components (number, duration, etc.) ☐ Workload tempo ☐ Workload saturation ☐ Supervisory surveillance of operation ☐ Judgment and decision-making ☐ Situational awareness (loss of)
Physical Work Environment	→	☐ Visibility restriction (glare, etc.) ☐ Work area lighting (low or high) ☐ Noise (excessive) ☐ Equipment vibration ☐ Heat or cold ☐ Weather (for external tasks and roles)
Communication	→	☐ Adequacy of written materials (availability, comprehension, currency, etc.) ☐ Misinterpretation of oral communications ☐ Language barriers ☐ Noise interference ☐ Team coordination ☐ Team non-verbal communications ☐ Equipment warning sounds and displays

Measuring maturity of work environment in respect of human factors, human performance and security culture

It can also be important to assess the maturity of an organization when considering human factors and human performance[7]. Below is a scale to help assess maturity, where 5 is considered as resilient (and so having a strong and effective security culture) and 1 is considered vulnerable (and so having a poor security culture). The assessment can be done by matching the characteristics set out at each stage against the actual indicators present in an organization. Where a mix of indicators across more than one maturity level is present, the level where the majority of indicators are present should be selected as the outcome.

5
RESILIENT

- There are defined and documented security policies in place that set organizational expectations and requirements for human factors and human performance. The maintenance of an effective, performance-based and tested security programme, which fully considers the human contribution to the security system and the factors which affect human performance, is a core organizational priority.
- All employees understand that human factors have the same priority in security as they have in safety, and that the human component is critical to ensure secure and safe aviation. Security is seen as everyone's responsibility – from the ground up and from the top down.
- Employee engagement on the subject of human factors and security is excellent, with the opportunity for feedback and learning lessons from experience.

4 PROACTIVE

- The majority of employees in the organization believe that human factors considerations are important to security and that their actions make a difference. Therefore they are engaged, perform work diligently and lead by example in their security behaviours and practices.
- Managers and employees understand that security vulnerabilities can be caused by a variety of events, sometimes including human factors. The work environment is therefore designed to help prevent human factors from impacting negatively on performance. Employees accept personal responsibility for security and take appropriate action when security weaknesses, including the potential for human error, are identified.
- The organization puts significant effort into proactive measures to prevent human factors, including engagement of employees and testing of security measures, from becoming a security weakness. Security performance is measured using all data available, including on human performance.

3 COMPLIANT

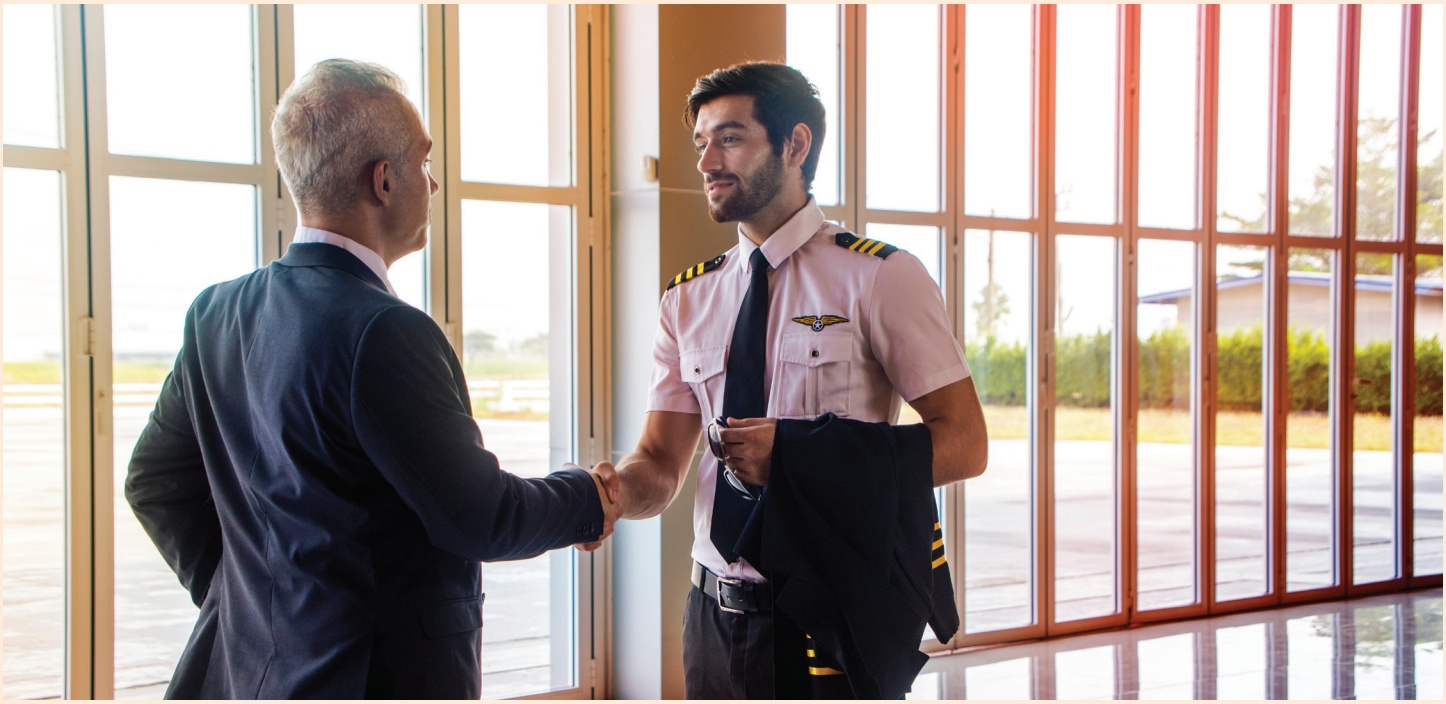
- Security, including the human component, is recognized as an important business risk and is overseen by senior managers and leaders. The organization believes in the importance of supporting human performance as part of the security mitigation measures in place. Employees at all levels are involved in helping to achieve a strong and effective security culture.
- The majority of employees are prepared to support security objectives and to take personal responsibility for their own performance. Employee engagement on taking account of human factors is developing. Security performance is monitored and some human performance indicators are considered.

