



This is a template only. Do not use this document without editing it to meet your needs. Users are responsible for acceptance of content and suitability for intended use.

Internal Evaluation Program

*See the document: **Working with Omni Manuals**
for editing instructions and procedures*

Revision: 4
20 Feb 2018

Serial Number: _____

Assigned to: _____

Position: _____

AIRCRAFT N _____ (if applicable)

Date of Assignment: _____

If found, please return this program to:

Your Company
6421 South Dorset Road
Spokane, WA 99224
USA
Tel. +1 509.838.8121

This program is the property of Your Company, and contains proprietary information. It may not be copied, printed or reproduced in any manner without the express written consent of YCO. The person to whom this program has been assigned is responsible for the safekeeping of this program and the timely insertion of all revisions in accordance with the procedures contained herein.

THIS PAGE INTENTIONALLY LEFT BLANK

Record of Revisions

Program Serial Number: _____

Insert all revisions immediately. Briefly describe the revision or change, and enter the revision effective date and initials of the person inserting the revision.

Revision	Description of Change	Revision Effective Date	Revision Inserted By
Original	Original Issuance	04 April 2012	N/A
1	Inclusion of Compliance Monitoring	08 Nov 2014	PMS
2	Align / update with FAA SMSVP Standard	29 July 2016	PMS
3	Integrate with OmniSMS™ v4 Web App.	04 June 2017	PMS
4	Integrate Quality System Findings	20 Feb 2018	PMS
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

THIS PAGE INTENTIONALLY LEFT BLANK

List of Effective Pages (LEP)

Revision No. 3

Effective Date: 20 Feb 2018

<i>PAGE.</i>	<i>REV. NO.</i>	<i>EFFECTIVE DATE.</i>
RECORD OF REVISIONS		
1	3	20 Feb 2018
2	3	20 Feb 2018

LIST OF EFFECTIVE PAGES		
3	3	20 Feb 2018
4	3	20 Feb 2018

TABLE OF CONTENTS		
5	3	20 Feb 2018
6	3	20 Feb 2018

1. POLICIES AND PROCEDURES		
1-1	3	20 Feb 2018
1-2	3	20 Feb 2018
1-3	3	20 Feb 2018
1-4	3	20 Feb 2018
1-5	3	20 Feb 2018
1-6	3	20 Feb 2018
1-7	3	20 Feb 2018
1-8	3	20 Feb 2018
1-9	3	20 Feb 2018
1-10	3	20 Feb 2018
1-11	3	20 Feb 2018
1-12	3	20 Feb 2018
1-13	3	20 Feb 2018
1-14	3	20 Feb 2018
1-15	3	20 Feb 2018
1-16	3	20 Feb 2018
1-17	3	20 Feb 2018
1-18	3	20 Feb 2018
1-19	3	20 Feb 2018
1-20	3	20 Feb 2018
1-21	3	20 Feb 2018

Your Company Acceptance:

FAA Acceptance:

THIS PAGE INTENTIONALLY LEFT BLANK

Internal Evaluation Program

Table of Contents

1.1 OVERVIEW	1
1.2 SCOPE	1
1.3 OBJECTIVES AND GOALS	1
1.3.1 REGULATORY COMPLIANCE.....	1
1.3.2 RISK CONTROL PERFORMANCE AND EFFECTIVENESS	1
1.3.3 SATISFACTORY PROCESS OUTPUTS	1
1.3.4 CONTINUAL IMPROVEMENT.....	2
1.4 RESPONSIBILITIES AND AUTHORITIES	2
1.4.1 ACCOUNTABLE EXECUTIVE.....	2
Interface – SMS Manual 7.3.2	2
1.4.2 DIRECTOR OF SAFETY	2
Interface – SMS Manual 7.4.1	2
1.4.3 DEPARTMENT MANAGERS.....	3
Interface – SMS Manual 7.6.1	3
1.4.4 SAFETY ACTION GROUP	4
Interface – SMS Manual 7.5.2	4
1.4.5 PERSONNEL.....	4
Interface – SMS Manual 7.7.1	4
1.4.6 AUDITORS	4
1.5 AUDITOR COMPETENCY REQUIREMENTS	5
1.5.1 GENERAL KNOWLEDGE AND EXPERIENCE.....	5
1.5.2 SPECIALIZED KNOWLEDGE AND EXPERIENCE	5
1.5.3 APPOINTMENT OF AUDITORS.....	5
1.6 GENERAL AUDITING PROTOCOL	5
1.6.1 OPENING AND CLOSING MEETINGS	5
1.6.2 FINDINGS AND OBJECTIVE EVIDENCE	6
1.6.3 DISPUTE RESOLUTION	6
1.7 DEPARTMENTAL AUDITS	6
1.7.1 AUDIT PLANNING.....	6
1.7.2 BASELINE STANDARD	6
1.7.3 FREQUENCY OF DEPARTMENTAL AUDITS	7
1.7.4 DEPARTMENTAL AUDIT PROCEDURES	7
1.8 EXTERNAL PROVIDER AUDITS	7
1.8.1 EXTERNAL PROVIDER AUDIT CHECKLISTS	7
1.8.2 BASELINE STANDARD.....	7
1.8.3 FREQUENCY OF EXTERNAL PROVIDER AUDITS.....	8
1.8.4 EXTERNAL PROVIDER AUDIT PROCEDURES	8
1.8.5 DISPOSITION OF EXTERNAL PROVIDER AUDITS	8
1.8.6 EXTERNAL PROVIDER AUDIT STATUS LOG	9
1.9 INTERNAL EVALUATIONS	10
1.9.1 EVALUATION PLANNING.....	10
1.9.2 BASELINE STANDARD.....	10

