ICAO

Security Culture
Discussion Cards

SECURITY IS EVERYONE'S RESPONSIBILITY

For more information: www.icao.int/Security/Security-Culture

What is Security Culture?

Security culture is a set of security-related norms, values, attitudes, and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel within the organization.

Effective security culture is about:

- Recognizing that effective security is critical to business success;
- Establishing an appreciation of positive security practices among employees;
- Aligning security with core business goals; and
- Articulating security as a core value rather than as an obligation or a burdensome expense.

Benefits?

The benefits of a strong and effective security culture include:

- Employees are engaged with, and take responsibility for, security issues;
- Levels of compliance with protective security measures increase;
- The risk of security incidents and breaches is reduced, given that employees are thinking and acting in more security-conscious ways;
- Employees are more likely to identify and report behaviours/activities of concern;
- Employees feel a greater sense of security; and
- Security is improved without the need for large expenditure.

Security Culture Components

There are several individual cards for each of the following ‘security culture components’. Each card introduces a different issue for reflection or discussion.

- Positive Work Environment
- Training
- Leadership
- Understanding the Threat
- Vigilance
- Reporting Systems
- Incident Response
- Information Security
- Measures of Effectiveness

How to use these cards

These cards are designed to help organizations initiate meaningful discussions about security culture with their staff. There are various methods in which the facilitator may use these cards to generate different discussions. The facilitator may wish to combine ideas from different methods or do one exercise following another.

Methods:

1. Pick a card
2. One from three
3. Reflect on experience
4. Compare views
5. Focus on
6. Asset-based security
7. World café
8. Influence map
9. Textual analysis
10. Solution-focus

Facilitator: If you are using the cards in a group, one person may need to act as a discussion facilitator. The facilitator should choose the method and plan the exercise, considering the advice on these cards.

How to use these cards

Background and purpose: Think carefully about the purpose of the session. Explain why the session is taking place, what is expected to be different as a result, and how this will happen. An exercise should be seen as relevant and meaningful to the participants.

Group size: Discussions tend to work better in small groups, e.g., 4 or 5 participants.

Group composition: Consider whether groups should be homogeneous (e.g., same occupations) or heterogeneous (e.g., different occupations). For heterogeneous groups, the cards chosen must provide common ground for discussion.

Card selection: When working with groups, it is wise to start with a very small number of cards per person. You may need to focus on specific cards for specific purposes or people (e.g., front line staff, managers). It can help to start longer workshops with more concrete security topics (e.g., Procedures and Training, Staffing and Equipment).

Note-taking: Paper charts or a writing board can help provide a visible record of the discussions.

Context of use

Small groups: Small group sessions are especially effective. Sessions can be focused specifically on card exercises, or card exercises can be used to break up meetings and presentations. Discussion groups should normally comprise 4-5 people.

Large groups: With large groups, each person will typically focus on one card, though this may be chosen from a small selection (e.g., 3). Simpler exercises are best suited to large groups.

Individually or in pairs: Some exercises are suitable for individuals and pairs. These can be more personal or complex/analytical.

Common spaces: Cards can be left in shared staff spaces, such as rest areas and cafeterias, as prompts for informal discussion on security.

Posters and websites: Cards can be printed as posters, or displayed on websites, perhaps with a means of making contact to share feedback and ideas concerning security culture.

Method 1: Pick a card

Purpose: Reflect openly on a security experience, situation, event or idea

This is the simplest of exercises. In a small group, each person takes just one card, or the whole group considers one card. The card may be selected:

- **Randomly from the whole pack;**
- **Randomly from a particular component (e.g., Leadership or Training); or**
- **Selectively based on a previous discussion or presentation.**

Each card may be discussed for a set time, e.g., 5-20 minutes. This exercise may focus on the present situation and past experiences (the first question on each card) or ideas for the future (the second question on each card), or both.

The exercise may be used as a standalone exercise or to introduce more interactivity in a meeting, e.g., to start a meeting, or in between or following presentations. The exercise can help to introduce new security perspectives about a situation or event, either wanted or unwanted.

Method 2: One from three

Purpose: Reflect on a security experience, openly or using question prompts

Give each person three cards, chosen randomly. Allow each person to choose one card and ask them to describe an experience that they have had concerning the general issue on the card (the explanatory text on each card). The story may be told freely, or you may wish to develop some question prompts, such as:

- **What happened?**
- **What did you think and feel about the experience at the time?**
- **How do you look back at the experience now?**
- **Have others had related or similar experiences?**
- **What can be learned from these stories?**

It is important that people feel safe to tell their story and talk about security without blame or adverse judgement (concerning the person telling the story, or those in the story) from others. There may therefore need to be some discussion and agreement about the use of feedback and language.

