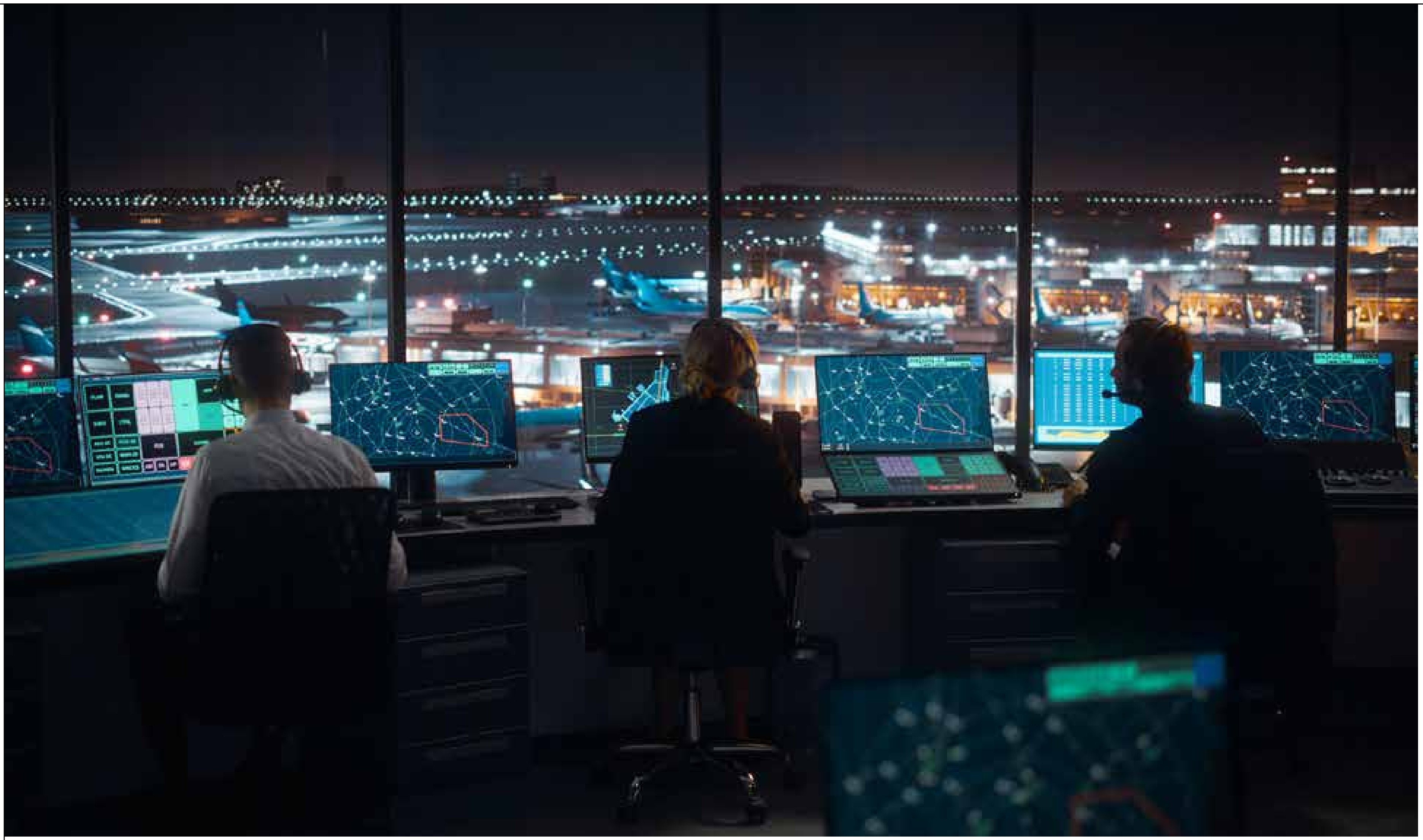

Picture credit: iStock

ATTAINING THE STANDARD

Phil Robinson *explores what's required under the ASSURE scheme and how airports can get the most out of the process*

Cybersecurity is a pressing issue in the aviation sector. During 2020, 62 percent of airports were subjected to attack, according to a report by the Airports Council International (ACI), with warnings that the sector can expect to see more organised and potentially state-sponsored sustained attacks in the future. To help improve cyber security posture, the ASSURE scheme was launched in January 2020. The scheme accredits third-party cybersecurity audit companies to audit, assess and improve the cyber defences of airports, air carriers, air navigation providers and other organisations in the commercial aviation sector.