2
REACTIVE

- Security is seen in terms of regulatory compliance and the adherence to rules and procedures that have been set by the appropriate authority. Human performance and factors are only considered where required specifically by regulations. Security is reluctantly seen as a business risk, with investment in human performance and factors seen as an unavoidable financial overhead in context of a perceived small risk of incidents. The Security Department owns the security programme and human performance and factors are only considered periodically in reports to senior management. Employee engagement on performance is limited.
- Security performance is measured by reactive indicators, such as the number of security incidents – human performance is not actively considered. Senior managers react to human factors impacting performance and interventions are seen as intrusive by employees rather than supportive.

1
VULNERABLE

- Security is defined and thought about only in terms of compliance with regulations at minimum cost, with the human component seen as a financial burden. It is not seen as a key business risk, and factors impacting human performance are not considered to be critical. Security and its human component are the sole responsibility of the Security Department and there is little to no engagement with employees on this matter.
- Incidents and security failures as a result of human factors are not considered at their root cause and blame is assigned to individuals instead. Most employees do not understand their role in the security system and the factors that can impact their performance.



Actions at the national level

A number of actions can be taken at the national level to help ensure a resilient and mature working environment. Actions include:

- Encourage the inclusion of human factor principles when designing security policies. This can be achieved through new or existing regulatory means (including but not limited to Annex 17 – *Aviation Security*) and through guidance;
- Take into account human performance considerations when granting approval of equipment prior to use in aviation operations;
- Consider employees in security functions as professionals. They are a 'profession', where their unique skills and competencies merit recognition;
- Ensure that human performance and human factors elements are reflected in security programmes, including in the national quality control programme, as well as in national civil aviation training policies;
- Include learning outcomes that build competency in human factors principles in the national training requirements for managers, supervisors and instructors; and
- Encourage organizations to consider:
  - Hiring human factor expertise in the organization to support in the design and improvement of operations;
  - The integration of job design principles into job functions to support the motivation and performance of employees;
  - The continual assessment of employee needs, particularly after any change impacting the organization, such as restructuring; and
  - The importance of ensuring that managers, supervisors and instructors have a good foundation in human factors principles. Human factors principles should also be included in AVSEC training programmes (at the national and local levels), in order to ensure that all AVSEC employees have a working understanding of them. A model training outline is below:

Model training outline

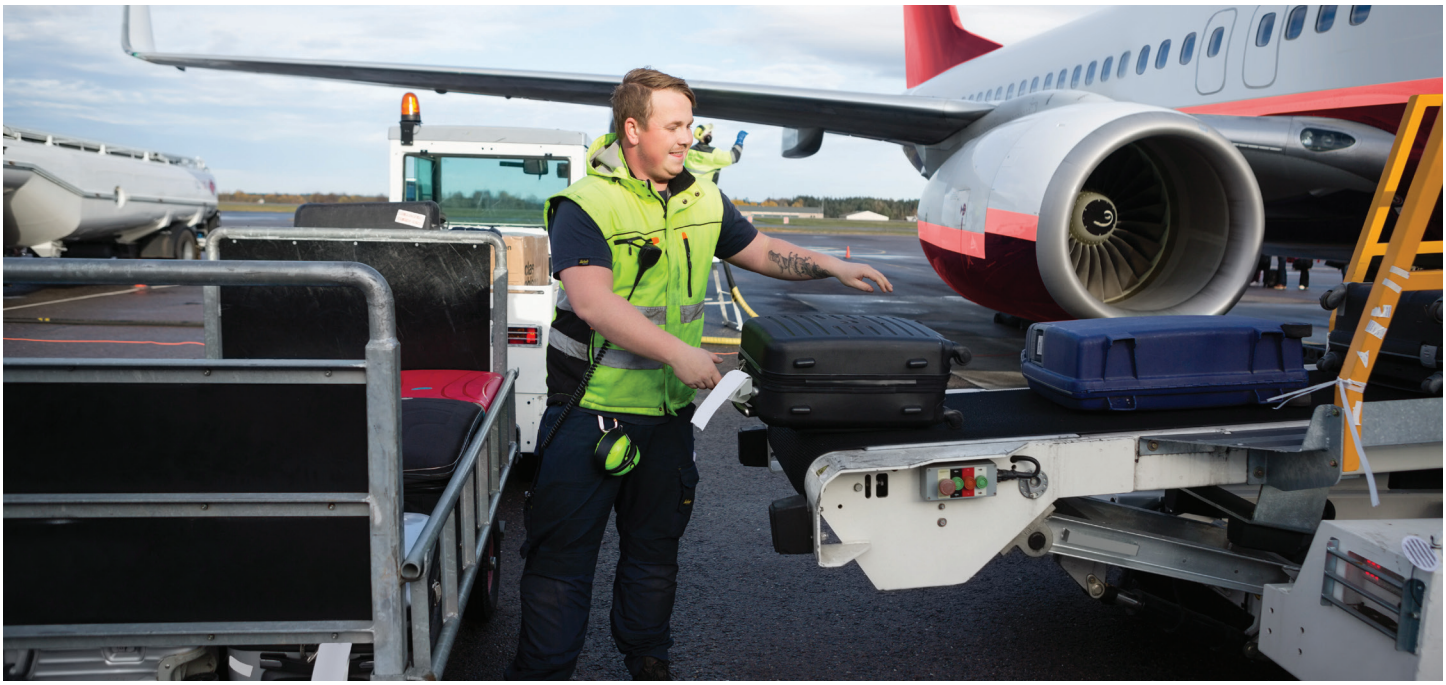
The training outline below can be used at the national or local (manager/supervisor) level to increase knowledge of human performance and human factors in aviation. The length of training and depth of detail of the material can be varied depending on the needs of the audience.