Sample only - some content may not display

1.9.3 FREQUENCY OF INTERNAL EVALUATIONS 10

1.9.4 COMPLIANCE WITH RISK CONTROLS 10

1.9.5 CONFORMANCE WITH RISK CONTROLS 11

1.9.6 CONFORMANCE WITH SMS OBJECTIVES 11

1.9.7 INTERNAL EVALUATION PROCEDURES 11

1.10 COMPLIANCE MONITORING 12

1.10.1 REGULATORY COMPLIANCE 12

1.10.2 CM AUDIT PLANNING 12

1.10.3 CM AUDIT PROCEDURES 12

1.11 FINDINGS 13

1.11.1 INITIAL ASSESSMENT 13

1.11.2 CLASSIFICATIONS OF FINDINGS / CONCERNS 13

Interface – AFR Form QA-010 13

1.11.3 INITIAL RISK ASSESSMENT 14

1.11.4 DOCUMENTING AUDIT FINDINGS 14

1.11.5 COMPLETING THE AUDIT FINDING REPORT QA-010 14

1.11.6 AUDIT FINDING REPORT DISPOSITION 15

1.11.7 APPLICATION OF QUALITY AND SAFETY RISK MANAGEMENT 15

1.12 ANNUAL MANAGEMENT REVIEW 16

1.12.1 SENIOR MANAGEMENT RESPONSIBILITIES 16

1.12.2 DIRECTOR OF SAFETY RESPONSIBILITIES 16

1.12.3 MANAGEMENT REVIEW BOARD MEMBERS' RESPONSIBILITIES 16

1.13 MANAGEMENT REVIEW PROCESS 17

1.13.1 MANAGEMENT REVIEW QUESTIONNAIRE 17

1.13.2 SYSTEM DESCRIPTION REVIEW AND UPDATE 17

1.13.3 SAFETY RISK PROFILE REVIEW 17

1.13.4 OPERATIONAL PERFORMANCE REVIEW 18

1.13.5 KEY SAFETY PERFORMANCE INDICATOR REVIEW 18

1.13.6 SMS PERFORMANCE REVIEW 18

1.13.7 REVIEW OF OPEN EMPLOYEE REPORTS 18

1.13.8 REVIEW OF VIOLATIONS AND SELF-DISCLOSURES 18

1.13.9 REVIEW OF AUDIT FINDING REPORTS 19

1.13.10 REVIEW OF THE INTERNAL EVALUATION PROGRAM 19

1.13.11 REVIEW OF THE EMERGENCY RESPONSE PLAN 19

1.13.12 MANAGEMENT REVIEW COMMUNICATIONS 19

1.14 DOCUMENTING MANAGEMENT REVIEWS 20

1.14.1 MANAGEMENT REVIEW FORM QA-017 20

1.14.2 AUDIT FINDING REPORT QA-010 20

1.15 EMERGENCY RESPONSE EXERCISES 20

1.15.1 ACCIDENT RESPONSE 20

1.15.2 MINOR EXERCISES 20

1.15.3 LOCAL EXERCISES 20

1.15.4 SPECIALTY EXERCISES 20

1.15.5 PRE-EXERCISE BRIEFING 21

1.15.6 POST-EXERCISE DEBRIEFING 21

1.15.7 SIMULATION SCHEDULING 21

Internal Evaluation Program

1. Policies and Procedures

1.1 OVERVIEW

- (A) The YCO Internal Evaluation Program (IEP) provides written guidance to managers and auditors when performing **departmental audits, internal evaluations, compliance monitoring, and external provider audits**. These safety and quality assurance activities are designed to:
- (1) Identify instances of non-compliance with regulations, as well as policies / procedures;
 - (2) Assure that safety risk controls conform to their intended design and are effective;
 - (3) Evaluate external providers' abilities to deliver quality products / services with a high level of safety.
- (B) **Quality system audits** may also be performed IAW the guidance contained herein, in order to identify:
- (1) Process deficiencies and nonconformances in products and services provided;
 - (2) Opportunities for improvement in quality or a process.
- (C) **Management reviews** further aid senior managers and process owners in identifying system / process deficiencies, and in meeting the objectives and expectations of both the SMS and the QMS.
- (D) Use of this Internal Evaluation Program enables managers to proactively identify both safety hazards and quality deficiencies. Data is then analyzed to reveal root causes and develop effective corrective action plans, resulting in continuing improvement over time.

1.2 SCOPE

- (A) Your Company provides safety and quality assurance covering the complete scope and life cycle of all systems and operational processes. Refer to the SMS Manual's **Introduction – Scope of Safety Management** for a complete listing of all systems and operational processes which are assured through this Internal Evaluation Program.

1.3 OBJECTIVES AND GOALS

1.3.1 REGULATORY COMPLIANCE

- (A) One primary objective of the IEP is to assure continued regulatory compliance with various regulations that apply to YCO's aviation activities, including applicable parts of the Federal Aviation Regulations (FARs) and other federal, foreign, state, and local requirements.

1.3.2 RISK CONTROL PERFORMANCE AND EFFECTIVENESS

- (A) The IEP measures performance and the effectiveness of risk controls. The objective of this safety assurance process is to correct non-conformities with risk controls within each specific department's operational processes, and to improve the performance of ineffective risk controls.

1.3.3 SATISFACTORY PROCESS OUTPUTS

- (A) **Internal audits, evaluations, system assessments, and management reviews** extend beyond measuring the performance of risk controls to identify and correct unsatisfactory operational process outputs, as well as SMS and QMS process outputs.

