LOGGING AND AUDIT TRAILS

Policy

TABLE OF CONTENTS

TABLE OF TABLES

1 INTRODUCTION

This document defines the framework and principles for logging and audit trails (LAT) management within DG TAXUD information systems. LAT management is essential for identifying security incidents, policy violations, unauthorised/fraudulent activity and other operational problems. Also, LAT management ensures that security events are adequately captured, analysed and stored.

DG TAXUD should prioritise its goals for LAT management. The prioritisation must be based on balancing DG TAXUD's reduction of the identified risks with the time and resources needed to perform the effective LAT management.

1.1 DOCUMENT PURPOSE

The purpose of this document is to extend DG TAXUD's Security Reference Manual [RD5] with a specific policy for the management of the logging and audit trails (LAT) from information systems.

This policy document:

- contains the definition of logs and audit trails;
- explains why LAT management is an important process to ensure the security of the data and systems;
- outlines the scope of log management, covering secured collection, analysis, and storage of LAT data;
- defines specific Security Policies related to LAT management.

1.2 TARGET AUDIENCE

The intended readership of this document is:

- computer security staff
- sector leaders, project leaders, system owners and system managers
- system, network, and application administrators
- computer security incident response teams
- internal or external persons in charge of security audits
- all teams involved in projects specifications, development, operations and maintenance.

1.3 BUSINESS CONTEXT

In order to support European Union taxation and customs policies, DG TAXUD IT activity includes:

- The management of a number of operational activities:
  - a closed and secure trans-European communication network (named CCN/CSI);
  - several trans-European information systems and databases;
- The management of new projects that will later join the range of operational tasks;
- The support of DG TAXUD IT users.

The definition and maintenance of a coherent Logging and Audit Trail policy by DG TAXUD IT and the correct implementation of this policy is a crucial part of the IT Security Policy of DG TAXUD.

1.4 SCOPE

This LAT policy is applicable to all of DG TAXUD; including its external service providers in charge of the development, maintenance, support and operation of the Trans-European IT systems.

The LAT policy is applicable to all information systems owned by DG TAXUD, including those that are operated or managed by external service providers. Additionally, this policy is applicable to external service provider's information systems used in the provision of services to DG TAXUD. The only exception is DG TAXUD information systems hosted at the DG DIGIT Data Centre: this LAT policy only applies to the DG TAXUD boundaries (i.e. components for which it is responsible and which are under its control), not the LAT management by DG DIGIT. Nevertheless, key elements of this LAT policy should be integrated into OLAs concluded with DG DIGIT.

The LAT policy applies to systems in production. It can be extended to development and test environments.

Also, key elements of the LAT policy should be recommended to National Administrations and other Third Parties whose information systems are interconnected with those of DG TAXUD.

1.5 STRUCTURE

The Policy document is organised as follows:

- Section 1: An introduction to the Logging and Audit Trails Policy
- Section 2: Policy description, Strategic and Organisational Context, Security Principles

1.6 ASSUMPTIONS AND CONSTRAINTS

This document will need yearly review. In particular, it is important to maintain the coherence with the other sections of DG TAXUD's Information Security Reference Manual.

1.7 ACRONYMS AND ABBREVIATIONS

Acronym or Abbreviation	Description
DG TAXUD	Directorate General - Taxation and Customs Union
IS	Information System(s)
ISMS	Information Security Management System
LAT	Logging and Audit Trails
LISO	Local Information Security Officer

Table 1: List of acronyms and abbreviations

1.8 GLOSSARY

The terms used in this reference manual are compliant with the TEMPO Glossary of Terms [RD1]. This Glossary has been developed to provide a common language throughout the Commission, and to avoid confusion over local or national differences in terminology.

Term	Description
Audit Trail	A chronological record of events, such as system access, network load, unsuccessful logon attempts, and so on, that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Data Owners	Ensure the consistency and validity of the information in the domain in which the information system is used. They define the security needs of the data for which they are responsible and inform system owners of these needs.
Event (or information security event)	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Event Correlation	Correlating events (finding relationships between them) by matching multiple LAT entries from a single source or multiple sources based on logged values, such as timestamps, IP addresses, and event types.
Information Security Incident	An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information Security Management System (ISMS)	Is a management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structures, policies, planning activities, responsibilities, practices, procedures, processes and resources.
Information System	A set of equipment, methods and procedures, and where relevant also persons, organised to perform information processing functions.
IT Service Providers	IT service providers provide system owners with a range of structured and managed IT resources such as electronic communications networks, equipment and software. They maintain the level of security of their IT resources by applying the information systems security policy.
LAT Analysis	Studying log entries to identify events of interest.

