TECHNICAL AND COMPLIANCE COMMITTEE

Tenth Regular Session

24 – 30 September 2014

Pohnpei, Federated States of Micronesia

ANNUAL REPORT ON THE INTEGRITY OF THE VMS, IMS AND RFV

WCPFC-TCC10-2014-RP08_rev1[1]

22 September 2014

SECURE

Paper Prepared by Secretariat

1. This 2014 annual report for the Commission was prepared by Deloitte & Touche LLP Guam, and currently available in the secure section of the Commission website. The scope covers the Commission Vessel Monitoring System (VMS), Information Management System (IMS) and Record of Fishing Vessels (RFV). The agreed-upon procedures scrutinized 'integrity of data', 'access controls', 'data protocols used for both incoming and outgoing data', 'configuration and redundancy of the systems', and 'confidentiality of data'.

Key Issues

2. This is the third such independent annual report prepared by Deloitte & Touche LLP, 361 South Marine Corps Drive Tamuning, GU 96913-3911 USA. The core team members were: Daniel S. Fitzgerald Partner, Assurance & Advisory Managing Partner who served as the Lead Engagement Partner and Lead Client Service Partner (LCSP). He oversaw all services provided to WCPFC. Jason Kraus, CISSP, MCTS Deloitte Southeast Asia Security Officer/Systems Engineer, is a Manager in Deloitte Southeast Asia practice and is responsible for IT security policies and procedures in that region. He coordinated all requests of data and documentation, and visited WCPFC headquarters from 30 June – 3 July 2014 as part of the 2014 security review of WCPFC VMS, IMS and RFV systems and applications. The Executive Director is pleased with the quality of work provided by Deloitte & Touche LLP Guam, and especially the results to CCM data held by the Secretariat.

3. This annual review is guided by the WCPFC Information Security Policy that was adopted by the 3rd Regular Session of the Commission, and can be found at https://www.wcpfc.int/doc/data-03/information-security-policy. The focus has been a holistic appraisal of the integrity and security of the Commission's VMS, IMS and RFV data, thereby providing a practical and incremental implementation of recommendations to address all findings. Many affordable best practice solutions have now been successfully completed. But the list of findings and recommendations cannot all be done at once, and the Executive Director proposes to continue with the current practice which scopes and prioritizes the more serious work over a 12-month period.

4. The 2014 report also confirms that many of the recommendations from the 2012 and 2013 annual reviews have been addressed by the Secretariat, for example there were a number of website enhancements which have strengthened the security of communications and login arrangements between the website and the intranet. The virtualization of the WCPFC servers, and the inclusion of a third server in 2014, has also improved redundancy

[1] This version includes the final version of the review report (the previous version was a draft for final checking)

of IT operations to the Secretariat and to CCMs information in online systems. The Secretariat, under the leadership of the internal IT Security Committee, is currently developing a work plan to review, prioritize and scope the other remaining recommendations from the review. Included within this planning by the internal IT Security Committee, is a review of the current Disaster Recovery Procedures and options for maintaining online services for RFV publishing, and Annual Report Part 2/CMR reporting will be among the aspects that will be considered.

5. In 2012, the Executive Director awarded the annual security review contract to Deloitte & Touche LLP Guam for three years, 2012 -2014. It is proposed to be advertised again under tender for the work over the next three years from 2015-2017. The expectation is to continue with the process that has been followed for the reports of 2012-2014, and still guided by the current WCPFC Information Security Policy.

Recommendation

6. TCC10 is requested to note this 2014 Annual Report on the Integrity of the VMS, IMS and RFV.

Deloitte & Touche LLP
361 South Marine Corps Drive
Tamuning, GU 96913-3911
USA

Tel: (671)646-3884
Fax: (671)649-4932
www.deloitte.com

Independent Accountants' Report On Applying Agreed-Upon Procedures

Mr. Sam Taufao
ICT Manager
Western and Central Pacific Fisheries Commission
Kaselehlie Street
PO Box 2356
Kolonia, Pohnpei State, 96941
Federated States of Micronesia

Dear Mr. Taufao:

We have performed the procedures enumerated below, which were agreed to by the Executive Director of Western and Central Pacific Fisheries Commission ("WCPFC") to assist you with respect to your overview of the infrastructure supporting the Information Management System ("IMS") applications, the Record of Fishing Vessels ("RFV") and the Vessel Monitoring System ("VMS).