Method 3: Reflect on experience

Purpose: Reflect on a security experience using a framework

This exercise can be done alone or in groups of two or three. Choose a card from a small selection of cards or consider a security culture component that brings to mind an experience that has had a lasting impact. Answer the following questions.

1. **Observations** – What did I actually observe (described neutrally, as if viewing the event on film)?
2. **Reactions** – How did I react emotionally to what I observed? What feelings did I experience?
3. **Judgements** – What did I think about all of this? How did I evaluate what happened at the time?
4. **Interventions** – What did I do or not do? How did I intervene or not intervene to make something happen?

Following this, the person can go back through the cycle once again looking for alternative observations, reactions, judgements, and interventions that one could make. The person may then invite supportive questions or comments from others. The learning experience can help to re-frame past security experiences, open the mind to new ways of interpreting interactions, and take action based on the insights gained.

Method 4: Compare views

Purpose: Evaluate aspects of security culture and check agreements between groups

Have people arrange themselves into groups of around 3-4 people based on similarities OR differences between them (e.g., same or different occupational groups). Give each group the same selection of cards (around 8-16 cards) and ask them to sort each selection into two piles

Strengths	Weaknesses

...or four piles:

Strengths	Weaknesses
Opportunities	Threats

Then compare the piles and discuss:

- **Where did we agree, and why?**
- **Where did we disagree, and why?**

When done with existing groups (e.g., same profession), this exercise will tend to focus on how things work within the group. When done with mixed groups, this exercise will tend to focus on how things work between groups.

Method 5: Focus on...

Purpose: Evaluate a particular security culture component

Choose a specific component, or two components with a small number of cards, and take those cards for discussion. Discuss each card in depth with your colleagues. You may consider only security strengths and assets, or only weaknesses and deficits, or both. Each of these will elicit a different kind of discussion.

You may sort the cards and consider questions such as:

Strengths and assets

- What's going well? Where have we improved?
- What are some examples of this?
- What contributes to this going well?
- How might we defend and share this?

Weaknesses and deficits

- What is not going well? Where can we improve?
- What are some examples of this?
- What is stopping us from improving?
- How can we improve the situation? Has this been successfully addressed elsewhere?

Method 6: Asset-based security

Purpose: Improve security collaboratively, based on both what's strong and what's wrong

Have people arrange themselves into groups of around three people based on similarities OR differences (e.g., same or different occupational groups).

Choose a specific component, selection of cards, or card. For each component, selection, or card, answer the following questions in order:

1. What's going well concerning the issue(s)? **(Assets & Strengths)**

2. What is not going so well? What dilemmas, trade-offs or compromises do we have to make as a result? **(Deficits & Dilemmas)**

3. What do we want to happen? **(Wants)**

4. What are we prepared to offer to help make this happen? Or what would we be able to offer as a result of this happening? **(Offers)**

It is useful to split into small groups for some parts of the discussion (e.g., 1 & 2), then return to the larger group.

Method 7: World Café

Purpose: Use the cards to help host a large group to discuss security

The World Café method is a simple and flexible format for hosting large groups, split into smaller tables, ideally with refreshments and writing paper.

Arrange round tables in a room, with each table being suitable for 4 people (maximum 5). The space should be inviting and comfortable. Each table may have a dedicated 'host', who welcomes each group and takes brief notes. Preselect cards before the session, depending on the security focus. In some cases, all cards may be used, or just one component, or a smaller selection of 4 (or 5) cards.

Leave the cards on each table, which participants will take when they join a table. The cards on each table may be different (but related), or the same. Each participant then reads their card, answers the questions, and invites others to share their security perspectives.

In addition to open discussion, you may wish to add an overarching question, such as "What were the most interesting new security insights?" and "What did each group consider to be the best ideas to take forward for security improvement?"