There is often a gap when it comes to understanding cyber exposure and risk

The ASSURE audit falls under CAP 1753 otherwise known as the Cyber Security Oversight Process for Aviation and is just one part of a six-step process. This begins with engagement before moving on to critical systems scoping, cyber self-assessment, the ASSURE cyber audit, the provisional statement of assurance and the final statement of assurance and certificate of compliance. Underpinning the process are four key objectives – managing security risk, protecting against cyber attack, detecting cyber security events and minimising the impact of cyber security incidents – which form the basis of the assessment.

ASSURE confers a number of advantages. To start with, it's carried out by cyber professionals that need to go through a stringent accreditation process by either the IASME or CREST industry body. These professionals must specialise in at least one of three key areas – cyber audit and risk management, technical cyber security or Industrial Control Systems (ICS)/Operational Technology – meaning the organisation stands to benefit from the critical eye of someone who lives and breathes security and is up to speed on the latest threats.

The process will also be the first time many airports have taken a holistic approach to their cybersecurity as it addresses IT, OT and Process Control Networks. As a result, the assessment encompasses parts of the organisation that were previously siloed and leads them to have security conversations with one another, enabling residual gaps to be identified. This unprecedented level of oversight promises to significantly reduce the risk of security breaches and maintain continued availability of critical tech and key safety controls.

We have found there is often a gap when it comes to understanding cyber exposure and risk. While some have a good understanding and mature processes in place around governance and risk, as well as good technical knowledge, others – especially the smaller aviation operators who have maybe outsourced their IT and rely upon some select cloud applications – don't have a great understanding of the requirement for robust and mature security controls. By enabling them to review their systems, the process highlights these gaps and the associated risks involved.

But for all its advantages, ASSURE has been a far from easy ask for airports. Still reeling from the pandemic, many are extremely cost sensitive right now and are still coaxing back staff into the workplace, so resources are thin on the ground. This has made it very difficult to devote the time and manpower needed to carry out the lengthy self-assessment process which requires teams to produce a variety of evidence constituting not just documents and manuals, but interviews with key personnel. Small wonder, then, that many have sought an extension to submitting their audit reports, as compliance was initially mandated for year-end 2021.

Moreover, as the scheme borrows heavily from established standards (the Cyber Assessment Framework for Aviation is based on a similar framework from the National Cyber Security Centre) it's not always tailored to the needs of the sector. A good example here is legacy radar systems, which aren't internet-enabled but must nonetheless complete this section. The complexity of the supply chain is another. Many organisations have outsourced the maintenance and/or operation of their systems to either the equipment supplier or a third party, so do not have any oversight of whether the requirements of the CAF process are being met.

Let's say, for example, an airport outsources the hold baggage checking to a third party, which provides staff for monitoring the baggage screening and is responsible for the staff training to an acceptable standard. For that training they use a web-based package supplied to them by a fourth party. The third party may also source maintenance support for the hardware from a couple of vendors (one for the baggage belts and one for the scanning machines). All of these systems and training are "in-scope" for the CAF as a critical system, however, the airport has no direct contract of oversight of the system operating and maintenance, hence they hold no evidence that supports the process. This requires auditors to interview suppliers for evidence and this evidential process relies upon the good will of the supply chain: none of this was covered in the original contract of deliverables and may in some cases require the renegotiation of contracts and services, further complicating matters.

Such issues will undoubtedly be resolved as the standard beds down, but for now airports are looking for ways in which they can comply as cost effectively as possible. Many have decided that rather than undertake the self-assessment process themselves they will turn to a third party, such as their existing IT service provider. However, IT teams seldom have the oversight needed to understand all the aviation functions. For this reason, most elect to employ an ASSURE cyber professional for the self-assessment stage. This is perfectly permissible provided the organisation uses another assessor to carry out the audit to avoid any conflict of interest.

