CIVIL AVIATION AUTHORITY
OF NEW ZEALAND
Te Mana Rererangi Tūmatanui o Aotearoa

Enhancing your organisation's security culture

SECURITY CULTURE GUIDANCE
FOR THE CIVIL AVIATION SECTOR

Contents

Foreword

A positive security culture underlies everything we do to keep aviation safe and secure.

New Zealand is dependent on aviation, much more so than many other countries – we're geographically remote and aviation enables strong connections to the rest of the world, within our islands, and supports our economic and social wellbeing. Internationally and domestically, aviation is a critical transport mode for trade, tourism and the transport of high value and critical products that must reach markets in a timely way.

We keep the aviation system safe for the public but also for people who work in it and use it, as well as keeping it protected (secure) from people who may wish to cause harm to it.

Security is everyone's responsibility. Working together and living the values of me mahi tahi – collaboration and me mahi tiki – integrity, we can build the layers needed to keep each aspect of the aviation system safe. I trust this guidance will be a useful resource for current and future managers and trainers in the aviation sector.

Thank you for your commitment and dedication to keeping people safe, and feeling safe when they fly.

Keith Manch
Chief Executive and Director
Civil Aviation Authority of New Zealand

Security culture guidance

This handbook is aimed at senior leadership, managers, security staff and trainers in the aviation sector.

It provides guidance, concepts and practical tools that can be adopted and implemented as part of internal security management and training, designed to help your organisation enhance security culture. It is also a useful reference guide for staff to consult to learn more about enhancing security culture in the aviation sector.

The advice in this document has been adapted from International **Civil Aviation Organisation's Toolkit on Enhancing Security Culture (www.icao.int)**.

This guidance has been developed as a modular resource to assist with designing initiatives to measure and improve the security culture of your organisation, and different aspects of this guide can be applied across your organisation to improve your overall security culture.

What is effective for you will depend on who you are, what you do, where you are located, the size of your organisation, your risk profile and your other strategic priorities and pressures. This guidance is flexible and scalable. It is intended to be the starting point for your journey of security culture enhancement and to help you understand different components of security culture, evaluate your current approach to security, and enhance security by using the practical tools within each component.

This guide covers the eight key components of security culture, shown below. They represent intervention points where positive influence and action can help to enhance your organisation's security culture.

What is security culture?

Security culture comprises the values, norms, beliefs, attitudes, and assumptions that are built into the daily operations of your organisation.

It is reflected in the actions and behaviours of all staff, personnel and stakeholders involved with your organisation. Security is everyone's responsibility—including high-level management and operational staff—and a positive security culture is built and reinforced across all levels of an organisation. When security is included as part of core business goals and values, everybody is clear on their role, and everybody benefits.

A positive security culture is about:

- recognising that effective security is critical to the success of your organisation or business and of the aviation sector
- building an open and honest organisation where security issues are openly shared, understood and solved
- establishing an appreciation of positive security practices among employees at all levels of your organisation
- articulating security as a core value of your organisation, rather than as an obligation or burdensome expense
- understanding that an effective security culture will contribute to the safety and security outcomes your organisation desires
- recognising that there is not a 'one-size-fits-all' way to create a good security culture: what is effective for your organisation will depend on what you do, where you are located, your organisational makeup, threats faced, and your risk profile.

Security culture goes beyond security awareness, and good security awareness does not automatically imply good security culture. Policies, procedures, and the environment created by an organisation that can enable an understanding of security at a deeper institutional level, results in positive and effective practice and outcomes.

A positive security culture means that security is in the DNA of your organisation and an integral part of everything people do.

Why do organisations need good security culture?

The aviation system depends on a layered approach to security.

These layers are designed to create multiple barriers to harmful acts that might target the aviation sector and the people within it (including staff and the public). All people in your organisation, regardless of their roles or responsibilities, play an important part in ensuring the different layers of security are effective in mitigating any threat to the system. Developing a robust security culture by embedding positive behaviours and mindsets in your people presents an additional protective layer in the wider security system, and an additional barrier to detect and prevent a potential act of harm.

A robust security culture is increasingly recognised internationally as a key pillar of aviation security and is necessary to build a strong and resilient aviation sector. Developing and sustaining an effective security culture is a vital part of achieving and sustaining positive security behaviours, that are integrated into organisational and management practice.

Benefits of enhancing your organisation's security culture

Enhancing and sustaining an effective and positive security culture is a vital aspect of your organisation's overall security regime and helps to protect against threats that could cause harm to people, infrastructure, and assets; and to reduce vulnerabilities in the wider aviation system. It's important to develop a security conscious workforce and promote the desired behaviours you want from staff.

Enhancing your security culture can help to:

- provide a cost effective, easily achievable, and effective layer of security protection
- encourage collective responsibility for security
- engage employees with, and encourage them to take responsibility for, security issues
- increase levels of compliance with regulatory security standards and recommended best practices
- reduce the risk of security incidents and breaches through an established practice of staff demonstrating a high level of security consciousness
- encourage employees to proactively identify risks and report behaviours or activities of concern
- enable employees to feel more secure in their workplace
- allow a company to present itself as a robust, safe and secure organisation to customers and other stakeholders.

The eight key components of security culture

1. Security leadership

Good security culture depends on an environment where managers and leaders—including those at the highest level—lead by example and support their staff to implement good security practice. Leaders should be actively involved in managing and implementing good security, understand the threat and risk picture, and work to continuously improve security practice across their organisation. Leaders should always act as role models by recognising and demonstrating that security in the aviation sector is critical to success.

Executive commitment and oversight

A robust security culture requires clear commitment, support and leadership from executive management ensuring security considerations are integrated into the organisation, and the appropriate level of priority, responsibilities and accountabilities are made clear.

Organisational commitment to a robust security culture includes producing a charter and governance structure for security responsibilities. Ensure it is clear how this structure supports the board and/or executive leadership to gain meaningful insights into information to inform their decision-making on key security issues.

The charter should:

- Incorporate security responsibilities and accountabilities into senior management position descriptions, to set a clear expectation that security plays a core role in each leaders' duties.
- Establish clear and measurable security targets for your organisation. Determine an appropriate way you can measure security performance within your operating context and track this over time to understand overall security behaviours.
- Ensure your organisation has a clear understanding of the relationship between financial targets and required security practices and outcomes.

Effective leadership communication on security

Strong communication from leadership is key to successfully building a strong security culture. Taking opportunities to promote messaging and highlight responsibilities through leadership engagement with staff, reinforces the importance of security matters as a management priority and sets clear expectations for staff to follow. Communication from leaders should be clear, concise, meaningful, timely and accurate.

Ways to communicate your security culture:

- Communicate clear messages on the threats and risks that security measures are designed to protect the aviation sector against, to achieve buy-in and ensure staff, managers and leaders have a good understanding of their threat/risk environment.

- Use organisational or sector publications, blogs, or articles to cover security updates relevant to all staff. Publicising the importance of security in your workplace signals to staff the role it plays in your organisation's conduct and culture.
- Raise awareness of security incidents and the lessons derived from them. Security breaches and incidents are invaluable learning opportunities. These should be shared across your organisation in a positive way so that all staff may learn from them and adjust their processes or procedures accordingly to close security vulnerabilities.

Be a role model

Managers and leaders are stewards of the security system and play a vital role in both influencing requirements and ensuring correct behaviours become habitual. Aviation sector leaders should always lead by example, be role models for security behaviours, and inspire positive security practice from staff through their own actions and attitude.

- Apply security equally to everyone, all the time. Senior managers should not be given exemptions from security measures, nor should they encourage workarounds or circumvent ordinary processes.
- Leaders should be seen to respect and champion security practice, and fully participate in required security activities. Do not cut corners to save time or money in developing security policies and procedures.

Support your staff to be security aware

Leaders have a special role in supporting staff to be security aware and enabling them to understand and appreciate the importance of security initiatives in aviation and sector environments. Security awareness may not come naturally to all individuals; often these requirements are supplementary to what are already busy and demanding jobs. This reality further increases the importance of leadership support in enhancing the security culture of your organisation.

Ways to support staff to develop their security culture:

- Allow staff the necessary time and resources to comply with security measures, especially when under pressure from business-as-usual work commitments.
- Show patience and understanding when reinforcing positive security behaviours. Staff come from a range of backgrounds, and all have different levels of appreciation of issues. Allow time and support staff to develop and grow their knowledge.
- Become actively involved in security awareness events and staff briefings. Taking the time to attend sends the message to staff that managers and leaders prioritise security and are supportive of ongoing security initiatives.

Acknowledge positive security behaviour

Proactively acknowledging positive security behaviours can be a highly effective means of fostering a culture where security is talked about, valued, and prioritised by staff in your organisation. Recognise when positive security behaviours are demonstrated, acknowledge any shortcomings, and incentivise good security practice across the whole organisation.

