Western and Central Pacific Fisheries Commission

TECHNICAL AND COMPLIANCE COMMITTEE
Sixteenth Regular Session
Electronic Meeting
23-29 September 2020

Review of Integrity of Secretariat VMS Data and IMS and RFV

WCPFC-TCC16-2020-RP09
15 October 2020

Paper prepared by the Secretariat

Introduction

1. This 2020 report, "Independent Accountant's Report on Applying Agreed-Upon Procedures" provides the findings and recommendations of an independent security audit on the integrity of the Commission Vessel Monitoring System (VMS), Information Management System (IMS) and Record of Fishing Vessels (RFV) systems and data. The work was carried out by Deloitte & Touche LLP, Guam, USA. The on-site field work at the WCPFC Secretariat took place from the 10-17 November 2019.

2. The key findings and/or recommendations have been extracted and grouped into related themes in the next section of this paper together with the Secretariat responses.

Key Findings and/or Recommendations and Management Response

Data and Access

Management should consider assessing relevant risks associated with VMS data that is stored on workstations beyond required retention periods.

- The Secretariat is aware of subsets of data being stored on a very limited number of workstations for the purposes of ad-hoc analysis and quality control purposes. The risk of this data being accessed is extremely low and the limited identifier information stored with the data further reduces the risk.

The Commission may consider utilizing a VMS User Access Form as documentation of user access creation. The form would include access levels, duration of access and approval.

Consider utilizing User Access Forms to document user access approvals. Consider adopting a user access review process and task supervising officer(s) to cross-reference actual permissions against intended permissions.

Document user access review procedures performed. The review should determine whether users are appropriate to have access and whether the level of access is appropriate. Such review documentation may include procedures performed, results of the review and actions taken related to noted exceptions

- The Secretariat is formalizing the granting of access to VMS data by users including recording the level and duration of access. This will be implemented during the first half of 2021.

- The Secretariat currently undertakes periodic reviews of data access roles and permissions for all ICT infrastructure. While not currently formalized or documented it is an ongoing process required for a constantly changing technical landscape. A routine will be established to regularly match user access documentation with data access permissions on completion of the documentation.

ICT Infrastructure

The Commission may consider developing a regular monitoring procedure to verify that antivirus and antimalware software are current.

The Commission may consider preparing server and workstation maintenance checklists on a quarterly basis, which could include software updates

The Commission may consider preparing a log of issues noted during the scanning and testing, which can be completed together with BMC. The log will help the Commission monitor vulnerabilities noted by BMC during quarterly tests and the procedures performed to address those vulnerabilities

We recommend that workstation encryption be utilized as required by the Commission's Data Encryption Policy and that exceptions be documented in writing

Physical topology for the local network needs to reflect the correct network links upon completion of the switch upgrades

- All of these recommendations have been either actioned or are underway in the order of priority as presented. Expected completion date is end of first quarter 2021.

Policy, Procedures and Training

Management should consider conducting a Business Impact Analysis (BIA), which takes into account different disaster scenarios. The BIA includes an assessment of the likelihood of these scenarios and their potential impact on the Commission. The Commission may use the BIA results in developing a business continuity plan, which, among other matters, takes into account the determination of an acceptable time as Recovery Time Objective (RTO) and to develop a priority list of actions, which will guide the Commission to meet RTO.

Conduct a Risk Assessment and BIA as required by the Business Continuity Policy.

Conduct Vendor Risk Assessments and establish corresponding monitoring procedures.

- The Secretariat agree with the recommendations above however as a result of changes to operations as a result of COVID-19 prioritised remote access security (an aspect of business continuity) over disaster recovery. It is in progress and likely to be completed mid 2021.

Provide Information Security Awareness Training to new and existing employees as required by the Information Security Policy.

- Acknowledging the rise in cybersecurity threats as a result of human vectors, security awareness training was given priority this year, particularly due to the increased remote working of staff. The Secretariat engaged the services of KnowBe4, a leader in the field of security awareness and training programs. All staff have been tested several times with phishing test emails to provide a baseline from which to measure training efficacy.

Management to review draft policies and consider establishing appropriate monitoring of compliance with such policies.

Update IT Asset Inventory per the new Asset Management Policy

Conduct regular reviews of User Access and document procedures based on the Access Management Policy.