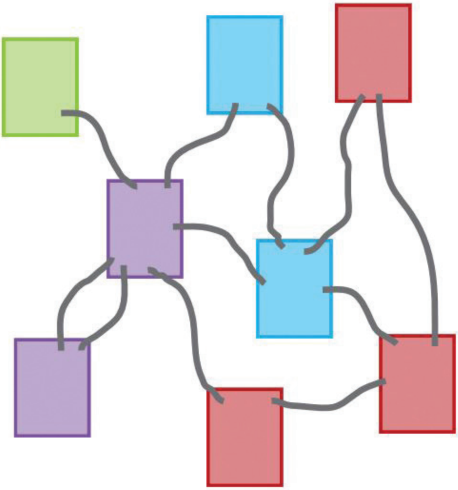
Method 8: Influence map

Purpose: Understand how security issues relate or interact

Organize cards into patterns to show how the security issues relate to one another for a specific event or situation, or more generally.

For instance, some cards may have a strong or obvious influence on one another, while others may influence each other in a more subtle way.

These influences can be indicated with arrows on large sheets of paper, or on cards or sticky notes. Discuss how these relationships work.



Method 9: Textual analysis

Purpose: Analyze text to help understand security culture issues

This method requires labelling text from security culture case studies. Read the text carefully and label areas of text using the nine security culture components, e.g. Training, Vigilance, Leadership.

You may need to apply more than one component to each piece of text.

Re-read the text and reference the appropriate heading(s) from the card(s) to each piece of text, e.g. trust, training requirements, communication.

Against each note, detail whether the text describes a positive or negative security culture indicator.

Once the exercise has been completed, participants should share their conclusions and discuss appropriate actions to mitigate identified negative security culture indicators. Further discussion should be held around positive indicators and their contribution in establishing a robust security culture.

This method may be used with 'Method 8: Influence Map', to map common associations between cards.

Method 10: Solution-focus

Purpose: Use the cards to help manage security problems and realize opportunities to improve security culture

This solution-focused exercise may be used with many of the previous exercises. It starts by prioritizing security issues (problems or opportunities), then looking at goals, before moving on to solutions, and how to implement them to help develop a positive security culture.

1. What are the security issues to work on?
Consider which issues might be relatively easy or especially motivating to implement.
2. What do we want? From a clear statement of what you want to happen - your security goal(s).
3. What are the possibilities for security improvement? Be open-minded and creative in considering possibilities.
4. Which of these possibilities might be most effective in meeting our goals? Some possibilities will have more potential than others, considering the nature of the security issue.
5. What needs to happen to realize the chosen solutions?
Consider the required support, incentives, people, environment, time, etc.
6. What do we need to do next? Agree the next step.

Security Culture

Discussion Cards

POSITIVE WORK ENVIRONMENT

For more information: www.icao.int/Security/Security-Culture

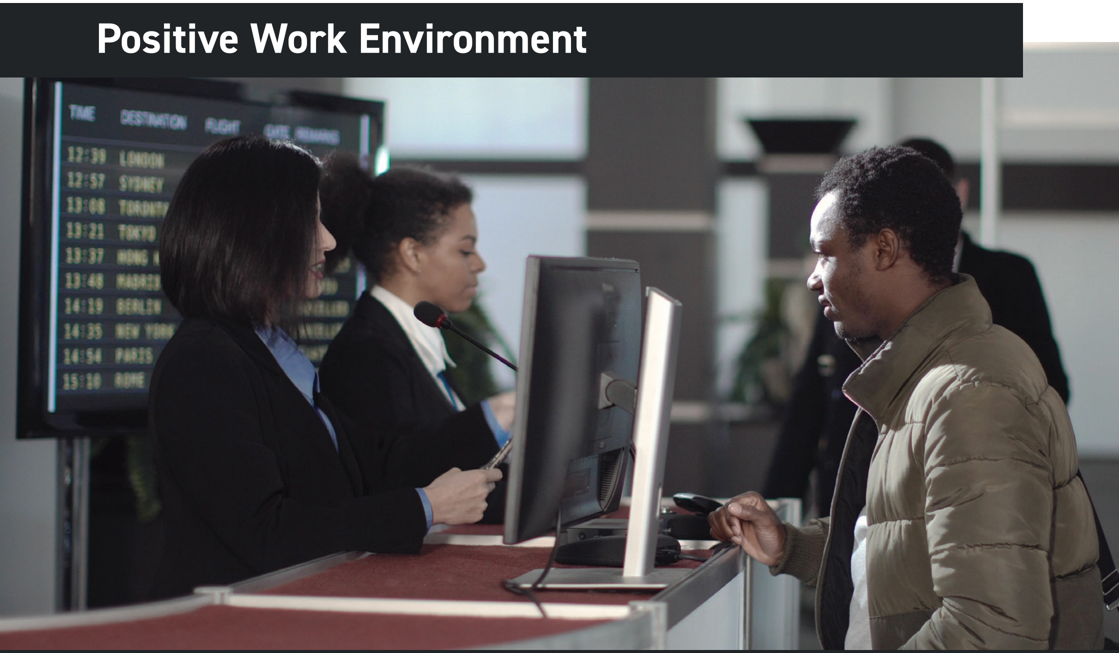
Status quo

Is security taken seriously in your organization?

