AVIATION ISAC

CISO SURVEY RESULTS

2025

CONTENTS

03

Executive Summary

04

Threat Landscape

05

Survey Results

07

Top 5 Categories of Risk Reduction Efforts

13

Analyzing the Results by Industry Segment

15

Summary

EXECUTIVE SUMMARY

As Aviation ISAC enters its second decade, we present the 8th edition of our Aviation Cyber Risk Survey. This year's survey results are mapped to the updated version of the National Institute of Science (NIST) Cyber Security Framework (CSF), version 2.0.

The purpose of the survey is to provide a tool for industry CISOs to benchmark their strategies, program maturity, and management of resources. The Aviation ISAC staff also utilizes this information to direct efforts into the areas upon which our members are focused in the coming year.

Ahead of the survey results we have again included our TLP Clear version of the aviation cyber threat landscape. We continue to see cyber threat actors with varied motivations seeking to disrupt or degrade the aviation ecosystem through attacks on the digital infrastructure and software driven technologies. The attack surface continues to expand as new technological functions are introduced to aviation and the industry continues its strong growth. Cyber actors are getting more skilled at developing zero days and accelerating the time from breach to impactful actions within networks.

Identity management, authentication, and access control continue to dominate the focus of CISOs in aviation. Governance, a new function in the NIST CSF 2.0, fared prominently in the survey, with two governance categories in the top 5 areas of concern: organizational context and supply chain risk management. Asset management and continuous monitoring rounded out the top five priority areas. We also highlighted additional focus areas and noted emerging concerns as reports emerge that quantum computing may be coming sooner than originally anticipated.

Thank you to all who participated in the survey. We hope this information can provide guidance and insight into your strategic planning and prioritization of initiatives to enhance the resilience of the aviation industry amidst the ever growing stream of cyber attacks on our sector.

Jeffrey Troy
President, CEO
Aviation ISAC

THREAT LANDSCAPE

Over the past ten years, cyber threat actors have demonstrated an ability to negatively impact the global commercial aviation system. Airline and airport operators, aircraft manufacturers, satellite companies, and the complex aviation supply chains that support them will continue to be targeted. Certain companies have experienced significant operational disruption, loss of sensitive data, and financial losses. This report by Aviation ISAC provides an overview of the risk posed by various types of malicious cyber incidents impacting the aviation sector.

Three types of cyberthreat actors are targeting the commercial aviation sector: nation-state Advanced Persistent Threat (APT) groups, organized cybercriminal groups, and hacktivists.

The large and growing digital infrastructure which supports the commercial aviation sector provides attackers a broad and extensive cyber-attack surface. Furthermore, the increased reliance upon managed service providers (MSPs) and cloud service providers increases the risk of indirect data breaches, when these providers are targeted by malicious cyberthreat actors.

Although cyberthreat actors continue to exploit known computer vulnerabilities in organizations that have not fully mitigated these flaws, they are also becoming increasingly adept at finding and exploiting zero-day vulnerabilities before they are made public. Cyber threat actors are also getting much better at avoiding traditional signatures-based intrusion detection systems and maintaining network persistence through living-of-the-land (LOTL) tactics.

The Aviation ISAC assesses that some cyberthreat actors likely possess the ability to inflict serious, but localized, disruption upon the global commercial aviation sector.

High regional tensions in Eastern Europe, the Far East, and the Middle East regions serve as driving forces behind increased malicious cyber activities emanating from these areas. In addition, regional conflicts have led to an increase in GPS jamming/spoofing that has impacted commercial aviation flights, as well as increased risk of accidental kinetic attacks.

SURVEY RESULTS

How do we get the data?
Each year we survey CISOs in our community to understand their strategies for cyber risk reduction heading into the new year. The survey poses just one question, “What are the 3-5 things you committed to getting done in 2025 to reduce cyber risk?”

How do we analyze the data?
The responses are catalogued using the National Institute of Standards and Technology’s Cyber Security Framework (NIST CSF 2.0). We aggregate the responses and summarize where cyber security efforts are focused. We present the results along with highlights from the CISO narratives.

26% of our members participated in our annual one question survey. The question posed seeks to elicit the big rocks which our members are trying to move out of the way of creating a secure environment for their networks, OT, IOT, and in their product development. We tabulated and analyzed the results from several perspectives. We looked at overall responses by function (Governance, Identify, Protect, Detect, Respond, and Recover), category, and sub-category.

