Corte dei conti

LA SEZIONE DI CONTROLLO

PER GLI AFFARI COMUNITARI ED INTERNAZIONALI

Composta dai Magistrati:

Dott.	Giovanni	COPPOLA	Presidente
Dott.	Giacinto	DAMMICCO	Consigliere
Dott.	Carlo	MANCINELLI	Consigliere

Nell'Adunanza del 21 maggio 2018

Visto il mandato di *external auditor* dell'*International Civil Aviation Organization (ICAO)* conferito alla Corte dei conti dal *Council* dell'ICAO e ratificato dall'*Assembly* dell'Organizzazione nella sua 38ª Sessione tenutasi il 4 ottobre 2013, nonché il rinnovo del mandato per un ulteriore triennio, deliberato, su proposta del *Council* dell'ICAO, dall'*Assembly* dell'Organizzazione nella sua 39ª sessione con risoluzione n.A39/36, in data 29 settembre 2016;

Visti i principi INTOSAI;

Visti i principi internazionali di audit applicabili all'attività delle Istituzioni superiori di controllo (*International Standards of Supreme Audit Institutions* –ISSAI);

Visto lo *Special Report* relativo al *performance audit* dal titolo: "*The Cybersecurity Framework at ICAO*";

Udito il relatore Consigliere Carlo Mancinelli ed esaminato e discusso su sua proposta lo *Special Report* relativo al *performance audit* dal titolo: "*The Cybersecurity Framework at ICAO*";

DELIBERA

di approvare lo *Special Report* relativo al *performance audit* dal titolo: "*The Cybersecurity Framework at ICAO*"

DISPONE

di trasmettere copia di detto *report* al *Secretary General* dell'*International Civil Aviation Organization* (*ICAO*).

IL RELATORE	IL PRESIDENTE
F.to Carlo Mancinelli	F.to Giovanni Coppola

Depositata in Segreteria il 19 giugno 2018

Il Dirigente

F.to Maria Teresa Macchione

Corte dei conti

SPECIAL REPORT OF THE EXTERNAL AUDITOR

INTERNATIONAL CIVIL AVIATION ORGANIZATION

The Cybersecurity Framework at ICAO

2018

The Team

All assessments are carried out by the Corte dei conti's Audit Chamber for European and International Affairs.

For this special assessment report, the team was led by Mr. Carlo Mancinelli, Counsellor, and was composed of Mr. Mancinelli himself and Mr. Stefano Penati, senior auditor. Due to the special purpose of this assessment, the team was integrated with a group of IT experts of the Corte dei conti, guided by Mr. Michele Melchionda and Mr. Luca Di Bari.

This report was approved by the Audit Chamber for European and International Affairs.

Table of Contents

Glossary and abbreviations

ANSI	American National Standards Institute
CIIP	critical information infrastructure protection
CISQ	Consortium for IT Software Quality
COBIT	Control Objectives for Information and Related Technologies
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks.(Ref: NIST)
EAAC	Evaluation and Audit Advisory Committee
EAO	Evaluation and Audit Office
ETSI	The European Telecommunications Standards Institute
FS	Financial Statements
IAS	Information management and general administrative service
ICT	Information Communication and Technology
IEC	International Electrotechnical Commission
Information Security	Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. (Ref: SANS)
ISA	International Society for Automation
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information Technology
IT/ICT security	Information Technology Security also known as, IT Security is the process of implementing measures and systems designed to securely protect and safeguard information (business and personal data, voice conversations, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions. (Ref: SANS)

ITIL	Information Technology Infrastructure Library
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology

Executive Summary

I. Our assessment focused on the preliminary analysis of the cybersecurity management at ICAO, following a specific request of the EAAC.

II. Our work took into account the audit on “Cyber security management at ICAO” carried out by the Evaluation and Internal Audit Office of the ICAO (EAO). We concluded by acknowledging the EAO recommendations and taking note of the action plan made by Management, though considering that further improvements are needed.

III. It is important to note that this report presents our assessment of the existing EAO audit as well as responses to our questionnaire, and is not a full-scale performance audit.

