UK Civil Aviation Authority International

CAAS Civil Aviation Authority of Singapore | Singapore Aviation Academy

# Working together for a Cyber Resilient Future in Aviation

**Wednesday 24th July 2024**

# Before we start

The session will not be recorded

There will be opportunities throughout the webinar to ask questions. Questions should be logged using the Slido only.

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

Please give a ‘thumbs up’ to questions you would most like answered.

Following the webinar, all questions will be published. There will be a survey at the end of the webinar.

Or scan this QR code with your smartphone to access Slido

# Agenda

1. Welcome and opening
2. Overview of the current regulatory landscape and potential changes on the horizon
3. Capacity building to maintain a sustainable and resilient system
4. In-sights from pre-webinar cybersecurity survey

BREAK – 10 MINUTES

5. Cyber threats and challenges
6. Harmonisation and prioritisation of cyber, safety and security risks
7. Summary and conclusions
8. End webinar

# 1. Welcome

- **Matthew Margesson**
  Managing Director, CAAi
- **Ho Kee-Vin**
  Director, Cybersecurity and Data Governance, CAAS
- **Simon Sheeran**
  Head of Cybersecurity Oversight, UK CAA

# 2. Overview of the current regulatory landscape and potential changes on the horizon

- **Ho Kee-Vin**
  Director, Cybersecurity and Data Governance, CAAS

- **Jonathan Hogben**
  Cyber Security Policy Lead, UK CAA

# Overview

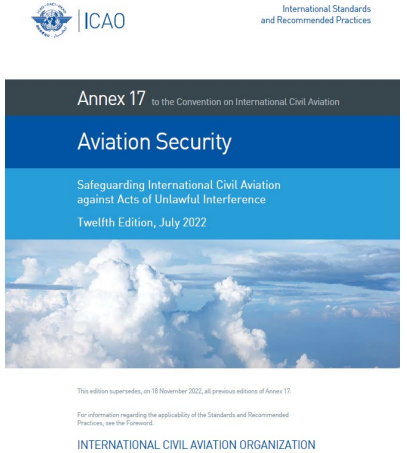
- Introduction
- Global Cybersecurity Regulatory Outlook
- Cybersecurity Regulations in Singapore
- Cybersecurity Regulations in the United Kingdom

# Global Cybersecurity Regulatory Outlook

# ICAO – Cybersecurity in Civil Aviation

Resolution - A40-10


- International Cooperation
- Governance
- Legislation and Regulation
- Cybersecurity Policy
- Information Sharing
- Incident Management & Emergency Planning
- Capacity Building Training & Culture




Resolution - A41-19

INTERNATIONAL CIVIL AVIATION ORGANIZATION
*A United Nations Specialized Agency*

# CHICAGO CONVENTION

## Annex 17 - Security

| | |
|---|---|
| Annex 1 | Personnel Licensing |
| Annex 2 | Rules of the Air |
| Annex 3 | Meteorological Service for International Air Navigation |
| Annex 4 | Aeronautical Charts |
| Annex 5 | Units of Measurement to be Used in Air and Ground Operations |
| Annex 6 | Operation of Aircraft |
| Annex 7 | Aircraft Nationality and Registration Marks |
| Annex 8 | Airworthiness of Aircraft |
| Annex 9 | Facilitation |
| Annex 10 | Aeronautical Telecommunications |
| Annex 11 | Air Traffic Services |
| Annex 12 | Search and Rescue |
| Annex 13 | Aircraft Accident and Incident Investigation |
| Annex 14 | Aerodromes |
| Annex 15 | Aeronautical Information Services |
| Annex 16 | Environmental Protection |
| Annex 17 | Security |
| Annex 18 | The Safe Transport of Dangerous Goods by Air |
| Annex 19 | Safety Management |

- Provides Standards and recommended practices to safeguard civil aviation & its facilities against acts of unlawful interference
- Requires each State to establish its own civil aviation security programme

# Annex 17 - Security

**4.9 Measures relating to cyber threats**

4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

4.9.2 **Recommendation.**—Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.

# ICAO – Cyber Panels & Harmonisation

ICAO

Safety ANC

Security ATB

ANC Panels

Trust Framework Panel **TF-P**

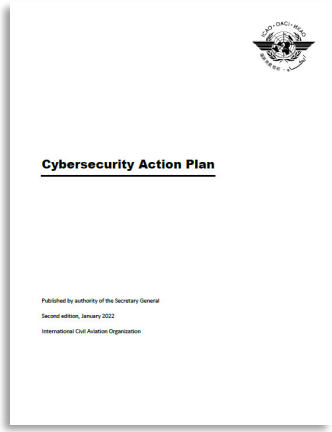
AVSEC/ Facilitation Panels

Cyber-security Panel **CYSEC-P**

Annex 15

Annex 17

- Updated January 2022
- Develops on the 7 Pillars
- 32 Priority Actions
- 51 Tasks
- Drives the work of CYSEC-P


Cybersecurity Action Plan

Published by authority of the Secretary General
Second edition, January 2022
International Civil Aviation Organization

Safety ⟷ Security

Ad Hoc Cyber Coordination Committee

Future Task Forces

# Cybersecurity Regulation in Singapore

# Civil Aviation Authority of Singapore (CAAS) and Singapore Aviation Academy (SAA)

The CAAS plays a crucial role in maintaining Singapore's reputation as a global aviation hub, ensuring regulatory oversight and safety in Singapore's aviation sector.

The SAA, which is the training arm of the CAAS, focuses on professional training, to support the development and advancement of aviation professionals globally.

Together, we oversee and promote safety in the industry, and develop Singapore as a centre of excellence for aviation knowledge.

# Overview of the Cybersecurity Regulations in Singapore

**NATIONAL**

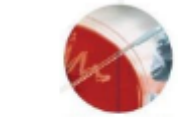
## CYBERSECURITY AUTHORITY OF SINGAPORE (CSA)

CSA is the national Cybersecurity regulator responsible for overseeing cybersecurity strategy, policy and perform regulatory oversight of CII in Singapore

**SECTORAL**

## SECTOR LEAD (CAAS)

CAAS is the aviation regulatory authority responsible for overseeing civil aviation activities in Singapore to ensure the safety, security, and resilience of aviation systems and operations


SECURITY & EMERGENCY


ENERGY


INFOCOMM


WATER


GOVERNMENT


AVIATION


BANKING & FINANCE


HEALTHCARE


MEDIA


Maritime


LAND TRANSPORT

**ORGANISATION**

## CRITICAL INFORMATION INFRASTRACTURE OWNER (CIIO)

Aviation operators are responsible for implementing cybersecurity measures and comply with the regulatory requirements to protect critical aviation infrastructure

# Singapore Aviation Cybersecurity Regulations

## CYBERSECURITY ACT

Framework to protect critical information infrastructure (CII) against cybersecurity threats. It includes measures for oversight,  responding to cybersecurity incidents, and maintenance of national cybersecurity.

## Cybersecurity Code of Practice (CCoP)

It specifies the minimum cybersecurity requirements that all CII owners must implement at the national level.

## Aviation Code of Practice (ACCoP)

This complements the CCoP and specifies additional protection policies and requirements that the aviation CII owners must implement to ensure the cybersecurity of their aviation CII systems.

# Cybersecurity Act

| Protection of Critical Information Infrastructure | Investigation of Cybersecurity Threats and Incidents | Information Sharing | Licensing of Cybersecurity Service Providers |
|---|---|---|---|
|  |  |  |  |
| Strengthen the protection of CIIs against cyber-attacks. | Authorise CSA to prevent and respond to cybersecurity threats and incidents. | Establish a framework for sharing cybersecurity information. | Establish a light-touch licensing framework for cybersecurity service providers. |

Implemented in 2018, the Cybersecurity Act provides a framework for the oversight and maintenance of national cybersecurity. It mandates critical infrastructure sectors, including aviation, to report cybersecurity incidents and adhere to specified cybersecurity measures.

*Referenced from the Cybersecurity Agency of Singapore (CSA)*

# Potential changes on the horizon

Singapore

## REGULATORY MEASURES

**Major Cyber attacks**

- SolarWinds
- Colonial Pipeline

### CSA Regulatory Frameworks

- Key Amendments to Cybersecurity Act and CCoP2.0 to address evolving threats:
  - **Supply Chain vulnerabilities** (e.g. risk assessments, vendor risk management)
  - **Cybersecurity Incident Reporting Requirements**: To report all cyber security incidents to regulatory authorities
  - **Regulate both physical and virtual CII systems (Oversight of Cloud Services)**
  - **Regulate CII owners supporting an essential service from overseas**
  - **Entities of special cyber-security interest**
  - **Amplified Regulatory Powers**

To address shifts in cybersecurity and operational challenges, the Cybersecurity (Amendment) Bill which accounts for technology changes was passed in the Singapore parliament on 7 May 2024.