What did we learn?
The results for 2025 reflect that the update to the NIST CSF was very much needed. Of the responses, 31% reflected the need for governance work across the industry. Governance work was most certainly being done in previous years. However, the prevalence of that work was masked as governance work was embedded as a category or subcategory under the other five functions in NIST CSF 1.0. Governance is owned at the C-Level of every company. Seeing such a significant level of governance work being highlighted in this year’s survey results underscores the importance of all business executives, across all the functions in aviation, who are acknowledging their ownership of cybersecurity within those business functions. Many of the governance initiatives were the creation of cybersecurity policies to ensure the companies were meeting regulatory requirements, reducing supply chain risk, and calling out the need for business functions to better manage cyber risk.

As in prior years, work being done in the protect and identify functions followed as the top areas of emphasis. Protect initiatives were mentioned much more significantly for 2025 over 2024. Governance initiatives consumed much more of the space previously allotted for protect and identify functions than that of the other functions. Interestingly, detect initiatives remained consistent at 18% in 2025, slightly more than those called out in 2024.

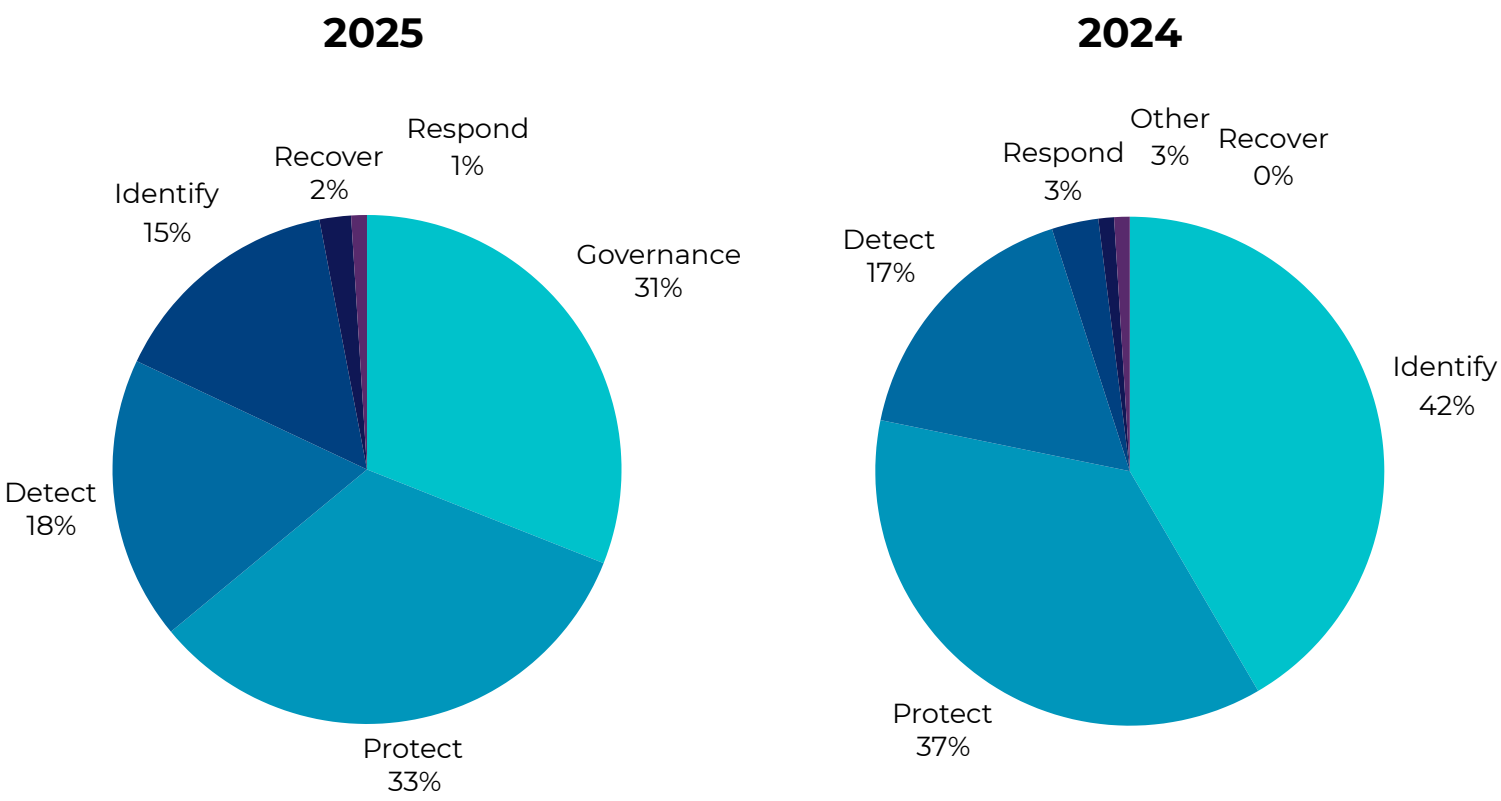


Figure 2 survey results for all segments mapped to NIST CSF 1.0 in 2024

A deeper dive into the categories, sub-categories, and specific projects mentioned by the respondents are provided below. The NIST CSF has significantly less categories and sub-categories in the respond and recover functions, thus it is expected that we would see less initiatives in these areas.

TOP 5 CATEGORIES OF RISK REDUCTION EFFORTS

1. Protect: (PR.AA) Identity Management, Authentication, & Access Control
2. Governance: (GV.OC) Organizational Context
3. Identify: (ID.AM) Asset Management
4. Governace: (GV.SC) Supply Chain Risk Management
5. Detect: (DE.CM) Continuous Monitoring

Of those participating in the survey, 37 of the respondents identified initiatives in Protect: Identity Management, Authentication, Access Control (PR.AA), followed by 22 in each of the categories of Governance: Organizational Context (GV.OC) and Identify: Asset Management (ID.AM). Twenty-one (21) initiatives were called out in Governance: Supply Chain Risk Management (GV.SC) and, rounding out the top five, 20 CISO emphasized 20 initiatives to improve Detect: Continuous Monitoring capabilities (DE.CM). In the narratives below we call out only the subcategories in NIST CSF 2.0 for which we received input. Following these charts are additional details on strategies, projects and initiatives for the categories within which we received the most feedback.