Term	Description
LAT Archival	Retaining LAT files for an extended period of time, typically on removable media or on a centralized log server.
LAT Clearing	Removing all entries from a LAT file that precede a certain date and time.
LAT Entry	An individual record within a LAT file.
LAT File (or Log File)	A record of the events occurring within an information system or network.
LAT File Integrity Checking	Comparing the current message digest for a log to the original message digest to determine if the LAT file has been modified.
LAT Filtering	The suppression of LAT events from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
LAT Management (or LAT lifecycle)	The process (or lifecycle) of generating, transmitting, storing, analyzing, and disposing of LAT events.
LAT plan	A document describing the LAT requirements of the information system and all relevant information required to manage the LAT activities thereof.
LAT Preservation	Keeping LAT data that normally would be discarded, because they contain records of activity of particular interest.
LAT Retention	Archiving LAT files on a regular basis as part of standard operational activities.
LAT Rotation	Closing a LAT file and opening a new one when the first LAT file is considered to be complete, or a pre-defined duration has passed. By this rotation process, the content of the initial file is later overwritten, after archiving or not.
Logging	The process of storing information about events that occurred on a system or network.
Project Leaders	Project leaders are responsible for the installation and hand-over of the information system to the system owner. They shall specify the security requirements on the basis of the security needs defined by the latter, in the light of a risk assessment if necessary. They ensure that the design, installation and implementation of the project are in accordance with the security requirements of the information system and the information systems security policy.
System Managers	System Managers manage the operation of the information system on behalf of the system owner. They may manage the specific security measures directly themselves, or subcontract their management to IT service providers.
System Owner	System Owners bear responsibility for the security of their information system. They define the security needs of the information system and the information processed therein. To this end, they take note of the needs expressed by data owners and users.
System Supplier	System Suppliers construct and ensure the maintenance and development of the information system in accordance with the security requirements drawn up by the project leader and approved by the system owner.

Table 2: Glossary

1.9 REFERENCE DOCUMENTS

RD#	Title	Originator	Version	Date
RD1	TEMPO - Glossary of Terms (tmp-gen-gls)	DG TAXUD/A3	2.04-EN	01/08/2007
RD2	Decision 2002/47/EC, ECSC, Euratom - Commission Decision of 23/01/2002 amending its Rules of Procedure			24/01/2002
RD3	RFC 2119/EC - Key words for use in RFCs to Indicate Requirement Levels			March 1997
RD4	Information Security Policy	DG TAXUD/A3	1.2	27/11/2006
RD5	Information Security Reference Manual	DG TAXUD	1.1	08/11/2006
RD6	Decision 2006/3602/EC - Commission Decision concerning the security of information systems used by the European Commission	DG ADMIN/DS	1	11/08/2006
RD7	Personal Data Protection Guide	DG TAXUD/A3	1.5	16/11/2006

Table 3: Reference documents

1.10 TERMINOLOGY

In line with RFC 2119 [RD5] the following words are to be interpreted as defined below.

Word	Meaning
MUST	This word, or the terms '*REQUIRED*' and '*SHALL*', mean that the policy element is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase '*SHALL NOT*', means that the policy element is absolutely prohibited by the specification.
SHOULD	This word, or the adjective '*RECOMMENDED*', means that there may exist valid reasons in particular circumstances to ignore a particular policy element, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase '*NOT RECOMMENDED*' means that there may exist valid reasons in particular circumstances when the particular policy element is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective '*OPTIONAL*', means that a policy element is not obligatory and discretion can be used in determining whether to implement it or not.

Table 4: Terminology

2 THE POLICY

2.1 ROLES & RESPONSIBILITIES

The LISO is responsible for defining and maintaining the LAT Policy.

System Owners have the overall ownership of the LAT plans of the information systems they have been designated as owners. They must ensure that LAT policy elements are adequately addressed and incorporated into these systems.

System Managers and Project Leaders involved in projects specifications, development and maintenance must ensure that LAT policy elements are included in the systems they are developing or maintaining. System Managers and Project Leaders are responsible for managing the LAT plans for particular information systems on behalf of the System Owners.

2.2 STRATEGIC AND ORGANISATIONAL CONTEXT

2.2.1 LAT Policy Objectives

The objective of this policy is to address DG TAXUD's need to monitor its information systems in order to effectively identify security events and handle any information security incidents[1]. Appropriate configuration and monitoring of LAT is essential to ensuring the continued protection of DG TAXUD's information systems.