### International Collaboration and Standards Alignment

- Collaboration with international partners and alignment with global cybersecurity standards and best practices.
- Participation in international cybersecurity initiatives, information sharing partnerships, and efforts to harmonize regulatory frameworks with global norms.

# Cybersecurity Regulation in the United Kingdom

# UK Civil Aviation Authority

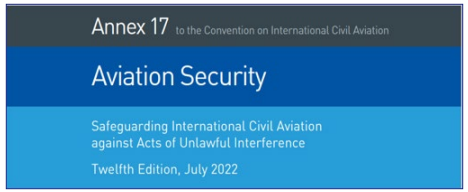
- The aviation industry meets the highest **safety** standards
- Consumers have choice, value for money, are protected and treated fairly when they fly
- Through efficient use of airspace, the environmental impact of aviation on local communities is effectively managed and CO2 emissions are reduced
- The aviation industry manages **security** risks effectively

UNDERSTANDING AND ADDRESSING RISK | DELIVERING UNIQUE VALUE | ACTING PROPORTIONATELY | ENGAGING PROACTIVELY AND TRANSPARENTLY | ACTING ON OUR COMBINED INSIGHT

# UK – Cyber Security Regulatory Overview

**Global**

- Aviation Cybersecurity Strategy
- Air Traffic Management Security Manual
- Guidance on Traffic Light Protocol
- Cybersecurity Policy Guidance
- Cybersecurity Culture in Civil Aviation




ICAO SAFETY

**Regional**

European Parliament

NIS Directive 2018 (EU) 2016/1148

European Commission

Regulation (EC) No 300/2008

EASA European Aviation Safety Agency

**National**

UK NIS Regulation

UK GDPR 2018

PSTI 2024

Civil Aviation Act
Air Navigation Order

**Aviation**

OES

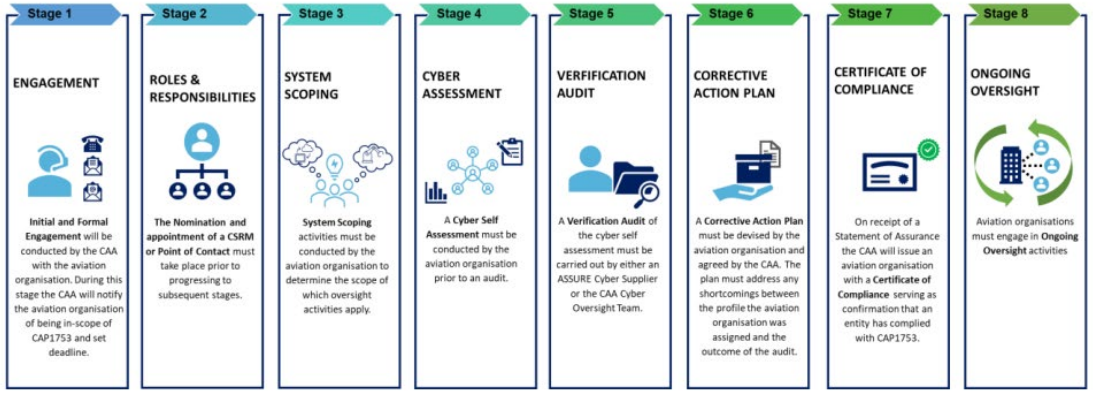
National Aviation Security Programme
Chapter 13 of the Single Consolidated Direction (SCD)

CAP1753

Safety Regulations
Basic Regulation 2018/1139

# UK – Cyber Security/Safety Regulations

- Proportionate structured approach across 3 tiers
- Focus on critical systems and risk mitigation
- Utilities established frameworks developed in association with NCSC
- Platform for oversight of NIS, NASP and applicable safety regulations


Regulation 373/2017
Air Traffic Management/ Air Navigation Services

Regulation 139/2014
Aerodromes

Regulation 73/2010
Aeronautical Data & Information

**Aerodromes & Air Navigation Service Providers**

Regulation 1321/2014
Continuing Airworthiness of Aircraft & Parts

Part CAMO/ Part 145
Maintenance and Repair Station Organisations

Part 21J/ Part 21G
Design and Production Organisations

Regulation 965/2012
Air Operators

**Design Production and Maintenance**

Regulation 748/2012
Initial Airworthiness

**Initial Airworthiness**

Space Industry Act 2018

**Space**

Regulation 2019/947 **UAS**

**RPAS**

# UK – Cyber Security Governance & Future Approach

UK Civil Aviation Authority
Department for Transport
National Cyber Security Centre
a part of GCHQ

Aviation Cyber Security Strategy

Collaboration

Air Carriers
Airports
Government
Manufacturers
ANSPs
NCSC
Academia

## Future Regulatory Direction

- Information Security Management Systems (ISMS)
- Safety – Security a Horizontal Rule
- Proportionate risk based regulatory framework
- Integration with existing SMS/SeMS approaches
- Understand the threats posed by the Supply Chain
- Incident Reporting and Sharing mechanisms
- Cyber security culture

# Questions & Answers

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

# 3. Capacity Building to maintain a sustainable and resilient system

- **Ng Hoo Ming (Facilitator)**
  President, ASEAN Chief Information Officer Association & Advisor (Cybersecurity), CAAS
- **Alcus Erasmus (Panellist)**
  Head of Cyber Security Engineering, MAG (Airports Group)
- **Calvin Ng (Panellist)**
  Director, Cybersecurity Programme Centre, Cyber Security Agency of Singapore
- **Ho Kee-Vin (Panellist)**
  Director, Cybersecurity and Data Governance, CAAS

# Questions & Answers

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

# 4. Pre-Webinar Survey Results & Key Findings

- **Kevin Sawyer**
  Head of International Operations - Aviation Security, CAAi

# ICAO 7 Pillars

The Aviation Cybersecurity Strategy by the International Civil Aviation Organisation (ICAO) aims to enhance global civil aviation's resilience to cyber-attacks while promoting safety, security, and innovation. It is built on seven pillars.

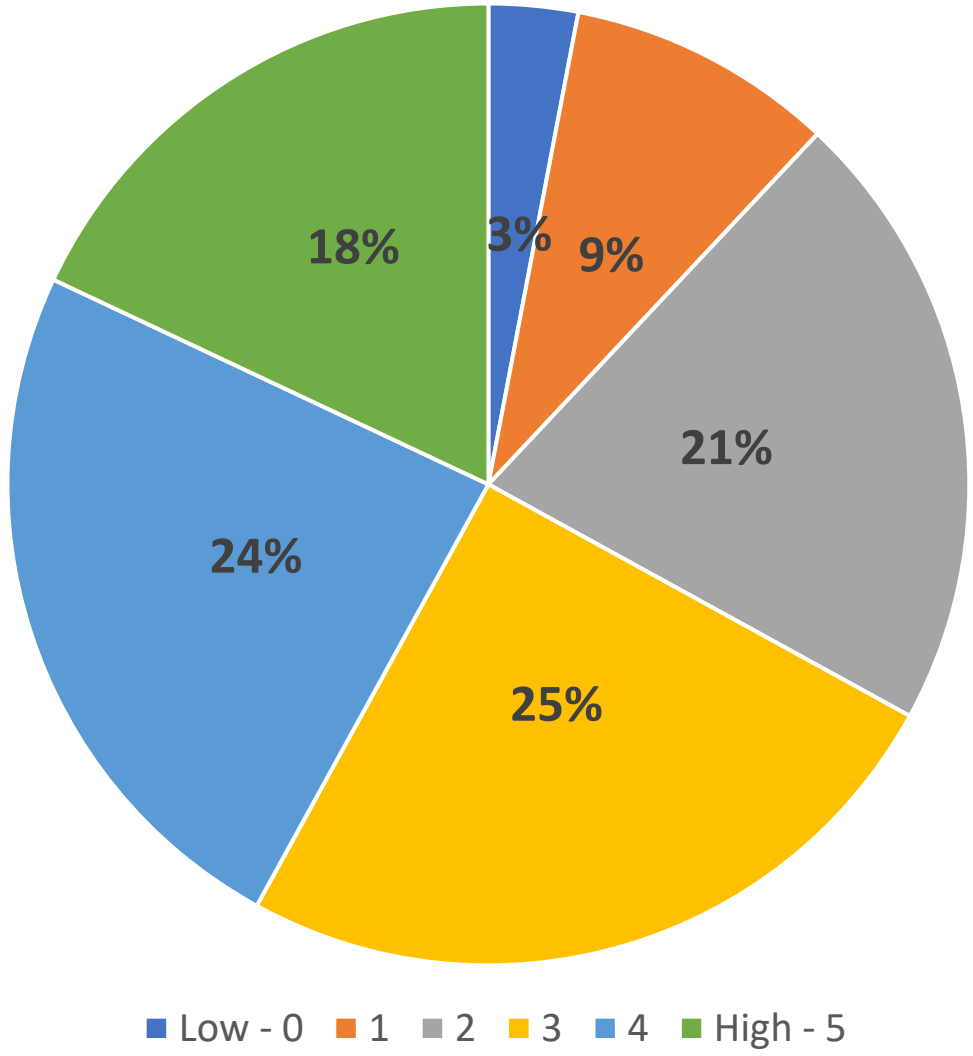
Based on these seven pillars, the survey asked responders to rather how they felt their organisation performed using a slide scale.

