Atributions for Security Audit and Assessment Team

The Security Audit and Assessment Team (SAAT) is a non-official body of the Organisation for the Prohibition of Chemical Weapons (OPCW) that provides valuable external advice to the Director-General regarding information security.
The Director-General of the OPCW invites States Parties to provide potential candidates for a new Security Audit and Assessment Team, for a period of four years.
The suitable candidates (who have extensive experience in IT auditing or similar experience) must sent the curriculum vitae, through their national authorities, to the OPCW.
The scope of the SAAT programme of work is to provide the Technical Secretariat with a mechanism for assessing the security status of the information systems used by it to process confidential or sensitive information.
This includes, but is not limited to, the Security Critical Network (SCN) and the Security Non-Critical Network (SNCN).
The scope of this mandate includes both paper- and electronic-based information-processing assets. The Information Security Management System (ISMS), as defined, includes in-house ICT assets, and also includes mobile devices (such as laptop computers and information storage media).

The mandate for the audit by the SAAT included a test of the following aspects of the information-processing environment of the Secretariat:
(a) the Verification Information System (VIS);
(b) audit logging and monitoring for both performance and access;
(c) change process and the software-release management process;
(d) incident-management controls;
(e) asset-management controls;
(f) records-management controls and the data-retention policy;
(g) the management of the life cycle of ICT resources, including media and identities;
(h) contract and acquisition management related to ICT services and ICT goods procured.
(i) the control of magnetic/removable storage media and procedures for managing laptops;
(j) physical security;
(k) the provision for disaster recovery , to include business continuity;
(l) an assessment of other open issues from previous evaluations, as required;
(m) the organisational governance of projects.