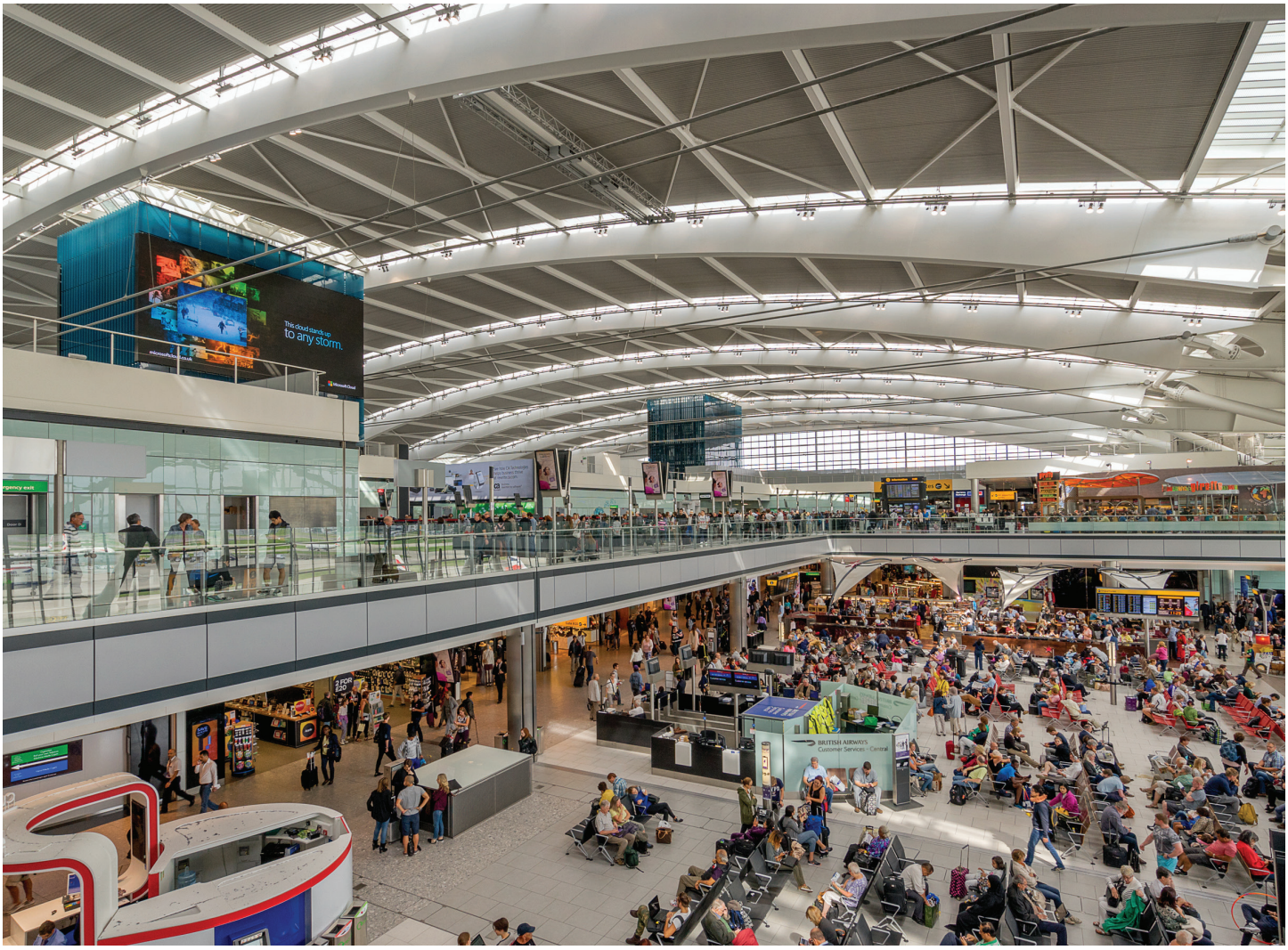
Human Performance And Factors	
Aim: To ensure the trainee understands how human factors can impact the performance of employees	
Learning outcome – trainees will	**Key content areas**
1. **Understand key definitions and principles**	• Defining human performance and human factors • Understanding the relationship between these concepts in a security setting
2. **Understand why human performance and human factors are important**	• Understanding that human performance directly impacts the effectiveness of security measures, including the security culture within an organization • Understanding that human input is critical to aviation security processes and decision-making • Realizing that human limitations and capabilities vary • Understanding how human factors can support employee performance • Preventing security incidents

Learning outcome – trainees will	Key content areas

3. Understand the factors affecting employee motivation	• Understanding the areas from which human factors stem:
	  - Organization
	  - Job role
	  - Personal
	• Understanding factors that improve employee motivation
	• Understanding factors that decrease employee motivation
	• Designing job roles to support employee motivation and development
	• Employing a user-centric design for equipment and environment

4. Understand the link between human factors and security incidents	• Identifying human factors that increase the likelihood of incidents occurring • Expecting incidents and planning proactively • Reviewing incidents and the *"local rationality principle"*
5. Understand their role in supporting human performance	• Processes • Include human factor principles in training • Ensuring supervisors and managers understand their role





Endnotes

1 www.icao.int/Security/Security-Culture/Pages/default.aspx

2 Amalberti, R. (2001) The paradoxes of almost totally safe transportation systems. Safety Sci. 37(2-3): pp. 109-126 and Oliver, N. et al (2017) Cognition, Technology, and Organizational Limits, Organization Sci.28(4): pp. 729-743