# Pillar One

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

## International Cooperation

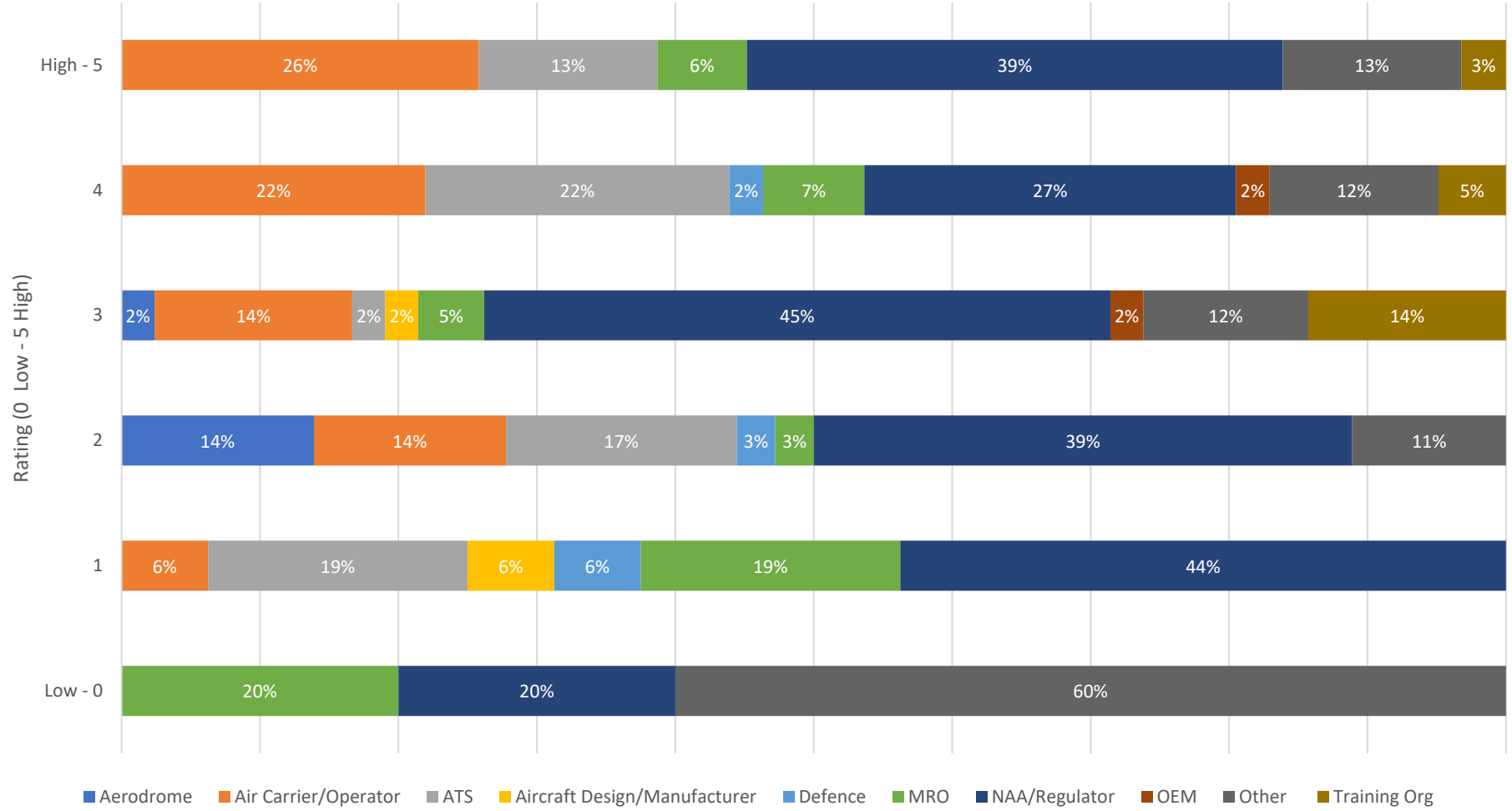
My organisation is in-line with aviation cyber-security requirements at both a national and international level, including engagement with ICAO cyber security events.