The sufficiency of these procedures is the sole 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 following is a summary of procedures, findings and recommended approaches.

1. SCRUTINIZE INTEGRITY OF DATA

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

Agreed-Upon Procedures

Scrutinize documentation for IMS, RFV and VMS and walk through data input processes. Simulate data input and scrutinize the data output. Scrutinize existing modules and applications.

Findings

A. IMS

1. The ICT Manager represents the Commission continues to use a physical server which is a domain controller that contains sharepoint portal server software for the support of WCPFS's regular sessions of the Commission, Scientific Committee and Technical and Compliance Committee. All three meetings are hosed outside the Commission Secretariat Office. This server is used to process member logins at so they can access secure documents locally, instead of via the internet. The ICT Manager represents that this will be done away at the 10th Regular Session of the Technical and Compliance Committee (TCC10).
2. Standard operating procedures have been developed to document the "eastern high seas pocket entry/exit report."
3. The ICT Manager represents the development of standard operating procedures to manage IMS is ongoing.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

Findings, Continued

B. RFV

Standard operating procedures have been developed and documented. New modules include the workflow to support the activation/deactivation of a vessel monitoring and tracking unit (MTU).

C. VMS

1. The VMS Manager represents he receives VMS user audit reports on a weekly basis.
2. ICT Manager represents the VMS is hosted by a 3rd party on Windows Server 2008. .
3. VMS Manager represents the 3rd party hosting provider is working to develop SmartTrac 5, but the VMS Manager represents there is no assurance the Commission will adopt this new platform.

Recommendations

A. IMS

Fully-develop and document the standard operating procedures designed to manage IMS. This will assist to provide continuity of service to the IMS database.

B. RFV

We have no further recommendations regarding the management of RFV.

C. VMS

Work with FFA/Polestar to upgrade the server platform upon which the VMS "SmartTrac 4.5" application runs before Microsoft no longer supports the server platform.

II. Where is VMS data hosted?

Agreed-Upon Procedures

Interview VMS operators and sample set of VMS users to inquire what data is stored on laptops, workstations and cloud services. Cross-reference this with classification guidelines of ISP (pg. 36) that ensure data stored outside VMS is in compliance with confidentiality classification and within the continuity classification (view whether data stored in VMS also). Scrutinize rules governing the use of VMS data.

Findings

A. VMS staff receives requests to access VMS via email. Accounts are created and the access request is stored with the account in the Monitoring Control and Surveillance database. While all VMS staff understand how to process these requests, there is no standard operating procedure to instruct VMS staff how to process the email request.

B. VMS computers contain confidential data but do not have encrypted hard drives.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

II. Where is VMS data hosted?, Continued

Recommendations

A. Document the workflow into a diagram and/or standard operating procedure to provide for continuity of service.

B. Encrypt VMS computer hard drives to help protect against data leakage.

III. Is the data backup routine documented?

Agreed-Upon Procedures

Discuss backup routine with FFA/Pole Star. Discuss VMS backup site implementation with WCPFC HQ staff. Scrutinize documented backup processes and procedures.

Findings

A. There exists no written documentation to detail the various backup routines in use at the Commission, to include:

- **i.** FFA/Polestar backup routine.
- **ii.** VMS Oracle Data stream backup process.
- **iii.** VMWare backup and snapshot routine.
- **iv.** Tape backup routine, tape rotation and backup schedule.

B. The data on PNIDC1 was not backed up within the time window allowed.

Recommendations

A. Document the various backup routines, schedules and tape rotation strategy to help provide for continuity of service to the Commission, in the event the ICT Manager is not available to provide these services.

B. Configure the data backup jobs to alert on backup failures and reconfigure the data backup sets or backup window so all data is backed up to tape as scheduled.