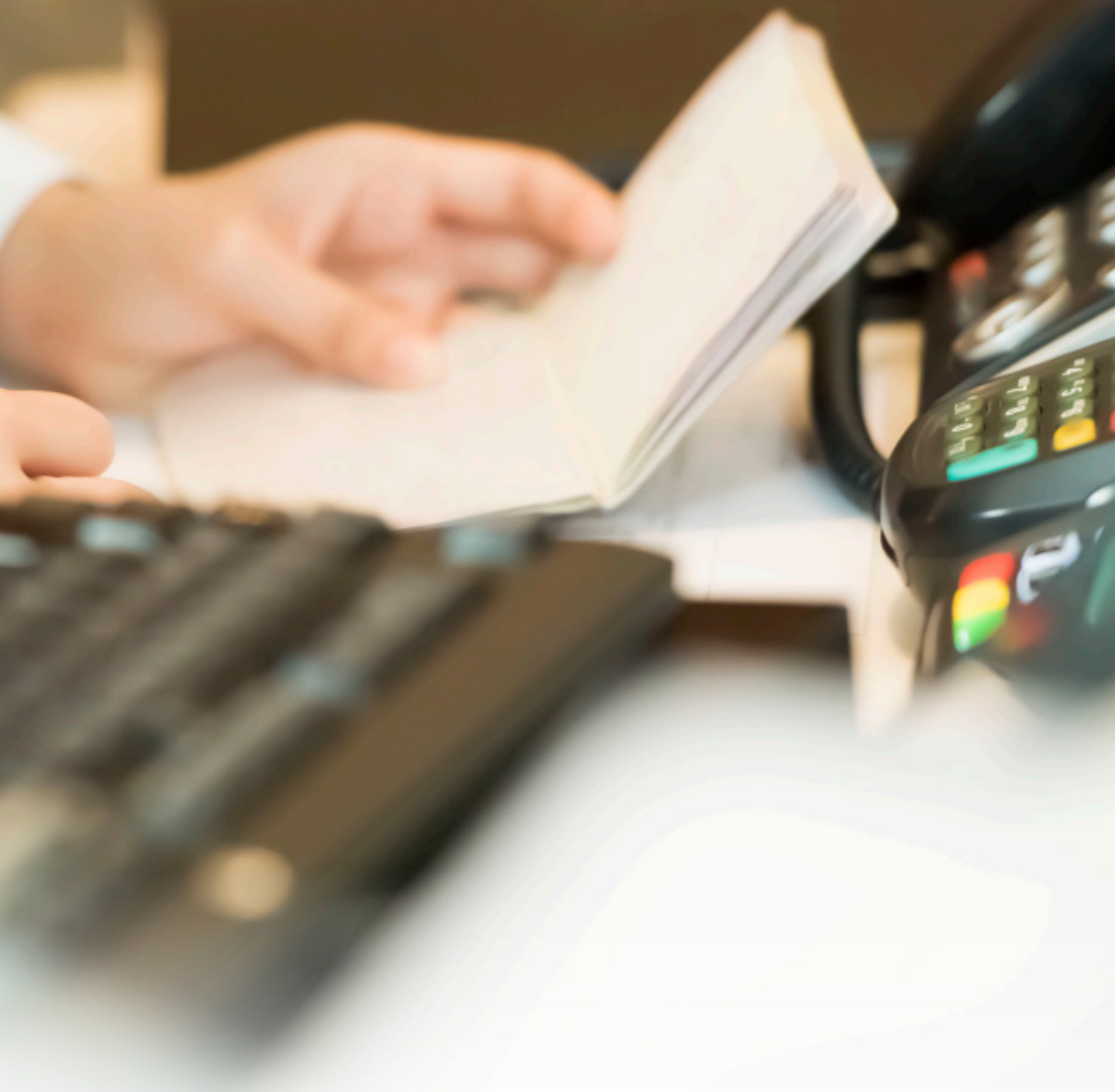
3 www.icao.int/safety/OPS/OPS-Normal/Pages/HPP.aspx

4 Local Rationality Principle: https://skybrary.aero/tutorials/principle-2-local-rationality

5 Motivation and performance definition: https://psycnet.apa.org/doiLanding?doi=10.1037%2Fh0037447

6 https://skybrary.aero/bookshelf/books/2037.pdf

7 The text is modelled on the WINS scale: https://www.wins.org/document/1-4-nuclear-security-culture/



ICAO

SECURITY AND FACILITATION

icao.int