

STANDARD OPERATING PROCEDURE	ISSUE DATE	SOP NO. OSQA-0101 revision 3.0	Page 1 of 6
TITLE: Standard Operating Procedure for Performing Internal Safety and Security Audits			
ISSUING DEPARTMENT: Office of Safety			
PREPARED BY:			
APPROVED BY: AGM of Safety & Quality Assurance			
SUPERSEDES: Procedure number OSQA – 0101 revision 2.0			

1.0 Purpose

The purpose of this procedure is to provide a process for conducting Internal Safety and Internal Security Audits to be performed in accordance with the requirements of the following documents:

- *System Safety Program Plan (SSPP)*,
- *System Security Plan (SSP)*,
- *Security and Emergency Preparedness Plan (SEPP)*,
- Georgia Department of Transportation/State Safety Oversight (GDOT/SSO), *Georgia Program Standard for Rail Transit Safety & Security Oversight*, and
- Federal Transit Administration/Federal Register/49 CFR Part 659/Rail Fixed Guideway Systems: State Safety Oversight; Final Rule.

The Office of Safety utilize Internal Safety and Security Audits to monitor and evaluate the effectiveness of the *System Safety Program Plan*, the *System Security Plan* and the *Security and Emergency Preparedness Plan*. Internal Safety and Security Audits facilitate effective compliance and implementation of statutory and regulatory requirements set forth by the State of Georgia and the Federal Transit Administration (FTA). Furthermore, the audit program presents opportunities for [transit agency] Management to institute improvements in System Safety.

2.0 Scope

This procedure applies to all relevant departments that have responsibilities defined in the *System Safety Program Plan (SSPP)*, *System Security Plan (SSP)*, and the *Security and Emergency Preparedness Plan*.

The required audit elements for Internal Safety and Internal Security Audits are listed below:

2.1 The following audit elements are applicable to Internal Safety Audits:

STANDARD OPERATING PROCEDURE	ISSUE DATE	SOP NO. OSQA-0101 revision 3.0	Page 2 of 6
TITLE: Standard Operating Procedure for Performing Internal Safety and Security Audits			

- Policy Statement and Executive Approval
- Purpose, Goals, and Objectives
- Management Structure
- Plan Review and Update
- System Safety Tasks and SSPP Implementation
- Hazard Management Process
- System Modifications
- Safety Certification
- Safety Data
- Accidents/Incidents
- Emergency Response
- Internal Safety Audits and Internal Security Audits
- Rules Compliance/Procedures Review
- Facilities and Equipment Inspections
- Maintenance Program Audits/Inspection
- Training and Certification
- Configuration Management
- Compliance with Local, State, and Federal Safety Requirements
- Hazardous Materials
- Drug and Alcohol Abuse Program
- Procurement

2.2 The following audit elements are applicable to Internal Security Audits:

- Policy Statement and Executive Approval
- Purpose, Goals, and Objectives
- Management Structure
- Plan Review and Update
- GDOT/SSO Review Process
- System Security Plans and Activities
- Internal Security Audits
- Security Data
- Threat and Vulnerability Management and Countermeasures
- Safety and Security Certification
- Passenger and Employee Security

STANDARD OPERATING PROCEDURE	ISSUE DATE / /	SOP NO. OSQA-0101 revision 3.0	Page 3 of 6
TITLE: Standard Operating Procedure for Performing Internal Safety and Security Audits			

- Training and Certification
- Security Events and Incidents
- Emergency Response and Preparedness

3.0 Procedure

3.1 Standard Practices

The manager of System Safety will designate a lead internal auditor who will be responsible for the implementation of this procedure.

In addition to the approved SSPP, SSP and SEPP, the auditor may use internal departmental Standard Operating Procedures and other pertinent process documents as a basis for preparing a checklist before beginning the on-site audit. Some typical examples of these procedures and other pertinent documents are listed below:

- System operating rulebooks, bulletins, notices and procedures
- Maintenance manuals and procedures for vehicles, track and signals, automatic train control equipment, preventative maintenance inspection records, employee training records, environmental compliance procedures, and any other documents found to have significant importance in regard to system safety,
- Previous internal and external audit reports,
- Corrective action plans for accidents and unacceptable hazardous conditions reported to GDOT and,
- NTSB accident investigation reports and other agency peer review reports.