Security must be at the heart of the business, as a core value and everyone’s responsibility.

Do staff know what is expected of them when it comes to security?

Positive Work Environment



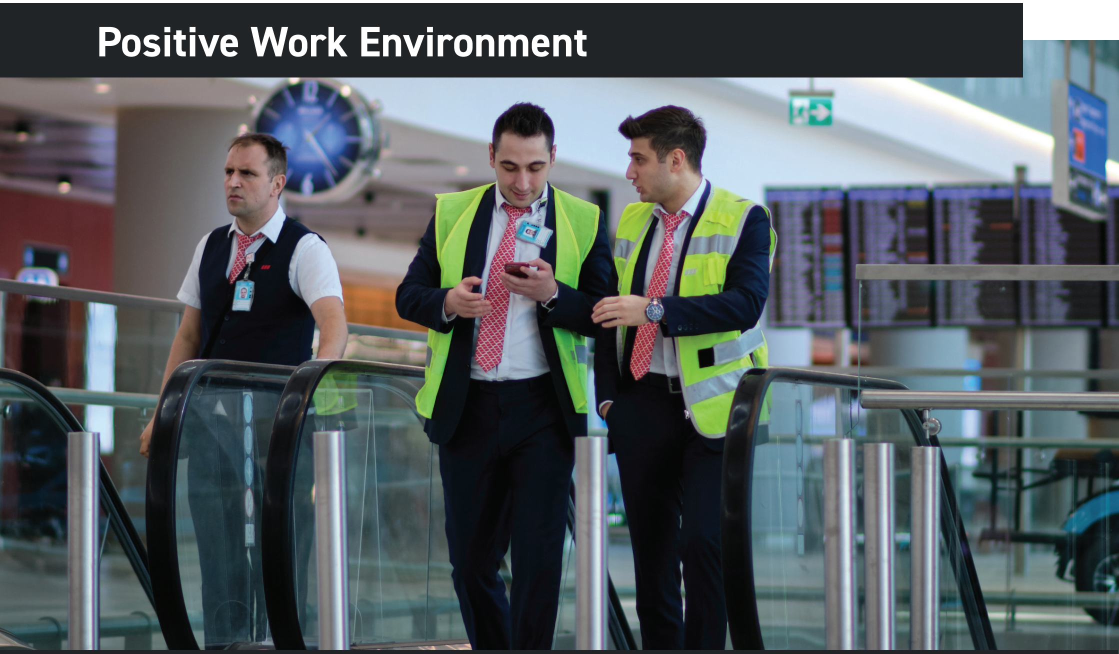
Communication

What messages are received from management about the importance of security?

Having the right context helps us understand why we are being asked to follow security procedures and protocols.

Do security messages reach all staff?