- The Secretariat agree on the need to document unwritten policies and will continue to progress these over the next intersessional period

In addition to the recommendations contained in the Auditors report the Secretariat have embarked on a significant body of work to update the on-premise virtual server infrastructure. We are now more than halfway through the server upgrades (to the latest operating system versions) and all known security patches are applied monthly according to industry best practice.

Deloitte.

Deloitte & Touche LLP
361 South Marine Corps Drive
Tamuning, GU 96913-3973
USA

Tel: +1 (671) 646-3884
Fax: +1 (671) 649-4265

www.deloitte.com

Independent Accountants' Report On Applying Agreed-Upon Procedures

Mr. Feleti Teo
Executive Director
Western and Central Pacific Fisheries Commission
Kaselehlie Street
PO Box 2356
Kolonia, Pohnpei 96941
Federated States of Micronesia

Dear Mr. Teo:

We have performed the procedures enumerated below, which were agreed to by the Board of Directors of Western and Central Pacific Fisheries Commission ("WCPFC" or "Commission"), solely to assist you in evaluating the infrastructure supporting the Vessel Monitoring System ("VMS"), the Information Management System ("IMS"), the Record of Fishing Vessels ("RFV") and the Compliance Monitoring System ("CMS").

This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of the procedures is solely the responsibility of the user specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

The procedures that were performed and our findings and recommendations are as follows:

1. SCRUTINIZE INTEGRITY OF DATA

I. Briefly explain the data entry process for VMS, IMS, RFV and CMS.

Agreed-Upon Procedures

Scrutinize documentation and walk through data input and output processes for the following systems:

a. Vessel Monitoring System (VMS)
b. Record of Fishing Vessels (RFV)
c. Information Management System (IMS); and
d. Compliance Monitoring System (CMS)

Inquire about new modules and applications as well as changes to existing ones, if any.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

I. Briefly explain the data entry process for VMS, IMS, RFV and CMS., Continued

Findings

1. Amongst all types of VMS data, the Commission considers vessel location records as most critical. Vessel locations are transmitted from the vessels to the cloud database through satellites. Tracking units such as Mobile Transceiver Units (MTU) or Automatic Location Communicators (ALC) are installed on each authorized vessel and transmit the data location to the cloud database in Amazon Sydney. The VMS webserver pulls data from the cloud and is accessed by VMS Users and Administrators online through web browsers.

2. RFV, CMS and IMS are hosted through the Commission's Sharepoint portal. The Sharepoint portal is an online portal and a database of reports and documents, which users with appropriate permissions may access through web browsers.

3. We noted no significant changes or new modules added to the above-mentioned systems.

Recommendations

No recommendations arose as a result of performing these procedures.

II. Where is IMS, RFV, VMS and CMS data hosted?

Agreed-Upon Procedures

Interview VMS operators and sample a set of VMS users to understand what data is stored locally on laptops, workstations and what is stored externally on cloud services. Scrutinize rules governing the use of VMS data.

Findings

1. VMS data is primarily stored in Amazon Web Services (AWS), through database centers located in Sydney, Australia. Backup data is stored in the Amazon Cloud and Trackwell database centers. VMS data is also stored in user workstations, as users have the capability of downloading VMS data. VMS Users are authorized to have VMS data in their workstations and it appears that data no longer relevant to users may continue to be retained on workstations due to lack of review procedures.

2. RFV, CMS and IMS data are managed within a Sharepoint portal and are primarily stored within the Commission's network servers. Backup data is created through the VEEAM backup application and is stored in an iLand cloud server through data centers located across the U.S. Mainland. Section V of the High Seas VMS Data Rules and Procedures covers the retention and destruction requirements of non-public domain data.

3. Information Security Policy governs the general use of all Commission systems, including data. VMS Standard Operating Procedures serve as guidelines for the Commission to manage VMS, including the use of VMS data.

Recommendation

1. Management should consider assessing relevant risks associated with VMS data that is stored on workstations beyond required retention periods.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

III. Is the data backup routinely documented?

Agreed-Upon Procedures – Part A

Discuss backup routine with FFA/Trackwell. Discuss VMS backup site implementation with WCPFC Head Quarters (HQ) staff.

Findings

1. The VMS back up process is managed by Trackwell, the Commission's VMS software vendor. VMS Database backup runs daily from AWS to Trackwell database centers for redundancy.

