THIRTEENTH REGULAR SESSION
FINANCE AND ADMINISTRATION COMMITTEE
Tenth Session
Denarau, Fiji
4 - 9 December 2016

COST OF IMPLEMENTING THE IT AUDITOR'S RECOMMENDATIONS

WCPFC13-2016-FAC10-12
17 November 2016

Purpose

1. The purpose of this paper is to table to the FAC the financial considerations for implementing the IT Auditor's findings in the Auditor's report tabled at TCC12 in meeting paper WCPFC-TCC12-2016-RP08 (Review of integrity of VMS data and IMS and RFV) that is posted on the secure website.

Introduction

2. The Auditor's Report contained the findings and recommendations by an independent security auditor 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 and the report was tabled at TCC12.

3. The recommendations with financial implications (see Annex 1) have been grouped into three categories. First, are those recommendations that simply involve the procurement of IT hardware (Annex 1 section F). The second category is for recommendations that related to backups and disaster recovery (Annex 1 sections B and E). The final category are those recommendations that related to IT policies (Annex 1 sections A, C, D, G and H).

Recommendations related to the purchase of hardware

4. The Auditor recommends that the Secretariat has a spare firewall in place in case the primary firewall breaks. Currently, if the primary firewall were to break, the office has an older firewall that could work as a backup. The older firewall has far less functionality and is presently sufficient for use during SC, TCC and the annual meeting as part of the meeting server setup. The Secretariat agrees with the auditor's recommendation to acquire a suitable spare replacement for the primary firewall.

5. Cost of a spare firewall: USD8,000

Recommendations related to backups and disaster recovery

6. The Auditor recommends that the Secretariat has off site backups, a business continuity plan and a disaster recovery plan. Since the audit, the Secretariat has resumed keeping an off-site backup of the IMS and CMS data. Due to the large amount of data that is now hosted on the Secretariats IT systems, the current off-site backup solution is no longer viable as a long term solution. In order to maintain both a backup and disaster recovery solution, the Secretariat has implemented a cloud-based technology for all WCPFC system backups. The cloud based technology provides a "DRaaS" (Disaster Recovery as-a-Service) for the Commission's response to disasters and ensures a basic level of business continuity to CCMs and the Secretariat.

7. The next phase of implanting the cloud-based recovery is currently in progress. The second phase will address the technical aspects of offsite backups/restore processes, disaster recovery objectives, timeframes for recovery, data encryption, "Failback" and "Failover" to return critical systems at a recovery site after a disaster. The second phase is expected to be completed in by the second quarters of 2017.

8. While the technical systems are in place for recovering from a disaster, the IT audit recommends that explicit policies and procedures for disaster recovery and business continuity need to be developed to better support the recovery from a disaster. This body of work is dependent on funding. Online systems such as CMR, VMS, RFV and Compliance case file management are now established components of the Commission's work. A certain level of system availability is expected from CCMs, staff and other stakeholders. Disaster recovery and business continuity policies and procedures are therefore recommended by the auditor. With the current technical system being implemented, and assuming that certain key factors are within the scope of the Secretariats control, the Secretariat's timeframe for "expected downtime until operations can be restored" is estimated to be 3 to 7 days. If a shorter recovery period is required by the Commission a different, and higher cost solution, will need to be developed.

9. Cost of developing policies and procedures for disaster recovery and business continuity: USD15,000

Recommendations related to the development of IT Policies

10. The Auditor recommends that the Secretariat develop specific policies regarding the operations of the IT system. Currently the Commission has an Information Security Policy (http://www.wcpfc.int/doc/data-03/information-security-policy) that was adopted at WCPFC3 in 2007. This policy was based on the International Organization for Standardization's ISO17799. ISO17799 was developed in the 1990's as a code for providing a comprehensive policy for information security management and was developed for multinational organizations/companies. ISO17799 includes many items that are not directly relevant to a small organization. The ISO17799 standard has been revised twice since being implemented and the most current version is ISO/IEC 27002.