1.3.4 CONTINUAL IMPROVEMENT

- (A) This Internal Evaluation Program provides a structured, documented method of establishing and promoting a system of continual improvement through quality management. The goal of these efforts is to proactively identify weaknesses in YCO management systems, operational processes, procedures, and employee training in order to efficiently target continual improvement strategies.
- (B) As departmental audits, external provider audits, internal evaluations and management reviews are performed, findings may reveal new hazards and existing system / process / control deficiencies. Each finding is reported into the OmniSMS application as a **Finding** for analysis of data and risk assessment (see [SMS Manual para. 3.1.9 Analysis of Data](#)).
- (C) Deficiencies in operational processes / existing risk controls and newly identified hazards are recorded in the OmniSMS application, and safety risk management (SRM) processes are applied. Follow-ups recorded within OmniSMS assure the effectiveness of resulting risk controls and corrective actions.
- (D) Results of SRM are communicated to appropriate personnel through memos, safety comms, and lessons learned. This results in continual improvement, and enhances safety and quality throughout the organization.

1.4 RESPONSIBILITIES AND AUTHORITIES

1.4.1 ACCOUNTABLE EXECUTIVE

Interface – SMS Manual 7.3.2

- (A) **RESPONSIBILITIES:** The Accountable Executive, as an authorized representative of senior management, is responsible and accountable for the accomplishment of this Internal Evaluation Program. This includes establishing the frequency of all **departmental audits, internal evaluations and management reviews**. The Accountable Executive is further responsible for [REDACTED] Internal Evaluation Program.
- (B) **AUTHORITY:** The Accountable Executive, as an authorized representative of senior management, is authorized to [REDACTED] supplement this IEP with external audits from outside sources, and to direct the revision of this IEP as necessary. The Accountable Executive is authorized to [REDACTED] records in the OmniSMS database, and to implement Corrective Action Plans (CAPs) to address valid audit findings.

1.4.2 DIRECTOR OF SAFETY

Interface – SMS Manual 7.4.1

- (A) **RESPONSIBILITIES:** The Director of Safety (DOS) is responsible for [REDACTED] Executive and the Safety Action Group, the results of each internal evaluation performed. The DOS is responsible for the organization, filing, security and maintenance of all internal evaluation records, including associated Audit Finding Reports and records within the OmniSMS database.
- (B) **AUTHORITY:** The Director of Safety is authorized to [REDACTED] conduct reviews of various tasks within OmniSMS that have been requested of department managers or other process owners, as they apply to audit and evaluation findings, including:
 - (1) Investigations of contributing factors and root causes;
 - (2) Development of Corrective Action Plans;

- (3) Completion of Fixit! tasks and other corrective actions;
 - (4) Implementation of individual risk controls;
 - (5) Monitoring (if required) and follow-up on risk controls that have been implemented.
- (C) The DOS is authorized to [REDACTED] authority to establish and modify or revise this IEP as necessary, in accordance with the requirements of the company's SMS Manual and YCO document revision procedures.
- (D) The Director of Safety is authorized to [REDACTED] is warranted.

1.4.3 DEPARTMENT MANAGERS

Interface – SMS Manual 7.6.1

- (A) **RESPONSIBILITIES:** Department managers are responsible for the planning and conduct of **departmental audits** and **compliance monitoring** within their respective departments. This includes [REDACTED] managers are further responsible for:
- (1) The planning, conduct and completion of all **external provider audits** (such as contracted fueling, deicing or maintenance companies) for products and services received from external providers that apply to the operational processes each manager owns;
 - (2) Developing and implementing Corrective Action Plans (CAPs) within their respective departments;
 - (3) Monitoring (as required) and follow-ups on all risk controls that apply to the processes they own;
 - (4) Communicating CAPs and lessons learned to appropriate department personnel.
- (B) Department managers are responsible for [REDACTED] provider audit status logs, and associated finding reports. Each manager is responsible for the prompt recording of all audit findings within the OmniSMS application, and for the prompt reporting of all NCP-R (non-compliance with regulations) findings to the Accountable Executive.
- (C) Department managers shall maintain full cooperation with the Director of Safety (or his delegated auditor) during the conduct of internal evaluations and for assisting the Director of Safety in the collection of data during these evaluations.
- (D) **AUTHORITY:** Department managers are authorized to [REDACTED] department staff members, but delegated auditors shall not audit their own work. Department managers are authorized to direct an accelerated audit schedule, repeat audits, follow-ups and audits of external providers for products and services that pertain to the operational processes they own.
- (E) During the performance of a departmental audit, department managers are authorized to take IMMEDIATE ACTION, including cessation of flight operations or maintenance activities, to mitigate risk if a finding indicates that **HIGH / RED / UNACCEPTABLE** levels of risk may exist. Managers are also authorized to make [REDACTED] should be brought to the attention of the Director of Safety for disposition.
- (F) Department managers are NOT AUTHORIZED to discuss findings of apparent violations until reviewed by the Accountable Executive for proper liaison with regulatory authorities, in order to protect YCO and all personnel involved from potential certificate action and/or civil penalties.

1.4.4 SAFETY ACTION GROUP

Interface – SMS Manual 7.5.2

(A) **RESPONSIBILITIES:** Members of the Safety Action Group are jointly responsible for:

- (1) Review and validation of [REDACTED] more than one department;
- (2) Gathering of additional data if [REDACTED] finding;
- (3) Reviewing and [REDACTED]

[REDACTED] at regularly scheduled meetings. For valid findings that warrant corrective action, the SAG is authorized to review and accept Corrective Action Plans (CAPs) designed to mitigate risk, as developed by department managers. In the event audit findings are of an urgent nature, the [REDACTED]

[REDACTED], and take whatever actions are necessary to mitigate risk, in the best interest of Your Company.