2. The Commission's Sharepoint portal that hosts RFV, IMS, and CMS data, is backed up in an iLand cloud server with data centers located across the U.S. Mainland. The backup is done through the VEEAM backup application and is serviced by the Commission's third party IT service provider, BMC.

Recommendations

No recommendations arose as a result of performing these procedures.

Agreed-Upon Procedures – Part B

Scrutinize documented backup procedures and chain of custody. Make recommendations to improve security, where possible.

Findings

1. VMS backup procedures are maintained by Trackwell and an overview of the backup procedures is documented in the VMS System handbook.

2. The Commission maintains a separate document for system backup procedures that are hosted within the Commission's head office in Pohnpei. The backup procedures include daily tasks, administrator roles and regular backup tests.

Recommendations

No recommendations arose as a result of performing these procedures.

IV. Is the Commission prepared to deal with a disaster? How will the Commission provide continuity of service in the event of a catastrophe?

Agreed-Upon Procedures – Part A

Scrutinize the virtualization implementation, disaster recovery processes and procedures and business continuity plan.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

IV. Is the Commission prepared to deal with a disaster? How will the Commission provide continuity of service in the event of a catastrophe?, Continued

Agreed-Upon Procedures – Part A, Continued

Findings

1. The disaster recovery plan which was completed in June 2018, is currently being reviewed by the Commission for further revision. Included as part of the disaster recovery plan are standard operating procedures, which serve as guidelines for preparation and maintenance of backups and recovery procedures for the Commission's IT systems. The Commission; however, has not conducted a Risk Assessment and Business Impact Analysis (BIA) that addresses specific disasters such as building fire, flood, typhoons and earthquakes.

2. BMC, the third party IT service provider, has provided the ICT Manager with VMWare restoration procedures for the Commission's data center and is in a position to provide backup and restoration services in the event the ICT Manager is unavailable or requires assistance.

Recommendations

1. Management should consider conducting a BIA, which takes into account different disaster scenarios. The BIA includes an assessment of the likelihood of these scenarios and their potential impact on the Commission. The Commission may use the BIA results in developing a business continuity plan, which, among other matters, takes into account the determination of an acceptable time as Recovery Time Objective (RTO) and to develop a priority list of actions, which will guide the Commission to meet RTO.

Agreed-Upon Procedures – Part B

Perform a restoration test wherein data is restored at the VM level, database level and file/folder level.

Findings

No recommendations came as a result of performing these procedures.

Agreed-Upon Procedures - Part C

Document whether antivirus/antimalware versions are up to date and view antivirus system connection to central server.

Finding

1. The Commission uses Symantec as antivirus software and Malwarebytes as antimalware software. Both are centrally managed by the IT Department in the server's management consoles. Workstations are set to update upon reboot. ICT Manager represents that all Commission workstations and servers have anti-virus and anti-malware installed. Scrutiny of the Symantec Endpoint Protection Client Inventory details noted that 17 of 48 workstations are not reporting to the management console. Scrutiny of Malwarebytes Client Inventory details also noted that 24 of 48 workstations are not reporting to the management console.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

IV. Is the Commission prepared to deal with a disaster? How will the Commission provide continuity of service in the event of a catastrophe?, Continued

Agreed-Upon Procedures - Part C, Continued

Recommendations

1. The Commission may consider developing a regular monitoring procedure to verify that antivirus and antimalware software are current.

V. Is the network diagrammed and is the diagram readily accessible to the ICT Manager, VMC and anyone else who would need access to it in an emergency situation?

Agreed-Upon Procedures

Scrutinize the network documentation and means of providing access to necessary parties. Scrutinize existing security policies, processes and procedures to protect client data. Make recommendations for improvement, where applicable.

Findings

1. The Commission's server diagram is limited to its servers. Physical topology for the local network was prepared in 2019. However, the new physical topology does not reflect current network structure due to ongoing switch upgrades. These diagrams are placed in a shared folder within the Commission's network and necessary parties are given access to that shared folder.

2. The Commission's Information Security Policy, including its appendices, serves as the main governing policies and procedures when it comes to the protection of client data. Employees sign a Non-disclosure Agreement Form, as a covenant not to disclose or misuse confidential information.

Recommendation

1. Physical topology for the local network should reflect the correct network links upon completion of the switch upgrades.