IV. At the end of this report, we make six recommendations and one suggestion, with the aim to add value to the ICAO cybersecurity framework, starting from EAO’s work, through the implementation of some additional measures.

Introduction

A brief resume

1. In the first year of the mandate of the Corte dei conti as external auditor at ICAO, in our report on FS 2014, we issued the suggestion n. 8, regarded "*the possibility of adding to the EAO staff a permanent IT auditor, who could perform also other kinds of audits, leaving the existing budget: a) to enhance the training program for the staff, and b) to occasionally hire external audit experts in technical matters, related to the core business activity of ICAO (the aviation sector), in order to cover risks in these technical areas*". The comment of the former Secretary General to the suggestion was "Accepted. The possibility of creating an additional post for an IT auditor will be considered as part of the budget setting process for the 2017 to 2019 triennium".
2. The lack of IT audit resources, in fact, was always reported by the EAO, which, for this reason, was also obliged to postpone the internal audit of the "Systems Development Life Cycle", planned in its work programme for 2016.
3. Due to this lack of dedicated and specialized resources in EAO to carry out IT audits, the Chairman of the EAAC, at the end of 2016, asked the External Auditor to include, in its audit plan for 2017, an IT audit on the "cyber security at ICAO", instead of one of the two annual performance audits requested by the Council when the Corte dei conti's mandate was renewed.
4. The President of the Chamber for International Affairs agreed to carry out a "preliminary analysis" on this issue, instead of a performance audit according to International Standards, partly in view of both the economic resources and technical requirements needed in order to complete an IT audit, which are not comparable with the resources normally required by an ordinary performance audit. Anyway, in this report we will use the word "audit" as a synonym of "assessment" and also "preliminary analysis".
5. The request of EAAC's Chairman was presented to the Corte dei conti rather contemporarily with the EAO's draft 2017 work programme, which was submitted by the Chief EAO for comments on 19 October 2016; the programme did not include any IT audit, with the motivation that "No IT audits will be carried out in 2017 due to an ongoing lack of resources in EAO. These are specialised audits which need to be undertaken by, and managed by, a trained IT auditor".
6. However, in the final version of the document presented to the 209th Council session (C-WP/14528), EAO did include an audit on "Cybersecurity" in its 2017 work programme. Chief EAO referred that the Secretary General asked to delete the

sentence above and to insert an IT audit in the EAO final 2017 work programme, considering that the consulting allotment attributed to EAO in 2017 should be enough, or if necessary could be increased, to pay for an external consultant. In spite of his reservations due to the lack of resources (both professional and economic), Chief EAO agreed to Secretary General's request, proposing an IT audit on "Cybersecurity", as this topic was very high in EAO's risk assessment. It should be noted that this proposal was made before the discovery and disclosure of the compromises of ICAO systems.

7. With regard to the potential duplication and overlapping of the two audits, programmed on the same topic, we highlight that, although we recognise that the IT environment presents potential inherent and control risks and although the function of the External Auditor differs from that of the internal auditor, our work will consider EAO's risk analysis, as presented in its 2017 Work Programme.

8. Furthermore, in order to avoid possible overlapping, we had several meetings and exchange of ideas with EAO and the IT expert hired to carry out the audit. We then consulted our experts, with the aim to give an added value to the work done by the EAO.

Scope and approach

9. Notwithstanding the considerations listed in the introduction, we also believe that an analysis has to be conducted in the spirit of helping the Organization to progress in its processes and procedures of cybersecurity. About the wording, we will mainly use, in this report, the term “cybersecurity” to represent the object of our work. However, we could also use the locutions “IT security” or “ICT security” with the same meaning (although we acknowledge the difference), for instance quoting some sentences or parts of other works.

10. For these reasons, the main questions, on which our work was based, were:

    (a) Is the cybersecurity at ICAO managed effectively and efficiently?

    (b) Is the ICAO cybersecurity framework compliant with international standards and practices such as ISO 270001 and NIST?

11. The work was carried out from November 2017 until end of March 2018. The timeline took into account the EAO’s related audit. It is important to highlight that EAO shared transparently and regularly information with the External Audit from the preliminary draft till the final report.