1.4.5 PERSONNEL

Interface – SMS Manual 7.7.1

- (A) **RESPONSIBILITIES:** All personnel are responsible for aiding and assisting department managers during the conduct of departmental audits, and for assisting the Director of Safety (or his delegated auditor) during the conduct of internal evaluations. During these audits and evaluations, personnel are encouraged to bring to the attention of management any related safety concerns or perceived process deficiencies, without fear of retribution.
- (B) **AUTHORITY:** All personnel are authorized to accept risk associated with audit findings that are assessed as **LOW / GREEN / ACCEPTABLE**, and to accomplish **Fixit!** action requests or other corrective actions as requested by department managers.

1.4.6 AUDITORS

- (A) **RESPONSIBILITIES:** Auditors report directly to [REDACTED] of Safety when conducting internal evaluations. If, during the course of an audit, the auditor determines that he or she is being asked to audit his or her own work, that portion of the audit must be completed by another qualified auditor. **In no case may an auditor audit his or her own work.**
- (B) Auditors are responsible for [REDACTED] apparent finding that may be considered high risk. Auditors shall take whatever measures are necessary to prevent injury or accident if areas of high risk are discovered during an audit.
- (C) Auditors should openly share with [REDACTED] department manager or external provider POC, an initial assessment of each apparent audit finding to determine if the potential exists for regulatory non-compliance. Auditors are further responsible for prompt and thorough submission to appropriate managers all completed departmental audits and external provider audits, and to the Director of Safety all completed internal evaluations, together with any audit findings.
- (D) **AUTHORITY:** Auditors are authorized to [REDACTED] Safety and senior management. In the event audit findings appear to reveal an area of high risk, auditors are authorized to take immediate actions to prevent injury or accident.

1.5 AUDITOR COMPETENCY REQUIREMENTS

1.5.1 GENERAL KNOWLEDGE AND EXPERIENCE

- (A) YCO auditors should have training and/or experience in one or more of the following disciplines and areas of study: Quality assurance auditing, systems analysis, root cause analysis, risk assessment, and auditing principles / techniques.
- (B) Any one or combination of the following could accomplish this training:
 - (1) In-house prepared courses;
 - (2) eLearning courses from a reputable industry source;
 - (3) Home study course materials;
 - (4) Industry seminars and workshops.

1.5.2 SPECIALIZED KNOWLEDGE AND EXPERIENCE

- (A) Knowledge and experience specific to the department or operational process being audited is essential for the auditor to understand the processes he or she is evaluating. For example, even with the general knowledge and experience required above, a pilot without an A&P license or maintenance experience would not make an appropriate auditor of maintenance department processes.

1.5.3 APPOINTMENT OF AUDITORS

- (A) Auditors should be selected by the Director of Safety jointly with each department manager. Only those persons with substantial knowledge of the department and various department processes should be selected to be an auditor for that department. After an auditor candidate has been mutually agreed upon by the Director of Safety and the appropriate department manager, the auditor candidate should receive training and be formally appointed by Letter of Appointment from the Director of Safety or appropriate department manager.

NOTE:

All letters of appointment should specify which departments and/or operational processes the auditor is authorized to audit and evaluate. Letters of Appointment are retained and filed by the DOS.

1.6 GENERAL AUDITING PROTOCOL

1.6.1 OPENING AND CLOSING MEETINGS

- (A) When possible, each scheduled audit or evaluation should begin with an opening meeting. The purpose and goal of the meeting is to ensure that the person responsible for the operational process or department being audited understands the reason for the audit, how the audit will be conducted, and what will be accomplished at the completion of the audit.
- (B) A closing meeting should be accomplished with the department head or external provider Point-of-Contact (POC) to ensure the responsible person completely understands any and all non-conformance issues discovered during the audit process. Areas that exceed company requirements should also be discussed during the closing meeting.

1.6.2 FINDINGS AND OBJECTIVE EVIDENCE

- (A) When determining whether a finding will be recorded, auditors must base their assessment on a representative sample of objective evidence of conformance or non-conformance to documented regulatory requirements, standards, [REDACTED] and observations of work in progress.
- (B) Any findings that represent a critical failure of a system, process or function should be corrected on the spot, whenever [REDACTED] example, if safety-critical suspected unapproved parts (SUP) [REDACTED] investigation reveals they may have been installed on aircraft in service, aircraft may need to be grounded until all suspect aircraft can be inspected.
- (C) Some apparent findings may be [REDACTED] cases, on-the-spot corrections should be made and documented by the auditor on the Audit Finding Report.
- (D) Findings are recorded on **Audit Finding Report (AFR) Form QA-010**.

1.6.3 DISPUTE RESOLUTION

- (A) All personnel should understand that audits and evaluations are not intended to locate blame, finger-point or find fault. Rather, they should be [REDACTED] result in disputes which are not resolved during the closing meeting, will be arbitrated and decided by the Safety Action Group.

1.7 DEPARTMENTAL AUDITS

1.7.1 AUDIT PLANNING

- (A) A departmental audit determines conformity with risk controls pertaining to the department's operational processes, and assesses the performance of those risk controls.
- (B) To plan for a departmental audit, department managers should [REDACTED] weight & balance, required inspection items, de-icing / anti-icing, carriage of dangerous goods, etc.) should be given more consideration and scrutiny than those with less safety significance.
- (C) The results of previous audits for the processes being audited should also be reviewed, and any audit findings from previous audits incorporated into the planned audit.