** Based on 171 responses*

# Pillar One

**Pillar 1 - International Cooperation**
**Responses by sector**



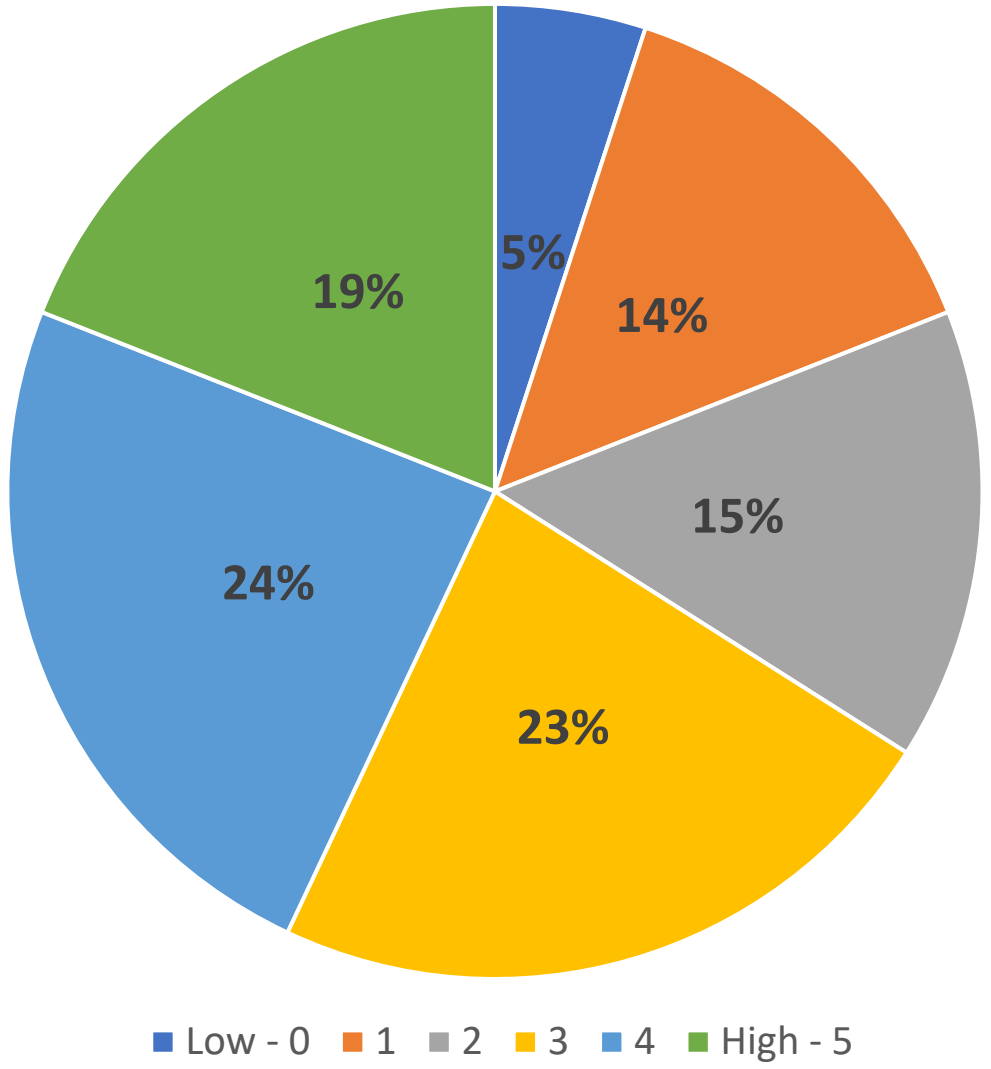

** Based on 171 responses*

# Pillar Two

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

## Governance

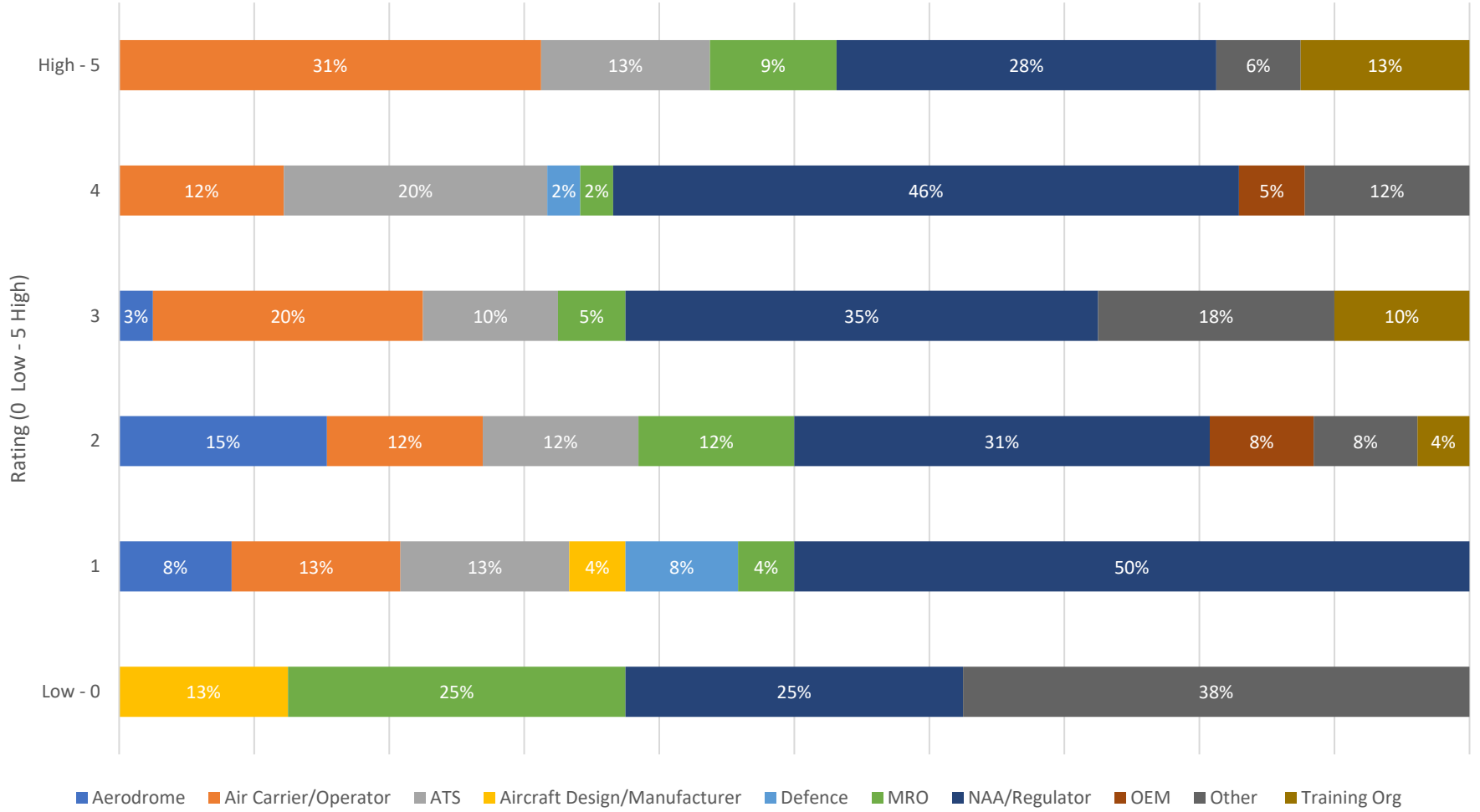
My organisation has developed clear governance and accountability for civil aviation cybersecurity, including coordinating with the competent authority (where appropriate), having effective communication between State authorities and industry entities, and aligning with the relevant regulations and guidance.