1 Protect: Identity Management, Authentication, and Access Control

Year after year, Identity Management, Authentication and Access Control (IDM) has been the number one ranked category of initiatives. Survey respondents continue to highlight multi-year projects to implement multifactor authentication (MFA) across their networks and operating technologies (OT). Identity management is a critical pillar in Zero Trust (ZT) strategies and leveraging more IDM tools for analytics. Aviation companies are most focused on four IDM subcategories: PR.AC-1 credential management, PR.AC-5 network integrity, PR.AC-4 Access permission management, and PR.AC-7, Authentication and MFA.

PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	29.7%
PR.AA: Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	24.3%
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	21.6%
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	16.2%
PR.AA-04: Identity assertions are protected, conveyed, and verified	5.4%
PR.AA-03: Users, services, and hardware are authenticated	2.7%

PR.AA, PR.AA-05: There was a diversity of initiatives identified in this category. The most prevalent types of initiatives were focused on introducing MFA to customers and other 3rd party accesses, using identity management as a part of the implementation of Zero Trust and new cloud identity management capabilities. CISOs also called out the implementation of IDM tools for the cloud. Several members called out plans to address IDM but were still working out the strategies and tool selections. CISOs are also looking at moving to password-less environments.

PR.AA-01: Active Directory was the hot topic in this subcategory. CISOs strategies are on both ends of the spectrum, with some expanding the use of Active Directory and others looking to eliminate it. At the expansion end, projects included using AD for IDM in the Operational Technology side of the house and adding technologies to supplement better AD management. At the other end of the spectrum, the fact that ransomware actors are frequently attacking AD has CISOs investigating other solutions. CISOs continue reviews of Privileged Access Accounts and non-human identities with an eye toward reducing the breadth of access wherever possible.

PR.AA-02: Airline and airport members mentioned their intent to try to reduce internal and external fraud through better identity controls and management. These strategies included extending the use of single sign-on and multifactor authentication to more applications.