2. SCRUTINIZE ACCESS CONTROLS

I. Is access to the network and its resources controlled and documented?

Agreed-Upon Procedures

View Domain Users list and cross-reference with "active" VMS users. Attempt login with a haphazard sample of active users and attempt to log in using credentials unknown to the database. Scrutinize the means by which access to network and its resources is granted, reviewed and revoked.

Findings

1. Domain Users under VMS Active Directory Group are consistent with the list of WCPFC staff. We haphazardly selected one VMS workstation and performed a test login from Sharepoint Portal and VMS website using invalid credentials and the test login did not allow access.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

I. Is access to the network and its resources controlled and documented?, Continued

Findings, Continued

2. The VMS Software can be accessed from any web browser, including personal computers and mobile devices of any user with VMS account credentials. RFV, VMS and CMS applications are accessed through the Commission's intranet, WCPFC Sharepoint Portal and are managed by the ICT Manager and Admin Manager. The Access Control section of the Information Security Policy serves as general guidelines for user access management. Procedures for registration, maintenance, and termination are discussed within a supplemental policy, "Establishing and Reviewing Data Access Permissions".

Recommendations

1. No recommendations arose as a result of performing these procedures.

II. Who grants and who administers requests to access server(s) or domain?

Agreed-Upon Procedures

Inquire how access requests are submitted, documented, by what criteria access is granted and what level of access each user is permitted (read, read/write, modify or full control). Scrutinize domain setup against intended security settings, to include Admin and User roles. Scrutinize Sharepoint Server configuration including Admin and User access roles. Scrutinize MS Unified Access Gateway configuration against security requirements.

Findings

1. Access-granting procedures for both VMS and Sharepoint are documented through email communication between supervising officers and ICT Manager. There is no documentation of periodic review and of comparing users' actual permissions against intended permissions.

Recommendations

1. Consider utilizing User Access Forms to document user access approvals. Consider adopting a user access review process and task supervising officer(s) to cross-reference actual permissions against intended permissions.

III. How many have administrative rights to the server(s) where VMS data is stored?

Agreed-Upon Procedures

Discuss password policies, complexity requirements, password history and change requirements. Inquire whether the ICT has these policies and procedures documented and review/secure documentation. Discuss access requirements for accessing VMS data.

Findings

1. We obtained the VMS Users list and noted that there are six accounts with administrative privileges to the VMS servers with capabilities to add or edit VMS user accounts. Three of these accounts are for the Commission's authorized admin users, namely the ICT Manager, VMS Manager and Compliance Manager, and two WCPFC test accounts managed by the VMS Manager. One admin account is managed by the software vendor Trackwell.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

III. How many have administrative rights to the server(s) where VMS data is stored?, Continued

Findings, Continued

2. Passwords are required to be more than eight characters, which are different from previous passwords and should not be the same as the User ID. The password requires a mixture of letters and numbers and/or special characters. Passwords are set to expire automatically every six months.

3. The Access Control section of the Information Security Policy governs user access management. Procedures for registration, maintenance, and termination are discussed within a supplemental policy entitled, "Establishing and Reviewing Data Access Permissions".

4. Access to VMS is given to the Commission's staff members, Member Countries, Cooperating Non-Members, and Participating Territories and requires approval from the Commission's VMS Manager. We sampled new VMS users and noted that granting and termination of user access is currently documented solely through email communication.

5. Third party access to VMS requires an approved Data Request Form. We obtained a sample Data Request Form and noted approval from the Compliance Manager and the Executive Director.

Recommendations

1. The Commission may consider utilizing a VMS User Access Form as documentation of user access creation. The form would include access levels, duration of access and approval.

IV. Document maintenance on VMS servers?

Agreed-Upon Procedures

Interview VMS Manager to document server maintenance and backup routine, updates and hardware/software upgrades.

Findings

1. The VMS Manager represents that VMS backups, updates or upgrades are serviced by Trackwell and Amazon Sydney.

Recommendations

No recommendations arose as a result of performing these procedures.

V. Are there firewalls in place to protect external interface of network(s)?

Agreed-Upon Procedures

Interview ICT Manager to understand which firewall and IOS version is in use in each location.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

V. Are there firewalls in place to protect external interface of network(s)?, Continued

Findings

1. Nextgen Barracuda Firewall is in place as an external firewall for the network. An ASA 5505 router is used as a firewall and router for VPN access by VMS and for the Commission's Website to pull data from the Sharepoint Portal. Another ASA 5505 router also serves as a firewall for all servers.