** Based on 171 responses*

# Pillar Two

**PILLAR 2 – Governance**
**Responses by sector**



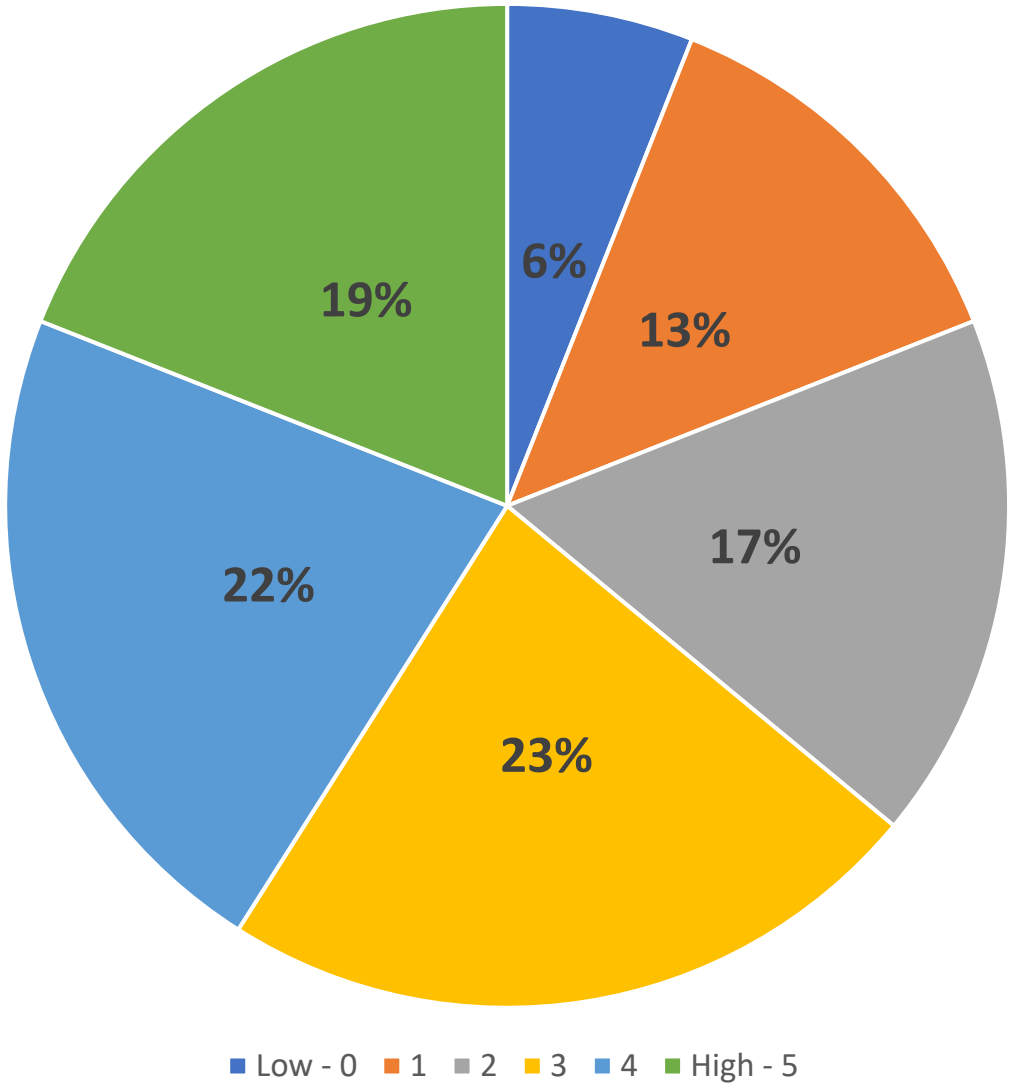

** Based on 171 responses*

# Pillar Three

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

## Effective Legislation and Regulations

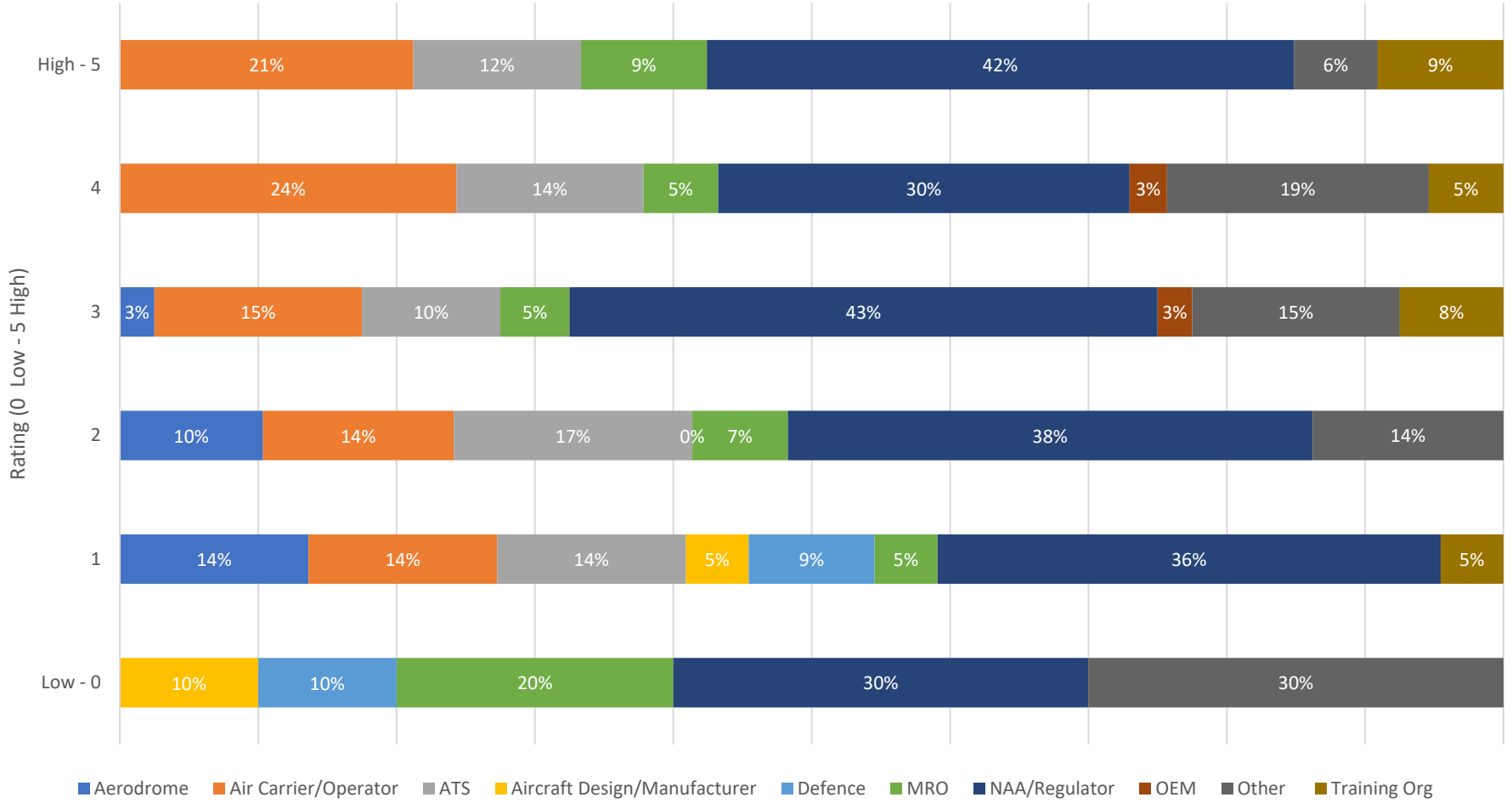
Through following legislation and regulations, my organisation is supporting the implementation of a comprehensive strategy to protect civil aviation and the travelling public from the effects of cyber-attacks.




** Based on 171 responses*

# Pillar Three

**PILLAR 3 - Effective Legislation and Regulations**
**Responses by sector**



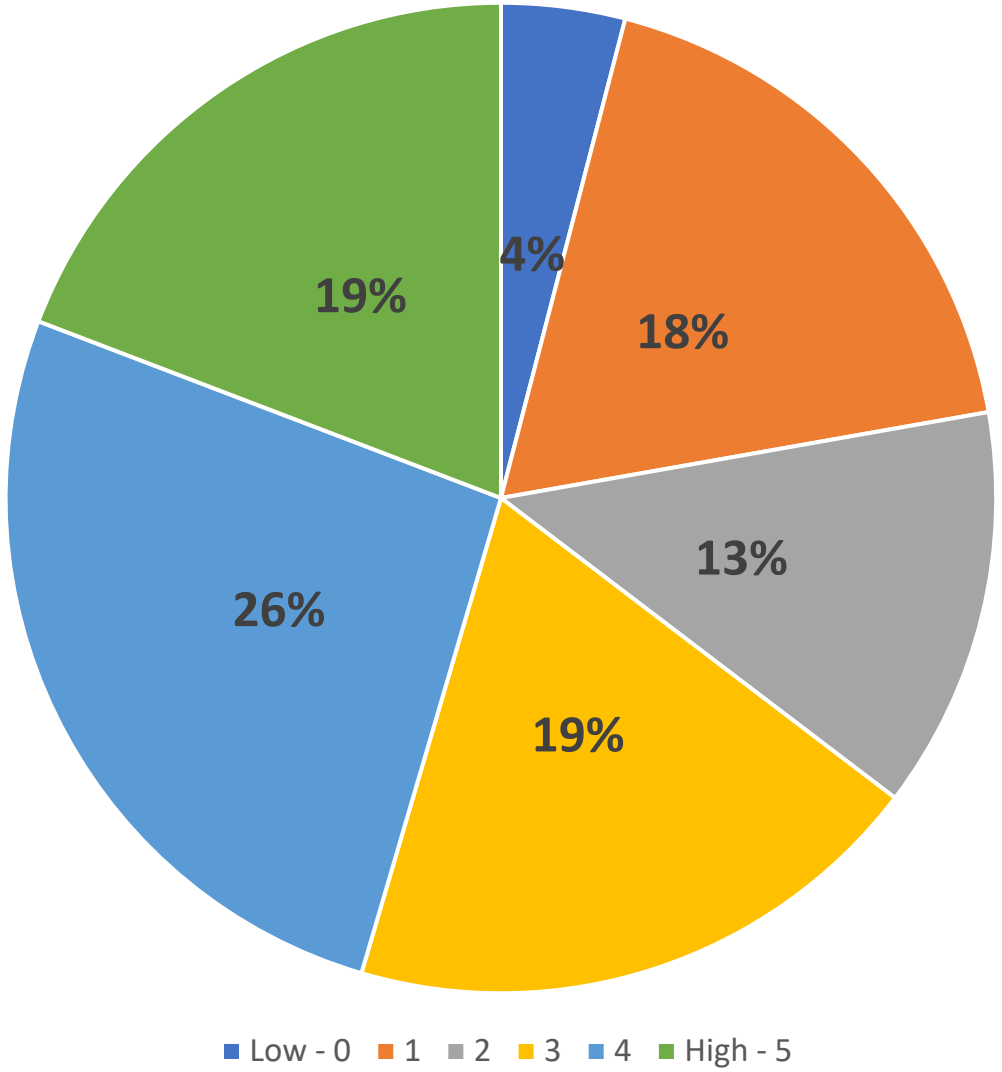

** Based on 171 responses*

# Pillar Four

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

## Cybersecurity Policy

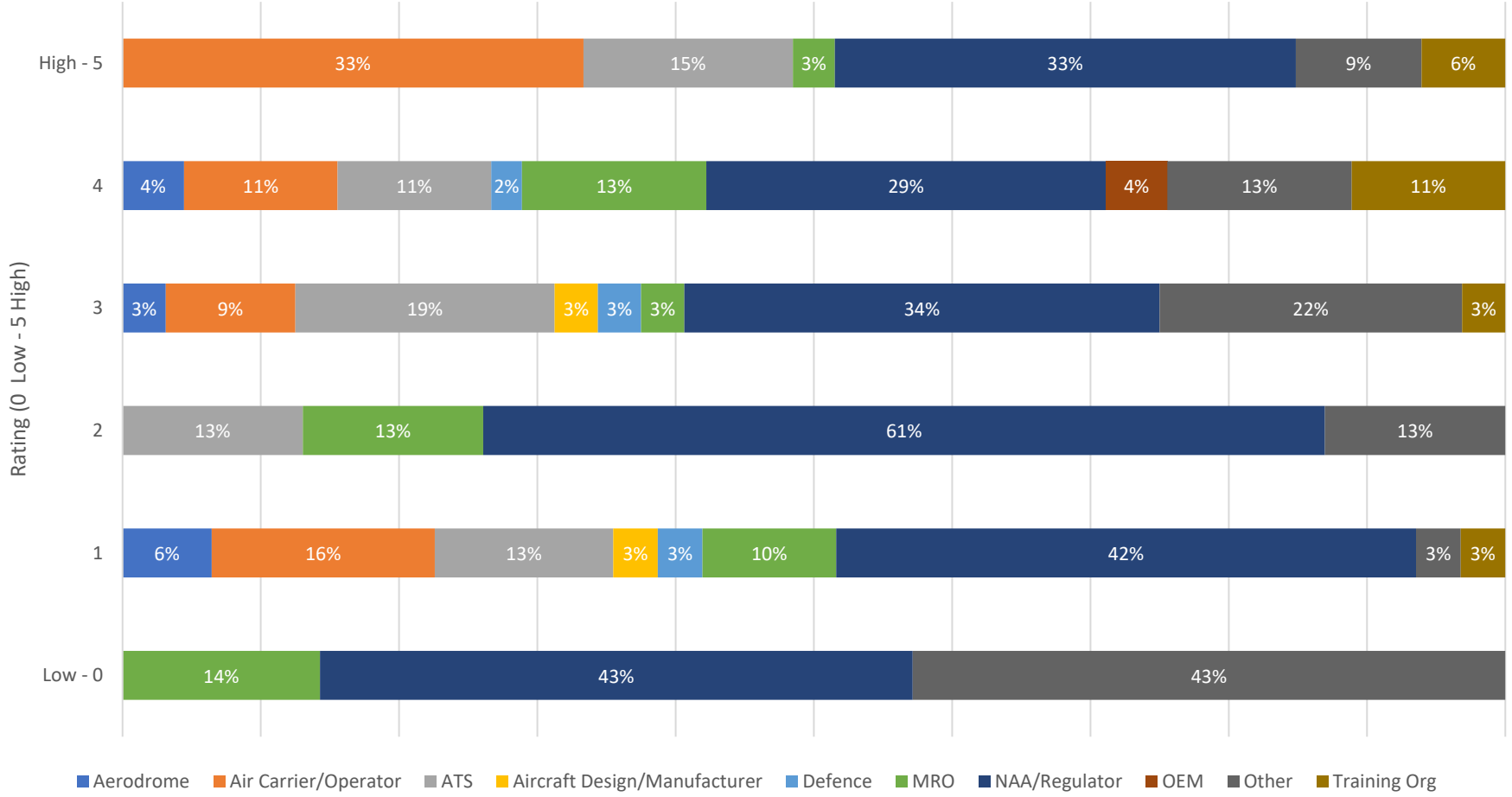
My organisation has cybersecurity policies which make use of the following tools and elements: cybersecurity culture, promotion of security by design, supply chain security for software and hardware, data integrity, appropriate access control, pro-active vulnerability management, improving agility in security updates without compromising safety, as well as incorporating systems and processes to monitor cybersecurity relevant data.