Positive Work Environment



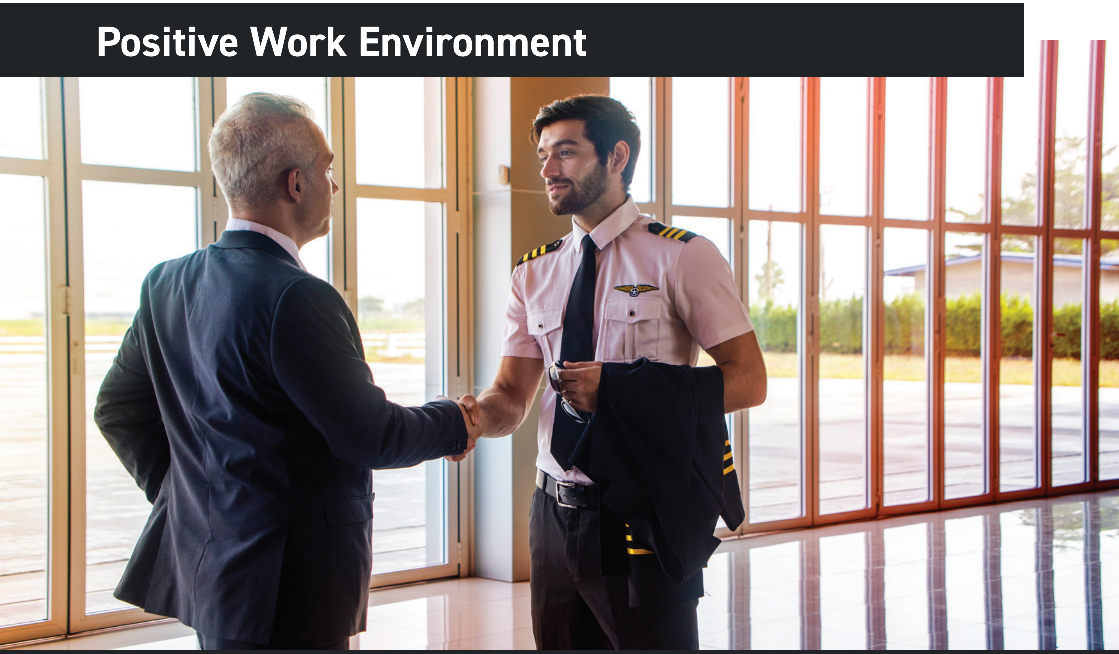
Trust

How much trust is there between staff, middle managers, and senior management with regard to security?

A work environment where all staff understand their security role and work together to create a positive work environment.

Would staff approach managers with security concerns?

Positive Work Environment



Security performance

Which aspects of security are getting better and worse in your organization?

Positive security culture enables a strong security performance.

Are there any easy wins to improve security?

Positive Work Environment

Doing the right thing

How is good security practice made easy for you in your organization?

If it is easy to follow security processes, it allows staff to display positive security behaviour and actions more easily.

What are the barriers to good security practice?

Positive Work Environment

Security Culture

Discussion Cards

TRAINING

For more information: www.icao.int/Security/Security-Culture

Training requirements

Do you have sufficient security training to understand and use the procedures relevant to your work?

Giving staff the right tools to support a positive security culture is important – this includes knowledge and skills.

Is security training in your organization sufficient?

Training

Refresh existing knowledge and skills

Do you have refresher training to help implement a positive security culture?

Skills and knowledge fade, even if exercised regularly – regular refresher training keeps them fresh and provides the opportunity to embed security knowledge.

How often should refresher training in security and for security culture take place?

Training

Management of change

Is adequate training provided when new security systems and procedures are introduced?

When new security systems and procedures are introduced, staff need to be trained to ensure they can effectively utilize the systems and new ways of working.

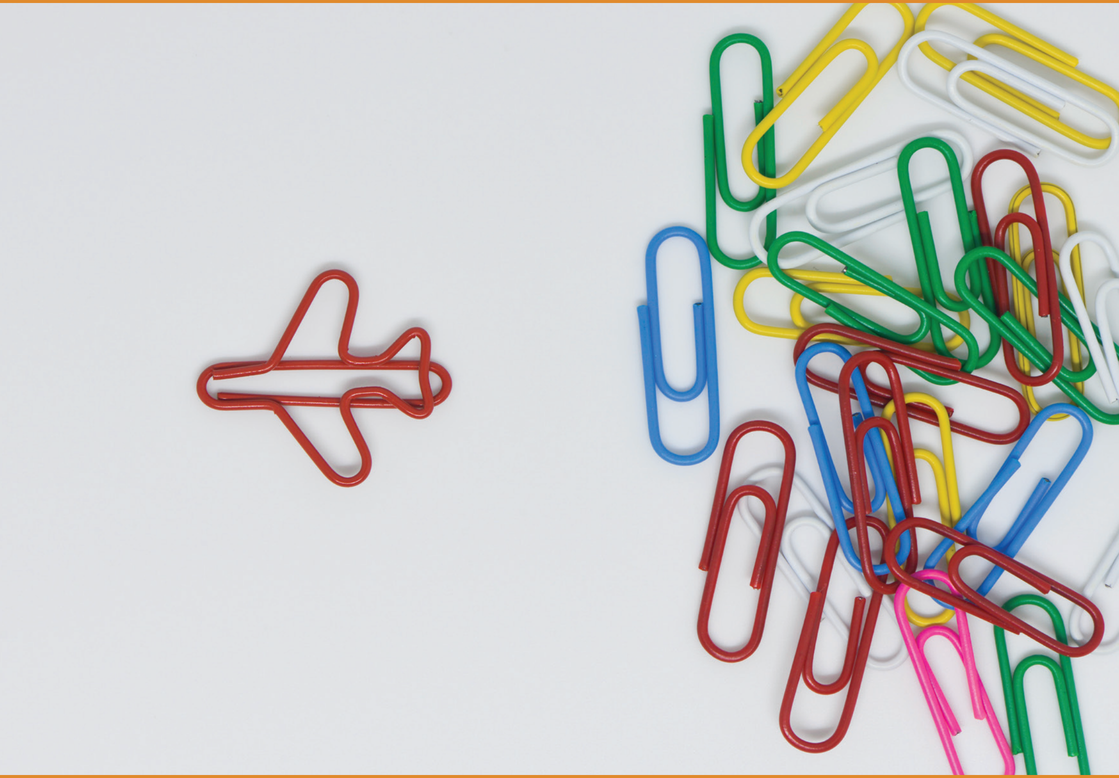
How can this security training be best facilitated?

