Corte dei conti

SPECIAL REPORT OF THE EXTERNAL AUDITOR

WORLD METEOROLOGICAL ORGANIZATION

The cyber security at WMO

2023

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, Ms. Angelica Cofano, Mr. Gianluca Antonelli and Mr. Pawel Jacek Szubert.

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

Table of Contents

Glossary and abbreviations

BIA	Business Impact Analysis
BC	Business Continuity
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks. (Ref: NIST)
DR	Disaster Recovery
EMM	Enterprise Mobility Management
EPS	Endpoint Protection Systems
IAS	Information management and general administrative service
ICT	Information Communication and Technology
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.
IDS	Intrusion detection systems
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.
IOO	Internal Oversight Office
IPS	Intrusion prevention systems
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISO/IEC 27000 family	A collection of standards that cover best practice in data protection and cyber resilience.

ISO/IEC 27001	ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS) and their requirements. This standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
ISO 22301	A standard that specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise.
IT	Information Technology
IT security	See ICT Security
ITIL	Information Technology Infrastructure Library
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework v. 1.1
Oracle EBS	Oracle e-business suite
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOC	Security Operation Center
XDR	Extended Detection & Response
WAF	Web applications firewalls
WMO	World Meteorological Organization

Executive Summary

I. Our assessment focused on information & cyber security framework, in particular processes and software present in WMO against the NIST Cyber Security Framework (CSF), in order to assess their effectiveness and efficiency.

II. In relation to our risk assessment, we considered this audit in our work programme for 2022. Our decision was further corroborated by a specific request made by the Secretary-General of the WMO.

III. Our work took into account the audit on “Internal Audit –Cyber Security Engagement 2021-IAS-05” carried out by the Internal Oversight Office (IOO) of WMO. We concluded by acknowledging the IOO recommendations and taking note of the action plan made by Management, though considering that further improvements are needed.

IV. It is important to note that this report presents our assessment of the existing Cyber Security framework, mainly focusing on the shared evidence and responses to our questionnaire.

V. At the end of this report, we make 9 recommendations and 5 suggestions with the aim to add value to the WMO cyber security framework, through the implementation of some additional measures.

Introduction

A brief resume

1. There were a number of attempts to divert funds from WMO following compromise of business email in September 2020. The cyber-attacks in 2020/21 likely started with a weak password and stolen credentials. The incident underlined the importance of having adequate measures in place and a strong cyber security culture. People are the biggest cause of security breaches, whether it is because they click on a link in a phishing email or hold a door open to an intruder who follows them into an office building. Access control is at the very heart of cyber security, which depends on organizations being sure that users are who they say they are and that they have permission to utilize specific network resources or to enter restricted areas. Not only does access control serve to secure assets, but, in the event of a breach, it can also help to trace actions and to determine the cause.

2. Security on the Internet and other networks is a subject of growing concern. Organizations around the world, in both government and industry sectors, are seeking ways to address and manage cybersecurity risks, including via baseline cybersecurity measures that can be implemented as requirements or guidance. The demonstrated security and economic value of utilizing existing best practices to develop approaches to cyber risk management has led organizations to assess how to use and improve upon existing approaches.

3. At the end of 2021, based on our risk assessment and taking into account what had been highlighted in the report of the Chair of the Audit and Oversight Committee to the EC-73, and – furthermore – accepting a specific request made by the WMO Secretary-General, we included an IT audit on the “cyber security at WMO” in our audit programme for 2022.

4. In this report we will use the word “audit” as a synonym of “assessment” instead of a performance audit according to International Standards

5. In accordance with the needs expressed by the WMO Management, the audit work was postponed until the new CIO joined the WMO and had full knowledge of the framework. Some informal meetings were held in October 2022, in order to acquire the preliminary information necessary for defining limits and scope of the audit.

Scope and approach

6. We conducted this analysis 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, by quoting some sentences or parts of other works.