Recommendations

No recommendations arose as a result of performing these procedures.

VI. What means of data replication are used to assist with business continuity?

Agreed Upon Procedures

Interview ICT Manager and investigate/document method of data replication in use. Inquire about Trackwell application security testing.

Findings

1. VMS data is stored in Amazon Web Services and is replicated to Trackwell database centers. RFV, IMS and CMS data is stored locally and is backed up in an iLand cloud server through VEEAM backup application.

Recommendations

No recommendations arose as a result of performing these procedures.

VII. Are VMS user rights documented?

Agreed-Upon Procedures

Document user rights of VMS staff so they may be viewed by FFA/Trackwell management or third party entities requiring knowledge of WCPFC staff user rights.

Findings

1. A list of VMS users can be viewed from the VMS Web application, by users with administrative privileges. It was represented by the VMS Manager that VMS access is reviewed on a monthly basis, but no documentation of this review was provided. The Commission's VMS Standard Operating Procedures cover the granting of access rights to individuals requiring access, but does not consider periodic user review including specific documentation evidencing that review.

Recommendations

1. Document user access review procedures performed. The review should determine whether users are appropriate to have access and whether the level of access is appropriate. Such review documentation may include procedures performed, results of the review and actions taken related to noted exceptions.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

VIII. What level of access does BMC have to the infrastructure at WCPFC? Is BMC's access to the infrastructure logged? Does the ICT Manager at WCPFC receive notice when BMC logs into the network via VPN? If so, by what means? If not, is there documentation detailing access rights and controls? Does the ICT Manager maintain and review VPN access logs on a regular basis to determine when third parties or others are accessing the network and/or server infrastructure?

Agreed-Upon Procedures

Discuss third party level of access, method of access, logging, alerting and processes of analyzing third party access to network via VPN.

Findings

1. BMC has administrative level access to the Commission's network drives primarily due to their service level agreement. BMC is required to maintain the network servers and this is performed through VPN. VPN access is recorded through the Barracuda firewall and the ICT Manager receives notifications of VPN access through email.

Recommendations

No recommendations arose as a result of performing these procedures.

3. SCRUTINIZE DATA PROTOCOLS USED FOR BOTH INCOMING AND OUTGOING DATA

I. What protocols are used to connect to, manage and transmit data?

Agreed-Upon Procedures

Scrutinize protocols in use (SNMP version, telnet vs SSH, ftp vs. sftp, etc.).

Findings

No recommendations arose as a result of scrutinizing protocols in use.

II. Are workstations and laptops using firewall software?

Agreed-Upon Procedures

Obtain a sample of computers and view whether firewalls are in place.

Findings

1. Selected one laptop and one desktop computer and noted that windows firewalls are activated and in place.

Recommendations

No recommendations arose as a result of performing these procedures.

3. SCRUTINIZE DATA PROTOCOLS USED FOR BOTH INCOMING AND OUTGOING DATA, CONTINUED

III. How are software updates managed?

Agreed-Upon Procedures

Scrutinize documented methodology, processes and procedures used to update software on servers, workstations, laptops, networking equipment and databases.

Findings

1. The Communications and Operations Management section of the Commission's Information Security Policy requires that equipment maintenance be documented. For workstations, software updates initially occur in a test environment prior to implementation on workstations. For the servers, VEEAM Snapshots are first created which creates a backup of the servers, prior to updating the servers. We noted however, that procedures performed for regular software server updates, workstations and other IT assets are not documented.

Recommendation

1. The Commission may consider preparing server and workstation maintenance checklists on a quarterly basis, which could include software updates.

4. SCRUTINIZE CONFIGURATION AND REDUNDANCY OF THE SYSTEM(S)

I. Are there redundant power supplies, hot spares and cold spares? How long does it take to receive spares when ordered?

Agreed-Upon Procedures

Scrutinize documented configuration of the virtual “host server” to document whether it has redundant power supplies, spare drives and RAID configuration of hard drives. Scrutinize the processes and procedures used to maintain and service the SAN.

“Redundancy of the system” also includes service to the systems. Interview the ICT Manager to document whether responsibilities for systems, servers, VPN, laptops, backups, etc. are available for use by replacement or substitute staff.

The above should also be included in a disaster recovery plan. Inquire about the status of integrating these items into the disaster recovery plan.