1.7.2 BASELINE STANDARD

- (A) As a baseline standard of minimum safety, each department manager should perform a **system assessment** within the OmniSMS database for all risk controls pertaining to operational processes within their respective departments. Particular attention should be paid to [REDACTED] r each risk control, review appropriate documents / records and observe related operational processes, in order to determine conformity and effectiveness of the control.

NOTE:

Refer to the SMS Manual Section 3, **paragraph 3.2.1 System Assessment** for instructions on how to perform a system assessment within the OmniSMS application.

1.7.3 FREQUENCY OF DEPARTMENTAL AUDITS

- (A) After each department's baseline standard has been established, a complete departmental audit (including a review of all applicable risk controls) should be conducted no less than once every 24 months. In addition, special audits which target specific safety-critical operational processes and/or areas of high risk may be conducted whenever:
- (1) Changes occur in YCO Operations Specifications;
 - (2) Changes occur to the YCO Safety Risk Profile;
 - (3) Changes occur in key management personnel;
 - (4) New equipment or types of operations are commenced.

1.7.4 DEPARTMENTAL AUDIT PROCEDURES

- (A) Perform a **system assessment** within the OmniSMS database to produce a list of all risk controls that pertain to the department's operational processes. Then review any findings from the department's previous audit and incorporate the risk controls and/or corrective actions from the previous findings into the planned audit.
- (B) Conduct the audit by systematically [redacted] and personnel. Audit findings are often subject to interpretation. In such a case, it is advisable to get a second opinion from someone within the department who has expertise in the area being audited. Procedures for assessing and recording valid audit findings may be found in [paragraph 1.11: Findings](#) below.
- (C) When conducting departmental audits, evidence of regulatory noncompliance may be revealed. It is possible for evidence of a past violation to exist in flight or maintenance records, for example, without an associated safety risk. Other violations may be [redacted] of operations, voluntary disclosure, and a comprehensive fix to prevent recurrence.

NOTE:

Regulatory violations may be indicative of serious safety concerns. They also present potential liabilities to YCO and its personnel in the form of civil penalties and/or certificate action(s). Any apparent violation demands immediate notification to senior management.

1.8 EXTERNAL PROVIDER AUDITS

1.8.1 EXTERNAL PROVIDER AUDIT CHECKLISTS

- (A) External provider audit checklists are developed by responsible department managers for use by delegated auditors. These checklists include both minimum standards (such as fuel grade specifications or facility requirements) and [redacted] that are not answered positively, or for which the auditor is unable to answer, may indicate risk requiring corrective action on the part of the external provider's Point-of-Contact (POC).

1.8.2 BASELINE STANDARD

- (A) As a baseline standard of minimum safety performance, each external provider utilized by Your Company for routine fueling, deicing, training, and contract maintenance services should be initially audited using [External provider Tabletop Audit Form VO-01](#). The initial audit should focus on those products or services which, if risk is not properly controlled, would result in the highest risk for Your Company. The YCO

manager responsible for the external provider's performance should perform a review of all risk controls the external provider has established to mitigate such risk.

1.8.3 FREQUENCY OF EXTERNAL PROVIDER AUDITS

- (A) After an external provider's baseline standard of performance has been established, the external provider should be routinely audited no less than once every 24 months. In addition, a special audit targeting specific areas of performance should be conducted whenever:
- (1) Areas of concern exist as determined by regulatory authorities;
 - (2) Aviation industry trends are identified;
 - (3) Abnormal reliability trends appear;
- (B) Operational processes or products [REDACTED] priority. Even the perception that a problem exists in a particular operational process or product / service is adequate justification for an external provider audit to be conducted.
- (C) Although an external provider audit may be conducted immediately following an incident or report of a hazard, it is essential for external [REDACTED], and to enhance system safety.

1.8.4 EXTERNAL PROVIDER AUDIT PROCEDURES

- (A) As a courtesy, both the responsible department manager and the individual(s) conducting the audit should contact the external provider's Point-of [REDACTED] area being audited will be assigned to audit external providers.
- (B) When possible, the audit should be scheduled to ensure minimum disruption of daily activities and work schedules. During the course of the audit, auditors should be careful to:
- (1) Foster a cooperative working relationship;
 - (2) Perform initial validation and risk assessment of apparent findings;
 - (3) Ensure the audit's smooth flow, resulting in minimum disruption to the external provider.
- (C) Perform a *find* within OmniSMS to produce a list of all reported hazards and occurrences that involve the external provider to be audited. Then review any findings from the external provider's previous audit and incorporate the risk controls and/or corrective actions from previous findings into the planned audit.
- (D) Conduct the audit by systematically reviewing audit criteria (e.g., applicable regulations, existing risk controls and previous audit results). Confirm compliance and conformance through review and careful evaluation of pertinent documents, records, [REDACTED] opinion from someone within the external provider's organization and / or the YCO responsible manager's department whose expertise will support finding assessment and validity.

1.8.5 DISPOSITION OF EXTERNAL PROVIDER AUDITS

- (A) An external provider audit's closing meeting provides opportunity to further cooperative working relationships and immediately improve external provider processes.
- (B) Form **QA-010 Audit Finding Report** (AFR) should be completed, and results shared at the closing meeting with the external provider POC (and other external provider personnel at the POC's discretion). This provides an opportunity for the external provider to promptly correct minor deficiencies (which can be recorded on the AFR as corrective action taken), or present additional information / evidence that could negate a finding.

NOTE:

Completed audit checklists and their associated AFRs are returned to the YCO responsible manager for disposition and follow-up with the external provider POC in accordance with **Paragraph 1.8.6** below.