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

Agreed-Upon Procedures

Scrutinize documented backup procedures and chain of custody. Refer to confidentiality classification that provides for backup media not to be transported or stored in unsecured location(s). Make recommendations to improve security where possible.

Findings

The current backup strategy involves storing backup data on tapes using encryption. These backup tapes are stored offsite in a safe. User credentials, network and device configuration scripts and other sensitive data is stored on an external USB drive in a safe. We have no recommendations as a result of scrutinizing these procedures.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

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

Agreed-Upon Procedures

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

Findings

A. The ICT Manager represents he has restored data from backup tapes, from VMWare snapshots and has restored servers from backup media. The processes/procedures required to perform these services are not documented.

B. The ICT Manager represents the Commission is procuring a third Storage Area Network device with ample storage space to assist with disaster recovery/business continuity.

C. The ICT Manager and 3rd Party IT Vendor (BMC) represent they are considering moving to adopt a cloud based backup strategy to provide additional means of disaster recovery/business continuity.

Recommendations

A. Document the processes and procedures required to restore data via various means, to include VMWare and Backup Exec.

B. Determine whether chosen cloud service provider meets the security objectives and requirements of the Commission and its constituents.

C. Amend the disaster recovery plan once a cloud provider is chosen.

D. Work with management to develop a business continuity plan, which, among other things takes into account the following aspects:

- **i.** Out-of-band communication requirements and capabilities available to staff.
- **ii.** Staff and Commission reporting requirements.
- **iii.** Secure alternate work site(s).
- **iv.** Spare/alternate equipment storage location(s).
- **v.** Storing copies of sensitive and essential data offsite in the event there is a loss of the building in which the Commission operates.
- **vi.** Documenting 3rd party vendors and providers' contact information.
- **vii.** Store a copy of installation media and installation keys offsite.
- **viii.** Determine acceptable time for a return to operation (RTO) and develop a priority list of actions which will guide the Commission to meet the RTO objectives.

1. SCRUTINIZE INTEGRITY OF DATA, CONTINUED

VI. 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

View data restoration logs. Witness a restoration exercise wherein data is restored at VM level, database level and file/folder level.

Findings

There are no issues to report as a result of performing these procedures.

Agreed Upon Procedures

Log into a sample set of systems to re-perform update of antivirus/antimalware updates and view system connection to central server.

Findings

There are no issues to report as a result of performing these procedures.

Agreed-Upon Procedures

Scrutinize network documentation and means of providing access to necessary parties.

Findings

Network documentation does not indicate the relationship between physical and virtual servers.

Recommendations

Diagram the relationship between physical servers and virtual servers to assist with identifying failed servers during disaster recovery procedures.

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 means by which access to network and network resources is granted.

Findings

No findings came as a result of performing these procedures.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

II. Are access requests granted by the same person who administers the 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
- Group Policies
- DHCP settings
- DNS server settings
- Print Server settings
- Active Directory FSMO role assignments
- Active Directory replication to secondary domain controller
- Active Directory backup and restore procedures

Scrutinize MS Unified Access Gateway configuration against security requirements.
Scrutinize Sharepoint Server configuration to include:
Admin and User access roles
Database location
Backup and Restore processes and procedures

Findings

A. Formal procedures do not exist to grant staff access to appropriate network resources.

B. Documentation does not exist to detail users' actual permissions against intended permissions.

C. Procedures do not exist to confirm actual permissions are as intended.

Recommendations

A. Create a form on the sharepoint portal which assists in documenting the appropriate permissions granted to new and transitioning staff. The form may include some of the following fields:
   i. Full Name
   ii. Domain Login Username
   iii. Security Group(s) Membership
   iv. Rights granted on local computer
      a. Administrator
      b. Power user
      c. User
      d. Etc., etc.
   v. Printer access
      a. Printer name
      b. Rights to printer

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

c. Print
d. Manage print jobs
e. Manage printer

vi. Network shares
a. Server name
b. Shared resources
c. Rights to shared resources
1. Full
2. Modify
3. Change
4. Read
5. Special permissions

vii. Sharepoint database rights
a. Area(s) of Focus
1. Author
2. Contributor
3. Reviewer

B. Take screenshots of the various permissions set for each user and store these screenshots as artifacts with each user's form which has been completed/stored on the sharepoint portal.