Findings

1. The Commission uses a standby power generator, which automatically switches on in the event of an island power interruption. Uninterrupted Power Systems (UPS) are in use to power the network servers. The Commission maintains spare hard drives and a firewall within the premises. All hard drives are configured at RAID 10 except for one configured at RAID 5. The Commission's SANs are being serviced by BMC, including monitoring and updating of Firmware. Both the Commission's IT Department and BMC share responsibilities for the systems.

4. SCRUTINIZE CONFIGURATION AND REDUNDANCY OF THE SYSTEM(S), CONTINUED

I. Are there redundant power supplies, hot spares and cold spares? How long does it take to receive spares when ordered?, Continued

Findings, Continued

2. Disaster Recovery Standard Operating Procedures (SOPs) serve as guidelines should the servers, workstations and network equipment fail. A spare Cisco 5512 device and spare disks for both the SAN and NAS devices are kept in the server room. The SAN device and switches are dual power supply systems with adequate spare capacity. The Commission has three VMware ESX servers, with two ESX servers being capable of supporting all existing VMS.

Recommendations

No recommendations arose as a result of performing these procedures.

II. Are servers configured to provide only those services for which they are designed and are server configurations documented and available for reference by necessary parties?

Agreed-Upon Procedures

Scrutinize server configuration, documentation and storage location of server configuration information.

Finding

No recommendations came as a result of performing these procedures.

5. SCRUTINIZE CONFIDENTIALITY OF DATA

I. What is the current configuration of the meeting server and how are drives handled as the server is shipped to/from the meeting location(s)?

Agreed-Upon Procedures

Scrutinize the configuration of the meeting server and drive handling practices.

Findings

1. The meeting server is a Windows server 2012 with its own domain and has no connection to the Commission's IMS and VMS. Separate login accounts are created for CCMs to access meeting documents during Scientific Committee, Technical and Compliance Committee and the Commission's Annual Regular Session meetings.

Recommendations

No recommendations arose as a result of performing these procedures.

5. SCRUTINIZE CONFIDENTIALITY OF DATA, CONTINUED

II. Does WCPFC utilize drive encryption for internal and external drives?

Agreed Upon Procedures

Scrutinize internal and external drive encryption policies and procedures.

Findings

1. The Data Encryption Policy states that all laptops and desktop computers are required to be encrypted and exceptions have to be approved in writing by management. 7 of 26 laptops have bitlocker encryptions enabled and all 23 desktop computers are not encrypted. The new policy has yet to be implemented and no approvals have documented the exemptions.

Recommendations

1. We recommend that workstation encryption be utilized as required by the Commission’s Data Encryption Policy and that exemptions be documented in writing.

III. Is VMS data stored on WCPFC staff computers during the process of posting it to the WCPFC IMS Sharepoint Portal or external website?

Agreed-Upon Procedures

Scrutinize the data handling/transmittal process and interview VMS operators to inquire what data is stored on laptops, workstations and cloud services. Cross-reference this with classification guidelines of the Information Security Policy. The Information Security Policy considers VMS vessel position, direction and speed highly confidential. Scrutinize rules governing the use of VMS data. If VMS data is stored outside the VMS server, it is not compliant with the confidentiality classification.

Findings

1. Data handling procedures depend on the type of data involved. The Commission's overall Data Classification Policy classifies data into either Confidential, For Official Use Only, or Public. The Commission’s Data Rules and Procedures further classify data based on Risk as either Lowest, Low, Medium or High.

2. Users are authorized to have VMS data in their workstations but only for the purpose of executing assigned duties and only for as long as the data is needed. VMS Data on Emails are kept for a period not to exceed a month, while VMS data on workstations is deleted within a 72-hour period. We noted, however, that data no longer relevant to users may continue to be retained on workstations due to lack of review procedures.

Recommendations

1. Management should consider assessing relevant risks associated with VMS data that is stored on workstations, personal computers and mobile devices beyond required retention periods.

5. SCRUTINIZE CONFIDENTIALITY OF DATA, CONTINUED

IV. Are external penetration tests conducted against external IP addresses managed by WCPFC? If so, how often?

Agreed-Upon Procedures

Discuss vulnerability scanning and external penetration testing with the ICT Manager.

Findings

1. Vulnerability scanning and penetration testing is conducted quarterly by the Commission's third party IT service provider, BMC. We obtained sample test results and noted that penetration tests were performed during the year. We noted that documented evidence that penetration test findings were reviewed and/or addressed was not in file.