Specifically, the implementation of a LAT Policy by DG TAXUD will allow it to meet some of the following key security objectives:

- to detect risk materialising
- to trigger alerts or launch a response
- to record the extent of unauthorised activity and recover from it
- to ensure the integrity of evidence so that it can (if needed) be used in legal proceedings
- check the effectiveness of controls implemented

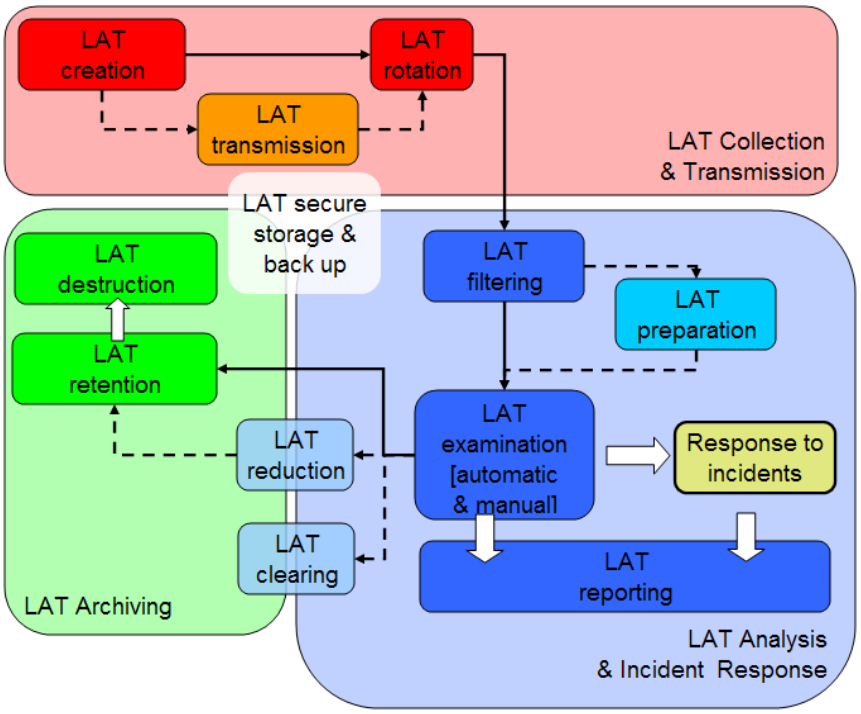
This is translated into the following security requirements:

- individual accountability
- the possible reconstruction of events
- the systematic detection of intrusion
- advanced incident analysis
- reliable alert management
- strict evidence preservation.

[1] This policy does not aim to cover capacity and performance monitoring objectives. Although these issues may be related, the intention is to focus solely on security.

2.2.2 The LAT Lifecycle

LAT data must be correctly and cost-effectively managed during the whole LAT lifecycle, from its creation to its deletion (after analysis and archiving). The LAT lifecycle of an information system is depicted and described below:



Secure collection & transmission of LAT data

- *Creation of LAT data:* Configuring systems to capture the necessary LAT events and generate LAT files.
- *Potential transmission of the LAT files to another system*
- *LAT rotation:* Closing a LAT file and opening a new LAT file when the first one is considered to be complete at a defined frequency (e.g. weekly, monthly).

Analysis of LAT data and incident response

- *Filtering and preparation of the LAT files:* The suppression of events from analysis and reporting because their characteristics indicate that they are unlikely to contain information of interest. If necessary, log data may be adjusted to a standard format.
- *LAT examination (automatic or manual):* Studying log entries to identify events of interest. Also, event correlation may be performed to identify relationships between two or more log entries.
- *Response to identified events (automatic or manual)*
- *LAT reporting:* This entails regular and/or ad-hoc reporting of LAT activities.

Storage of LAT data

- *LAT reduction:* The suppression of events from long-term storage because their characteristics indicate that they are unlikely to contain information of interest or that they need to be made anonymous.
- *LAT clearing:* Removing all entries from a log that precedes a certain date and time.
- *LAT retention:* Retaining LAT files for an extended period of time, typically on removable media or a centralized log server.
- *Log file integrity checking:* Calculating a message digest for each file and storing the message digest securely to ensure that changes to archived logs are detected.
- *Destruction of out-dated LAT data following expiration of the retention period*

For the whole lifecycle, it is necessary to define flexible LAT management methods that generate relevant volumes of LAT to manage. The log volume should be configurable, allowing for adjustments over time based on:

- the existing level of risk
- the damage that can be caused to the system
- the technology used to analyse the information produced.

2.3 SECURITY PRINCIPLES

2.3.1 General

Any LAT management activities (e.g. logging, examination, storage etc.) carried out on DG TAXUD information systems must comply with all relevant legal requirements, including personal data protection.

The LAT process must be activated on all DG TAXUD information systems. The amount and type of LAT events being generated should not disrupt the normal operation of the information system.

Any LAT related information (e.g. LAT file contents, LAT configuration, LAT plans, LAT analysis results etc.) of DG TAXUD information systems must be assigned the appropriate classification level (see Decision 2006/3602/EC - ANNEX I [RD6]). Any LAT related information must not be disclosed to any unauthorised persons.