** Based on 171 responses*

# Pillar Four

**PILLAR 4 - Cybersecurity Policy**
**Responses by sector**



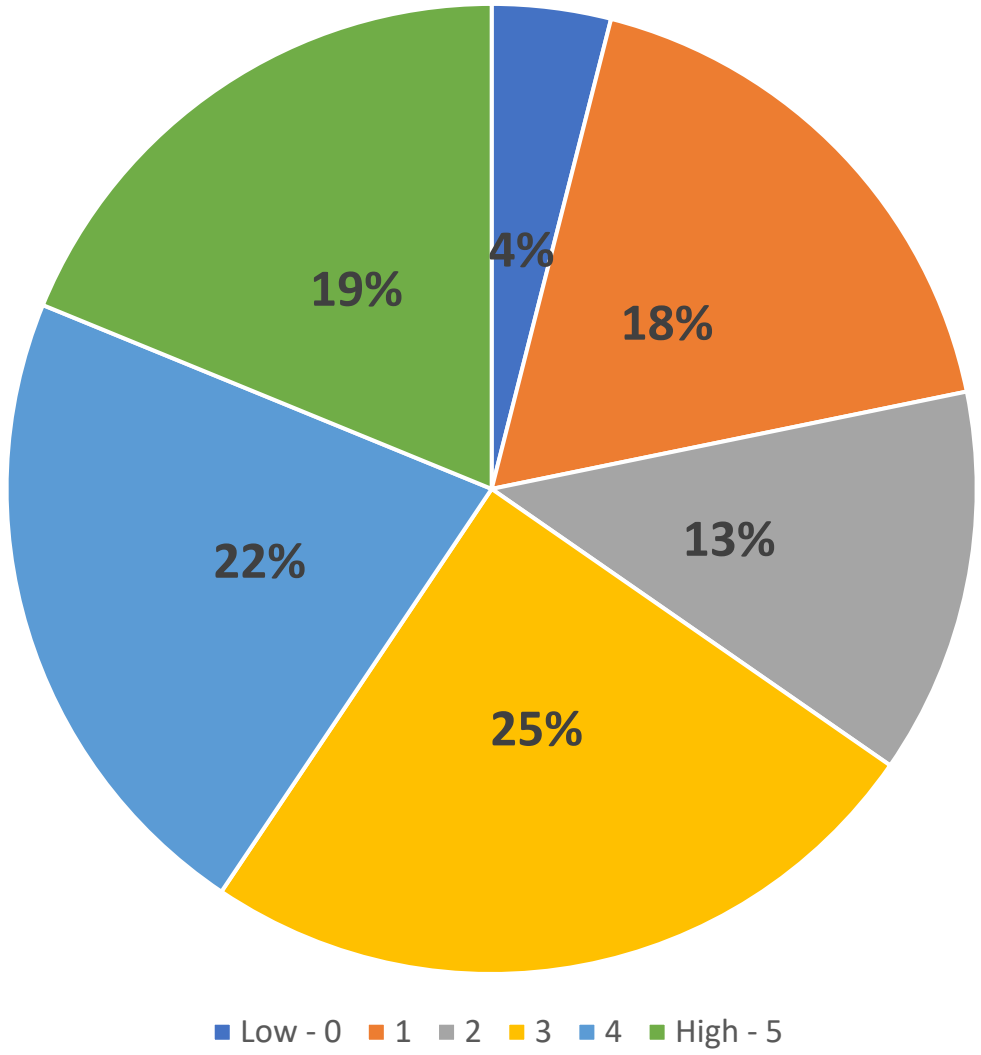

** Based on 171 responses*

# Pillar Five

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

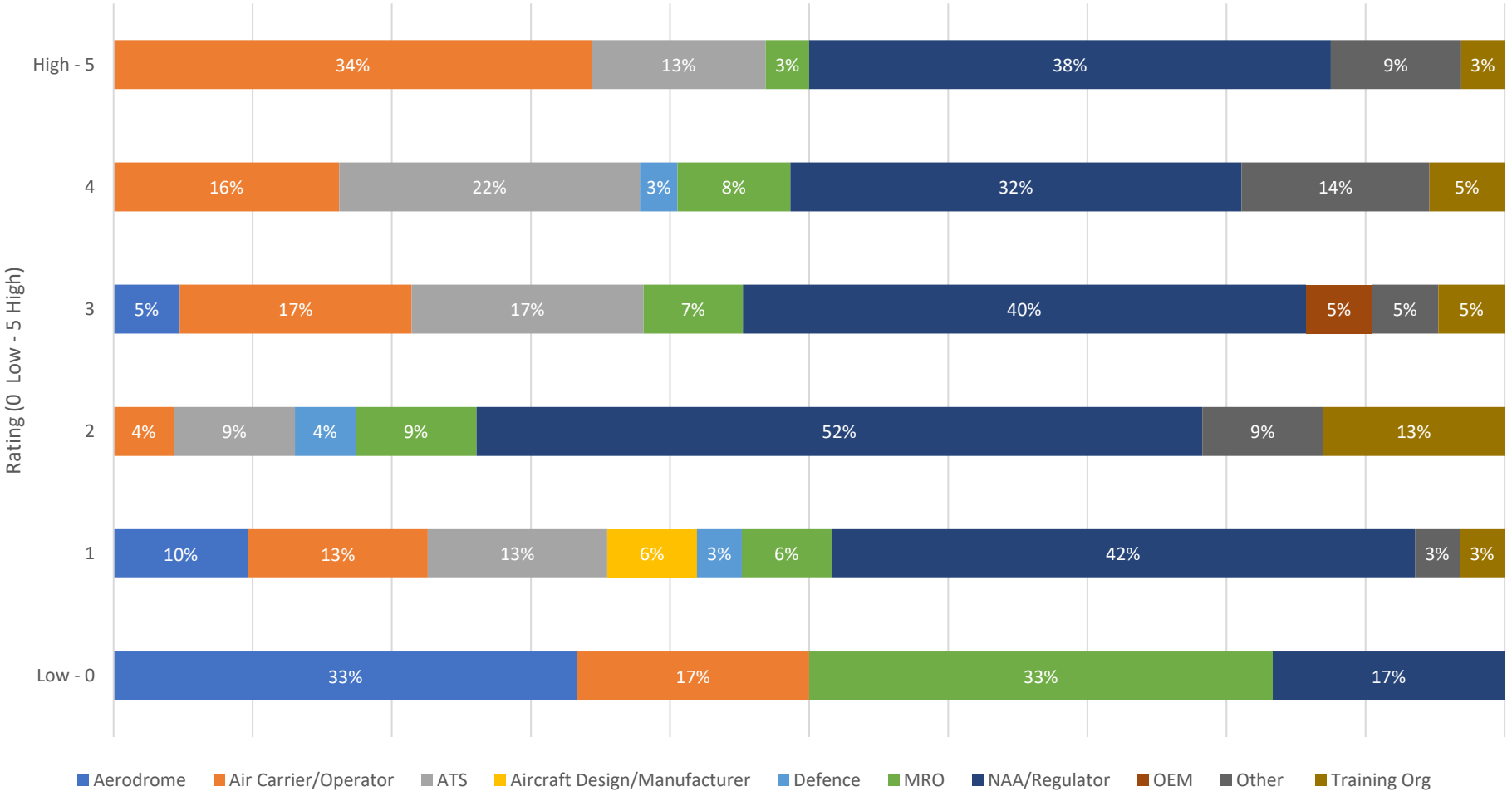
## Information Sharing

My organisation shares information on vulnerabilities, threats, events, and best practice, to enable prevention, early detection, and mitigation of relevant cybersecurity events before they lead to wider effects on aviation safety or security, including having a well-developed information culture.