You can acknowledge staff by:

- Writing 'thank you' messages to acknowledge those who have performed effective security behaviours, including reporting suspicious activities or security breaches. Small gestures reinforce positive security behaviours and motivate staff to continually do the right thing.
- Recognising those who have performed security behaviours, in organisational newsletters or internal communications. This recognition is effective in highlighting what success looks like and becomes a model for others to follow.
- Considering employee rewards scheme to promote and reward positive security behaviours. These schemes are effective in tracking staff performance, incentivising positive actions, and demonstrating the importance of security to all staff in your organisation.
- Speaking openly about improvements that can be made to organisation security practices to make expectations clear for all staff.

Assess your security leadership - see Appendix 1 page 42

2. Positive work environment

A positive work environment that enables and drives a strong security culture helps to reinforce positive security behaviour, empowers staff to act consistently with security policies and procedures, and encourages them to demonstrate positive security behaviours confidently and willingly. Your work environment should make positive security behaviours easy, effective and an enabler of—not a hindrance to—daily tasks. Your security culture is only as positive as your work environment.

Clear and consistent policies, processes, and procedures

Security culture should be organised, systematic and embedded into the day-to-day activities of your organisation and its people. Security expectations should be written into corporate policy and procedures, including those without a primary security focus. This includes employee manuals, codes of conduct and standard operating procedures. Anywhere staff routinely consult organisational information is a potential vehicle for reinforcing key security messaging. In addition to being accessible, security information should always be easy to understand, concise, simple to follow and readily accessible to all staff – including new employees and those who need to refresh their understanding.

Ways to include security information:

- Include a security section in any document where staff read corporate information, even outside of your security exposition. This reinforces key messages and reminds staff that security is part of the fabric of your organisation and the aviation sector; not an optional extra.
- Consider operational or frontline staff without access to routine security updates and develop alternate and reliable ways to ensure they are receiving the information they need. This might mean delivering physical copies of communications or speaking to staff in person.
- Use plain language to communicate security messages. Make sure procedures are concise, easy to follow, are not open to interpretation and are not contradictory. Review documents to ensure they are complete, clear, and easy to grasp.
- Seek and incorporate feedback from staff to ensure that security instructions are complete and clear, and that there is no confusion or misunderstanding as to how security measures must be applied.

Provide the resources required to meet security goals

Achieving necessary security outcomes requires resources. This might be equipment, technology, time, space or personnel. A positive security culture is enhanced by your staff seeing investment being made in their work environment to enable strong security performance. Staff who are operating with inadequate resources, technology or equipment to effectively undertake their responsibilities may not feel supported by their workplace. Ensuring the appropriate resources are applied to security challenges is vital to ensuring your staff and the public remain safe and secure.

To ensure the correct resources are in place:

- Identify and prioritise the most important resources to achieve security outcomes in your organisation. These might be additional screening equipment, extra staff or updated computer systems or technology. It may also mean allowing a few extra minutes to implement security related measures.
- Seek feedback from operational staff on what can be done in your workplace to enable positive security behaviours, including consulting on what resources or tools they may need to do their jobs more effectively. There may be simple fixes that have positive impacts on achieving security goals and reducing vulnerabilities.

Display important security messaging in prominent places

Posting meaningful security messaging within physical and virtual work environments is an important way of reminding staff about key measures and embedding security into your organisation's culture. This highlights security as fundamental to the way you do business. Placing reminders of policies, procedures or advice in prominent places keeps security front and centre for your staff so that it becomes a core value in how they conduct their duties.

You might consider:

- Posting key security messages in high traffic locations such as in corridors or bathrooms. Regular reminders can embed good practice and remind staff of what to do during a security incident.
- Placing security communications in appropriate and relevant locations to the messages you are trying to get across. For instance, include a notice on a doorway that an Airport Identity Card needs to be displayed in a certain area, or to check that a secure door has closed before departing the area.
- Regular rotation of security messages on a notice board.
- How technology can help with displaying security reminders. This can include an electronic roster in a breakroom that staff look at every day, pop-up messages on computer systems, or changing system backgrounds/lock-screens to include relevant security messages.
- Using concise, relevant, and accurate language on security prompts, or using catchy phrases and slogans (such as 'See it, Hear it, Report it') to communicate key messages.
- As part of your security management, be aware of the security breaches or incidents that occur most frequently in your workplace. Target your security messages to improve performance in these areas, and then track what works best for your organisation.

Encourage staff engagement and measure staff performance

Engaged staff are more likely to promote strong security behaviours and embed security within the culture of your organisation. Staff who are involved in security decisions are more likely to champion and actively promote positive security behaviours. There are many ways to include staff in decision-making and encourage participation in security processes, raising overall performance, and entrenching security as part of the way all your staff do business. Measuring the performance of your staff against expected security behaviours can provide practical incentives to perform well, and track improvements in security practice and understanding.

Ways to encourage your staff:

- Set up a suggestion box to allow staff the opportunity to suggest ways in which security could be improved. Incentivise contributions by offering rewards for ideas that are implemented within the organisation, encouraging the natural thought-leaders in your organisation.
- Consult staff when security decisions might impact their work. They may have ideas that can benefit the whole organisation by providing improved security outcomes in more efficient or cost-effective ways.
- Document expected security behaviours within appraisals and performance development plans for all staff. This provides a measurable way to ensure staff are performing in line with requirements and expectations. Provide feedback on their security behaviours, including recognition for positive actions to incentivise repeat performance, and constructive feedback where security behaviours fall short.
- Promote positive security behaviour through a rewards and recognition programme and highlight organisational successes in corporate communications. Track organisational performance and provide concrete rewards to reflect measurable performance. This can encourage staff to strive to reach security goals and encourage security to be part of regular performance discussions. Recognition can be as simple as writing a 'thank you' message or email.

Assess your positive work environment – see Appendix 2 page 46

3. Security training

Staff who have the knowledge, skills and capability to practice good security are fundamental to developing and maintaining a positive security culture. The mindset, knowledge and behaviour of your staff can have a real impact on the risks and vulnerabilities of your organisation. This is driven by a strong, well-developed security education and training programme which needs to be a continuous process. Training should be present and prioritised at every stage of the employee lifecycle. Regular security training helps to ensure that strong security practices are part of the fabric of your organisation.

Effective induction training

Applying a strong security culture begins on day one. A new employee's induction is the perfect opportunity to introduce the desired security mindset of your organisation and embed strong security culture. Staff who join an organisation that highlights the importance of positive security behaviour are more likely to reinforce these behaviours as part of their ongoing routine. As new staff become more experienced, these behaviours will be passed down to subsequent new starters, where the cycle continues, enhancing the wider organisational security outcomes.

- Equip new staff with the knowledge, skills and abilities to practice good security from the beginning. Security education should be iterative, so staff are not overwhelmed; focus initially on security practices that new starters need to know immediately and grow their understanding over time.
- Give new employees the 'why'. New staff may have a limited understanding of why aviation security matters. A meaningful induction programme that defines why security is important to your organisation and to the aviation sector can help new staff to understand why they need to develop a security conscious mindset. This sets the foundation for more advanced lessons as your staff develop their security knowledge and understand the organisation's security goals. This buy-in requires the organisation to provide the solutions for new employees to embrace.
- Consider how to best communicate security messages to new staff. Set a journey of education over the lifecycle of staff and customise messages to the needs of different positions. Keep training materials engaging and interesting and encourage questions.

Regular refresher training

Regular refresher training provides an opportunity for staff to review and renew their knowledge of security matters, update their awareness of new policies and procedures, and to understand new and emerging threats and risks. Reinforcing key security messages and providing updates on best practice ensures staff remain regularly engaged with security matters. Refresher training means moving beyond basic compliance-orientated training; the objective is to motivate staff to proactively reach security objectives, rather than simply following the rules.

As part of your refresher training:

- Review what has changed recently in your organisational security policies, check if any new guidance applies, and make sure staff are updated in the latest developments.
- Provide briefings and training on evolving threats and risks to keep knowledge current across your organisation. Having current knowledge on global aviation security threats reinforces the importance of a strong security culture.
- Tailor refresher briefings to the role. General briefings on security procedures, aviation security threats, insider threats and suspicious behaviours that need to be reported are relevant to all your staff, so ensure this information is made widely available. Middle and senior managers may require more in-depth and detailed briefings to influence their decision-making.
- Keep refresher training new and interesting. Reference recent events domestically or overseas to highlight the importance of positive security behaviours. This can be even more effective if training draws from events within your own organisation.

Continuous learning

Complacency can creep in when security is not talked about, or when it seems far removed from employees who feel they may not have a role or responsibilities related to security. This can undermine the security culture of your organisation. Promoting security messages continuously throughout the year with awareness-raising activities that target all staff is an important means to reaching everyone and reinforcing key security messaging. This is especially important in New Zealand, where staff can feel far removed from security issues observed overseas.

Ways to support continuous learning:

- Designate a 'security week' once per year or a 'security day' once per month to encourage engagement with current security messages. This might include daily outreach, education sessions and guest speakers, and information campaigns.
- Encourage and support staff to attend external courses and training opportunities on security, even when this may not be their core function. Bring in guest speakers or specialist security staff to draw attention to a topic of interest. These steps can help to get staff talking about security and establish security training as a regular fixture on the calendar.
- Keep learning methods creative and interesting. Novel ways to understand security can be more effective at making the messages stick, especially when staff are engaged or involved in the learning process. For example, undertake 'red team' exercises whereby staff are invited to think like someone who would target the aviation sector through your organisation. This is an interesting and engaging way to identify vulnerabilities in your organisation that can be strengthened. You might also ask staff to think through how they might deal with the consequences of such an attack.