12. This work focused on the assessment of the finding and results gathered by EAO through its audit on “Cybersecurity management at ICAO” (IA/2017/2) and on further compliance with other international standards and practices, as recommended by our experts.

13. The audit work was conducted by (i) means of two checklists, mainly based on ISO 27001, prepared by our experts to the IT management, (ii) the creation of a focus group of internal IT experts chosen by Corte dei conti, which has closely cooperated with the auditors, (iii) the analysis of relevant documents (reference to paragraph 15 below) and (iv) interviews and constant exchange of information with EAO.

14. In particular, the provided answers have been shared with the EAO for the purpose of its audit and submitted to our experts, and duly analysed.

15. The data collected is all document-based; below, a non-exhaustive list:

    (a) Information Security Management Group (ISMG) – Terms Of Reference;

    (b) Information Security Management System – Terms Of Reference;

    (c) ICAO Administrative Instructions on the Acceptable Use of ICT Resources;

    (d) Administrative Instructions on Identity and Access Management Access Control on ICAO IT resources;

    (e) Administrative Instructions on Information Classification and Handling;

    (f) ICAO Information Security Administrative Instructions;

    (g) ICAO - Internal Audit Report - ESI 20161122 V1.0.pdf ;

(h) Internal Audit 25102016_AO ISMS REC XXX - ICAO v1 FINAL.docx;

(i) the Internal Audit Report on “Cybersecurity management at ICAO” (IA/2017/2)

(j) ICT_Security_ Disaster Recovery Standardsv101.docx;

(k) InformationSecurityIncidentManagementProcedure.docx;

(l) InformationSecuritySDLC.docx;

(m) ISO 27001.Statement of ApplicabilityV2.0.1.docx;

(n) ITChangeControlProceduresRulesRegulations.docx;

(o) Technical Instructions on Continuous Vulnerability Monitoring & Management;

(p) Critical_Vuls_2017.xlsx.

16. The analysis was focused on the Headquarters’ data centre hosting information assets and supporting technologies.

17. The analysis’s scope covers:

A. ICAO information assets processed, stored and transferred in the business systems which are operated and maintained by ICAO ICT operation.

B. ICAO ICT business functions/processes

C. The ICT services supporting business functions

D. The ICT services provided in the HQ to preserve the confidentiality, integrity, and availability of ICAO information assets

E. The ICT support personnel providing and managing the ICT services

18. Furthermore, it is important to highlight that compliance with good-practice framework created by international professional association for information technology (IT) management or IT governance and audit (as for instance COBIT 4.1 and 5.0 by ISACA or ITILv3), and, also all third parties providing services were out of the scope of our audit, as well as hosted/external services, customer services infrastructure from third-party sites, or hosted outside ICAO headquarters, also outsourced functions, processes and suppliers, as well as ICAO regional offices.

Observations

Background Information

19. Overall, cybersecurity controls are safeguards to avoid, detect, or minimize security risks to information and systems. Cybersecurity controls, without following an IT security standard such as implementing an information security management system (ISMS), tend to be somewhat disorganized.
20. ISO/IEC 27001 is an ISMS standard, a part of the ISO/IEC 27000 family of standards, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001 specifies an ISMS that provides a framework of policies and procedures that includes all legal, physical, personnel and technical controls involved in an organization's information risk management processes.
21. In general, ISO/IEC 27001 requires, beyond other requirements, that management (i) regularly assesses the organization's information security risks, taking account of the threats, vulnerabilities, and impacts; (ii) designs and implement a comprehensive set of security controls and (iii) ensures that the information security controls meet the organization's information security needs on an ongoing basis.
22. Other standards in the ISO/IEC 27000 family of standards provide additional guidance on certain aspects of designing, implementing and operating an ISMS, for example on information security risk management (ISO/IEC 27005).
23. Furthermore, ISO/IEC 27032:2012, as defined by ISO, "*provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: (i) information security, (ii) network security, (iii) internet security, and (iv) critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides: (i) an overview of Cybersecurity, (ii) an explanation of the relationship between Cybersecurity and other types of security, (iii) a definition of stakeholders and a description of their roles in Cybersecurity, (iv) guidance for addressing common Cybersecurity issues, and (v) a framework to enable stakeholders to collaborate on resolving Cybersecurity issues*".
24. Further to the ISO family, cybersecurity-related standards, guidelines and best-practices to ensure the availability, confidentiality and integrity of the information assets of an organisation with the principal objective to mitigate risks inherent in the cyber world to the business defined acceptable level, are, *inter alias*:
    i. ETSI Cyber Security Technical Committee (TC CYBER);
    ii. CISQ (Consortium for IT Software Quality);
    iii. NERC (North American Electric Reliability Corporation);