** Based on 171 responses*

# Pillar Five



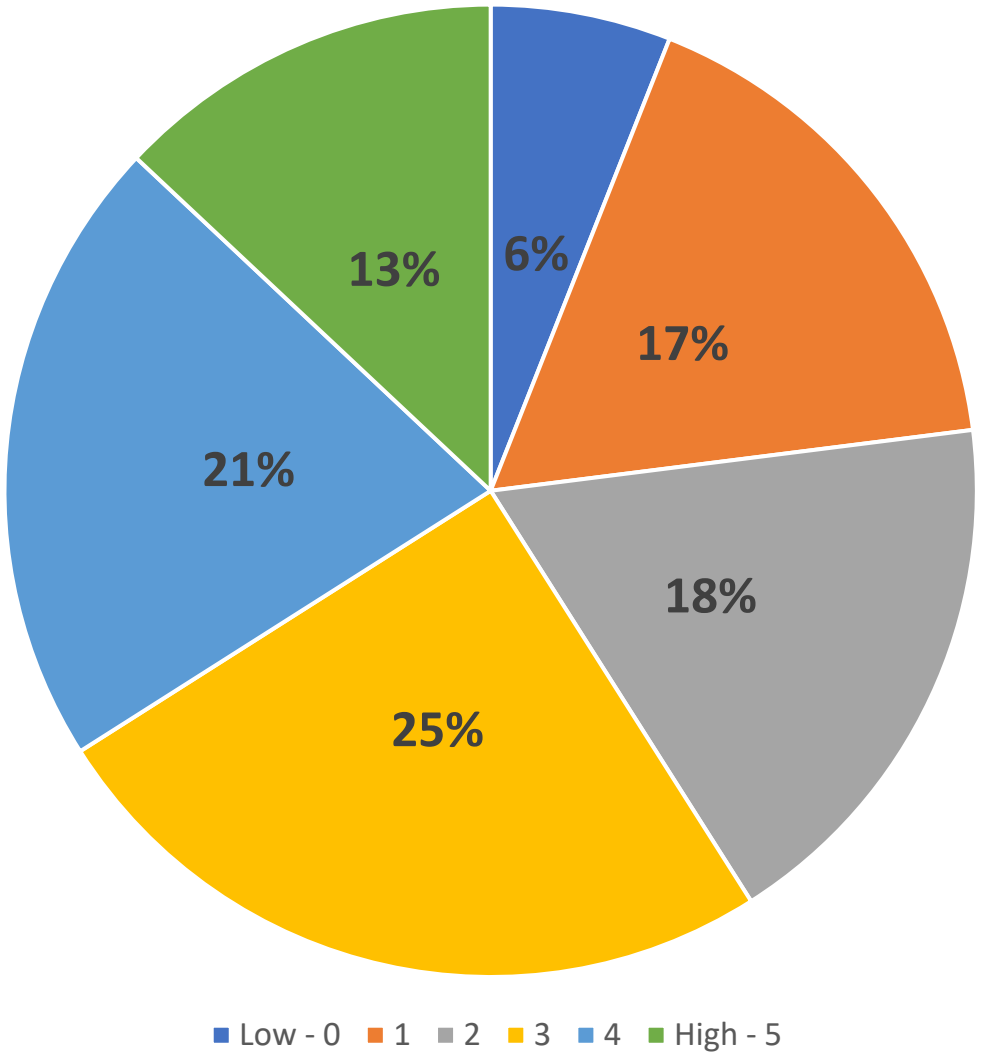

** Based on 171 responses*

# Pillar Six

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

## Incident Management and Emergency Planning

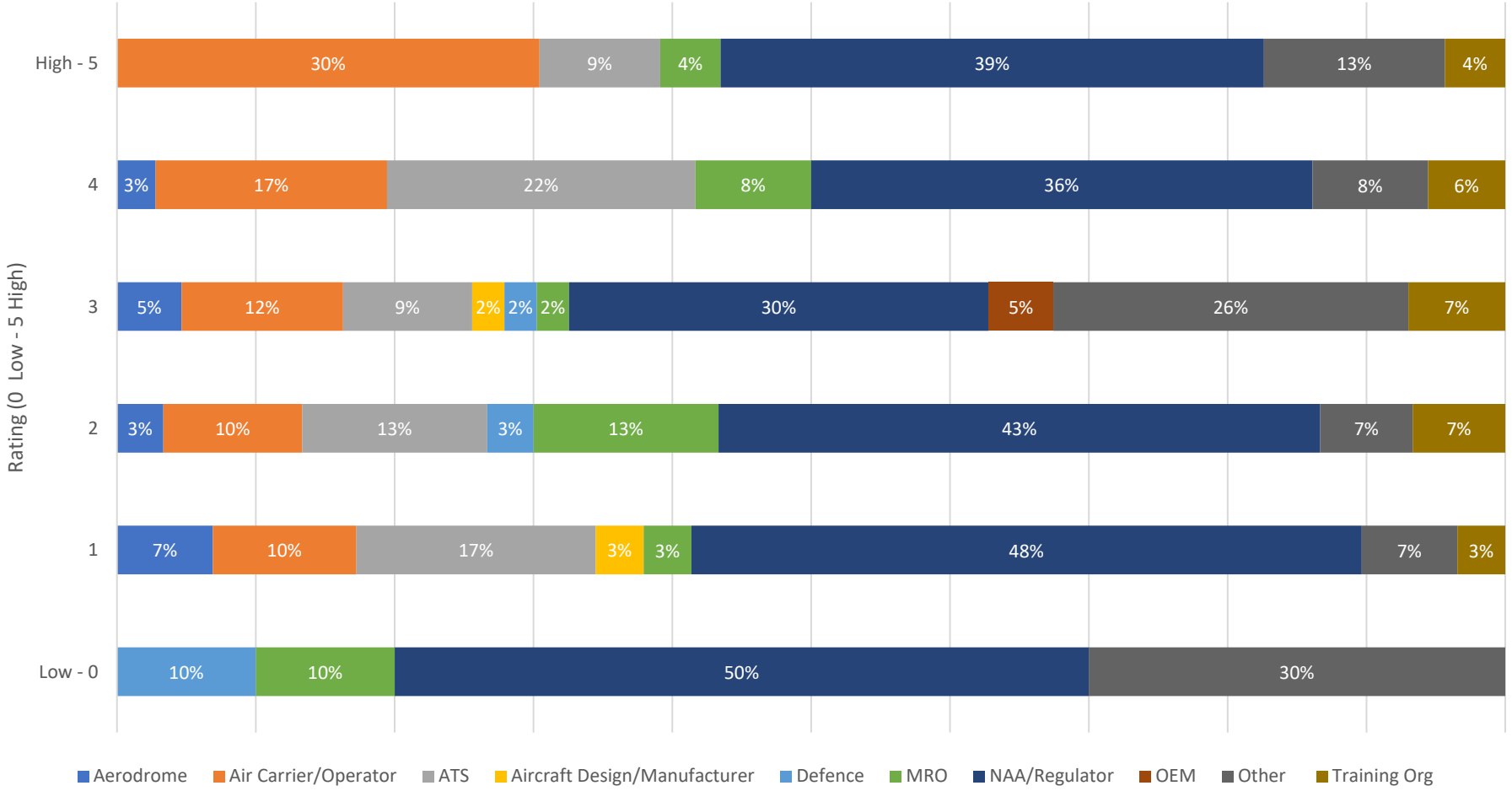
My organisation has appropriate and scalable plans that provide for the continuity of air transport during cyber incidents. To this end, my organisation makes good use of cybersecurity exercises to test incident management and emergency planning.