7. For the above reasons, the main questions, on which our work was based, were:

   (a)Is the cybersecurity at WMO managed effectively and efficiently?
   (b)Is the WMO cybersecurity framework compliant with international framework NIST?

8. The work was carried out from January 2023 until April 2023. It is important to highlight that WMO shared transparently and regularly information with the External Audit, from the preliminary approach till the final report.

9. Our work focused on the assessment of the cybersecurity five areas: Identify, Protect, Detect, Respond and Recover, and on their compliance to NIST CSF and with other international standards and practices, as recommended by our experts.

10. The audit work was conducted through: (i) NIST CSF framework version 1.1 and a specific checklist, 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; (iv) interviews and constant exchange of information with WMO.

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

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

    1) *ID.AM.1 - Asset Inventory*
    2) *WMO - Network Infrastructure Update - ToRs Final*
    3) *ID.AM.2 - Service Catalog*
    4) *ID.AM.3 - IT System Inventory*
    5) *ID.AM.4 - Endpoint Manager*
    6) *organigram of the Date Exchange and ICT Division (DEICT)*
    7) *ID.BE.2 - Chapter 1 - INTERNAL ORGANIZATIONAL MANAGEMENT - January 2023*
    8) *ID.GV.2 - Network Diagram*
    9) *ID.GV.1 - ERP Diagram*
    10) *ID.GV.4 - CyberSecurity Org Chart*
    11) *Information Security Plan 2022*

12) *.ID.GV.5 - WMO Information Security Policies Framework*
13) *Computer Security Incident Handling Procedure 11-9-2007 OCR*
14) *Information Security Policy (2007)*
15) *WMO Cyber Security Policy 2020*
16) *WMO Information Security Policy v2.0 (Under approval)*
17) *policy on ICT use July 2007*
18) *WMO Acceptable Use Standard v2.0 (Under approval)*
19) *Privileged Access Management and Review Procedure v3.1*
20) *WMO Information Security Risk Management Procedure*
21) *WMO Password Management Standard*
22) *WMO IT Standing Instruction Framework 2020 v1*
23) *ID.RA.1 - WMO Information Security Risk Management Procedure.pdf*
24) *Service Note No. 29/2020 Introduction of chapter 14 of the standing instructions on risk management*
25) *ID.RA.2 - Risk Treatment Plan*
26) *2022 08 - IT CyberSecurity Metrics*
27) *2022 07 - IT Risk Assessment*
28) *AC-34 Doc 4 on risk management and Annex 1: Risk Catalogue*
29) *ID.RM.2 - ISSAC Meeting Minutes*
30) *EC-73 Decision on risk appetite statements*
31) *ID.SC-2 - WMO General terms and conditions template*
32) *ID.SC-2 - Security clauses in contractual agreements*
33) *WMO Password Policy 2020 – ELIOS*
34) *WMO_User Account Management Procedure-Final*
35) *System Administrator Access Review Procedure v2.2*
36) *System Administrator and Database Management Access Review Procedure v3.0*
37) *AD Privileged User Account Review Q3 2021 v3*
38) *WMO Mobile Device and Teleworking Policy 2020*
39) *Authorization Matrices ver 2 2019.09.03 (approved by ASG)*
40) *Tables of Authorization Matrices 2020.11.30 submitted to GS*
41) *PR.IP.8 - WMO - Joiner Process(Main KB)*
42) *PR.IP.8 - WMO - Leaver process for WMO Staff*
43) *PR.AC.9 - 2022 Q4 - AD Privileged User Account Review*
44) *PR.AT.1 - Information Security Bulletin - Password Security*
45) *PR.AT.1 - Information Security Bulletin - Phishing emails using misleading domains*
46) *PR.TR.1 - 2022 11 - Information Security Awareness - Phishing*
47) *Change Management Procedure*
48) *Information Risk Management Procedure - Annex A*
49) *Backup and Restoration Procedure*
50) *PR.IP.3 - Audit Tracker*
51) *Report 2021-05- Cybersecurity Final*