iv. NIST (National Institute of Standards and Technology), in particular the Cybersecurity Framework (CSF);

v. ISA/IEC-62443 (formerly ISA-99) prepared by International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) document.

Our Analysis

ISO certification requested by ICAO management

25. Organizations may choose to be ISO-compliant officially by an accredited certification body and, in general, what controls will be tested as part of certification to ISO27001 is dependent on the certification auditor. This can include any controls that the organisation has deemed to be within the scope of the ISMS and this testing can be to any depth or extent, in the way that the auditor assesses as needed to test that the control has been implemented and is operating effectively.
26. ICAO management determines the scope of the ISMS for certification purposes and may limit it to, for example, a single business unit or location.
27. During our work we observed that the ICT management requested ICAO ISMS to be ISO-compliant; Management referred that ICAO ISMS is informally compliant with ISO 27001, but no certificate has been obtained yet. Furthermore, at the date of our assessment, several recommendations have been issued by the certification entities, many of which are yet to be implemented.

Our assessment on the checklists

28. In relation to the checklists of ISO 27001 compliance, we noted that some of the answers provided were not addressing the specific point and/or supporting evidences were not duly provided.
29. Chief EAO agreed to continue his assessment requesting to the accountable officer more clarification on the matters.
30. During our audit of the answers provided in the checklist, we observed that some questions were not exhaustively answered; in addition, some weaknesses were detected and could be summarized as follows:

    I. The ISMS includes a large number of documents, determined to be necessary for the management of information security, electronically stored and available to those who require access. We observed that not all documents were in the appropriate format, or accessible, neither contained information that they have been subject to control (e.g., version numbers, evidence of approval, etc.).

II. The organization has defined and documented a risk assessment and treatment process, which presents criteria relating to the impact and likelihood of risk events, but lack of criteria related to risk acceptance. Risks levels are based on likelihood and impact, then adjusted to reflect the criticality of the business system and the impact on the organization. However, it was not determined how the calculation of risk level was performed, in a manner that could provide comparable and valid results.

III. There was no evidence of existing mechanisms to record nonconformities and opportunities for continual improvement, nor records to indicate that ICAO identified any nonconformities or opportunities for improvement. This may indicate that nonconformities or incidents have not arisen, but also that nonconformities are not being identified, recorded and properly addressed.

31. All this can be attributed, in part, to the lack of maturity of security capabilities to identify, prevent, detect, response to and recover from cyber threats. So, ICAO should develop an action plan to handle these areas, provide the required resources to implement the plan, and ensure that the progress of the action plan is monitored to secure completion within agreed timescales.

Several recommendations on "Cybersecurity management at ICAO" issued by EAO to be implemented

32. As explained in our introduction, EAO carried out an audit on "Cybersecurity management at ICAO". We received the final version of the Internal Audit Report (IA/2017/2) on 14 March 2018 by Chief EAO; we discussed the findings and results gathered by EAO.

33. As stated in its report by EAO, the objectives of that audit "*were to:*

- *Assess, in comparison with ISO 27001 standards, the effectiveness and efficiency of recent organizational measures taken to enhance the Information Security governance, risk management and controls, which may include but may not be limited to the organizational positioning, policies, procedures, corporate risk registers and staffing arrangements.*
- *Assess the effectiveness of the information security management action plan (CyberSec Action Plan) put in place to address the organizational weaknesses (staffing, processes and technology) in information security and related areas*".

34. Consequently, the scope of the audit was oriented to cover "the effectiveness of the management action plan in remediating the identified vulnerabilities that were exploited to compromise ICAO information systems by unknown threat actors", with the clarification that "*the Audit did not cover the information security requirements specific to Regional Office ICT, Council or Delegate information security*".