Targeted education plan

It is important that all security education is tailored to the audience that you are trying to reach. Targeting education demonstrates that you know the audience you are pursuing with your security training campaign, and ensures these messages are conveyed in the most relevant, efficient, and effective way for that audience. Communications should have clear and concise messages that can be easily understood by staff who may not encounter security issues on a day-to-day

basis. Likewise, specialist staff, or those with primary security responsibilities, should be provided additional information and guidance to enhance their ability to perform their security-related roles.

Target the right audience by:

- Considering the range of channels through which security communications can be delivered. Posters, flyers or leaflets can be left in break rooms, or emails or social media posts can be used to quickly share important messages to the right people.
- Communications plans should motivate staff to become engaged in security, not scare them into complying. Pitching information effectively and most importantly including the 'why' for all staff ensures understanding of why security is needed and encourage positive behaviours.
- Consider inviting experts or sector figures to endorse important security practices. External speakers can bring credibility and authority to education and communications strategies and can often draw greater interest from the whole team.

Assess your security training - see Appendix 3 page 50

4.

Understand your threat and risk environment

The aviation sector faces a complex set of threats. These threats are constantly evolving, becoming more sophisticated and are increasingly designed to undermine effective security measures implemented by the sector. At the same time, your organisation holds specific and often unique security risks, and potentially significant vulnerabilities.

It's important that all staff understand these threats and risks, the importance of security in their daily operations, and that they appreciate why they are required to do certain things in the name of security. Understanding what is at stake is at the heart of a good security culture: staff who understand are more likely to exhibit good security behaviours and achieve positive security outcomes for your organisation and the sector.

Understanding threat and risk

Threat describes a person or group with the intent and/or capability to undermine security protections, or exploit a vulnerability, to cause loss or harm.

Risk is the potential for loss or harm as a result of a threat exploiting a vulnerability. It considers the likelihood of the threat materialising, the consequences that could result, and any residual vulnerabilities or weaknesses in your organisation that could be exploited following the implementation of relevant security controls.

Understand your threat environment

Maintaining an up-to-date understanding of security threats is vital to ensuring the security measures applied remain appropriate. Senior managers and security personnel should be well versed on the threats present within the aviation system and should be able to speak about these to staff with credibility and explain clearly to employees the reason why security measures are so important in the aviation sector. Security culture is enhanced when staff feel comfortable that senior members of the organisation are aware of the threat environment and take appropriate measures in response, including interpreting these threats and communicating them across the organisation.

Gain understanding of the threat environment by:

- Developing systems and processes to increase your understanding of the current threat environment: maintain an awareness of overseas and domestic security events that impact the security of the aviation sector and how these may impact your threat locally; and ensure that the threat environment is regularly scanned and reviewed, and understood by executive leadership to enhance security decision-making.

- Considering subscriptions to commercial, sector, or government newsletters or alerts relating to aviation security matters, both domestically and internationally. This information will inform your understanding of developing threats to the sector and keep you updated on any emerging issues of concern that may require a response.
- Drawing on resources available within your organisation, or within wider sector groups, to identify experts with security knowledge to keep your knowledge current. These could be IT, HR, security personnel, or anyone else with security roles and responsibilities.

Understand your organisation's risk profile

Your organisation's individual risk profile is often highly specific to the type of work you conduct and where you are located. It is important to have a clear understanding of the unique features that may create security risks for your business, and how these can impact the security of the aviation sector. There should be a focus on risk identification and management, including an emphasis on the mitigation or treatment of risks, either to reduce the likelihood of a harmful event taking place, or to minimise the consequences should it transpire. Translating the threat environment into the tangible implications on the risks for your business is important for building security culture and practice: it helps to contextualise security for your specific circumstances and leads to the development of specific measures needed to keep staff and the aviation sector secure.

Understand and assess the risks for your organisation:

- Consider using standard risk assessment practice and methodologies, such as ISO 31000, to develop your own risk profile. Assessments of risks should be reviewed regularly to ensure they are still correct considering the overall threat environment.
- Make risk information available to operational staff so they understand the reasons why security measures are important, making them more likely to adhere to policies and procedures.
- Ensure senior leadership have a high level of familiarity with the security risks facing the organisation so that strategic decisions can be well-informed and appropriate resources can be allocated to security matters. An executive leadership team with a strong understanding of security risk is better equipped to ask the right questions and make good decisions relating to security matters, enhancing leaders' ability to influence security culture throughout the wider organisation.
- Consider vulnerabilities that are specific to your organisation when assessing risks. This might include staff, information your organisation handles, digital access maintained, swipe card access maintained, or equipment used. Ensuring security risks are specifically assessed for your organisation's profile and context is vital to making risks and identified vulnerabilities relevant to your staff.

Communicate threat and risk information to staff

Once senior members of the organisation have a clear understanding of the threat environment, and risks within the organisation, it is important to bring staff along on the journey, gaining buy-in and understanding of these threats and risks too. The aim is to encourage staff to adopt positive security behaviours not just because they are required to, but because they understand the reasons behind them. Threat and risk information should be clearly communicated to all staff, with clear messaging about exactly what your security measures are trying to protect. Staff who

become complacent about security or believe that they do not have a role in protecting aviation can be a negative influence on the overall security culture of your organisation. Their complacency may cause security lapses that leave the organisation and the aviation system vulnerable.
A baseline understanding of global aviation security threats, and how these are relevant to their roles, better informs staff as to how they can act to mitigate threats and close vulnerabilities.

Inform staff by:

- Delivering training specifically on security threats and risks in the aviation context. Regular specific briefings on security threats, risks and vulnerabilities are important to grow security knowledge and understanding as there is a constantly evolving nature of threats and risks in the aviation sector.
- Incorporating real-world examples in threat and risk communications where possible, including security incidents, vulnerabilities, attacks, failures, and successes (both locally and globally) to help staff grasp the reality of threats in their environment and the possible consequences when things go wrong.
- Engaging staff in the security risk assessment process as they are often, the best placed to understand their environment, where specific vulnerabilities exist, and what mitigations might be possible to lower residual security risk. Staff who input into the process are more likely to feel engaged, and exercise better security behaviours in the future.

Regularly review procedures in response to your environment

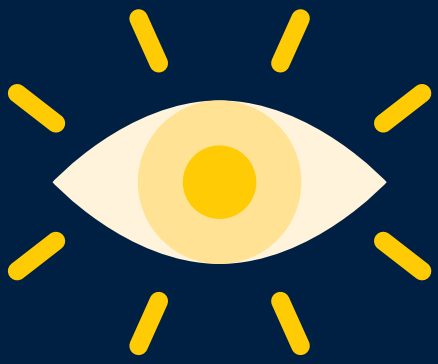
The security threat environment is constantly evolving; therefore, your risk environment is never fixed or static. Risk assessments and security procedures require continual review, adjustment, and revision to make sure they are fit for purpose in your current environment. Security processes and procedures should be flexible and responsive to changes in the external threat environment locally, nationally, and internationally. An elevation in security threats should see a review of internal processes to match. Likewise, any internal changes or specific risk information relevant to your organisation should be taken seriously, and new or adjusted mitigations applied to match. Proactive and relevant security procedures build good security culture by keeping security at the fore of your organisation's planning and operations, helping staff understand that security is an organisational priority, and part of the fabric of how business is done.

Test, review and improve your procedures regularly:

- Implement systems for threat and risk information to be used to influence security behaviours in a practical and effective way. Developing procedures in response to a changing environment demonstrates to staff that security is taken seriously, and that the measures they are required to implement are tied to a practical and systematic process.
- Run workshops to test whether your current security procedures stand up to a real-world threat scenario. Adjust processes or procedures that do not achieve the security outcomes desired.
- Develop methods to maintain awareness of emerging threats to your immediate security environment, and the aviation sector, and consider how your organisation may be vulnerable to any changes or emerging threats.

Assess your understanding of your threat and risk environment - see Appendix 4 page 54

5. Staff vigilance



Promoting staff vigilance highlights the importance that all members of your organisation play in keeping the aviation sector safe. Vigilance is about supporting your staff to be additional 'eyes and ears' of your organisation. A vigilant security culture, where staff are alert, aware and empowered to respond to security issues, reinforces the protective barrier that staff present, deters potential threat actors from undertaking harmful acts, increases chance of detection, and reinforces positive security behaviours in the workplace. Vigilant staff are better equipped to identify security issues, engage with those breaching security, and to report behaviours of concern. Vigilant staff pay attention to their surroundings and are supported by their organisation to advocate for good security practice.

Empower your staff

Staff need to feel empowered to be vigilant. Empowered staff understand their environment, the threats they face, and potential security risks in their workplace. Empowered staff are less likely to become complacent or consider that they have no role to play in security, but instead comprehend the complexity of the security environment beyond those risks that may be most obvious. Staff should also have knowledge of the security system as whole: knowing their role in the wider picture can help them contextualise their contributions and understand how they can help. Staff who are empowered and motivated are your organisation's greatest security asset.