52) *PR.IP.5 - ERP SDA*
53) *PR.PT.1 - SLA Patching*
54) *PR.AC.9 - 2022 Q4 - AD Privileged User Account Review*
55) *DE.AE.3 - Endpoint Protection Solution*
56) *PR.PT.1 _CSA-Incident_ - Observed phishing campaign used a compromised UN account*
57) *DE.CM.3 - RE_ Typo Squatting Observations - DRP (WMO)*
58) *DE.DP.4 - INC7980640 - Re_ User at risk detected*
59) *DE.DP.5 - KB3013852-WMO – Security alerts, how to handle them*
60) *RS.MI.1 - WMO – Handling suspicious mail (spam)*
61) *RC.IM.2 - Lessons Learnt*
62) *ID.SC.5 - Public Website Supplier review*
63) *ID.SC.5 - Annual Vendor compliance review*

13. The scope of the analysis covers:

A. WMO Cyber Security policies and procedures
B. WMO Cyber Security business functions/processes
C. WMO Cyber Security services supporting business functions
D. The WMO personnel providing and managing the Cybersecurity services

14. Furthermore, it is important to highlight that the 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, outsourced functions, processes and suppliers, as well as WMO regional offices.

Observations

Background Information

15. Overall, cybersecurity controls are safeguards to identify, protect, detect, respond and recover to cyber security threats. Cybersecurity controls, without following an IT security standard or framework such NIST CSF or ISO/IEC 27000 family of standards, tend to be somewhat disorganized.

16. The main objective of the NIST Cyber Security Framework is to identify the attack surface that can be exploited by malicious attackers, reduce that surface by the application of procedural and technical controls, detect possible threats and malicious events, respond and contain cyber security events and recover from any damage that has been caused.

17. The security controls are divided in five areas:

    a) The Identify Function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities
    b) The Protect Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services
    c) The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner
    d) The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact
    e) The Recover Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

18. NIST (National Institute of Standards and Technology) is a non-regulatory government agency located in Gaithersburg, Md. Founded in 1901 and now part of the U.S. Department of Commerce. NIST develops, promotes and maintains metrics and standards for several industries.

19. The Framework is a voluntary guidance, based on existing standards, guidelines, and practices for organizations, to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders

20. The Framework can help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources.

21. In the following paragraphs, we show the results of our analysis, grouped by the above five areas.

Our Analysis and findings

AREA 1 – IDENTIFY FUNCTION

22. Control 1 – Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

- A service catalogue is defined and it is present an IT System Inventory that contains also the cloud solutions adopted. The applications are classified based on their criticality. WMO is running a survey to review and identify additional IT system or services.
- Asset inventory is limited to laptops and does not cover mobile devices (smartphones and/or tablets) and network devices (routers/modems, switches, firewalls, etc.). Most of the services are fully managed by the provider that is UNICC for ERP and network elements or by SaaS cloud providers. Network Diagram has been updated as part of the network infrastructure upgrade as defined in the ToRs.
- WMO installs basic software on endpoints, and users do not have admin rights to install new software and a standard operating environment is defined.
- WMO manages their laptops via Microsoft Endpoint Manager and will extend the use of Microsoft Endpoint Manager also to mobile devices as part of the risk treatment plan.

23. Control 2 – Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

- The business environment is well documented and the organization's mission, objectives, stakeholders and activities are understood and prioritized.

24. Control 3 – Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

- Most cybersecurity policies, processes and procedures are outdated, but a full review of the information security policies framework is in progress.
- No data classification policy/standard is yet defined, but its definition is in progress.
- There is no evidence of a previous exhaustive analysis of information & cybersecurity context of the organization.
- An Information security plan, as well as cybersecurity roles, description and cybersecurity responsibilities are defined.