35. The Internal Auditor issued eighteen (18) recommendations, split into four areas:

A. “*Governance*”, with six recommendations;

B. “*Staffing*”, equally with six recommendations;

C. “*Process*”, where the recommendations were four;

D. “*Technology*”, with two recommendations.

36. We also noted that some of them contain different actions to be implemented, increasing the number of findings and actions required.
37. It is worthwhile mentioning that information gathered during the respective audits have been exchanged and discussed with Chief EAO throughout the reference period.
38. All recommendations have been accepted by Management, whose action plan is shown in the Annex 2 of the report. Looking at this, we note that the first deadline for the implementation is the third quarter of this year, only for one recommendation, for some the implementation is provided for the end of 2018, most of them should be implemented during 2019, whereas one requires a longer period, until the end of 2020.
39. After having analysed the Report, we share the EAO’s view and the eighteen (18) recommendations issued, which ICAO management should implement.
40. In particular, in relation to EAO’s Recommendations n. 3 (“Network Segmentation”), n. 7 (“Telework, Remote Access and Mobile Devices”) and n. 13 (“Expand Log Management”), we have further detailed them, and we have issued three further ones (refer to “Conclusions and Recommendations Section”).
41. Considering the action plan’s deadlines and the new measures recommended with this report, a future revision of the framework is certainly needed, but only after having assessed, through a deep follow-up exercise, the full implementation status of all the measures.

A full assessment of cybersecurity at ICAO against best-practices and internationally-accepted standards, further to ISO, is currently underway, but not yet completed.

42. As seen above (see para. 33), EAO’s audit on “Cybersecurity management at ICAO” focused, in particular, on the compliance to ISO standards, in particular to ISO 27001 and its background, as mentioned in the report, arise from the fact that “*ICAO has suffered numerous breaches of its ICT systems with a potentially severe breach occurring in 2017*”.
43. As already stated in previous paragraphs (for instance, refer to paragraph 24), in addition to the international standards related to the ISO family, there are several cybersecurity-related standards, guidelines and best-practices, built for protecting the cyber environment of an organization, with the main goal of mitigating cyber risks (some of them are better specified in mentioned paragraph).

44. We consider as a real added value that ICAO management will assess cybersecurity at ICAO evaluating the current ICT security framework against these best-practices and internationally-accepted standards; it is worthwhile mentioning that, on the contrary, we observed that such analysis has not yet been performed by ICAO Management. In this regard, Management agreed and clarified that they will undertake additional assessments as recommended when ICAO security capabilities becomes more mature, as (also) recommended by EAO in its report (see also paragraph 27).

Conclusions and recommendations

45. By our analysis, we conclude that EAO's audit on the cybersecurity management at ICAO correctly sets the major issues, and the recommended measures should be implemented.
46. Notwithstanding this conclusion, we highlight that some other elements merit further analysis to improve the efficiency and effectiveness in this sensitive area. In this sense:

Recommendation n. 1.

47. In relation to the EAO's recommendation n. 3 ("Network Segmentation"), where is recommended performing "*a redesign of the existing LAN segmentation to better accommodate ICAO business and security needs*", we share the EAO's view and further recommend that ICAO start from a collection of services maps that show relationships between every business service and their IT components. In this way, it should be possible to applicate segregation "vertically" (front-end, DMZ, back-end, etc.) but also horizontally, relying on the different critical level of each service.

Comments by Secretary General:

Recommendation accepted.

Already, a set of projects in the Cybersecurity Action plan address the issue of Network segmentation. A preliminary report by a reputable third-party Information Security service provider was presented to ICAO, which will form the basis of the network re-design, and the projects are planned for 2018. The new design will be informed by the relevant Business Service vs. ICT component maps as recommended. A comprehensive programme for Enterprise Architecture for ICT within its own dedicated unit has also been established in the ETS Section. This unit will oversee the creation and maintenance of these maps.

Recommendation n. 2.