All users must be notified that their activities on DG TAXUD information systems may be monitored.

2.3.2 Collection

The System Manager and Project Leader, in co-operation with the System Owner, are responsible for defining the LAT requirements of each DG TAXUD information system. The type of events to be logged and the frequency of LAT examination must be based on the information system's classification, risk level and legal requirements. The following parameters should be considered when defining the LAT requirements:

- data classification
- security incident history of the information system
- system interconnections (especially interconnection of DG TAXUD systems with non-trusted systems or networks).

As a minimum, the following types of LAT events must be logged at the network level:

- Time and date of every event
- Successful and unsuccessful attempts to access network resources
- Source/Destination Address and Network Service
- System configuration modifications.

As a minimum, the following types of LAT events must be logged at the operating system level:

- Time and date of every event
- Successful and unsuccessful login attempts
- Use of privileged accounts, e.g. root, administrator
- Service start/stop
- System start-up and shut down

As a minimum, the following types of LAT events should be logged at the operating system level:

- User and access right modifications (including: 1-addition/update/deletion of users; 2- changes to user permissions; 3- password changes)
- Successful and unsuccessful access to critical system files
- Security configuration modifications.

As a minimum, the following types of LAT events must be logged at the application level:

- Time and date of every event
- Successful and unsuccessful login attempts
- Application service/function accessed
- User and access right modifications (including: 1-addition/update/deletion of users; 2- changes to user permissions; 3- password changes)
- Security configuration modifications
- Unsuccessful attempts to access application data and resources
- Use of privileged accounts, e.g. administrator, super-user

Logging of sensitive information (such as passwords) must be disabled to avoid disclosure in case unauthorized persons get access to LAT files.

Any changes to LAT configuration parameters must be approved by the System Manager and Project Leader.

All information system clocks must be synchronised with an accurate time source. The objective of this requirement is to ensure the accuracy of LAT, which may be required for investigations or as evidence in legal or disciplinary cases.

A LAT Plan must be developed and maintained by the System Manager and Project Leader, in co-operation with the System Owner, for every information system owned by DG TAXUD. The LAT plan will define the LAT requirements of the system and all relevant information required to manage the LAT activities thereof. The LAT Plan must be approved by the LISO. Any changes to the information system that affect its LAT requirements should be adequately reflected in an updated LAT plan.

A review of LAT plans should be regularly (at least annually) performed by System Managers and Project Leaders to ensure the continued effectiveness thereof and that risks identified for the information systems continue to be appropriately managed.

2.3.3 Analysis

LAT analysis of DG TAXUD information systems must be performed in order to ensure the timely detection of security incidents (potential or actual) and system errors/malfunctions. The method used to perform LAT analysis (either automated or manual) should be determined by the System Manager and Project Leader, in co-operation with the LISO. Regular reporting must be performed of the LAT analysis activities (regardless of whether an alert has occurred or not) and the results of such activities must be documented.

Any suspicious LAT events must be immediately reported and all necessary actions for handling the incident taken.

The surveillance level (e.g. analysis frequency, LAT events to be alerted to etc.) of an information system that has been affected by a security incident must be increased for an extended period of time that must be determined by the System Manager and Project Leader, in co-operation with the LISO.

2.3.4 Storage

The System Owner, in co-operation with the System Manager and Project Leader, is responsible for defining the retention requirements of the LAT files (e.g. retention period, integrity protection (digital signing), classification etc.) for each DG TAXUD information system. The retention period must be based on legal and business requirements.

The storage capacity of systems hosting the LAT files must be periodically monitored to ensure the continued adequacy of storage media and therefore prevent the loss of the LAT recording (logging) capability. Also, these systems should be configured to how they will respond when the storage capacity approaches low levels and how this will affect logging.

Appropriate mechanisms for backing-up LAT files of DG TAXUD information systems must be implemented by the System Manager and Project Leader.

3 POLICY EXCEPTIONS

The principles and policies stipulated in this document must be strictly applied; unless otherwise stated, no exceptions are permitted. Any deviation that is necessary must be appropriately justified, documented and agreed with the LISO.

REVISION HISTORY

Edi.	Rev.	Date	Description	# Pages
1	40	20/10/2006	Initial Release	22
2	00	06/06/2008	New Release	22
2	02	20/05/2009	Updated draft version	17
3	00	26/06/2009	New Release	17

This document has been produced by the LISO (Local Information Security Officer) of Unit A3 (Information Technology) of Directorate General TAXUD (Taxation and Customs Union).

Comments regarding this document, or requests for further information, should be addressed to:

DG TAXUD/ Unit A3 LISO

Email address: TAXUD-LISO@ec.europa.eu

Reproduction of this document is authorised, except for commercial purposes, provided that the source of the document is acknowledged.