11. Since the current Information Security Policy is outdated and is overly complex for a smaller organization, it is recommended that the policy be revised and made relevant to the needs of the Secretariat. It is envisioned that the new policy would incorporate all relevant portions ISO/IEC 27002 and include the policies recommended in the IT audit.

12. Cost of updating the Information Security Policy: USD20,000

Impacts of not providing funding for the recommendations related to backups and disaster recovery and recommendations related to the development of IT Policies

13. Funding of the recommendations will ensure that the necessary hardware and IT Policies can be prioritized and progressed during 2017. However given the importance of the work, if funding is not provided for all the recommendations the Secretariat will make best attempts as time and resources permit to nonetheless progress work on updating the existing policies and development of a disaster recovery plan and business continuity plan.

Recommendations

14. The Committee is invited to consider the IT Auditor's findings and to provide necessary financial support for the Secretariat to implement those findings.

Annex 1

Key Findings and/or Recommendations with Related Management Response

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

The Commission may consider implementing a policy regarding accessing VMS Data from personal computers and mobile devices.

Management Response: To be completed in Q1 2017 dependent on funding.

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

1. Develop a disaster recovery plan in line with objectives and requirements of the Commission and its constituents, to include the cloud backup of its servers.
2. Work with management to develop a business continuity plan, which, among other things takes into account the following aspects:
   a. Determine acceptable time for a return to operation (RTO) and develop a priority list of actions which will guide the Commission to meet RTO objectives.
   b. Store copies of sensitive and essential data offsite in the event there is a loss of the building in which the Commission operates.
   c. Spare/alternate equipment storage location(s) and secure alternate work site(s).
   d. Out-of-band communication requirements and capabilities available to staff.
   e. Staff and Commission reporting requirements.
   f. Develop an emergency call list
   g. Develop an emergency notification call tree

Management Response: To be completed in Q3 2017 dependent on funding.

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

Adopt a user access review process and task the supervising officer(s) to cross-reference actual permissions against intended permissions.

Management Response: To be completed in Q3 2017 dependent on funding.

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

Develop policies and formalize standard operating procedures governing user access to include some of the following:

a. Granting of access to a new user;
b. Removal of access of a terminated user;
c. Periodic review by VMS Manager of user access; and
d. Method of reporting user access management.
e. A policy of mandatory password change every ninety days

Management Response: To be completed in Q1 2017 dependent on funding.

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

1. Resume performance of tape backup procedures or maintain an offsite backup for IMS and CMS until the cloud backup system has been established.
2. Work with management to develop a business continuity plan.

Management Response: To be completed in Q3 2017 depending on funding.

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

Consider having a spare firewall in place.

Management Response: To be completed in Q1 2017 dependent on funding.

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

a. Adopt a data retention policy regarding retention of VMS data within workstations.
b. Develop procedures to review user's compliance with data retention policies.

Management Response: To be completed in Q3 2017 dependent on funding.

H. SCRUTINIZE ORGANIZATIONAL POLICIES, PROCESSES AND PROCEDURES

A. Security Incident Handling:
    1) Security incident handling processes and procedures, to include escalation procedures.

B. Security Awareness – campaign to inform, advise and educate staff about the following areas:

    1) Safe computer usage tips.
    2) Device security.
    3) Security threats affecting enterprise environments:
        a. Phishing and Spear Phishing.
        b. Social Engineering.
        c. Browser hijacking.
        d. Social Media usage.

C. Mobile Device Management – develop policy to govern the use of mobile devices:
    1) Encryption requirements.
    2) Password protection.
    3) App installation restrictions.
    4) Use of Commission-issued vs. personal devices.

D. Teleworker policy – set requirements to:
    1) Keep systems updated.
    2) Hotspot restrictions – use VPN when connected to hotspots when transmitting sensitive information.
    3) Use Commission-issued devices vs. personal devices.

E. Change Management – adopt ITIL-oriented processes to govern changes in environment.

F. Asset Management
    1) Security requirements when traveling with Commission-issued assets.

Management Response: To be completed in Q3 2017 dependent on funding.