48. With reference to the EAO's recommendation n. 7 ("Telework, Remote Access and Mobile Devices"), which recommends that "*a new Instruction should be developed considering controls from the ICAO Acceptable Use document to be combined with controls for teleworking and remote access*", we share the view of the internal auditor and we recommend also that ICAO, apart from developing of a technical instruction about teleworking and remote access, develop a strict policy to regulate such activities, as, for instance, which services are available for teleworkers, which information can be accessed through telework, etc.

Comments by Secretary General:

Partially accepted. Teleworking is outside the scope of this audit. ADB/ETS will develop Technical Instructions on Remote Access to ICAO IT resources. These instructions will fully document the services currently in place including the security criteria to be applied and the user's obligations when using such services.

Recommendation n. 3.

49. Referring to the recommendation n. 13 of the EAO ("Expand Log Management"), where is recommended "*implementing a full log management system within and controlled by dedicated ICT log management personnel and revising SIEM input requirements to take into account full log inputs and expected additional technical inputs*", we share the EAO's view and we recommend, in addition: (i) that logs be collected in order to prevent non-repudiation, e.g. sending them in real time to a central repository where they are digitally signed, (ii) that all system be synchronized on the same time server, (iii) that the personnel that has the administrative assignment on log management infrastructure be dedicated to security monitoring, without having at the same time other administrative tasks (even in other security areas, e.g. firewall administration), (iv) defining a policy of log retention, which considers how long data must be stored, and (v) correlating events and spotting individual anomalies or patterns of behavior that may indicate a security breach also based on past security incidents.

Comments by Secretary General:

Accepted in principle and subject to the provision of necessary funding in the regular budget to implement the recommendation. An audit and transaction log management policy has been implemented. An information security operation center roadmap along with a SIEM implementation plan is being executed and monitored using key goal indicators (KGIs). A log system will be implemented for the entire ICT environment to further enhance ICAO information security capabilities. ICAO has outsourced some information security operations functions and will be looking for other opportunities to outsource security functions requiring a high degree of expertise and intensive workload.

Recommendation n. 4.

50. Considering that the current scope for the ISMS, as designed, may not accurately describe the boundaries and applicability of the ISMS itself, because some of the controls required for designating risks had been bypassed (see para. 30), we recommend that ICAO undertake a review to include controls of Standard ISO 27001:2013 that are currently neglected, such as A.14.2.7, outsourced development, and control objectives A.15.1 and A.15.2, related to third parties.

Comments by Secretary General:

Accepted. ICAO recently created a CISO position and is in the process of filling the position. Once the CISO is appointed, reviewing the current ISMS situation and the appropriate control standards will be addressed as a matter of priority.

Recommendation n. 5.

51. For a more focused analysis on cybersecurity aspects, we recommend that Management adopt a specific framework, like NIST cybersecurity framework, possibly using an integrated approach with a robust IT management framework. Firstly, and in particular, the "*detect and respond functions*" should be implemented, to allow the ICAO to face sophisticated attacks, like multi-stage malware and advanced persistent threats, that can compromise not only data but also critical services or infrastructures.

Comments by Secretary General:

Accepted. ICAO recently created a CISO position and is in the process of filling the position. Once the CISO is appointed, reviewing the Information Security posture and selecting the best security framework will be addressed in priority. In 2017, ICAO conducted a comprehensive security posture assessment using ISO27001 and the NIST framework. Based on this information, ICAO Information Security drafted its strategic plan and developed the roadmap to achieve the required security capability maturity level.

Suggestion n. 1

52. Considering the core business of the organization, we suggest that Management consider the Framework for Improving Critical Infrastructure Cybersecurity released by NIST. It is worthwhile mentioning that this document is still in draft, however, in our opinion, it has important insights about the mentioned themes.

Comments by Secretary General:

Suggestion accepted, will be considered.

Recommendation n. 6.

53. We recommend that Management implement a successful cybersecurity strategy, to define a cyber threat information sharing network, which can increase the efficiency and effectiveness of an organization's cybersecurity capabilities. As an example, NIST Special Publication 800-150 can be used as a guideline to help the organization to establish information sharing goals, identify cyber threat information sources, engage with existing sharing communities, etc.

Comments by Secretary General:

Accepted. ICAO is already participating in the UN cyber threat network as well as civil aviation threat intelligence.