Audit Design Pattern Use Cases

# Recommendation 1: List of Proposed Audit Use Case Titles

* **Detect Audit Event**[[1]](#footnote-1)**:** Source detected audit event stub
* **Discriminate Audit Event**: Configure Event discrimination criteria and actions
* **Audit Record Creation and Disposition**: Audit event with creation with operational context, reporting sensitivity, etc.
* **Deliver Audit trail**: Delivers audit trail to configurable recording location, alarm service, or to other actions based upon disposition parameters
* **Record Audit Trail**: Records audit trail to enterprise store or exports/retrieves audit trail to/from archive.
* **Alerts and Alarms**[[2]](#footnote-2): Real time monitoring of known and unknown threats. Receives alarms. Immediately triggers or adds to collection to subsequently trigger an alarm and alarm response.
* **Perform Programmatic Action**: Performs program or special domain specific action based on audit trigger. Dynamic and real-time threat detection and response. For example: **Fraud Detection**
* **Security Analysis and Compliance Reporting**
* **Perform Analysis and Reporting**
* **Archive Audit trail/Restore from Archive**
* **Incident Investigation and Forensics**

# Recommendation 2: Use standard UML notation to document use cases:

## UML Diagram



# Recommendation 3: Use standard Use Case Descriptions

## Use Case Descriptions

### Use Case AU-1: Submit Audit Record[[3]](#footnote-3)

#### Description

Invoke a function to submit a record of an auditable event.

#### Assumptions

* In order for an audit trail to effectively support one or more distributed Audit Event Sources, those Sources, and all Audit Service components must maintain consistent time from a designated authoritative time service. The accuracy requirement of the coordinated timekeeping is a policy decision.
* Appropriate security controls are in place to ensure that adequate protection of the audit event information both in transit and at rest.

#### Actors

Audit Event Source

#### Trigger Event

The use case is triggered when one or more records of auditable events are ready to be transmitted[[4]](#footnote-4).

#### Pre-conditions

* The audit event source has been configured with the endpoint address of the Audit Service(s).

#### Post-conditions

* The Audit Service has accepted the audit event record(s).

1. VHA Audit Functional Model and SRSC audit requirements. [↑](#footnote-ref-1)
2. Both Monitors and responds to threats [↑](#footnote-ref-2)
3. An instance of the refinement of this use case into specifications at the Platform Specific level has been completed as DICOM Supplement 95 (ISO TS 12052), and the Record Audit Event transaction of the IHE ATNA specification (see Appendix B). These specifications are referenced in this document in the appropriate sections. [↑](#footnote-ref-3)
4. The use case is not necessarily triggered by the occurrence of an auditable event, although it can be. Generally, the Audit Event Source determines when conditions are appropriate to submit the audit event information. [↑](#footnote-ref-4)