1.8.6 EXTERNAL PROVIDER AUDIT STATUS LOG

(A) The **External provider Audit Status Log QA-011** is used internally by YCO responsible managers to track the progress of external provider audits and status of external provider POCs' corrective action plans / fixes, submitted to YCO in response to audit findings. Form QA-011 includes the following information:

- (1) Company name / department of the external provider / department being audited.
- (2) Type of audit being accomplished.
- (3) Name / department of the YCO manager responsible for oversight of the external provider's services.
- (4) Audit checklist(s) used to perform the audit and date the audit was initiated.
- (5) Name / tel. number / email [REDACTED]

[REDACTED] action plan (CAP) or fix that was initially rejected by the YCO responsible manager or Safety Action Group (SAG).

- (5) Date the POC's CAP or fix is due back from the POC. This date shall be within:
 - (a) 10 working days of the date the original AFR report was sent to the POC.
 - (b) 5 working days after the return of a CAP/fix initially rejected by the responsible manager or the Safety Action Group.
- (6) Date the POC's AFR response (CAP or fix) was received by YCO.
- (7) Acceptance or rejection of the POC's CAP/fix by the responsible manager and/or the Safety Action Group, together with the date thereof:
 - (a) If the CAP/fix for a specific [REDACTED] [REDACTED] and approved.
- (9) Follow-up date of the POC's affected operational process or functional area. This will be determined by:
 - (a) Safety-criticality of the external provider's product / service;
 - (b) Risk level of the finding;
 - (c) Complexity and time-to-implement of the external provider's accepted corrective action plan or fix.

NOTE:

Depending on the level of risk, an external provider's CAP/fix may be accepted by the responsible manager. Higher-risk acceptance decisions may require the external provider's CAP be accepted by the Safety Action Group. Refer to the SMS Manual **Paragraph 1.2.6: Risk Acceptance Authority for OmniSMS Risk Assessments** for more information regarding risk acceptance authority.

1.9 INTERNAL EVALUATIONS

1.9.1 EVALUATION PLANNING

- (A) The Director of Safety performs (or oversees the performance of) internal evaluations of operational departments. This begins by planning the evaluation. As a courtesy, the manager of the department being evaluated should be alerted, and the evaluation scheduled with input from the department manager to ensure minimum disruption of daily activities and work schedules.
- (B) During the course of the evaluation, auditors work together with the department manager and / or delegates to obtain quick access to [REDACTED] department.
- (C) When properly performed, internal evaluation of a department will:
- (1) Evaluate the department's compliance with policies, procedures, standards and best practices;
 - (2) Determine if risk controls within the department are conforming and effective;
 - (3) Determine if the SMS is conforming to [REDACTED].

1.9.2 BASELINE STANDARD

- (A) As a baseline standard, the Director of Safety performs [REDACTED], as these controls have a high level of associated risk and safety criticality.
- (B) Using these risk controls as a baseline standard, the Director of Safety (DOS) reviews assigned responsibilities for each risk control and analyzes each control in order to understand interfaces and interactions between personnel, departments and external providers.
- (C) Appropriate documents and records (to which each risk control relates) are reviewed, and operational processes are observed (if possible), in order to determine conformity and effectiveness of each control.

1.9.3 FREQUENCY OF INTERNAL EVALUATIONS

- (A) After each department's baseline standard has been established, the Director of Safety should [REDACTED] discovered that require correction and follow-up. In addition, internal evaluations may be conducted whenever a department has experienced significant turnover of personnel or has undergone significant changes in structure, management, facilities, or equipment.
- (B) In addition to internal evaluations, special audits or follow-ups may be performed by the Director of Safety or delegates to address specific management concerns, or to ensure that Corrective Action Plans (CAPs) implemented have been effective in rectifying deficiencies.

1.9.4 COMPLIANCE WITH POLICIES AND PROCEDURES

- (A) Internal evaluation checklists assess the performance of operational processes within each department, and determine if the department being evaluated complies with the contents of manuals, programs and other written guidance including policies, [REDACTED] (NCP-P). While internal evaluations are not intended specifically to verify regulatory compliance, checklists may contain references to regulations, and findings of **regulatory noncompliance (NCP-R)** may be revealed.

1.9.5 CONFORMANCE WITH RISK CONTROLS

- (A) A **system assessment** assesses risk controls that apply to operational processes managed by the department being audited. Together, the Director of Safety and the Department Manager evaluate whether these controls:
- (1) Continue to be applicable;
 - (2) Continue to conform with their intended design;
 - (3) Remain effective in controlling risk.
- (B) Deficiencies may produce findings of **risk control nonconformance (NCF-RC)**.

1.9.6 CONFORMANCE WITH SMS OBJECTIVES

- (A) Form **OM-02 Dept SMS Performance** is used to determine if the SMS is conforming to its expectations and objectives within the department being evaluated, and to identify any deficiencies therein. Examples include:
- (1) Whether hazard and occurrence reports are being received;
 - (2) Whether [REDACTED] completed in a timely manner and departmental audit schedules are being adhered to;
 - (4) The number of [REDACTED] shared with appropriate department personnel;
 - (6) Whether lessons learned are being incorporated into appropriate training curricula.
- (B) Deficiencies in SMS expectations and objectives may also be recorded as findings.