25. Control 4 – Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

- Risk assessment policy and procedures, as well as a recent risk assessment and relative remediation plan, were provided. Information security risk assessment has the following phases: identification of risk scenarios, assessment of impact and likelihood of each scenario and evaluation of the risk rating against the risk evaluation criteria to determine their acceptance and/or appropriate actions.
- A full Business Impact Analysis was not yet performed (no RTO and RPO were defined, even if the systems were classified per business criticality), and there is no awareness about all the systems of the organization. WMO is running a survey with the different departments to confirm and identify additional business critical systems, critical suppliers and to evaluate RTO and RTO for the most critical systems as part of the BIA.

26. Control 5 – Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

- A risk management strategy was defined, as well as the risk appetite for the organization. Reports with security risk assessment result were provided and there is evidence of the management approval for the remediation plan.
- Cyber security risks are also reported and managed in the organizations Enterprise Risk Management (ERM)

27. Control 6 – Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

- There is generic evidence about WMO General terms and conditions and on security clauses in contractual agreements.
- A vendor Security Review is planned as part of the risk assessment process and there is evidence that such a review has been performed. Furthermore, there is evidence of an annual review of the supplier's compliance with the main ISO certifications and other certifications (ISO27001, ISO 22301, …).

AREA 2 – PROTECT FUNCTION

28. Control 1 – Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users,

processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

- Evidence of security policies, methodologies and technologies adopted for the administration, verification, revocation and security audit of digital identities and access credentials for user, as well as for management and control of privileged users, was provided.
- Physical security is fully outsourced and the physical security of paper documents and assigned company assets is managed through a code of conduct/policy for the acceptable use of assets. We suggest implementing regular monitoring of the supplier.
- Security policies adopted for remote access for internal and external personnel, as well as evidence of their application, were provided.
- Evidence of user groups and their privileges was provided only for Oracle EBS.
- No detailed network security policy and description of segmentation was provided.

29. Control 2 – Awareness and Training (PR.AT): The organization's personnel and partners are provided with cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

- Security training is provided in the onboarding phase of newcomers, awareness sessions on best practices to protect assets and phishing campaigns are performed on a regular basis, but no evidence of what instructions (e.g., cybersecurity/personal data treatment instructions) and training each user has received was not provided.
- Top Management cybersecurity training and simulations are not carried out. Cyber Security Tabletop activities will be scheduled when the response process will be finalized.
- We suggest implementing regular monitoring of the physical security behaviour (e.g., clean desk, Tailgating).

30. Control 3 – Data Security (PR.DS): Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- No security policies provided for data protection at rest, in transit (logical nor physical) or in use.
- Laptops HDs are encrypted (BitLocker) but no protection for mobile devices is in place. This finding will be addressed as part of the risk treatment plan.
- Backup procedure is outdated but the configuration of the managed IT Systems has not been drastically changed in the recent past. There was evidence of a backup planning and strategy by some vendors.

31. Control 4 – Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

- Password management and acceptable use standard were provided.
- The suppliers of the managed services are audited and there is evidence of recommendations addressing the findings.
- No Business Continuity plan defined, but evidence in the proposals of the suppliers of the managed services for DR.

32. Control 5 – Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

- Only a change management procedure in place, but no security policies provided about the maintenance of WMO Systems were provided.

33. Control 6 – Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

- Most of the IT Systems/Services are outsourced to service provider and WMO relies on the security measures of the suppliers.
- Some firewalls are installed, but no evidence of IPS nor management procedure (the network management is fully outsourced and managed by UNICC).
- There are dual connections to the Internet and dual connection to UNICC, the WMO IT Service provider.
- No Vulnerability management process in place and no vulnerability assessment activities planned. Evidence of planned Pen Test activities on a subset of the IT systems. Some evidence for security log management.
- A SOC will be established for the end of the year as part of the risk treatment plan.