Empower your staff by:

- Offering staff briefings or tours of the security aspects of your organisation. Introduce them to security staff to add to their overall understanding of the whole security system and show them in practice how they can help protect the aviation system.
- Using repeat messages, briefings, and reminders to educate staff on threats and risks. Staff who understand their environment, including the nature of the threats and risks they are trying to protect against, will be more energised to practice positive security behaviours.
- Encouraging staff to proactively advance positive security behaviours, including challenging those who are not complying with security policies and procedures in the right way. A workplace where staff feel equipped to respectfully speak out when they observe poor security practice demonstrates that good security is at the core of how work is done.

Staff are alert and aware

To demonstrate vigilance, staff need to be alert to their surroundings and aware of all the behaviours of concern that they are required to be on notice for. The presence of staff who appear alert to their surroundings is an effective deterrent to wrongdoing, and broad awareness of behaviours that are out of the ordinary will allow staff to recognise when something is not right.

A security culture where all your staff—not just those with security roles—are alert and aware, multiplies the number of people on the ground who can detect potential threats or risks.

Encourage awareness by:

- Conducting regular education sessions on what staff need to look out for in your context. This can include easy things to look out for, for example, people loitering near entrances to restricted areas, unattended bags, or inappropriate approaches, that need to be reported. Staff who are aware can develop a 'gut instinct' that something may be wrong. They should be encouraged to trust this instinct and report their concerns.
- Using posters and signage in prominent positions around your workplace to remind staff to remain alert and aware. Include contact details on posters so that staff or visitors know how to report their concerns.

Staff are equipped

Equip your staff with all the resources they need to be vigilant and to reinforce a positive security culture. Ensure they know who to approach if they have any questions or concerns with their responsibilities.

Ensure staff:

- Have a toolkit of resources they can draw on to enable their vigilance. This might include instructions on what to say or do when challenging suspicious security activities. A simple, polite question ('Can I help you?') is sometimes all staff need to do to detect potential security issues.
- Have phone numbers of key points of contact on hand to enable them to report and follow up quickly if they need to. This might mean programming key numbers into phones, placing a number readily available near a phone, or program a speed dial. Simple measures like this ensure staff are well equipped to act if needed.
- Are prepared in a way that is relevant to their role. Staff with specific security positions require clear guidelines on their roles and responsibilities, and your organisation's policies and procedures when responding to security issues.

Staff are supported

Vigilance should be endorsed from the top of your organisation and embedded as an expectation of staff and as part of your security culture. Organisational support for staff will help them to feel supported when they act or speak out when something is not right and will help staff know that they are acting consistently with organisational principles, even if they feel uncomfortable. Staff who are supported by the organisation to act with confidence when undertaking security responsibilities can strengthen the security culture of the whole organisation.

Support your staff:

- Written communications from senior managers are essential to connect staff to the organisation and remind them of the actions they can undertake to be secure and vigilant.
- Management should be seen to support initiatives that empower staff to be vigilant. This means following security policies themselves, and supporting staff when they follow organisational policies and procedures relating to security. Security must be seen by all staff to apply to everyone, at all levels of the organisation, including the executive.

- Staff should have clear guidance, policies, and procedures to refer to when making security related decisions. Knowing exactly what procedures to follow allows staff to act with the confidence they need and be assured that their actions will be supported by the organisation.

Assess your staff vigilance - see Appendix 5 page 58

6.

Reporting systems and incident response

Having robust reporting systems and procedures in place is an important part of exposing security threats and risks to the aviation sector, and a positive reporting culture is inseparable from a positive security culture. But the simple requirement for staff to report incidents of concern is not enough. The type of culture built around your reporting system is crucial to ensure that staff feel encouraged to make a report, are comfortable with how their report will be handled, and understand the role reporting plays in the improvement of security practices. This is all part of establishing a 'just culture', where staff are supported to report incidents, and understand that honest mistakes will be free from repercussions.

A 'just culture' approach to reporting

A reporting system is a fundamental aspect of your security culture. However, a reporting system that is punitive or retaliatory, will discourage reporting. This may lead to incidents that are covered up and gaps in the security system remaining unplugged. In a 'just culture' reporting environment, individuals are not blamed for honest mistakes and the root causes of an incident are investigated and corrected to prevent an incident from reoccurring. A 'just culture' focuses on learning from incidents through the sharing of information for the benefit of the entire security system. 'Just culture' requires a high level of trust and places the responsibility on senior managers to eliminate fear of punishment when things go wrong.

Implementing a just culture reporting approach:

- Publicise your 'just culture' principles. By making it clear to staff upfront that security reports will be handled in this way, you can establish the trust needed to facilitate effective reporting and eliminate fear that staff may be punished for reporting simple human error.
- Actively promote security reporting requirements and help staff know exactly what they need to report. Reporting requirements should be set as widely as possible to ensure nothing is missed and that staff have no doubts about whether they should be reporting a potentially significant issue.
- Make reporting easy and convenient. Staff at all levels of your organisation should have access to the systems or tools to make a security-related incident report. Consider offering a range of reporting methods to maximise the chance a report will be made, whether in person, by phone, email, or a purpose-made reporting form.
- Consider implementing a reporting education and awareness campaign for your organisation or region to regularly remind staff of their reporting responsibilities and the mechanisms (phone numbers, email addresses) through which they can make reports.
- Incorporate reporting of security breaches and incidents into your induction training, along with training on the functioning of a 'just culture' system, and the roles and responsibilities of all your staff in the reporting process.

Rewards, recognition, and feedback to encourage reporting

While a positive security culture should drive staff to report because it is the right thing to do, it is also important to recognise staff who have gone above and beyond, or whose reporting of a breach or incident has had a positive impact on the security of your organisation and the sector. Small gestures can go a long way to incentivise continued engagement and build positive security culture around this crucial activity. By acknowledging the efforts of staff when they come forward, you can help to reinforce the importance of reporting, and gain greater trust that reports will be handled with confidence and care. Feedback is also crucial. There is an inherent desire from those who report incidents or breaches to know that something has been done with the information provided. A formal feedback loop is an important aspect to encourage ongoing reporting, reassuring staff where possible that they have been listened to, and that action has been taken.

Encourage staff to report security issues or incidents:

- Implement a formal rewards programme with clear milestones and behaviour expectations linked to security reporting. Rewards do not have to be big, but small tokens to show staff their efforts are appreciated can grow the positive culture around reporting.
- Recognise staff who have played a key role in reporting a security incident or breach in organisation newsletters or other publications. By dedicating space in internal communications to reporting, you can highlight its importance as well as the value the organisation places on staff who make reports.
- Establish processes to formally provide feedback to those who have reported security concerns. Even if a follow-on investigation determined that nothing of concern occurred, it is important to feed this back to those who reported it, while communicating gratitude for them highlighting the issue. Where a report has led to a successful security outcome, share this feedback more widely so more staff understand their role to report security concerns and the impact it can have.

Clear and accessible response procedures

No matter the size of your organisation, response procedures are an important aspect of a security system. All staff need to be equipped and empowered to react in the event of a crisis. A crucial part of this is having clear processes and procedures that are accessible for all staff who might have a role in a security response. Response procedures might mean calling emergency services or another authority, and it is important staff are aware of this and know when and how they need to act. Responses should be considered in the short term and long term: immediate response procedures should be clear about what needs to happen to mitigate immediate issues or risks, whereas longer term processes should be used to reflect on a situation and learn valuable lessons for the future.

Have response procedures available:

- Create an aide-memoire or other convenient means for staff to quickly identify the steps they need to take in an emergency or when responding to a threat. This could take the form of a set of instructions placed on a lanyard or wallet card issued to each employee to allow for easy retrieval and action. This should contain any phone numbers staff may need to call in an emergency, and any other immediate response procedures relevant for your organisation.
- Review emergency responses to identify any lessons that could help improve procedures in the future. Consider what went wrong in a response to a security incident, and also focus on what

went well. Focusing on positive aspects of a response can help to incentivise strong security behaviours, and highlight that security is a positive thing for your organisation.

- Involve operational staff in any post-response reviews to feed their perspectives into an evaluation and assist them in improving their response next time.
- Understand the root cause of factors that led to a security breach, incident, or response to identify indicators or warnings that could assist you in anticipating an issue ahead of time in the future.

Contingency planning

Contingency planning is a crucial element of your overall response procedures. Planning should consist of coordinated strategies, procedures, and response initiatives to undertake during and following a security event. Contingency planning provides assurance to staff that plans are in place to respond to a range of emergency scenarios. This level of preparation will be reflected in the overall security culture of the organisation, and the behaviours that your staff adopt. Contingency plans make sure your organisation remains agile to evolving threats, and ready to respond when required.

