Agenda Item 11 | Executive Board Meeting 4 March 2015 | Memo No 6/15

Status: OFFICIAL

INFORMATION SECURITY MANAGEMENT FORUM:

ANNUAL REPORT 2014-15

Purpose

1. To provide EB members with a briefing on the work of the Information Security Management Forum during the year as a precursor to their reporting on its work in the annual governance statements.

Background

2. As Chair of the Information Security Management Forum (ISMF) and FC Senior Information Risk Owner (SIRO), I am required to provide this Annual Report on protective security and information risk management to the Executive Board.

3. This Annual Report summarises the progress made to identify and address key information risks and reflects the work of the ISMF as the group which co-ordinates and controls the implementation of information security across the Forestry Commission (FC). The report is intended to help EB members to understand the overall FC position in the context of their own responsibilities. It is used by individual SIRO's to assist in completion of their own annual report to their respective executive boards, Accounting/ Accountable Officers and Audit and Risk Committees; by Finance Directors to complete the annual Governance Statements; and the Head of Internal Audit to offer overall assurance to Accounting/ Accountable Officers.

The Information Security Management Forum

4. The forum met three times during 2014-15. The members were as follows:

Paul Snaith/Wilma Harper(from August 2014)	FC SIRO
PK Khaira/Richard Barker(from October 2014)	FCE SIRO
Ann Robertson	FCS SIRO

Hugh Williams	FR SIRO
Stuart Fletcher	Departmental Security Officer (DSO)/IT Security Officer (ITSO)
Fiona Alexander	FC Data Protection Officer
David Felstead (from Jan 2015)	Director IS

All SIROs are members of their respective management boards. The Head of Internal Audit or nominated representative also attended and received all papers.

Assessment and reporting of Risk

5. The FC conducts an annual risk assessment to establish the effectiveness of protective security and information assurance risk management against the Security Policy Framework (SPF). It is known as the Departmental Security Health Check (DSHC) annual report which is required by the Cabinet Office. The HMG Security Policy Framework issued by the Cabinet Office has been radically amended as from last April and is now a higher level policy document monitoring Outcomes in 8 key policy areas. The new Departmental Security Health Check contains statements on where we have any concerns on compliance with the SPF, Pulse test questions (on current hot topics), Cyber security questions and a statement on our compliance with the 10 Steps to Cyber Security.

6. The DSO and I share responsibility for conducting the annual review process and completing the DSHC. In this task we are supported by ISMF members and independent assurance is provided by Internal Audit. The report is approved by the Director FC England as Accounting Officer before submission to Cabinet Office in June. Overall compliance is reported via a short statement in the Governance Statement in the annual accounts.

7. The devolved administrations may complete a DSHC on a voluntary basis. We have agreed to forward a copy of our DSHC to DEFRA and the Scottish Government if they require it.

8. In determining its approach, the FC has taken the view that, in comparison with other government departments its information systems are low risk in that they hold a relatively small number of records and all information remains in the OFFICIAL Government Security Classification, with only a small proportion of that being at the OFFICIAL-SENSITIVE Government Security Classification. The ISMF has agreed that all FC information will continue to be classed within the OFFICAL classification.

9. Overall, we continue to make progress but it is worth bringing to your attention the specific areas below.

Investment in the FC's ICT Infrastructure

10. The FC has developed a strategy for the development of the ICT infrastructure that, when complete, will allow full disaster recovery capability. The NRS facility is now capable of recovering the FC's internal systems, connection to the internet and external email is not yet in place but can be implemented at short notice in the event of a disaster. This is a better situation than we have had before. There remains some work to do to achieve full Disaster Recovery, which is targeted for completion by April 2017.

11. Work on the ICT infrastructure is on-going and more systems are being moved to the new architecture as part of that process, as opportunities to carry out the work arise. The FC's PSN re-accreditation has been submitted and we await feedback on this from the PSN Authority. This allows us to connect to, and exchange information with, other parts of the government network and also provides a framework for ensuing good practice in how our systems can be kept secure. Further work has been carried out over the year, specifically:-

- External facing systems, which are now maintained at the latest patch/update levels to ensure they meet the good practice requirements for these types of services.
- Work started on the implementation of Windows 7, which has proved more difficult than expected, but we expect some 35% of systems will have been upgraded by end of April 2015 and have a target to complete the upgrading of 80% of computers by end Sept. 2015.

Preparatory work is underway to allow following to be done next year:

- Implementation of a security logging and alert tool is targeted for September 2015
- Implementation of a more secure external facing firewall infrastructure. Scheduled for April 2015

Other work which still needs to be addressed, such as the use of unsupported systems on internal servers, is currently being reviewed by IS.

12. The PSN Code of Connection report was submitted on 20th February 2014. The PSN Authority will respond to the progress in that report in April. Although we are not as far advanced with the Windows 7 roll-out as we hoped, Director IS believes that, in view of the progress which has been made, the PSN Authority

will maintain our accreditation with a time-bound requirement for completion of key actions.

Promoting a culture that values and protects information

13. FC Scotland has created a network of Information Asset Owners (IAO) who have asset registers of information they are responsible for and understand their responsibilities. Work is continuing in FC England and FR to implement this across the FC, as required by the Data Protection Act. It will be followed up with appropriate training for the IAOs.

14. Under the new Government Security Classification policy it is the responsibility of all staff to know how they should handle information, whether it is marked or not, and of managers to ensure that their staff know how to do this. The new GSC has largely been incorporated into the FC's daily work and all relevant staff have now completed the Responsible for Information training as well as the GSC training. A reminder on when to use the OFFICIAL-SENSITIVE marking will be issued at the end of February, as there has been some over use of this marking. Another round of IA refresher training will be undertaken in 2016, to meet our obligations to carry this out every 18- 24 months and keep staff aware of their responsibilities.

Security Incidents

15. There have been a number of security incidents over the last year:

- Loss of backup tapes in Alice Holt
- Staff being threatened in connection with Wild Boar Cull
- Lost HR Documents – reportable to the ICO.
- 3 items lost or stolen – all encrypted
- Breach in server security at Alice Holt through internal management problems
- Loss of FC bank account details by external supplier.
- Scam ICT support calls

All of these were followed up by the relevant SIRO and the DSO and reported to the ISMF.

Improving the procedures for managing information risk

16. There are generally well established procedures within the FC intended to address risk. These measures will be, or have been, strengthened through the actions shown below.

- Privacy Impact Assessments, as recommended by the Information Commissioner, have been introduced, and being used by staff, when building or procuring new systems that handle personal, or sensitive, information. For example, the proposed installation of number plate recognition in car parks has required considerable support.
- Review of Information risk management and Information Assurance roles, in line with new government policy and the developing guidance.
- Completion of the implementation of IAOs in all parts of the organisation.
- ISMF will discuss what further work may be required to maintain awareness of security issues across the FC.

Recommendation

17. That the EB note progress made in managing the risks associated with information security across the FC and considers any additional information they may require for their own Accounting/Accountable Officer reports.

Wilma Harper
ISMF Chair/FC SIRO
February 2015