Utilizing the above listed materials, the auditor shall prepare an audit checklist. The checklist should cite the sources that compel compliance to the checklist question. When possible the applicable reference documents that establish the acceptance criteria should be cited in the checklist.

Checklist audit questions have the following evaluation criteria:

- 1 – Meets Plan Requirements,
- 2 – Meets Plan with Comments,
- 3 – Needs Improvement/Finding,
- 4 – Unable to Audit, and
- 5 – N/A.

The audit procedures and checklist will determine if all audited elements are performing as intended. Checklists will be developed with sufficient criteria, for each audit, to verify compliance to the [agency] SSPP, SSP, SEPP and the requirements of the *Georgia Program Standard for Rail Transit Safety & Security Oversight*, and relevant internal agency documents, plans, policies, and procedures. The auditee will be required to demonstrate compliance with objective and verifiable evidence as the checklist questions require. The checklist will be submitted to GDOT for review thirty days prior to the start of each audit. The pre-audit checklist is preliminary and subject to modification as the audit progresses.

The lead auditor will schedule a pre-audit briefing and the audit; these arrangements should be agreed upon and acceptable to all parties. The pre-audit briefing will include the following:

STANDARD OPERATING PROCEDURE	ISSUE DATE //	SOP NO. OSQA-0101 revision 3.0	Page 4 of 6
TITLE: Standard Operating Procedure for Performing Internal Safety and Security Audits			

- A tentative checklist,
- Areas of audit,
- Relevant procedures/work instructions (authorized, controlled, and released), and
- The audit approach.

Auditors must be independent and can not conduct an audit in the direct or functional area in which the auditor is assigned. An auditor can not conduct an audit against his/her manager's area of responsibility.

The director, general superintendent, superintendent, or manager may participate in the audit or designate a facilitator and escort from the department being audited. The Director, General Superintendent, Superintendent, or Manager shall be at the exit meeting to be briefed, to review the results of the preliminary findings (if any), and to receive a preliminary verbal report.

The lead auditor shall review the documents provided to ensure they are relevant to the scope and purpose of the audit. The audit shall be conducted in an interview format by using the audit checklists to verify conformance to selected requirements against the specified reference criteria.

Objective evidence must be used to determine a finding. A finding is a non-conformity to policies, procedures, work instructions or any authorized document that requires compliance.

Objective evidence is verifiable qualitative or quantitative information, records or statements of fact that is based on observation, measurement, or test.

Verification shall be accomplished by:

- Interviews and discussion with personnel,
- Review of procedures and records,
- Firsthand observations of operations and maintenance activities, and
- Visual examinations and measurements.

Additional documents needed for verification should be requested in the interviews.

At all times, the auditor must:

- Perform a fact-based, verified audit which focuses compliance with the SSPP, SSP, and SEPP;
- Identify areas that merit safety improvements, which although compliant, should be considered for inclusion in the department's processes or program;
- Operate without personal bias, personal interest, and without placing, or identifying blame;
- Use open-ended questions and interview techniques to elicit discussion of safety programs, attitudes, and practices;
- Illuminate good practices culled from successful safety practices in the industry; and
- Provide professional support for corrective actions and safety program development.

Any audit finding which is deemed by the auditor to be an unacceptable hazard, that presents imminent danger, will be immediately resolved.

When appropriate, safety critical audit elements will be identified through a risk assessment (formal or informal), and an audit checklist will be developed to reflect the risk assessment. If any of these safety critical items are

STANDARD OPERATING PROCEDURE	ISSUE DATE //	SOP NO. OSQA-0101 revision 3.0	Page 5 of 6
TITLE: Standard Operating Procedure for Performing Internal Safety and Security Audits			

found to be non-compliant, the organization will work to implement effective corrective actions and set appropriate due dates commensurate with the risk index.