Training

ICAO

Security Culture
Discussion Cards

LEADERSHIP



For more information: www.icao.int/Security/Security-Culture

Communication

How well do management and staff communicate about security?

Security should be a topic of regular discussion and communication to reinforce that security is everyone's responsibility.

Is security regularly discussed and is effective communication implemented?

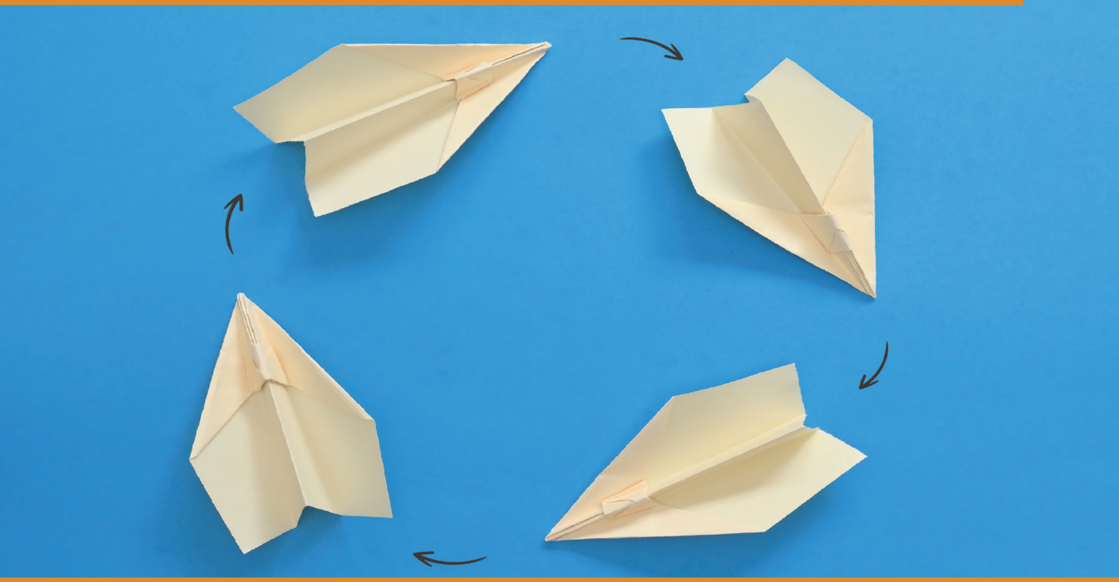
Responding to security concerns

How do managers and senior managers respond to concerns about security?

A positive security culture requires management to affirm direction and acknowledge all concerns raised.

What are the barriers to good security practice?

Leadership



Keeping in touch

Do managers have enough contact with staff?

This provides opportunity for staff to directly engage with managers and for managers to hear security feedback first-hand.

How can staff contact with management be facilitated?

Perception vs. Reality

How important is security for senior management?

To enable a positive security culture to be maintained, security must be a core value in the organization and have equal priority to other objectives, such as, safety and the passenger experience.

Is security a priority at all times in your organization?

Leadership

Leading by example

Are senior management in your organization setting a good security example?

‘Talking the talk and walking the walk’ – being seen to display positive security behaviours and actions is a powerful message from managers that security is everyone’s responsibility.

How can managers lead by example on security?