ASSURE ACCREDITS THIRD-PARTY COMPANIES TO IMPROVE THE CYBER DEFENCES OF AIRPORTS

The self-assessment, a complete list of the critical systems and diagrams from the critical systems scoping template, the completed CAF for Aviation covering all in-scope systems and all supporting evidence forms the basis of the Audit report. The auditor will then submit these elements together with a Corrective Action Plan with supporting documents and details on the cyber organisation structure (all of which are referred to as the Statement of Assurance). Following the receipt and review of this, the Authority will issue the Certificate of Compliance, which details future cyber security oversight activity because the process is iterative in that it should lead to further improvement.

So what else can the organisation do to make the process easier? Odd as it may sound, one of the most efficient things to do is to start creating the Corrective Action Plan at the beginning of the process when completing the CAF. Identifying corrective actions as and when gaps are identified between the score and the profile stages means these corrective actions can then also be documented in the CAF evidence, which will add to the Authority's sight that corrective actions are underway. It makes sense to compose the Corrective Action Plan in the tool usually used for task management and then actions raised can be separated out for reporting.

It's also really important to identify those systems that are deemed in scope at the start, both internally and with third parties, to save everybody time and effort. Including systems that shouldn't have been or omitting to include systems can significantly add to workloads. There's also the option to group systems together following guidance in CAP 1849. An example of this would be the baggage belts, x-ray machines and explosive detection machines that may comprise a hold baggage system. Grouping them together can

▶

reduce the compliance burden provided they all share the same architecture and controls.

ASSURE auditors will readily tell you that the scoping documents tend to be the least complete aspect of the evidential data passed to them yet these play a vital role and can help the organisation derive the maximum value from the process. These documents provide context and a diagrammatic representation that ensures accurate CAF assessment and recommendations for improvement. It is worth noting that reviewers at the Authority are not privy to the documented evidence and will only see the CAF, scoping documents, report and Corrective Action Plan, so it's important to invest time and effort into these.

> THIS UNPRECEDENTED LEVEL OF OVERSIGHT PROMISES TO REDUCE THE RISK OF BREACHES

Another area where aviation organisations are tempted to reduce spend is in limiting the number of parties involved in completing the CAF. In reality this is a false economy, particularly if you just use one individual, because it limits perspective and can even skew results thereby forcing the auditor to dedicate more time to querying the evidence and carrying out supplementary interviews. The wider you throw the net, the more likely you'll capture sufficient evidence so do include the system owner and managers not just IT.

Where you can save time and money is in referencing the evidence gathered during the self-assessment. Careful cataloguing in the CAF can pay dividends by making it easier for the auditor to locate and navigate to the correct data. So with large documents, reference the chapter, page or paragraph and for interviews, record the name of the person and their role but also provide summary information in the comments field. This enables the auditor to verify the interview without needing to find and trawl through it to document the evidence.

Finally, remember that honesty really is the best policy. Trying to second guess how you should pitch responses when completing the CAF is liable to backfire. Being overly optimistic will see the organisation fail to realise value and bring into question its evidential process while being overly pessimistic can see more issues added to the Corrective Action Plan. As the latter is developed prior to submission to the CAA and is unplanned and unscheduled, a long litany of issues could eat up auditor hours.

Following the submission of the final statement of assurance and award of the certification of compliance, the organisation is expected to begin implementing and maintaining the cyber security controls identified in the Corrective Action Plan. It is also still under obligation to notify the Authority of any reportable incidents and of any cyber security changes as well as to any information requests, so this is very much the start of a journey. The ultimate aim of ASSURE? To create an effective and appropriate oversight regime for the airport that enables it to manage and address its cyber security risk going forward ●

Phil Robinson – Principal Consultant at Prism Infosec – has over 25 years' experience in infosecurity with expertise in penetration testing, red teaming and securing cloud and on-prem architectures and enterprise applications. He and his team are ASSURE accredited by CREST.

Many airports have taken a holistic approach to their cybersecurity as it addresses IT, OT and Process Control Networks

Picture credit: iStock