02 Governance: Organizational Context

Last year, Governance broke into the top 5 areas of action for CISOs in our survey. Governance, under NIST CSF 1.0 was a subcategory under Identify. This year governance is a function which took two of the 5 top slots.

Four of the six organizational context subcategories within the governance function aligned with projects identified by CISOs. Our global membership was reflected in the many different legal and regulatory schemes which our member companies must document their compliance through policy changes, process changes and audits.

GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	68.2%
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	18.2%
GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	9.0%
GV.OC: The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood	4.5%

Members called out regulatory compliance challenges in Europe, the Asia Pacific, the Americas and from industry associations specific to aviation and other voluntary and mandatory requirements such as SOC2, and PCI. European members are focused on NIS2, and Part IS. Some members are flying into countries which are restricted by other countries and or are using technologies which may be restricted for deployment in other countries and the CISOs are ensuring the use of these tools is allowed. In the United States, some members are voluntarily looking at CMMC. Members also mentioned projects to automate audit evidence collection and collaborating more with legal and privacy experts to better understand reporting requirements in advance of an event.

03 Identify: Asset Management

Similar to the never-ending challenge of identity management, year over year asset management initiatives are a part of the cyber risk reduction strategies for CISOs in 2025.

ID.AM-01: Inventories of hardware managed by the organization are maintained	18.2%
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	18.2%
ID.AM: Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to organizational objectives and the organization's risk strategy	13.6%
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	13.6%
ID.AM-04: Inventories of services provided by suppliers are maintained	9.1%
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	9.1%
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	9.1%
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	9.1%

CISOs working initiatives in asset management were primarily focused on getting a better handle on their Operational Technology (OT) and Internet of Things (IoT) environments. In addition, original equipment manufacturers (OEMs) noted an emphasis on getting a better view into their factory floor environments. Several CISOs noted plans to update their asset management policies. Additionally, several CISOs noted they would be conducting workouts with a focus on asset management process improvements for 2025.

04 Governance: Supply Chain Risk Management

There were numerous responses to the survey noting initiatives to reduce supply chain risk. Most of the subcategories in this function speak directly to CISOs engagement of their company's executives managing the business functions as well as ensuring cybersecurity is a part of the enterprises overall risk management plan.

GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	40.0%
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	10.0%
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	10.0%
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	10.0%
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	5.0%
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	5.0%
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	5.0%
GV.SC-04: Suppliers are known and prioritized by criticality	5.0%
GV.SC-06: Planning and due diligence are performed to reduce risks before entering formal supplier or other third-party relationships	5.0%
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	5.0%

Supply chain risk management (SCRM) challenges are pervasive across our industry. CISOs identified numerous initiatives starting with a complete review of their SCRM strategy. Interestingly, many of the CISOs identified this as an area of focus, however the path to success was not defined. Several CISOs noted the path would include increased continuous monitoring of key suppliers. Further noting this year, they will be searching for better ways to do SCRM. Ideas which were highlighted included doing more common assessments with aviation partners, increasing cyber security clauses in supplier contracts, and requiring suppliers to provide software bills of material.

05 Detect: Continuous Monitoring

CISOs noted several environmental factors which are driving continuous monitoring initiatives. Many CISOs have had the same SIEM toolsets in place for five or more years and are open to looking at new vendors. The integration and/or planned integration of artificial intelligence into many security tools is also driving reviews into replacement of security operations center tooling and network monitoring tools.

DE.CM-01: Networks and network services are monitored to find potentially adverse events	70.0%
DE.CM-02: The physical environment is monitored to find potentially adverse events	10.0%
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	10.0%
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	5.0%
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	5.0%

CISOs are focusing more on enhancing visibility into their OT and IoT environments by implementing improved logging practices. Similarly, many CISOs are seeking to gain better visibility into their cloud environments. These CISOs are considering both the cloud native monitoring tools and third-party options. Some CISOs are focused on enhancing their insider threat programs with the deployment of enhanced user behavioral analytic (UEBA) tools and through increased partnering with legal, physical security, and human resources departments.

Other Notable Responses from the Survey

Detect: Adverse Event Analysis

Numerous member companies will be replacing their SIEMs, updating other tools within their SOCs and seeking more automation of event analyses. Several members noted their plans to add a case management capability on top of their event management platforms. CISOs noted SIEMs continue to have too much noise and will restart efforts to better tune the alerting. Members continue to implement bug bounty programs and will increase the amount of threat intelligence collected by their teams.