AREA 3 – DETECT FUNCTION

34. Control 1 – Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.

- Endpoint Protection Systems (EPS) are managed only for laptops, but are not monitored; implementation of EDR is planned in the risk treatment plan.
- Mobile devices are not managed by an MDM/EMM and neither monitored, but it's planned to address this finding in the risk treatment plan.

- Network traffic is filtered by a couple of firewalls managed by the UNICC provider, there has not been shared evidence of network log monitoring.
- No evidence for the presence of Intrusion detection systems (IDS), Intrusion prevention systems (IPS), Web applications firewalls (WAF) in the WMO network;
- The physical security is fully outsourced and not audited.

35. Control 2 – Security Continuous Monitoring (DE.CM**):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

- The security Continuous Monitoring performed by Cyber threat intelligence analysis managed by UNICC and CommonSecure used to get notifications on relevant threats from different sources.
- No continuous security vulnerability scanning (e.g., security scanner) has been revealed.
- In the risk treatment plan, it has been planned to implement EDR, MDM and SOC to monitor security events.
- There is evidence of continuous improvement of the detection process.

36. Control 3 – Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

- The roles and responsibilities for detection and escalation of security events are not well defined
- No evidence of log monitoring and detection of unapproved software for mobile devices. For managed devices (laptops), the presence of only approved software relies on the lack of administrative privileges for the users.
- Basic SIEM correlation rules for suspicious login attempts.
- No evidence for methodologies and technologies adopted for security event monitoring (except suspicious login attempts), but a quarter-based monitoring of suspicious security event is performed and review of security event monitoring procedure is ongoing.

AREA 4 – RESPOND FUNCTION

37. Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

- IT Incident management policies and operational procedures, Cybersecurity incident response strategies and plan, security events classification and Incident classification scheme are outdated, but will be updated as part of the risk treatment plan.

38. Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

- No evidence of security events escalation paths; outdated Crisis management policy and Data breach management policy (will be updated as part of the risk treatment plan).

39. Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.

- No evidence, but Information security incident management process is being updated, the process should include at least:
  - the methods for receiving, analysing, classifying and responding to at least the information collected from security and detection systems
  - the processes, roles, responsibilities and technical tools for carrying out the activities updated Incident classification scheme

40. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

- Procedures are defined for the mitigation and response to a minor set of incidents, but Information security incident management process is being updated.

41. Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

- No evidence of register of the cybersecurity incident simulations carried out and of the participants, and related lessons learned, but Phishing simulation campaign is performed on a quarterly basis.
- The response plan and strategies should be kept up-to-date also taking into account the lessons learned during the necessary response activities.

AREA 5 – RECOVER FUNCTION

42. Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

- Backup & DR solutions provided by service provider for managed services.
- Backup plan for non-outsourced systems is outdated, but the systems have not undergone changes in the recent past.
- The Disaster Recovery Plan is being drafted.
- At organizational level, the production of a comprehensive Organizational Resilience Management System policy, to be aligned to the UN standards, is ongoing. After the

policy, it has been planned to define and enhance the crisis management plan and business continuity plans for key processes.

43. Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.

- No evidence of audit on the service provider for managed services, even if there is a formal process of verification for the supplier requirements.

44. Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

- No Crisis management policy. WMO started to work on a comprehensive Organizational Resilience Management System policy to be aligned to the UN standards.

Conclusions and recommendations

45. From our analysis, we conclude that IOO identified most of the major issues in the IT risk assessment audit. The risk treatment plan established to address the findings appears to be adequate and should be implemented.

46. Overall, an involvement and commitment of top management was found in improving the aspects related to information security and in particular to cybersecurity.

47. Cybersecurity policies are outdated and need to be updated. Furthermore, they do not exhaustively cover all aspects related to the topic.

48. The company processes have been defined, but there is no evidence of procedures that exhaustively cover all areas of cybersecurity.