1.9.7 INTERNAL EVALUATION PROCEDURES

- (A) Select one or more internal evaluation checklists that pertain to the department and operational processes being evaluated. Schedule the audit with the department manager and attach checklists to be used.
- (B) Perform a **system assessment** within the OmniSMS [REDACTED] findings from the department's previous evaluation and incorporate the findings (and corrective actions from the previous findings) into the planned evaluation.
- (C) Conduct the evaluation by systematically reviewing evaluation criteria (e.g., applicable regulations, existing risk controls and previous evaluation results), and confirming compliance and conformance through careful review and evaluation of pertinent [REDACTED] less safety significance.
- (D) Complete the internal evaluation checklist(s) and, if applicable, an audit finding report (AFR).
- (E) Findings are often subject to interpretation. In such a case, it may be advisable to get a second opinion from another department manager or someone within [REDACTED] **R), procedural non-compliance (NCP-P), risk control nonconformance (NCF-RC), and new hazards found (NHF) must be channeled back into risk management for corrective action.**

NOTE:

*Procedures for assessing and recording valid findings are described in **paragraph 1.11: Findings** below.*

1.10 COMPLIANCE MONITORING

1.10.1 REGULATORY COMPLIANCE

- (A) Compliance monitoring (CM) is a type of internal audit that enables YCO to monitor compliance with relevant regulatory requirements. In [REDACTED], and other requirements that apply to the department being monitored.
- (B) Department managers are responsible for regulatory compliance within their respective departments. Therefore in accordance with accepted auditing principles, compliance monitoring should be performed by an independent auditor from outside the department. The Director of Safety is responsible for the quality of the compliance monitoring process, and may delegate the performance of CM audits to individual(s) with the appropriate knowledge, background and experience.

NOTE:

Compliance monitoring may be performed by the Director of Safety in conjunction with an internal evaluation of the operational department being audited. If compliance monitoring is to be delegated, the Director of Safety must ensure that audits and inspections are carried out by personnel not responsible for the function or products being audited.

1.10.2 CM AUDIT PLANNING

- (A) Select the appropriate CM checklist that pertains to the department and operational process(es) being audited.
- (B) Schedule the audit with the department manager, and attach checklist(s) to be used.
- (C) Review any findings from the department's previous CM audit and include findings and corrective actions from the previous audit into the planned CM audit, in order to assure effectiveness of the previous corrective actions.

1.10.3 CM AUDIT PROCEDURES

- (A) During a CM audit, manuals, documents, operational processes and associated records are sampled for regulatory compliance. Conduct [REDACTED] of the YCO Compliance Statement.
- (C) During a CM audit, the responsible manager should be able to:
- (1) Demonstrate knowledge of regulatory requirements; or
 - (2) Know where to access current regulatory requirements; and
 - (3) Satisfactorily address all CM checklist criteria.
- (D) When apparent regulatory violations are encountered, they are recorded as findings of **regulatory non-compliance (NCP-R)**.

NOTE:

In the event a regulatory violation is discovered, enforcement incentives may be afforded by various programs such as ASRS, ASAP, and VDRP. An emergency SAG meeting may be convened to discuss options and provide affected personnel the opportunity to file individual reports.

1.11 FINDINGS

1.11.1 INITIAL ASSESSMENT

- (A) If an internal evaluation and/or CM audit is being conducted, the Director of Safety (or the Director of Safety's delegated auditor) should perform an initial assessment of each finding together with the appropriate department [REDACTED] injury or accident, including cessation of flight operations or disruption of work activity.
- (B) Initial assessment should determine if an apparent finding is:
- (1) An administrative error;
 - (2) An isolated incident;
 - (3) The result of a non-conforming or ineffective risk control;
 - (4) The result of a deficient process or procedure;
 - (5) An apparent violation of regulations.
- (C) Initial assessment by the Director of Safety (or his auditor) and the department manager should also determine if the apparent finding is valid and warrants being doc [REDACTED] re "carried forward" in the aircraft logbook or other written records, which could result in an apparent finding. Initial assessment with the department manager may reveal that an apparent finding is merely an administrative error, and does not warrant being recorded on the AFR.

NOTE:

Refer to the SMS Manual [Section 6: Employee Reporting System, Paragraph 6.3.9: Corrections to Written Records](#) for instructions on how to address this type of apparent finding.

1.11.2 CLASSIFICATIONS OF FINDINGS / CONCERNS

Interface – AFR Form QA-010

- (A) After initial assessment, **safety findings** are recorded on the AFR under the following classifications:
- (1) **NCP-R Noncompliance, regulatory** (violation of local or foreign CAA regulations)
 - (2) **NCP-P Noncompliance, procedural** (noncompliance with policies, procedures, manuals, contractual requirements)
 - (3) **NCF-RC Nonconformance, risk control** (control not conforming to design, ineffective, or process not conforming to control)
 - (4) **MSC Minor Safety Concern** (an area or process where safety could be improved)
 - (5) **NHF New Hazard Found** (an area or process where controls may be needed)
- (B) **Quality findings** are recorded using the following classifications:
- (1) **NCF-Q Nonconformance, quality** (product or service that does not conform to a quality standard)
 - (2) **OFI Opportunity for improvement** (an area or process where quality could be improved)
- (C) NCP-R findings must be reported immediately to senior management.
- (D) Correct findings that can be immediately corrected, and indicate "corrected" in the R/H column.
- (E) For NCF-RC findings on an existing risk control, correct the control within the OmniSMS application.

1.11.3 INITIAL RISK ASSESSMENT

- (A) The risk assessment (RA) matrix within OmniSMS will be used by the auditor and the department manager to initially determine the level of risk associated with a given finding.

CAUTION:
Any finding that has a risk factor of RED - HIGH will require immediate corrective action and notification of the YCO Accountable Executive.