When writing your contingency plans:

- Allocate responsibilities to senior staff to develop and implement effective contingency plans for your organisation. Ensure that these contingencies plans are communicated widely and effectively across all staff, so everyone understands their role.
- Focus contingency plans on a range of realistic scenarios based off your organisation's threat profile and risk assessments. Ensure the scenarios judged most likely to occur have comprehensive processes and procedures in place to keep personnel safe and secure.
- Conduct regular practical and tabletop exercises to review and stress-test your contingency plans. Testing plans as comprehensively as possible is important to make sure they can adequately hold up in a realistic setting. Involving staff in your exercises will test their ability to respond to a situation and provide practical experience that can enhance wider security understanding. Ensure staff understand you are testing your processes, not them personally.

Assess your reporting systems and incident response – see Appendix 6 page 62

7. Information security

A key part of a positive security culture is protecting information effectively to ensure vulnerabilities in the aviation security system cannot be identified and exploited. Your security system is only as strong as the protection of your information. Sensitive information should be stored, transmitted, and disposed of securely, and only shared with those who have a need to know. Information that is vital to the running of your organisation, and that may seem routine or innocuous, could provide a threat actor with critical information that could be misused to cause harm.

Cyber security induction training

Induction training should have a comprehensive cyber security component to ensure inexperienced staff understand how they are required to operate while using corporate systems or handling sensitive security information. New staff may not have a background that includes handling sensitive information, so consider what information your organisation handles that needs protecting and communicate this to new staff to ensure they understand how to keep this information safe.

Promote cyber security by:

- Standardising induction training for all new starters to your organisation to cover how information should be protected and shared. Training material should be set at a level that those without a strong background in information technology can understand and implement with ease.
- Offering refresher training on a regular basis to remind staff of key aspects of their cyber security responsibilities.
- Implementing a simple test or assessment to gauge staff understanding of cyber security requirements.
- Include specific information on the risks of information security breaches within education and training materials. This information helps to contextualise the reason for information security measures, and the risks should information get into the wrong hands.

Clearly documented policies and procedures

Information security should not be left to chance. Clear, cohesive, and effective policies and procedures are important to set a clear expectation of the information security management practices required of staff. Information security policies should contain relevant measures to help all staff keep your organisation's information safe and secure.

When creating your policies and procedures:

Think broadly about the information that should be protected within your organisation and prioritise security measures for the information most at risk, or most valuable. Information that needs security measures applied may not be immediately obvious. For instance, staff roster information could reveal gaps that could be exploited. Operational data may indicate gaps in security procedures that represent significant vulnerabilities for your organisation or the sector, that could enable a successful attack.

Clearly document policies and procedures relating to information security. These should include measures for electronic documents, but also control mechanisms for hard copy paperwork that may reveal security sensitive aspects of your organisation.

Ensure information security policies and procedures are accessible to all staff, and that these are written plainly and simply for staff with a lower understanding of the information security environment.

Regular information security messaging

Regular information security refresher training, and messaging, is important to embed sound practice within the security culture of an organisation. Information security measures can often be seen as a barrier to desired outcomes (e.g., sharing of information may be more difficult), which can lead to complacency and breaches over time. Information security can be more difficult to consider than traditional physical security threats. As a result, it is important to regularly remind staff of the need to keep information secure, and of the basic measures they can take to protect sensitive information.

Communicate information security messages:

- Conduct regular information security refresher campaigns to remind staff of their responsibilities. Consider a range of devices to communicate messages effectively: verbal briefings, email updates, posters placed in high traffic areas, or messages on your IT systems or intranet page.
- Tailor messaging to your environment, and at a level that your staff can understand. Include real-world examples of cyber security breaches and highlight the potential consequences a breach could have on the security of your organisation and the aviation sector.
- Quickly communicate any new or developing information security risks to staff and highlight any quick wins or key advice regularly to embed a high standard of practice.

Information security response plans

A timely response to a cyber incident is crucial to understanding its impact and minimising the damage caused. It is important to have response plans in place for staff to follow when things go wrong. The security culture of your organisation is enhanced when contingencies and responses are accounted for in any area, including cyber and information security. Staff should be aware of response plans and contingencies, including when these should be initiated and what their role is in any response.

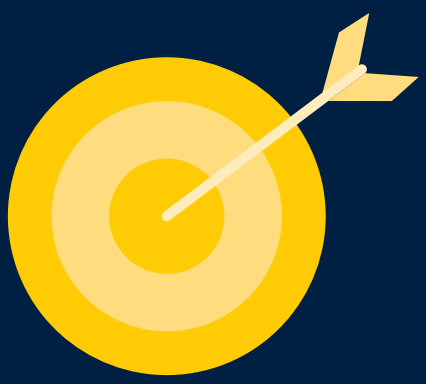
Ensure staff know their cyber response plans:

- Establish measures for all staff to remain aware of cyber incident response plans, and specifically their role in any follow up response.
- Test cyber security response plans on a regular basis to ensure measures meet the required standards in relation to the threat and your organisation's risk profile. Establish mechanisms to assess cyber security incidents and implement any recommended updates to your response plans.
- Establish means for staff to report suspicious activities, recognise poor cybersecurity practice or policy breaches, and to know when things they encounter might threaten your organisation's data.
- Consider creating aide-memoires to help staff recall the steps to take during an incident response.
- Institute a process for reporting and assessing risk from the loss or theft of organisational information (electronically, or through a misplaced/stolen laptop, phone, or documents).

Assess your information security - see Appendix 7 page 66

8.

Measure your effectiveness



Each component of your organisation's effort to improve its security culture requires constant monitoring and measurement to ensure that initiatives are effective and lead to continuous improvement. Understanding how your security culture is performing, how it is perceived by staff, where gaps or weaknesses exist, and where your areas of strength lie, can all provide valuable lessons on where to target practical measures to enhance your security system most efficiently and effectively. Measurement of your security culture can also help to identity risks and issues early and prevent them from escalating.

Undertake regular self-assessments

Self-assessments present an opportunity to take stock of your organisation's position and progress in developing your security culture by asking questions that reflect on the measures and initiatives against your established goals. Having a clear idea of your organisation's ideal end state is important to help contextualise your gains, direct efforts and identify areas of weakness for further work. Self-assessment provides the opportunity to evaluate your performance against objective indicators to ensure initiatives continue to have a positive impact.

Ways to assess your security culture:

- Use the questionnaires in the appendix, or other similar sector documents, to identify areas of strength for your organisation, and your key gaps. Your gaps are the areas that require the most improvement and should be targeted in the future to improve security culture.
- Continually reassess your progress by revisiting these questionnaires periodically to maintain current awareness of your organisation's progress and gaps.
- Conduct staff surveys, focus groups, interviews, and other organisational engagement activities to track your progress. Staff can provide an insight into the effectiveness of various initiatives and identify where organisational efforts may be failing or require additional work.

Internal audits, observations, and investigations

Formal processes that review your workplace's security performance in a 'real-world' setting are important ways to measure the success of security culture initiatives. These processes can offer a window into your organisation's day-to-day operations, staff conduct and performance, to help identify exactly how security behaviours are conducted in practice. It is important to be prepared to follow up audits, observations, or investigations with action, consistently with a 'just culture' approach, including by re-training staff or re-writing policies or procedures.

Review your security performance:

- Conduct targeted audits of specific elements of your organisation's security system to provide assurance and understanding of staff performance. Maintain a clear terms-of-reference to

guide your audit activity, monitor a sample of behaviour, and measure this against policies and security culture aims.

- Monitor the number of security breaches and infringements that occur within your organisation to determine if improvement measures are effective and reflected through an improvement in specific areas of concern. Undertake investigations when appropriate to determine and address the root cause of security issues.
- Observe security conduct as it occurs on a day-to-day basis within your organisation to help accurately appreciate security performance in real-time. It is important to understand real-world performance through hands-on experience to best appreciate where improvements to security culture can be made.

Review policies and procedures

Periodically reviewing organisational policies and procedures can provide insights into how your organisation's strategic documents match up with your ideal security culture end-state. Policies and procedures inform your organisational intent for action by staff. If these are not aligned to your ideal security culture, then adjustment and realignment may be needed to achieve target outcomes.

Review your policies and procedures:

- Review policies and procedures specifically considering the security culture outcomes your organisation is trying to reach. This can be an effective means of verifying whether other initiatives undertaken to improve security culture are potentially being undermined by historic or established organisational practice.
- Test policies and procedures with operational staff to determine if they are fit for purpose, making changes where necessary.
- Modify or re-draft policies and procedures that are not achieving adequate security performance. It is important to actively take positive steps to implement changes in response to any ineffective security outcomes, including by applying the lessons learned through self-assessment activities.

Use the data

The data collected through self-assessments, staff engagement, investigations, audits, and document reviews must be used effectively to be successful in influencing your organisation's security culture. Using the collected data, your organisation should assess the extent to which your current performance meets your desired security culture outcomes. This will identify where initiatives have been effective within your organisational context, or where further improvement is required.

Share the data:

- Consider the most effective way for your organisation to communicate progress in meeting your security culture performance goals. A series of dashboards indicating advancements in initiatives or security culture programmes, and overall security competency, can demonstrate to staff that their efforts are making a real difference. A strong understanding of progress can also clearly highlight specific areas where more work is needed.