Protect: Data Security

Two big themes emerged in the discussions concerning data security initiatives. CISOs prioritizing data security improvements in 2025 were focused on concerns about the risk of exposure for data being processed in applications using artificial intelligence. CISOs are continuing to drive the understanding around where data is processed and stored in these applications. This will impact governance around the use of the applications as well. The second focus was on the implementation or expansion of the use of data loss prevention (DLP) tools.

Protect: Platform Security

The CISOs noted a wide range of initiatives to enhance platform security. CISOs most frequently mentioned a focus on mobile security in 2025. OEMs noted product development initiatives to make the products more cyber resilient such as embedding more MFA into products. Similarly, CISOs noted many one-off projects to make their computer platforms more secure as well to include complete replacement of certain device types or manufacturer types for a more secure option and better USB device management.

Risk Management

Many CISOs mentioned they were completing or had recently completed regulatory risk assessments. The organizations were using or planning to use those assessments to prepare strategies to fill the gaps identified through these assessments. As a part of these discussions, CISOs noted the expansion of many regulatory schemes, both at the governmental and industry association levels, such as IST and PCI.

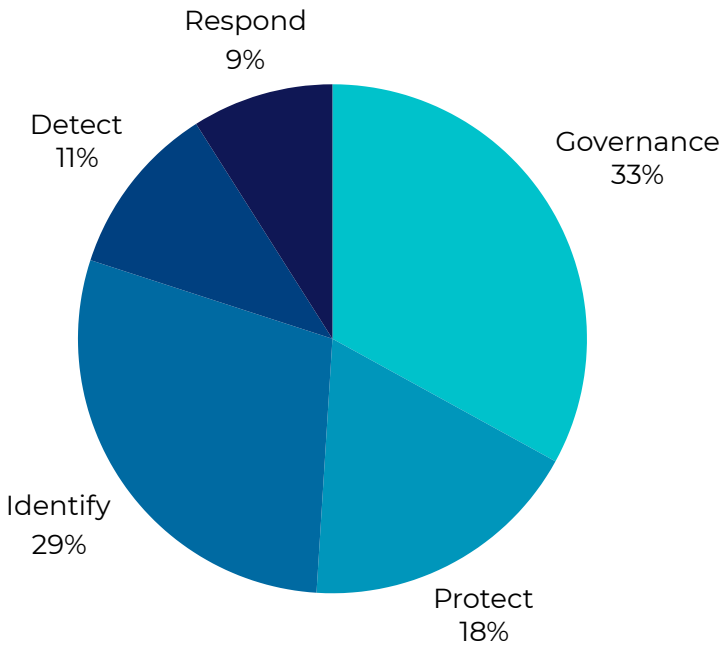
Each year we conduct this survey, one or two CISOs signal a concern which may trigger more attention on that issue across the industry. This year it is the concern over whether quantum computing should be on the risk management matrix. What risks does quantum pose to protection, prevention, detection, and resilience. The discussions primarily focused on a need to learn more and understand the risks and the timeline at which they may become impactful.