Leadership

ICAO

Security Culture

Discussion Cards

UNDERSTANDING THE THREAT

For more information: www.icao.int/Security/Security-Culture

Awareness of aviation threats and associated risks

Do you know the key threats that are relevant to your work?

Having an appreciation of the key risks we face better enables us to mitigate and manage them.

How best should threats to civil aviation and associated risks be communicated to you?

Understanding the Threat

Risk management

Do you understand how your role contributes to mitigating the threats facing civil aviation?

Without threat awareness, there will be a lack of desire to embed a positive security culture.

How can your role in protecting civil aviation be made real to you?

Understanding the Threat

Risk communications

Are you kept updated on threats that impact your organization?

Appropriate sharing of threat information contributes to staff understanding the important role they play in protecting civil aviation.

What opportunities exist to keep you better informed about security and aviation threats?

Understanding the Threat

ICAO

Security Culture

Discussion Cards

VIGILANCE

For more information: www.icao.int/Security/Security-Culture

Security awareness

Are current security awareness messages effective?

Having regular visual reminders of the key security messages helps embed the message in people's minds.

What security awareness messages can you recall?

Vigilance

Challenge

Do staff feel able to challenge those who do not comply with security processes?

Security is everyone's responsibility. Challenging those who do not abide by security rules and regulations should be second nature and encouraged.

What are the barriers to challenging colleagues about security?

Normal vs. unusual

Do staff pay attention to their surroundings and know what unusual and suspicious activity looks like?

Staff working regularly in the same areas know what security behaviours and actions are normal.

What type of incidents would you consider unusual or suspicious in your working environment?

Vigilance

ICAO

Security Culture
Discussion Cards

REPORTING SYSTEMS

For more information: www.icao.int/Security/Security-Culture

Focus on the issue

How are staff treated if they report an unintentional security breach?

Trust and fairness are key components of an effective reporting process. People will only report incidents if there is no fear of repercussions, especially if a security breach was due to an honest mistake.

How can we ensure the focus is on the contents of a security report, rather than on who reported it?

Speaking up

Do staff feel free to raise and report security concerns?

How we all react to security incidents can influence whether or not people feel safe to speak up.

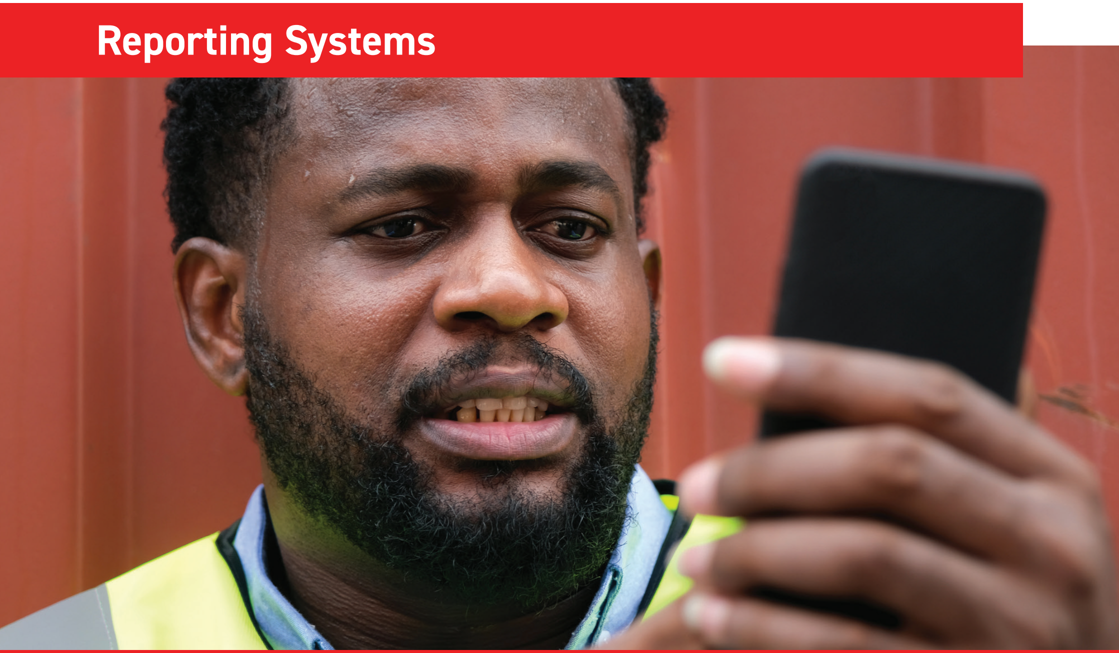
How can people be encouraged and supported to voice concerns about security?