C. Provide six-monthly list of user and their granted permissions to Compliance Manager so she can 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

Interview ICT Manager to document processes, procedures, and methods used to maintain access controls to VMS as well as criteria used to determine admin level access.

Password policy: determine complexity requirements, password history and change requirements.

Investigate whether the ICT has these policies and procedures documented and review/secure documentation.

Findings

A. VMS staff members are the same as last year and all require admin level access to perform their duties.

B. No recommendations came as a result of scrutinizing the policies/procedures.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

IV. Who performs maintenance on VMS servers?

Agreed-Upon Procedures

Interview ICT Manager to document server maintenance routine – backups, updates, hardware/software upgrades, access log monitoring and logging, etc.

Findings

For backup VMS servers in WCPFC Pohnpei office 3rd party IT Provider (BMC) performs routine maintenance tasks and monitors backups, software upgrades, logs, etc. For operations VMS servers hosted at Macquarie Center in Australia, that is the responsibility of the service provider FFA/Polestar.

Recommendations

Configure the following email alerts as part of routine monitoring:

i. failed backup jobs.
ii. windows software update server synchronization failures.

V. Is there local access to these servers only or is maintenance performed remotely?

Agreed-Upon Procedures

Interview ICT Manager to document method of remote access (presumably via VPN using domain credentials via remote desktop). Inquire about backup remote access in the event VPN link is down.

Findings

No issues to report as a result of performing these procedures.

VI. Are maintenance logs kept which details server/system maintenance?

Agreed-Upon Procedures

Interview ICT Manager to document maintenance/upgrade records are kept on virtual infrastructure, servers, workstations, and laptops.

Findings

A. 3rd Party provider maintains maintenance/upgrade records and provides to ICT Manager on a regular basis.

B. ICT Manager represents records are not kept to document maintenance and upgrades to workstations and laptops.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

Recommendations

Maintain records for each system in use at the Commission. Records may include the following information:

i. Computer mode
ii. Computer serial number
iii. Operating system installation key
iv. User to whom the computer is issued
v. Office suite installed
vi. Office suite installation key
vii. Warranty/service records

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

Agreed-Upon Procedures

Interview ICT Manager to determine what firewall, IOS version is in use in each location. Obtain .txt copy of firewall rules. Read firewall rules and inquire relative to whether they are consistent with the level of expectations for network security.

Findings

Firewall configuration files were analyzed using Nipper Suite Studio software. The resulting report lists security concerns and vulnerabilities for the Commission and 3rd party IT Vendor, BMC to consider and/or remediate.

VIII. 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 SmartTrac application security testing.

Findings

A. VMWare replicates VMS data from Macquarie Data Center in Australia to the Commission's data center in Pohnpei in "near real time."

B. The vessel monitoring software currently in use, SmartTrack 4.5, has not undergone security testing. We obtained approval from the IT Manager at FFA/Polestar to conduct a security vulnerability test of the remote access configuration and tested the site with a security vulnerability scanner. The test yielded four vulnerabilities and one potential vulnerability related to remote desktop sharing. The security vulnerability report was provided to the ICT Manager.

Recommendations

Work with FFA/Polestar to remediate the detected vulnerabilities by reconfiguring the remote desktop connection

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

IX. Are there VPN links in use?

Agreed-Upon Procedures

Scrutinize the VPN configuration and level of access. Scrutinize access credentials - password length, complexity and history requirements.

Findings

FFA/Polestar IT Manager represents VMS clients access SmartTrac 4.5 via remote desktop, use Cisco VPN client software and a site-to-site connection exists between Cisco firewalls.

Recommendations

FFA/Polestar to reconfigure remote desktop requirements to remediate the vulnerabilities detailed earlier in this report.