ANALYZING THE RESULTS BY INDUSTRY SEGMENT

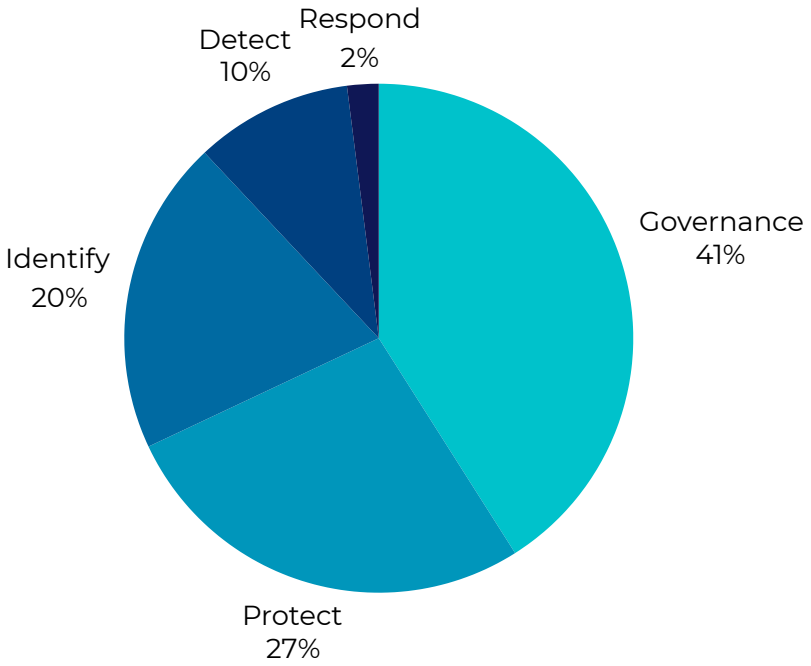
The charts below depict the percentage of initiatives by function for just this year. The charts are organized by each of the three segments used for this survey: Airports, OEM's/Service companies, and Airlines. With the release of NIST CSF 2.0, we are only presenting the industry segment analyses for 2025. When plotted against prior years, the data for 2025 did not align well with the data sets of previous years. Going forward, the analyses of the years 2025 and beyond will be more intuitive.

For all three of our segments, using NIST SCF 2.0, the top four priority areas are now completely aligned. The priorities rank in the following order across all segments: Governance, Protect, Identify and Detect. Airports were notably more focused on improving response capabilities than the other two segments.

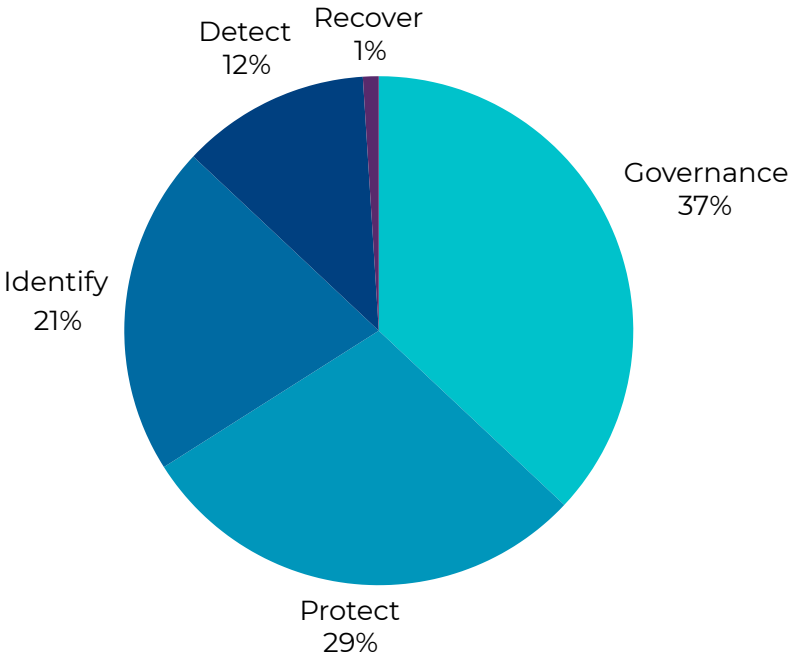
AIRPORT PRIORITIES 2025



OEM/SERVICE PROVIDER PRIORITIES 2025



AIRLINE PRIORITIES 2025



SUMMARY

This report is an industry trend analysis of annual cyber security priorities. It does not reflect the emphasis of any one company. The value of the report is in its ability to assist CISOs in aviation to benchmark their cyber security strategies, program maturity, and management of resources against the industry.

We want to thank the many CISOs who took the time to share their thoughts and strategies for 2025.

Cyber resilience in aviation demands a unified, community-wide commitment. At Aviation ISAC, we are a dedicated community driven by a shared passion for aviation and a commitment to safeguarding the industry. Our goal is to ensure a level playing field where companies can operate without the disruption of cyber threats. We provide a safe and trusted platform for sharing cyber threat intelligence and developing best practices to protect, detect, respond to, and mitigate cyber-attacks. To learn more about joining our community, visit us at www.a-isac.com.

CONTACT

1997 Annapolis
Exchange Pkwy
Suite 300
Annapolis, MD 21401

membership@a-isac.com
www.a-isac.com