- Allocate resources effectively in response to the lessons learned from your data collection. If your data highlights specific areas that need strengthening, then ensure initiatives are suitably targeted to address shortfalls.
- Actively implement the activities, initiatives or ideas from this guidance and other materials to enhance your security culture.
- Frequently re-evaluate your progress to ensure programmes and initiatives continue to have the right impact for your organisation. Re-evaluating your security culture will allow regular reviews of where efforts are directed and can help to detect emerging risk areas early.

Assess your measures of effectiveness - see Appendix 8 page 70

Appendices

Appendix 1
Assess your security leadership

Is security an organisational **priority** and **core value**?	○ Yes	○ No
Do employees believe that the organisation **takes security seriously**?	○ Yes	○ No
Do internal **policies and procedures** outline **what positive security culture looks like**?	○ Yes	○ No
Is the importance of security **led from the top**?	○ Yes	○ No
Are **security goals** and outcomes **clear** and **measurable**?	○ Yes	○ No
Is security culture **clearly defined** and **understood** within your organisational context?	○ Yes	○ No
Do leaders routinely **communicate** security messages?	○ Yes	○ No
Do managers **promote a positive security culture** by **endorsing security initiatives**?	○ Yes	○ No
Do managers **lead by example** and demonstrate **support** for security processes and procedures?	○ Yes	○ No
Does my organisation **support staff to learn security** effectively?	○ Yes	○ No
Does my organisation **recognise positive security behaviours**?	○ Yes	○ No

To enhance security leadership, my organisation can...

To assess your organisation, detach and fill the next page

Appendix 1
Assess your security leadership

Is security an organisational **priority** and **core value**?	Yes	No
Do employees believe that the organisation **takes security seriously**?	Yes	No
Do internal **policies and procedures** outline **what positive security culture looks like**?	Yes	No
Is the importance of security **led from the top**?	Yes	No
Are **security goals** and outcomes **clear** and **measurable**?	Yes	No
Is security culture **clearly defined** and **understood** within your organisational context?	Yes	No
Do leaders routinely **communicate** security messages?	Yes	No
Do managers **promote a positive security culture** by **endorsing security initiatives**?	Yes	No
Do managers **lead by example** and demonstrate **support** for security processes and procedures?	Yes	No
Does my organisation **support staff to learn security** effectively?	Yes	No
Does my organisation **recognise positive security behaviours**?	Yes	No

To enhance security leadership, my organisation can...

Date:

Appendix 1
Assess your security leadership

Is security an organisational **priority** and **core value**?	Yes	No
Do employees believe that the organisation **takes security seriously**?	Yes	No
Do internal **policies and procedures** outline **what positive security culture looks like**?	Yes	No
Is the importance of security **led from the top**?	Yes	No
Are **security goals** and outcomes **clear** and **measurable**?	Yes	No
Is security culture **clearly defined** and **understood** within your organisational context?	Yes	No
Do leaders routinely **communicate** security messages?	Yes	No
Do managers **promote a positive security culture** by **endorsing security initiatives**?	Yes	No
Do managers **lead by example** and demonstrate **support** for security processes and procedures?	Yes	No
Does my organisation **support staff to learn security** effectively?	Yes	No
Does my organisation **recognise positive security behaviours**?	Yes	No

To enhance security leadership, my organisation can...

Date:

Appendix 2
Assess your positive work environment

Does my organisation have clear **security policies and procedures** that are **accessible** to all staff?	○ Yes	○ No
Do employees **understand their security responsibilities** and how **these contribute** to the organisation's overall security?	○ Yes	○ No
Do employees have all the required **tools or equipment** to complete **security-related responsibilities**?	○ Yes	○ No
Do security messages in my organisation reach **all staff**?	○ Yes	○ No
Does my organisation display **security messaging prominently** in key locations?	○ Yes	○ No
Do staff have a means to **participate in the development** of security practices to **gain buy-in** to the organisation's security culture?	○ Yes	○ No
Is staff **performance measured** against their demonstrated security behaviour?	○ Yes	○ No
Does my organisation actively **recognise** positive security behaviours?	○ Yes	○ No

To enhance a positive work environment, my organisation can...

To assess your organisation, detach and fill the next page ›

Appendix 2
Assess your positive work environment

Does my organisation have clear **security policies and procedures** that are **accessible** to all staff?	Yes	No
Do employees **understand their security responsibilities** and how **these contribute** to the organisation's overall security?	Yes	No
Do employees have all the required **tools or equipment** to complete **security-related responsibilities**?	Yes	No
Do security messages in my organisation reach **all staff**?	Yes	No
Does my organisation display **security messaging prominently** in key locations?	Yes	No
Do staff have a means to **participate in the development** of security practices to **gain buy-in** to the organisation's security culture?	Yes	No
Is staff **performance measured** against their demonstrated security behaviour?	Yes	No
Does my organisation actively **recognise** positive security behaviours?	Yes	No

To enhance a positive work environment, my organisation can...

Date:

Appendix 2
Assess your positive work environment

Does my organisation have clear **security policies and procedures** that are **accessible** to all staff?	○ Yes	○ No
Do employees **understand their security responsibilities** and how **these contribute** to the organisation's overall security?	○ Yes	○ No
Do employees have all the required **tools or equipment** to complete **security-related responsibilities**?	○ Yes	○ No
Do security messages in my organisation reach **all staff**?	○ Yes	○ No
Does my organisation display **security messaging prominently** in key locations?	○ Yes	○ No
Do staff have a means to **participate in the development** of security practices to **gain buy-in** to the organisation's security culture?	○ Yes	○ No
Is staff **performance measured** against their demonstrated security behaviour?	○ Yes	○ No
Does my organisation actively **recognise** positive security behaviours?	○ Yes	○ No

To enhance a positive work environment, my organisation can...

Date:

Appendix 3
Assess your security training

Is security a core part of **induction training** for all new staff?	○ Yes	○ No
Is security training material tailored for those with a **limited understanding** of security in the aviation sector?	○ Yes	○ No
Do **training materials** contain a description of threats to aviation and relevant security processes?	○ Yes	○ No
Does **training material detail why** security matters and incorporate **processes** to build security culture?	○ Yes	○ No
Are the **elements** of a positive **security culture** built into all of your **training programmes**?	○ Yes	○ No
Is **security training** delivered in a range of ways to **keep staff interested** and engaged?	○ Yes	○ No
Is **refresher training available** for staff, and security resources accessible to reinforce key security messages?	○ Yes	○ No
Does your organisation encourage **regular security education opportunities and campaigns**?	○ Yes	○ No
Are a range of **communication** mechanisms used to **promote** positive security behaviours and **remind staff of their responsibilities**?	○ Yes	○ No
Are **specialist education and training** campaigns targeted at **different audiences**?	○ Yes	○ No

To enhance security training, my organisation can...

To assess your organisation, detach and fill the next page

Appendix 3
Assess your security training

Is security a core part of **induction training** for all new staff?	Yes	No
Is security training material tailored for those with a **limited understanding** of security in the aviation sector?	Yes	No
Do **training materials** contain a description of threats to aviation and relevant security processes?	Yes	No
Does **training material detail why** security matters and incorporate **processes** to build security culture?	Yes	No
Are the **elements** of a positive **security culture** built into all of your **training programmes**?	Yes	No
Is **security training** delivered in a range of ways to **keep staff interested** and engaged?	Yes	No
Is **refresher training available** for staff, and security resources accessible to reinforce key security messages?	Yes	No
Does your organisation encourage **regular security education opportunities and campaigns**?	Yes	No
Are a range of **communication** mechanisms used to **promote** positive security behaviours and **remind staff of their responsibilitie**s?	Yes	No
Are **specialist education and training** campaigns targeted at **different audiences**?	Yes	No

To enhance security training, my organisation can...

Date:

Appendix 3
Assess your security training

Is security a core part of **induction training** for all new staff?	Yes	No
Is security training material tailored for those with a **limited understanding** of security in the aviation sector?	Yes	No
Do **training materials** contain a description of threats to aviation and relevant security processes?	Yes	No
Does **training material detail why** security matters and incorporate **processes** to build security culture?	Yes	No
Are the **elements** of a positive **security culture** built into all of your **training programmes**?	Yes	No
Is **security training** delivered in a range of ways to **keep staff interested** and engaged?	Yes	No
Is **refresher training available** for staff, and security resources accessible to reinforce key security messages?	Yes	No
Does your organisation encourage **regular security education opportunities and campaigns**?	Yes	No
Are a range of **communication** mechanisms used to **promote** positive security behaviours and **remind staff of their responsibilitie**s?	Yes	No
Are **specialist education and training** campaigns targeted at **different audiences**?	Yes	No

To enhance security training, my organisation can...

Date:

Appendix 4
Assess your understanding of your threat and risk environment

Does my organisation have **processes and procedures** in place to ensure **awareness of developing threats** to aviation security?	◯ Yes	◯ No
Do **staff** have a clear **understanding** of the security threat environment?	◯ Yes	◯ No
Do **staff** understand the **specific vulnerabilities** within the organisation's risk profile?	◯ Yes	◯ No
Do **all employees** recognise their **roles in mitigating** these threats and risks?	◯ Yes	◯ No
Is **information** on the threat and risk environment **communicated regularly** to staff to provide them the purpose behind security measures employed?	◯ Yes	◯ No
Are **real-world examples** used in **education and training** to demonstrate real aviation security threats?	◯ Yes	◯ No
Are **staff involved in risk assessment** processes to benefit from their operational knowledge?	◯ Yes	◯ No
Are **processes and procedures actively reassessed** in light of changes in the threat or risk environment?	◯ Yes	◯ No
Are **processes and procedures routinely tested** to determine if they stand up to real-world threat scenarios?	◯ Yes	◯ No

To enhance understanding of the threat and risk environment, my organisation can...