X. Is the VPN configuration stored outside of the router?

Agreed Upon Procedures

View configuration information stored outside of router to confirm it is the same as is currently in use, and whether it secure and readily available in the event it must be restored to a replacement VPN router. Inspect location of this configuration information.

Findings

A. We witnessed the ICT Manager restore the VPN configuration information from an external USB drive to a spare VPN router.

B. Configuration data is stored on an external USB drive and is stored in a safe.

Recommendations

Keep the spare VPN routers in the server rack alongside the primary VPN routers.

XI. Are VMS User Rights Documented?

Agreed-Upon Procedures

Document user rights of VMS staff so they may be viewed by FFA/Polestar management or 3rd party entities requiring knowledge of WCPFC staff's user rights.

Findings

VMS Manager represents all VMS staff have the same level of rights to perform services. No recommendations are made as a result of performing these procedures.

2. SCRUTINIZE ACCESS CONTROLS, CONTINUED

XII. 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? Does the ICT Manager maintain and review VPN access logs on a regular basis to determine when 3rd party or other are accessing the network and/or server infrastructure?

Agreed-Upon Procedures

Discuss 3rd party level of access, method of access, logging, alerting and processes of analyzing 3rd party access to network via VPN.

Findings

ICT Manager and 3rd party IT Provider (BMC) represent BMC has unrestricted access to the Commission's network and servers via VPN. They do not log VPN access to the network because their access is routine and ad hoc throughout each work day/week.

Recommendations

Log BMC's VPN access to the Commission's network. This will assist in forensic investigations should suspicious network or server activity occur.

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

I. How is the network configured to connect the Commission's infrastructure to the VMS infrastructure at the Macquarie data center.

Agreed-Upon Procedures

Obtain copy of router configuration via soft copy (.pdf or .txt file) as well as hard copy. Scrutinize configuration against expectations of network security.

Ask Australia provider for documentation related to penetration testing. Have they performed penetration testing? Can they produce documentation? Can the service provider produce the Australian equivalent of an SSAE 16 report?

Obtain copy of network configuration (virtual and physical) via software backup as well as hard copy to document that firewall rules meet security expectations.

Findings

Network diagram does not indicate relationship of virtual servers to physical servers.

Recommendations

Create a network diagram detailing the relationship between physical and virtual servers.

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

II. 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

SNMP version 1 and 2, telnet and ftp are the current protocols used to manage the Commission's computing infrastructure.

Recommendations

Where possible, implement the use of SNMP version 3, SSH and SFTP to manage the computing infrastructure. These protocols utilize encryption, which prevents user credentials and data from being transmitted in clear text.

III. Are workstations and laptops using firewall software?

Agreed-Upon Procedures

Scrutinize workstations and laptop firewall software as well as domain group policy settings. Reference these settings against the intended security controls for information security.

Findings

No recommendations came as a result of scrutinizing these configurations.

IV. 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

3rd party IT service provider, BMC, represents they do not manage the security update process for 3rd party applications such as Adobe, Java, HP, etc.

Recommendations

Adobe and Java products are popular attack vectors for hackers. Implement a strategy to manage 3rd party application security updates. Common approaches involve creating logon scripts to install the latest version on all appropriate computers or adopting 3rd party application management programs such as Microsoft System Center Configuration Manager or Solarwinds Patch Manager.

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 the 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 to 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

A. ICT Manager represents the 3rd party IT service provider, BMC, has been identified as the redundant provider of service, in the event the ICT Manager is unable to provide service.

B. No recommendations came 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?

Agreed-Upon Procedures

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

Findings

A. Some servers are running unnecessary 3rd party applications such as adobe reader, java, etc. These applications are not updated automatically and contain known security vulnerabilities.

B. Computer PNIDC1 is a domain controller. It also hosts shared folders for user data.

Recommendations

A. Remove unnecessary software from servers.

B. Document 3rd party software running on each server and routinely update the software as security patches are released.