** Based on 171 responses*

# Pillar Six

**PILLAR 6 - Incident Management and Emergency Planning**
**Responses by sector**



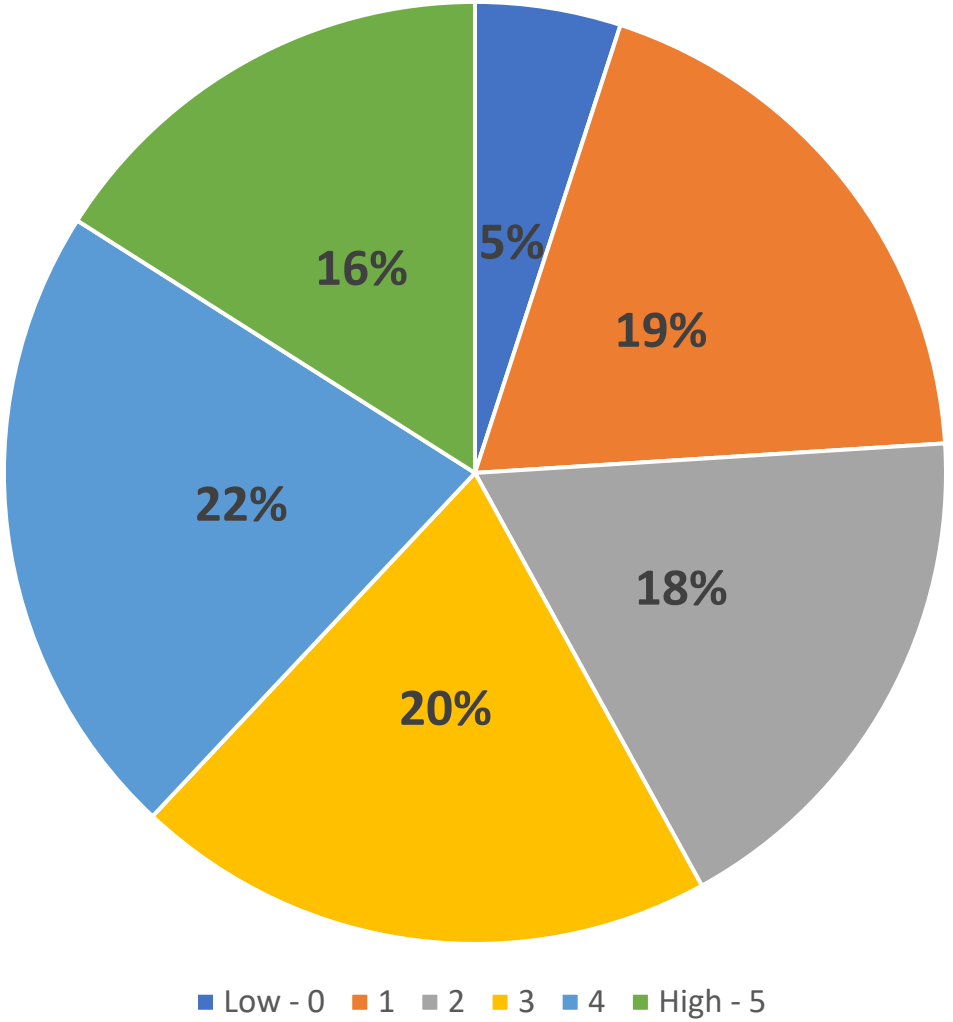

** Based on 171 responses*

# Pillar Seven

Based on ICAO's seven pillars of Aviation Cybersecurity Strategy, using a sliding scale (0-5), please rate how you feel your organisation performs against:

## Capacity building, training and cybersecurity culture

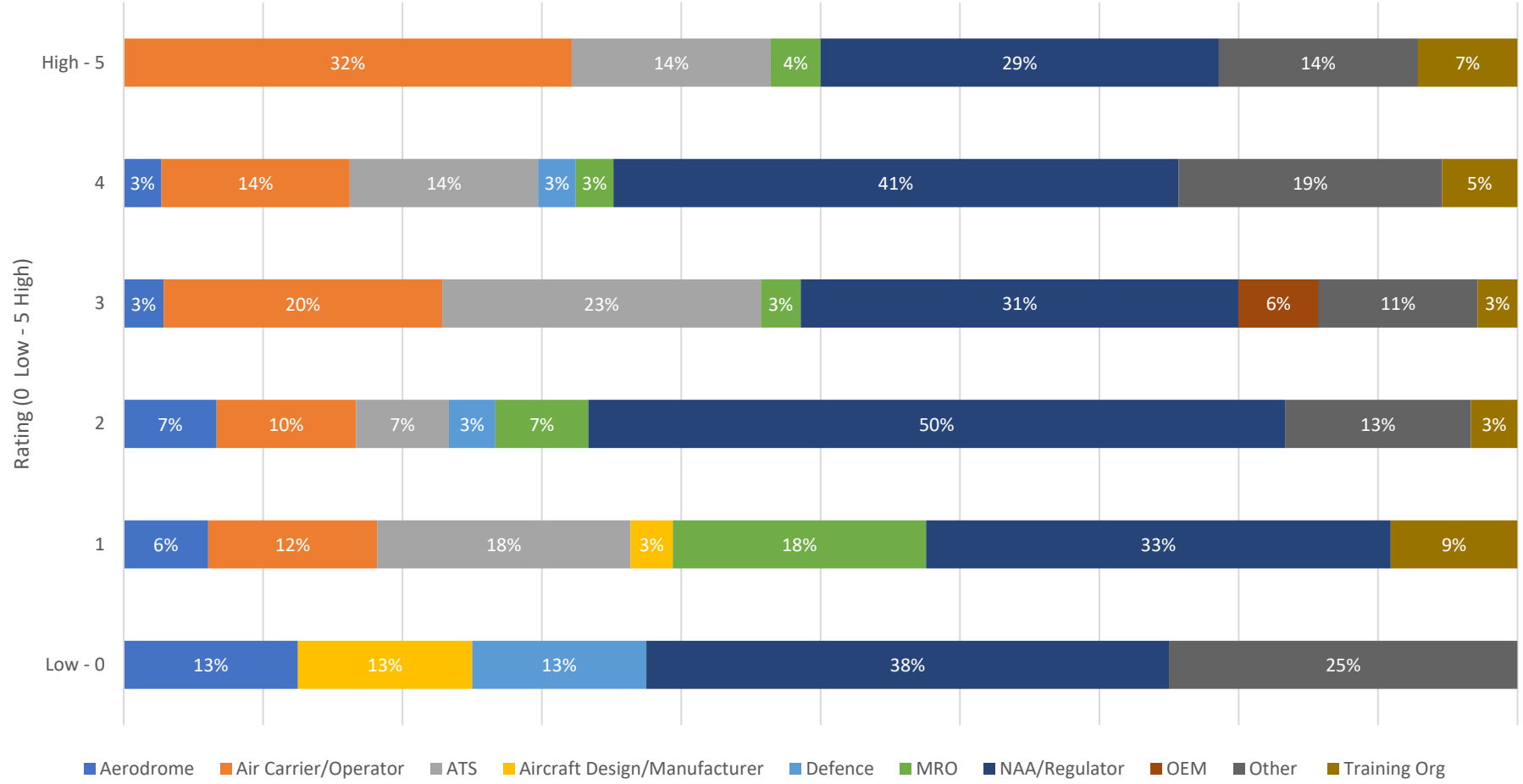
My organisation has or is taking steps towards increased numbers of personnel qualified and knowledgeable in both aviation and cybersecurity. My organisation deploys appropriate security culture promotion, as well as recruitment and training for cybersecurity. **Cybersecurity in my organisation is seen as everybody's responsibility.**




** Based on 171 responses*

# Pillar Seven

**PILLAR 7 - Capacity Building, Training and Cybersecurity Culture**
**Responses by sector**




** Based on 171 responses*

# Coffee Break

## 10 minutes

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

Or scan this QR code with your smartphone to access Slido

# 5. Cyber Threats and Challenges

- Interactive Q&A session using Slido
- Responses received in real time
- Expert Panel to react to and discuss results

---

- **Kevin Sawyer (Facilitator)**
  Head of International Operations - Aviation Security, CAAi

# 6. Harmonisation and prioritisation of cyber, safety and security risks

- **Kevin Sawyer (Facilitator)**
  Head of International Operations - Aviation Security, CAAi
- **Ho Kee-Vin (Panellist)**
  Director, Cybersecurity and Data Governance, CAAS
- **Simon Sheeran (Panellist)**
  Head of Cybersecurity Oversight, UK CAA
- **Guarav Keerthi (Panellist)**
  Executive Vice  President, Advisory and Emerging Business, Ensign InfoSecurity Singapore

# Discussion Point One

The civil aviation sector is global by nature and so is the interaction of systems and data flows that transience national borders and individual organisations. As such, holistically addressing cyber threats and risks against civil aviation must build on a global framework that is founded on cooperation and collaboration between States and all concerned stakeholders.

***How are States working together to make this happen?***

---

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

# Discussion Point Two

European Aviation stakeholders conclude that a cyber-incident may have a significant economic impact and a reduction of safety margins causing harmful effects on the population. Stakeholders acknowledge that a common strategy is necessary to reduce and mitigate the cybersecurity risk and that a collective effort is required to change the 'As Is' situation into a desired 'To Be' situation by facing the key challenges and difficulties with a robust plan.

***What developments or initiatives are you aware of to get us closer to this aim?***

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

# Discussion Point Three

The aviation sector is no stranger to risks. The discussion today focused on cyber risks, but in the real world, leaders need to deal with issues that have cyber, safety, and security risks. Sometimes these require trade-offs to be made.

***How should leaders think about handling complex issues like this?***

To participate, please use **Slido**:

- Visit: **www.slido.com**
- Event code: **3444249**
- Passcode: **qkiuwh**

# 7. Summary & Conclusions

- **Ho Kee-Vin**
  Director, Cybersecurity and Data Governance, CAAS
- **Simon Sheeran**
  Head of Cybersecurity Oversight, UK CAA
- **Matthew Margesson**
  Managing Director, CAAi


CAAS

Civil Aviation Authority of Singapore

SINGAPORE
AVIATION
ACADEMY