49. The strategic direction highlighted by the audit appears to be the use of cloud services in SaaS mode and the engagement of external vendors for the management of the remaining corporate systems, network and physical security, limiting the scope of internal IT to the management of endpoints, training and awareness-raising on cyber security issues. Endpoint management has a lack of effectiveness when it comes to mobile devices. We observe that the CISO is also engaged “as a service”, and he is not a WMO staff.

50. Even if there is a formal process for verifying suppliers, they are not asked for evidence on the actual application of the security measures offered.

51. Business continuity and Disaster Recovery is managed in an unstructured way, leaving the responsibility and decision-making autonomy to the suppliers in order to guarantee the operation of the WMO systems.

52. RTOs/RPOs of critical services/systems have also not been defined and asset inventory is not complete (limited to laptops only)

53. There is also a lack of a structured approach to crisis management.

54. We take note of all measures that the recently appointed CIO, together with the CISO, are addressing to improve the general framework, and we acknowledge that some of them require time to be satisfactorily implemented. For this reason, we will carry out another audit in the field of the cyber security once all measures are in place, to check their effectiveness and efficiency. Nevertheless, we issue the following recommendations and suggestions, with the aim of helping the Organization to improve this sensitive area.

Recommendation n. 1.

55. Cybersecurity policies are outdated and do not exhaustively cover all cybersecurity topics. **We recommend** updating the Information Security Policy and establishing the new planned standards (Mobile Device and Teleworking Standard, Identity and Access Management Standard, Vulnerability Management Standard) as stated in action plan “ID.RA.2 - Risk Treatment Plan” and “2022 10 - WMO Policy Framework”.

56. Furthermore, we have noticed that many IT procedures (e.g., change management, back-up) are outdated; **we recommend** updating them periodically.

Comments by Secretary General:

Accepted. Improving and updating the information security policy framework with additional cybersecurity topic specific policies and procedures is an ongoing that will be done during 2023-2024.

Recommendation n. 2.

57. In relation to "ID.RA.2 – Risk Treatment Plan", **we recommend** establishing an information security standard and implementing a data loss prevention solution that enables automatic tools to classify the information. **We** also **recommend** assessing the possibility of forcing the users to apply data classification for all documents.

Comments by Secretary General:

Accepted. This will be implemented as part of the 2024 treatment plan.

Suggestion n. 1

58. **We suggest** using Cyber Security Threat intelligence reports provided by the UNICC service and other sources (e.g., Gartner Top Security and Risk Trends in 2022) for risk scenarios identification and analysis.

Comments by Secretary General:

Accepted. This will be implemented as part of the 2023 treatment plan.

Recommendation n. 3.

59. Considering that, after the migration to Office 365 solutions, users can access the e-mail and Teams server also from mobile phones, and, in addition, the phones are used for the multi factor authentication, **we recommend** monitoring all mobile devices for anomalous activity (e.g., the installation of not official or malicious apps) and implementing a remote locking/wiping solution, using an MDM/EMM solution.

Comments by Secretary General:

Accepted. MDM/EMM solution will be implemented as part of the 2024 treatment plan on WMO-owned devices.

For non WMO-owned devices, this is dependent on the approval for a BYOD policy currently being drafted.

Recommendation n. 4.

60. As already highlighted by the IOO in recommendation n. 3 of its report 2021-IAS-05, the current IT security incident management procedure was last updated in 2007, and is therefore outdated in the current context. Furthermore, a procedure for crisis management has not been defined. **We recommend** completing the update of the security incident management procedure and issuing a specific procedure for the management of both operational and reputational crises.

Comments by Secretary General:

Accepted. This will be implemented as part of the 2023 treatment plan.

Recommendation n. 5.

61. In relation to the cyber security supply chain, we have taken note that, for new IT acquisitions, assessments of the suppliers are performed, and that an annual vendor compliance review has been implemented. **We recommend** defining a specific procedure that contains specific security and compliance requirements in the contracts, and the involvement of the information security team in the acquisition evaluation, as well as a periodical audit of the suppliers.