C. A domain controller typically performs the roles of maintaining active directory (AD) and providing name resolution as a domain name server (DNS). We recommend you remove the user shares from the domain controller and transfer them to a file server.

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

The ICT Manager represents the meeting server will be reconfigured as a non-WCPFC domain computer configured to allow WCPFC members the ability to log into the server with a common set of credentials.

Recommendations
No recommendations came as a result of performing these procedures.

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

Agreed Upon Procedures

Scrutinize internal and external drive encryption policies and procedures.

Findings

A. The ICT Manager represents some software does not run correctly on hard drives that have been encrypted with Microsoft's "Bitlocker" encryption. Therefore, laptops drives are not encrypted.

B. The data stored on external tape drives is encrypted.

Recommendations
Investigate alternate means of encrypting laptop hard drives.

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 (pg. 36). The Information Security Policy considers VMS vessel position, direction and speed highly confidential. Scrutinize rules governing the use of VMS data.

5. SCRUTINIZE CONFIDENTIALITY OF DATA, CONTINUED

Findings

The VMS Manager indicates represents the following:

i. For a formal non-public domain data request, a Commission members provides a completed data request form to the Executive Director for approval. A copy of the request and its associated approval are filed in the Incoming Information Register, as a record of receipt of request including notes on its outcome/fulfillment.

ii. Other requests are often, questions of clarification from Commission members during MCS operations, or during an inspection or for an investigation. On these occasions, some VMS data or information sourced from the VMS databases may be provided to a member over email.

iii. The current Information Security Policy provides for guidelines related to confidential information. These guidelines do not take into account the migration of confidential data from VMS servers to the IMS application.

Recommendations

i. We suggest WCPFC scrutinize the Information Security Policy and revise the classification of confidential information accordingly to account for this confidential data being migrated to IMS applications.

IV. Are server security logs archived and viewed on a regular basis? Are vulnerability scans and/or external penetration tests conducted against external IP addresses managed by WCPFC? If so, how often? Are vulnerability test/external penetration tests results provided to WCPFC? Is WCPFC advised how to remediate vulnerabilities discovered via vulnerability scanning and/or external penetration tests? Are internal network-attached devices scanned for vulnerabilities?

Agreed-Upon Procedures

Discuss vulnerability scanning and external penetration testing with ICT Manager.

Findings

A. ICT Manager and 3rd party IT vendor, BMC, represent they do not archive security logs. BMC represents they occasionally view security logs.

B. BMC indicates they conduct external penetration testing every three months and provide reports to ICT Manager.

C. BMC indicates they seek ICT Manager's approval to address detected vulnerabilities.

D. ICT Manager represents the internal network-attached devices are not scanned for known security vulnerabilities.

5. SCRUTINIZE CONFIDENTIALITY OF DATA, CONTINUED

Recommendations

A. Implement a mechanism to archive server security logs in the event forensic analysis needs to be conducted.

B. Adopt a secondary means by which external IP addresses are scanned. We worked with the ICT Manager to conduct a vulnerability assessment of external IP addresses and discovered three vulnerabilities and one potential vulnerability. The ICT Manager.is in custody of the report

C. Conduct vulnerability scans of the internal network-attached devices on a monthly basis to identify/remediate known security vulnerabilities which may exist with operating system and 3rd party applications as well as printers, routers, switches and network attached storage device(s). We worked with the ICT Manager to conduct a vulnerability scan against the servers. We discovered ninety-four vulnerabilities and fifty-three potential vulnerabilities. The report was provided to the ICT Manager.

D. Conduct vulnerability scan of web applications on a monthly basis to discover known security vulnerabilities. We worked with the ICT Manager to conduct "web application scan" vulnerability tests against the Internet-facing web application at wcpfc.int as well as the intranet-facing web application at intra.wcpfc.int. The web application scanner detected fifty-nine external vulnerabilities with the external-facing web application and one hundred twenty-four vulnerabilities with the intranet-facing web application. The ICT Manager is in custody of the report.

* * * * * * * *

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, RFV and VMS applications. Accordingly, we do not express such an opinion.

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

Deloitte & Touche LLP