Recommendations

1. The Commission may consider preparing a log of issues noted during the scanning and testing, which can be completed together with BMC. The log will help the Commission monitor vulnerabilities noted by BMC during quarterly tests and the procedures performed to address those vulnerabilities.

6. SCRUTINIZE ORGANIZATIONAL POLICIES, PROCESSES AND PROCEDURES

I. Is there an organizational chart indicating who is responsible for identifying, addressing and remediating security vulnerabilities?
II. Is there a workflow detailing how security incidents will be addressed?
III. Do staff members know how to deal with security incidents?
IV. Is there a security awareness campaign to inform staff about the latest threats to their computers and IT infrastructure?
V. Is there a list of people and/or organizations to contact in order to assist in dealing with security threats?
VI. Is there a policy to govern teleworkers and remote network access?
VII. Is there a policy and accompanying processes and procedures to assist with initiating, changing or terminating employment?
VIII. Is there a set of policies to govern asset management – procurement, inventory, and disposal?
IX. Is there an information classification system?
X. Are there policies in place governing the following:
   a. physical access to sensitive areas and/or systems;
   b. change management to the IT infrastructure; and
   c. mobile device management?

Agreed-Upon Procedures

Discuss policy, processes and procedures. Make recommendations for new and/or improved policies to govern these areas of Information Technology security.

6. SCRUTINIZE ORGANIZATIONAL POLICIES, PROCESSES AND PROCEDURES, CONTINUED

Findings

1. The Commission's Information Security Policy was last approved in 2007. The Commission outsourced a third party service provider from 2017 to 2018 to draft a revised Information Security Policy. Draft policies were completed in June 2018 but have not been approved due to subsequent required revisions. The latest version of the draft policy is as of August 2019.

2. Included as part of the Commission's overall Information Security Policy are individual policies which are referenced as appendices. These appendices serve as guidelines for the Commission to improve its security posture. These appendices include the following:

   a. Cyber Security Awareness and Training Policy
   b. Personal Device Use Policy
   c. Confidentiality and Non-Disclosure Agreement Policy
   d. Employee Handling Policy
   e. Change Management Policy
   f. Security Audit Logging Policy
   g. Establishing Baseline Permissions and Permission Review
   h. Encryption Policy
   i. Vulnerability Management Policy
   j. Incident Response Policy and Plan
   k. Disaster Recovery Plan Policy
   l. IT Asset and Vendor Tracking Policy

3. Incident Response Policy and Plan includes procedure guidelines, responsibilities of incident response teams and the incident workflow.

4. Teleworking Policy establishes conditions that must be met for staff and trusted third parties to work offsite or away from Commission premises.

5. VPN Usage Policy provides guidelines for remote access to the Commission's network.

6. Employee Processing Policy requires new employees to be are aware of the Commission's policies, processes and procedures. Outgoing employees are required to be processed in such a way that access permissions to physical and electronic assets are revoked.

7. IT Asset Management Policy requires the Commission to maintain accurate records of the Commission's physical computer and IT-related assets. Our review of the Commission's IT Asset Inventory noted that it was not up to date. Recent additions and removals were not reflected on the inventory.

8. Data Classification Policy is in place to provide a framework for securing administrative data in scope and to recognize the importance of handling data.

Recommendations

1. Management to review the draft policies and consider establishing appropriate monitoring of attendant compliance.

2. Provide Information Security Awareness Training to new and existing employees as required by the Information Security Policy.

3. Update the IT Asset Inventory per the new Asset Management Policy.

6. SCRUTINIZE ORGANIZATIONAL POLICIES, PROCESSES AND PROCEDURES, CONTINUED

Recommendations, Continued

4. Conduct Vendor Risk Assessments and establish corresponding monitoring procedures.

5. Conduct regular reviews of User Access and document procedures based on the Access Management Policy.

6. Conduct a Risk Assessment and BIA as required by the Business Continuity Policy.

* * * * * * * *

We were not engaged to, and did not, conduct an examination, the objective of which would be the expression of an opinion on the design, operation, efficiency, stability and security of the infrastructure that supports VMS, IMS, RFV and CMS applications. Accordingly, we do not express such an opinion.

This report is intended solely for the information and use of the Board of Directors of Western and Central Pacific Fisheries Commission and should not be used by anyone other than this specified party.

Deloitte & Touche LLP

September 30, 2020