To assess your organisation, detach and fill the next page

Appendix 4
Assess your understanding of your threat and risk environment

Does my organisation have **processes and procedures** in place to ensure **awareness of developing threats** to aviation security?	○ Yes	○ No
Do **staff** have a clear **understanding** of the security threat environment?	○ Yes	○ No
Do **staff** understand the **specific vulnerabilities** within the organisation's risk profile?	○ Yes	○ No
Do **all employees** recognise their **roles in mitigating** these threats and risks?	○ Yes	○ No
Is **information** on the threat and risk environment **communicated regularly** to staff to provide them the purpose behind security measures employed?	○ Yes	○ No
Are **real-world examples** used in **education and training** to demonstrate real aviation security threats?	○ Yes	○ No
Are **staff involved in risk assessment** processes to benefit from their operational knowledge?	○ Yes	○ No
Are **processes and procedures actively reassessed** in light of changes in the threat or risk environment?	○ Yes	○ No
Are **processes and procedures routinely tested** to determine if they stand up to real-world threat scenarios?	○ Yes	○ No

To enhance understanding of the threat and risk environment, my organisation can...

Date:

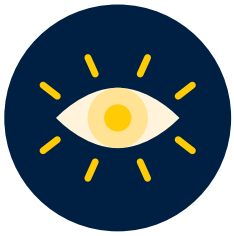
Appendix 4
Assess your understanding of your threat and risk environment

Does my organisation have **processes and procedures** in place to ensure **awareness of developing threats** to aviation security?	○ Yes	○ No
Do **staff** have a clear **understanding** of the security threat environment?	○ Yes	○ No
Do **staff** understand the **specific vulnerabilities** within the organisation's risk profile?	○ Yes	○ No
Do **all employees** recognise their **roles in mitigating** these threats and risks?	○ Yes	○ No
Is **information** on the threat and risk environment **communicated regularly** to staff to provide them the purpose behind security measures employed?	○ Yes	○ No
Are **real-world examples** used in **education and training** to demonstrate real aviation security threats?	○ Yes	○ No
Are **staff involved in risk assessment** processes to benefit from their operational knowledge?	○ Yes	○ No
Are **processes and procedures actively reassessed** in light of changes in the threat or risk environment?	○ Yes	○ No
Are **processes and procedures routinely tested** to determine if they stand up to real-world threat scenarios?	○ Yes	○ No

To enhance understanding of the threat and risk environment, my organisation can...

Date:

Appendix 5
Assess your staff vigilance

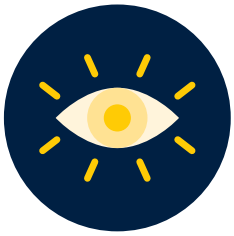


Do all staff, including those without specific security roles, **fully understand their powers and responsibilities** in relation to security?	◯ Yes	◯ No
Do all staff understand the **security infrastructure** of your organisation and where they fit in?	◯ Yes	◯ No
Are staff aware of **how to raise security-related issues or concerns**?	◯ Yes	◯ No
Do staff understand how to **identify suspicious behaviour**?	◯ Yes	◯ No
Are **visual learning devices** used to refresh staff on key security messaging?	◯ Yes	◯ No
Do staff have **access to resources and tools** to help them perform their security functions?	◯ Yes	◯ No
Do staff have all the **equipment** required to undertake security responsibilities, including phones, phone numbers and relevant processes and procedures?	◯ Yes	◯ No
Do staff receive **clear direction** from above on their security roles and responsibilities?	◯ Yes	◯ No
Are managers and leaders seen to **support** initiatives that **empower** staff to perform their security roles?	◯ Yes	◯ No
Does the organisation **support staff** to make decisions promoting positive security outcomes?	◯ Yes	◯ No

To enhance staff vigilance, my organisation can...

To assess your organisation, detach and fill the next page

Appendix 5
Assess your staff vigilance

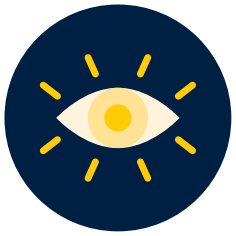


Do all staff, including those without specific security roles, **fully understand their powers and responsibilities** in relation to security?	○ Yes	○ No
Do all staff understand the **security infrastructure** of your organisation and where they fit in?	○ Yes	○ No
Are staff aware of **how to raise security-related issues or concerns**?	○ Yes	○ No
Do staff understand how to **identify suspicious behaviour**?	○ Yes	○ No
Are **visual learning devices** used to refresh staff on key security messaging?	○ Yes	○ No
Do staff have **access to resources and tools** to help them perform their security functions?	○ Yes	○ No
Do staff have all the **equipment** required to undertake security responsibilities, including phones, phone numbers and relevant processes and procedures?	○ Yes	○ No
Do staff receive **clear direction** from above on their security roles and responsibilities?	○ Yes	○ No
Are managers and leaders seen to **support** initiatives that **empower** staff to perform their security roles?	○ Yes	○ No
Does the organisation **support staff** to make decisions promoting positive security outcomes?	○ Yes	○ No

To enhance staff vigilance, my organisation can...

Date:

Appendix 5
Assess your staff vigilance



Do all staff, including those without specific security roles, **fully understand their powers and responsibilities** in relation to security?	○ Yes	○ No
Do all staff understand the **security infrastructure** of your organisation and where they fit in?	○ Yes	○ No
Are staff aware of **how to raise security-related issues or concerns**?	○ Yes	○ No
Do staff understand how to **identify suspicious behaviour**?	○ Yes	○ No
Are **visual learning devices** used to refresh staff on key security messaging?	○ Yes	○ No
Do staff have **access to resources and tools** to help them perform their security functions?	○ Yes	○ No
Do staff have all the **equipment** required to undertake security responsibilities, including phones, phone numbers and relevant processes and procedures?	○ Yes	○ No
Do staff receive **clear direction** from above on their security roles and responsibilities?	○ Yes	○ No
Are managers and leaders seen to **support** initiatives that **empower** staff to perform their security roles?	○ Yes	○ No
Does the organisation **support staff** to make decisions promoting positive security outcomes?	○ Yes	○ No

To enhance staff vigilance, my organisation can...

Date:

Appendix 6
Assess your reporting systems and incident response

Is **'just culture'** or a **'no-blame culture'** a fundamental value of your organisation?	◯ Yes	◯ No
Are **'just culture' principles publicised widely** within your organisation and **understood** by all staff?	◯ Yes	◯ No
Are **staff encouraged to report** security incidents, including anonymously?	◯ Yes	◯ No
Do **staff feel comfortable reporting** security breaches or infringements, even where they might have been **at fault**?	◯ Yes	◯ No
Does your organisation tie **reward and recognition programmes** to positive reporting behaviours?	◯ Yes	◯ No
Does your organisation **feed the outcomes** of security reports **back to staff**?	◯ Yes	◯ No
Do staff have **clear and accessible guidance** on how to respond to a security incident?	◯ Yes	◯ No
Are **response procedures** frequently reviewed for **relevance and suitability**?	◯ Yes	◯ No
Are **operational staff included** in reviews of incidents?	◯ Yes	◯ No
Are the **root causes** of security incidents or breaches **identified and remedied**?	◯ Yes	◯ No
Does your organisation have **contingency plans in place and accessible** to staff?	◯ Yes	◯ No
Are **staff involved** in contingency plan **exercises and reviews**?	◯ Yes	◯ No

To enhance reporting systems and incident response, my organisation can...

To assess your organisation, detach and fill the next page ›

Appendix 6
Assess your reporting systems and incident response

Is **'just culture'** or a **'no-blame culture'** a fundamental value of your organisation?	Yes	No
Are **'just culture' principles publicised widely** within your organisation and **understood** by all staff?	Yes	No
Are **staff encouraged to report** security incidents, including anonymously?	Yes	No
Do **staff feel comfortable reporting** security breaches or infringements, even where they might have been **at fault**?	Yes	No
Does your organisation tie **reward and recognition programmes** to positive reporting behaviours?	Yes	No
Does your organisation **feed the outcomes** of security reports **back to staff**?	Yes	No
Do staff have **clear and accessible guidance** on how to respond to a security incident?	Yes	No
Are **response procedures** frequently reviewed for **relevance and suitability**?	Yes	No
Are **operational staff included** in reviews of incidents?	Yes	No
Are the **root causes** of security incidents or breaches **identified and remedied**?	Yes	No
Does your organisation have **contingency plans in place and accessible** to staff?	Yes	No
Are **staff involved** in contingency plan **exercises and reviews**?	Yes	No

To enhance reporting systems and incident response, my organisation can...