The audit report shall include, when appropriate, the auditor's recommendations for correcting deficiencies revealed by the audit. However, the audited department or contractor has the ultimate responsibility for developing and implementing an appropriate corrective action. When corrective action is required, the Office of Safety may be needed to examine the scope and extent of the underlying causes that led to the audit findings.

Following the completion of the on-site audit, the Lead Auditor shall prepare an audit report with the completed audit checklist. The final audit report will be distributed to the Director of the department audited, all relevant personnel in the department, the Director of the Office of Safety and the Manager of Safety. If the Management of the department subject to the audit disagrees with the results of the audit, the disagreement will be resolved by the Director of the Office of Safety and the Director of the audited department.

3.2 Notification

The Office of Safety will schedule internal safety and security audits thirty days in advance. The exceptions will be ad hoc audits that are not in the normal regimen. The Office of Safety will notify GDOT in writing thirty days in advance of all audits that are required by the *Georgia Rail Oversight Program Standard*. The advance notice will indicate the audit's start date, areas, functional units, departments, or offices. The required elements to be audited will be enumerated in the checklist and the checklist will be provided with the thirty-day advance notification.

3.3 Corrective Action Monitoring

The lead auditor will track corrective actions through completion. Corrective action due dates will be commensurate with the magnitude of the task; corrective action due dates should be reasonable, feasible and mutually agreed upon between the lead auditor, the manager of System Safety and the management of the audited department.

The Internal Safety and Security Auditor monitors implementation of corrective actions. The audit findings and the corrective actions are tracked in a corrective action monitoring log. The auditor verifies the effective implementation of the corrective actions and reserves the right to continue monitoring the corrective actions for proof of sustainability.

The Office of Safety will maintain a *Quarterly Corrective Action Monitoring Log*. The log will track and state the status of corrective actions generated by Internal Safety and Security Audits and document the implementation of the corrective actions, noting the date the finding was closed.

[transit agency] will verify corrective actions with objective and verifiable evidence and document the justification for closing audit issues and findings.

The following items will be included in the *Quarterly Corrective Action Monitoring Log* when there are open items for the respective categories:

- Accident Investigations
- Unacceptable Hazard Investigations
- Internal audits
- Triennial reviews
- GDOT on-site monitoring exercises

STANDARD OPERATING PROCEDURE	ISSUE DATE //	SOP NO. OSQA-0101 revision 3.0	Page 6 of 6
TITLE: Standard Operating Procedure for Performing Internal Safety and Security Audits			

Corrective Action Plans and Corrective Action Reports are governed by the following process:

- For each noncompliant audit finding a corrective action plan shall be developed and documented by the management of the department the finding was assessed against.
- The corrective action plan will be submitted to the Office of Safety for review and approval.
- The corrective action plan will identify the following:
 - the noncompliance finding, hazard or deficiency
 - the corrective action plan to remediate the open item
 - the principal department responsible for implementing corrective actions
 - the due date for completion of the corrective action
- The Office of Safety and the auditee will evaluate the completion time required for the execution of the corrective action plan and establish a due date for the implementation of the corrective action.
- The corrective action plan due date will be determined by the conditions and constraints of the issue to be remediated.
- Corrective Action Plans shall be submitted to GDOT State Safety Oversight for approval within 30 calendar days after the finding is issued in the subsequent audit report.
- The Office of Safety will monitor the implementation of the corrective action plan.
- The closing of an open item requires a corrective action report that describes the process involved to address the open item and to describe the action taken to remediate the noncompliance.
- To close a corrective action the Office of Safety shall state in a report the objective evidence that validates the closing of an open item.
- The final corrective action report will be submitted to GDOT SSO ten days after the close of each fiscal year quarter.

3.4 GDOT SSO Audit Reports

At the conclusion of each Internal Safety Audit and each Internal Security Audit the Office of Safety will prepare a written report that documents findings, recommendations (if any), and any corrective actions identified as a result of the audit. [transit agency] Office of Safety and/or [agency] Police will make arrangements with external audit agencies for on-site review of any security-sensitive materials.

Applicable audit reports will be sent to GDOT ten days after the close of each fiscal year quarter with the *Corrective Action Monitoring Log/GDOT/State Safety Oversight Reportable*.