Comments by Secretary General:

Accepted. This will be added to the 2024 treatment plan.

Recommendation n. 6.

62. In relation to the Information security training & awareness, **we recommend** planning and performing a Cyber security Tabletop training, with the involvement of top management and key people, to simulate a disaster cyber security scenario

Comments by Secretary General:

Accepted. This will be added to the 2024 treatment plan.

Recommendation n. 7.

63. All laptop devices have installed Endpoint Protection Solution provided by Windows Enterprise. The mobile devices have no Endpoint Protection Solution at all. In relation to "ID.RA.2 – Risk Treatment Plan", **we** acknowledge the action plan and **recommend** implementing an Endpoint Detection & Response/Extended Detection & Response (EDR/XDR) solution on all WMO assets (included BYOD mobile devices), to monitor and manage security threats.

64. Following the deploy of the EDR/XDR solution, **we recommend** establishing a SOC as a Managed Security Services Provider service, or an internal SOC.

Comments by Secretary General:

Accepted. EDR/XDR will be implemented as part of the 2023 treatment plan. Besides, SOC will be implemented as part of the 2024 treatment plan after the implementation of the EDR/XDR.

For non WMO-owned devices, this is dependent on the approval for a BYOD policy currently being drafted.

Suggestion n. 2

65. Following the SOC implementation, for better synergy, we suggest including Incident Response services in the SOC activities.

Comments by Secretary General:

Accepted. Incident Response will be part of the SOC that will be implemented as part of the 2024 treatment plan.

Recommendation n. 8.

66. **We recommend** that additional controls to protect WMO Systems be implemented, such as: periodic vulnerability assessment and penetration test with relative remediation plans; vulnerability management program application security testing. The lack of such controls can expose WMO services to easy exploitable technical vulnerabilities, which could easily be avoided or fixed through the recommended controls.

Comments by Secretary General:

Accepted. Penetration test will be implemented as part of the 2023 treatment plan and vulnerability management as part of the network upgrade project.

Recommendation n. 9.

67. Although most of the IT systems used by WMO are managed or outsourced, WMO should increase the governance of the activities in Business continuity and Disaster recovery perimeter, at least for monitoring the suppliers. **We**, therefore, **recommend** completing the drafting of the Disaster Recovery Plan and performing a Business continuity analysis of disruption scenarios (e.g., No people, no facilities, no suppliers, no building, no IT services).

Comments by Secretary General:

Accepted. Disaster Recovery plan for the ERP will be updated by 2023 and Business continuity analysis of disruption scenarios for the IT department done by 2024.

Suggestion n. 3

68. For SaaS or external services, **we suggest** verifying during the cyber security supply chain audits that the supplier performs the security testing and implements the relative remediation.

Comments by Secretary General:

Accepted. For critical vendors, security testing will be validated via security assurance and audits reports (i.e. SOC 2 type 2, etc). Where such assurance reports are not provided, we will request the vendor for the security testing evidence.

Suggestion n. 4

69. As part of the cyber security supply chain monitoring, **we suggest** participating in disaster recovery tests performed by the suppliers or auditing the suppliers for evidence of such tests.

Comments by Secretary General:

Accepted. For critical vendors, DR test execution will be validated via security assurance and audits reports (i.e., SOC 2 type 2, etc).

Suggestion n. 5

70. The Wi-Fi access in the WMO HQs is not protected by a password, and anyone could connect to the network. Even if the physical perimeter is protected, if a threat agent manages to avoid physical security and connects to internal Wi-Fi, he could use it to gather information that could be used for malicious actions. We suggest implementing a solution to guarantee authentication (e.g., password), authorization (e.g., user ID or company mail), and accounting (logging) of the users using the Wi-Fi.

Comments by Secretary General:

Accepted. This will be implemented as part of the network upgrade project.