Date:

Appendix 6
Assess your reporting systems and incident response

Is **'just culture'** or a **'no-blame culture'** a fundamental value of your organisation?	Yes	No
Are **'just culture' principles publicised widely** within your organisation and **understood** by all staff?	Yes	No
Are **staff encouraged to report** security incidents, including anonymously?	Yes	No
Do **staff feel comfortable reporting** security breaches or infringements, even where they might have been **at fault**?	Yes	No
Does your organisation tie **reward and recognition programmes** to positive reporting behaviours?	Yes	No
Does your organisation **feed the outcomes** of security reports **back to staff**?	Yes	No
Do staff have **clear and accessible guidance** on how to respond to a security incident?	Yes	No
Are **response procedures** frequently reviewed for **relevance and suitability**?	Yes	No
Are **operational staff included** in reviews of incidents?	Yes	No
Are the **root causes** of security incidents or breaches **identified and remedied**?	Yes	No
Does your organisation have **contingency plans in place and accessible** to staff?	Yes	No
Are **staff involved** in contingency plan **exercises and reviews**?	Yes	No

To enhance reporting systems and incident response, my organisation can...

Date:

Appendix 7
Assess your information security

Does my organisation provide **standardised information security training** for new staff?	◯ Yes	◯ No
How frequently do staff undertake **refresher training** on **information security**?	◯ Yes	◯ No
Are specific **information security risks** made clear to staff during **induction training**?	◯ Yes	◯ No
Are **information security policies** and procedures documented clearly and **accessible**?	◯ Yes	◯ No
Do **information security policies** recognise the **value of information** and the **risks of unauthorised access or disclosure**?	◯ Yes	◯ No
Are **key documents identified** that should be afforded the **greatest level of protection**?	◯ Yes	◯ No
Is **information security messaging routinely communicated** to all staff?	◯ Yes	◯ No
Does my organisation have a comprehensive **information security incident response plan**?	◯ Yes	◯ No
Does my organisation **routinely test** its information security **incident response plan**?	◯ Yes	◯ No
Are **reporting procedures** relating to **suspicious cyber issues** clear and accessible?	◯ Yes	◯ No

To enhance information security, my organisation can...

To assess your organisation, detach and fill the next page ›

Appendix 7
Assess your information security

Does my organisation provide **standardised information security training** for new staff?	Yes	No
How frequently do staff undertake **refresher training** on **information security**?	Yes	No
Are specific **information security risks** made clear to staff during **induction training**?	Yes	No
Are **information security policies** and procedures documented clearly and **accessible**?	Yes	No
Do **information security policies** recognise the **value of information** and the **risks of unauthorised access or disclosure**?	Yes	No
Are **key documents identified** that should be afforded the **greatest level of protection**?	Yes	No
Is **information security messaging routinely communicated** to all staff?	Yes	No
Does my organisation have a comprehensive **information security incident response plan**?	Yes	No
Does my organisation **routinely test** its information security **incident response plan**?	Yes	No
Are **reporting procedures** relating to **suspicious cyber issues** clear and accessible?	Yes	No

To enhance information security, my organisation can...

Date:

Appendix 7
Assess your information security

Does my organisation provide **standardised information security training** for new staff?	Yes	No
How frequently do staff undertake **refresher training** on **information security**?	Yes	No
Are specific **information security risks** made clear to staff during **induction training**?	Yes	No
Are **information security policies** and procedures documented clearly and **accessible**?	Yes	No
Do **information security policies** recognise the **value of information** and the **risks of unauthorised access or disclosure**?	Yes	No
Are **key documents identified** that should be afforded the **greatest level of protection**?	Yes	No
Is **information security messaging routinely communicated** to all staff?	Yes	No
Does my organisation have a comprehensive **information security incident response plan**?	Yes	No
Does my organisation **routinely test** its information security **incident response plan**?	Yes	No
Are **reporting procedures** relating to **suspicious cyber issues** clear and accessible?	Yes	No

To enhance information security, my organisation can...

Date:

Appendix 8
Assess your measures of effectiveness

Does my organisation undertake **self-assessments to understand its security culture** and performance?	◯ Yes	◯ No
Does my organisation conduct **staff surveys, focus groups** or other engagement with staff to **understand security culture** and performance?	◯ Yes	◯ No
Are **audits and investigations** conducted to **observe security performance** in a real-world setting?	◯ Yes	◯ No
Are **metrics collected and analysed** to determine how performance is tracking and determine the **root cause of developing issues**?	◯ Yes	◯ No
Do **policies and procedures** reflect your **ideal security culture** and performance end-state?	◯ Yes	◯ No
Do **operational staff** have an opportunity to **contribute to policy and procedure** development?	◯ Yes	◯ No
Are **policies and procedures measured** for their effectiveness, and **amended** when needed?	◯ Yes	◯ No
Does your organisation **value the information it collects** and use it effectively?	◯ Yes	◯ No
Are **resources effectively reallocated** in response to **lessons learned**?	◯ Yes	◯ No
Does my organisation **prioritise implementing measures to understand and enhance security culture**?	◯ Yes	◯ No

To enhance measures of effectiveness, my organisation can...

To assess your organisation, detach and fill the next page

Appendix 8
Assess your measures of effectiveness

Does my organisation undertake **self-assessments to understand its security culture** and performance?	○ Yes	○ No
Does my organisation conduct **staff surveys, focus groups** or other engagement with staff to **understand security culture** and performance?	○ Yes	○ No
Are **audits and investigations** conducted to **observe security performance** in a real-world setting?	○ Yes	○ No
Are **metrics collected and analysed** to determine how performance is tracking and determine the **root cause of developing issues**?	○ Yes	○ No
Do **policies and procedures** reflect your **ideal security culture** and performance end-state?	○ Yes	○ No
Do **operational staff** have an opportunity to **contribute to policy and procedure** development?	○ Yes	○ No
Are **policies and procedures measured** for their effectiveness, and **amended** when needed?	○ Yes	○ No
Does your organisation **value the information it collects** and use it effectively?	○ Yes	○ No
Are **resources effectively reallocated** in response to **lessons learned**?	○ Yes	○ No
Does my organisation **prioritise implementing measures to understand and enhance security culture**?	○ Yes	○ No

To enhance measures of effectiveness, my organisation can...

Date:

Appendix 8
Assess your measures of effectiveness

Does my organisation undertake **self-assessments to understand its security culture** and performance?	Yes	No
Does my organisation conduct **staff surveys, focus groups** or other engagement with staff to **understand security culture** and performance?	Yes	No
Are **audits and investigations** conducted to **observe security performance** in a real-world setting?	Yes	No
Are **metrics collected and analysed** to determine how performance is tracking and determine the **root cause of developing issues**?	Yes	No
Do **policies and procedures** reflect your **ideal security culture** and performance end-state?	Yes	No
Do **operational staff** have an opportunity to **contribute to policy and procedure** development?	Yes	No
Are **policies and procedures measured** for their effectiveness, and **amended** when needed?	Yes	No
Does your organisation **value the information it collects** and use it effectively?	Yes	No
Are **resources effectively reallocated** in response to **lessons learned**?	Yes	No
Does my organisation **prioritise implementing measures to understand and enhance security culture**?	Yes	No

To enhance measures of effectiveness, my organisation can...

Date:

Further reading

Civil Aviation Authority of New Zealand Security Culture
(www.aviation.govt.nz/safety/security-culture/)

International Civil Aviation Organisation Year of Security Culture 2021
(www.icao.int/Security/Security-Culture/Pages/YOSC-2021.aspx)

International Civil Aviation Organisation Toolkit on Enhancing Security Culture
(www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx)

Civil Aviation Act 1990
(www.legislation.govt.nz/act/public/1990/0098/latest/whole.html)

Aviation Crimes Act 1972
(www.legislation.govt.nz/act/public/1972/0137/latest/whole.html)

Just Culture – what it means to the CAA
(www.aviation.govt.nz/about-us/what-we-do/operational-policies/just-culture-what-it-means-to-the-caa/)

CAA Advisory Circular AC100-1 Safety Management
(www.aviation.govt.nz/assets/rules/advisory-circulars/AC100-1.pdf)

NZ Government Protective Security Requirements
(www.protectivesecurity.govt.nz/)

Countering Violent Extremism and Terrorism - New Zealand Security Intelligence Service
(www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/)

New Zealand's Security Threat Environment 2023 - New Zealand Security Intelligence Service
(www.nzsis.govt.nz/assets/NZSIS-Documents/New-Zealands-Security-Threat-Environment-2023.pdf)

Disclaimer

The material in this guidance is to be regarded as a general information resource and is not intended to address the exact circumstances of any specific person or organisation. All reasonable measures have been taken to ensure the accuracy of the material contained in this guidance, however the CAA accepts no liability for any direct or indirect loss or damage of any kind arising from use of material in this document. The material should not be regarded as legal advice. The CAA may change the material within this guidance without notice.

Comments or queries?

Please contact: security.regulation@caa.govt.nz

CIVIL AVIATION AUTHORITY
OF NEW ZEALAND
Te Mana Rererangi Tūmatanui o Aotearoa

Version 1.0 December 2023