Ease of reporting

How easy is it to report security breaches and unusual or suspicious activity?

Reporting security incidents should be easy. You should have access to appropriate resources and time to report concerns.

How can reporting be simple and easy enough for everyone to understand and do?



Feedback

Are staff satisfied with the feedback received when security concerns are raised?

Staff should be acknowledged and encouraged to raise security concerns and to report unusual or suspicious behaviour.

How and when should feedback be provided to those reporting security concerns?

Taking action

Does reporting security concerns improve security?

Reporting security concerns is a rich source of information. It allows security lessons to be learnt and improvements to be made.

How can we make sure that security reporting makes a visible difference, and so encourage people to report their concerns?

Reporting Systems

Security Culture

Discussion Cards

INCIDENT RESPONSE

For more information: www.icao.int/Security/Security-Culture

Know your role

Do you understand the role you play in responding to a security incident?

Everyone will have a role to play in the event of an incident. It is vital that staff know and accept their roles.

If an incident occurred today, how well prepared would you be?

Incident Response

Lessons learnt

Does your organization learn lessons from security incidents?

It is important organizations learn lessons and put in place measures to prevent similar or more serious incidents occurring in the future.

How well do you and your colleagues learn from incidents?

Be prepared

What does your organization do to prepare for a security incident before it occurs?

The opportunity to test and rehearse response procedures is important.

When was the last exercise or drill you participated in?

Security Culture
Discussion Cards

INFORMATION SECURITY

For more information: www.icao.int/Security/Security-Culture

ICAO

Know-how

What is your role in keeping sensitive security information secure?

You may have privileged access to documentation and data, along with a wealth of sensitive information in the form of knowledge.

In addition to protecting written documents and procedures, what other measures do we need to take?

Information Security

Your digital footprint

Are policies and procedures for the use of electronic resources clearly communicated and understood?

Cybersecurity is everyone's responsibility. Use electronic resources responsibly. Keep passwords and devices secure. Report cybersecurity concerns.

Have you received adequate training and do you have access to appropriate resources and systems to enable you to identify and report cybersecurity risks?

Information Security

Protecting our assets

Is sensitive information protected appropriately in your organization?

Sensitive security, safety and commercial information takes many forms and needs to be protected for a variety of reasons.

What training do you receive about the different forms of sensitive information?

Information Security

Security Culture
Discussion Cards

MEASURES OF EFFECTIVENESS

For more information: www.icao.int/Security/Security-Culture

Making a difference

Does your organization take steps to assess the impact of security culture initiatives?

As culture is dynamic and ever-changing, it is essential that organizations evaluate the effectiveness of their security culture efforts.

Is the measurement of security culture included in your quality assurance programme?

Measures of Effectiveness

Honesty

Do you feel able to provide honest feedback about security?

For organizations to know whether their security culture efforts are effective, they need your honest feedback.

What might prevent you from being completely open and honest about security?

Measures of Effectiveness

Performance monitoring

Do you have Key Performance Indicators (KPIs) for security in your organization? Are these indicators shared, tracked, and openly discussed?

Monitoring performance helps to establish security as a core business goal and increases its visibility and importance.

What KPIs for security are you aware of in you organization?

Measures of Effectiveness

Useful resources

- **ICAO Security Culture website**
  https://www.icao.int/Security/Security-Culture/Pages/default.aspx

- **ICAO Toolkit on Enhancing Security Culture**
  https://www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx

- **ICAO Security Culture Self Assessment Tool**
  https://www.icao.int/Security/Security-Culture/Pages/State-self-assessment.aspx

- **ICAO/CAAi Introduction to Security Culture Training Course**
  https://caainternational.com/course/introduction-security-culture/

Credits

The content and design of these discussion cards is based upon EUROCONTROL's 'Safety Culture Discussion Cards - Edition 2', with permission of the author, Steven Shorrock.

Languages

These cards are available in all ICAO languages. Please visit the ICAO website (www.icao.int) and search for 'security culture'.

ICAO Logo

Materials that display the ICAO logo should not be edited or customized, in whole or in part, in any form and by any organization without the prior written permission of ICAO.

Contact

If you have any questions about these resources, please contact ICAO's Implementation Support and Development – Security (ISD-SEC) team at isd@icao.int.