- (B) NCP-R findings should be brought by department managers or the Director of Safety to the immediate attention of the Accountable Executive, in order to enable timely submission of a voluntary disclosure to appropriate regulatory authorities. ASRS and ASAP report submissions by affected personnel should also be considered.
- (C) All other findings that have a risk factor of **MODERATE / Yellow / ACCEPTABLE WITH MITIGATION** or higher will also require a Finding to be created in OmniSMS and CAP development to be completed within the appropriate timeframe.

NOTE:

The time frame for enacting a Corrective Action Plan will vary based on the severity of the problem and the scope of required corrections. The CAP's time frame should be appropriate to the finding's potential impact on operational reliability and the safety-criticality of the affected operational process.

1.11.4 DOCUMENTING AUDIT FINDINGS

- (A) The auditor completes an **Audit Finding Report (AFR) Form QA-010** for each audit performed and records audit findings thereon, but only after each finding is initially assessed and validated by the auditor, together with the department manager or POC as appropriate.
- (B) Each AFR may contain several separate audit findings. These audit findings are then evaluated to identify root causes. Risk management is applied through use of the OmniSMS application and procedures in the YCO **SMS Manual** to develop and implement Corrective Action Plans designed to eliminate or mitigate any unacceptable risks, or to reduce acceptable risk to a level that is as low a reasonably practicable (ALARP).

1.11.5 COMPLETING THE AUDIT FINDING REPORT QA-010

- (A) The **Audit Finding Report QA-010** (AFR) is utilized to record all initially-validated audit findings from departmental audits, external provider audits, external audits, internal evaluations, compliance monitoring, management reviews, and emergency [REDACTED], at a minimum:
- (1) General information pertinent to the audit, including:
 - (a) Date and type of audit;
 - (b) Company and/or department being audited;
 - (c) Responsible department manager or Point-of-Contact (POC for external provider audits);
 - (d) Audit protocol or [REDACTED].
 - (2) A brief summary of audit report findings.
 - (3) Any corrective actions taken (required if initial assessment indicates **RED / HIGH RISK**)

- (4) A numerical listing of all findings, including:
- (a) The classification of [REDACTED] or concern and objective evidence to support the finding;
 - (c) A reference for each finding or concern as it relates to regulations, state or local laws, company policy / procedures, contractual requirements, recommended practices, or other standard (if applicable).
 - (d) Whether corrective action was taken (yes / no) and a description of the action taken.
- (B) An audit commentary may be included within the AFR, or as an attachment. This commentary may pertain to one or more findings and include recommendations for corrective action(s).

1.11.6 AUDIT FINDING REPORT DISPOSITION

- (A) Completed Audit Finding Reports are attached to their associated departmental audit, internal evaluation, external provider audit, or other checklist, and uploaded to the OmniSMS application. When performing a departmental audit, auditors should provide the department manager with each completed audit checklist and a copy of the AFR as [REDACTED] and filing.
- (B) When conducting an internal evaluation, auditors should provide appropriate department managers with a copy of the completed checklist and all AFRs generated. The original evaluation and attached AFRs should be uploaded to the OmniSMS application or submitted to the Director of Safety for review and uploading.
- (C) Departmental audit, internal evaluation and external provider audit results are reviewed at the next regularly scheduled meeting of the Safety Action Group, for assurance that only valid audit findings have been entered into the OmniSMS database, and for evaluation of CAPs developed in response to audit findings.

1.11.7 APPLICATION OF QUALITY AND SAFETY RISK MANAGEMENT

- (A) For each finding that is confirmed to be valid, the DOS or responsible department manager creates a **Finding** in the OmniSMS application. Investigation is performed and root causes are determined (by the process owner), enabling affected department managers to develop a Corrective Action Plan (CAP) designed to mitigate risk and/or improve the quality of the affected operational process. If root cause analysis indicates that corrections are [REDACTED] POC) develops their own risk controls and/or corrective actions under the CAP.
- (B) When multiple departments are involved in the investigation and CAP development processes, appropriate managers should submit their risk controls and corrective actions to the Safety Action Group for congruency, and to ensure that each proposed risk control or [REDACTED] interfaces with the processes of other departments. If the proposed RC/CAs are acceptable, they are incorporated into the CAP for implementation and follow-up.

NOTE:

The CAP must be accepted by the appropriate risk-acceptance authority in accordance with [paragraph 1.2.6: Risk Acceptance Authority](#) of the SMS Manual.

- (C) Changes that are necessary to written guidance should be included in the CAP as individual and separate corrective actions for each document requiring revision, and assigned to department managers for accomplishment with expected due dates for completion.
- (D) Once a CAP is accepted, appropriate Safety Action Group members ensure that all changes in policy, procedures and/or YCO [REDACTED] is then performed and recorded within OmniSMS by the process owner, to determine conformity and effectiveness of the control or action.

1.12 ANNUAL MANAGEMENT REVIEW

- (A) Annual review of the SMS is performed by the **Management Review Board (MRB)**. Chaired by the Accountable Executive, the MRB is responsible for performing an annual review of the various manuals, programs, processes and data collection tools that comprise and support the SMS. If the MRB has not been established, management reviews may be performed by the Safety Action Group (SAG).

1.12.1 SENIOR MANAGEMENT RESPONSIBILITIES

- (A) The Accountable Executive chairs the annual management review meeting. The Accountable Executive may choose to provide information regarding events of the year in review, and / or senior management's goals and plans for the coming [REDACTED] aircraft, areas of operation, crew bases, maintenance facilities, etc. will be implemented in a manner that will ensure the highest level of safety.
- (B) The Accountable Executive or other members of senior management are authorized to call an SMS management review meeting at any time in the interest of safety.

1.12.2 DIRECTOR OF SAFETY RESPONSIBILITIES

- (A) The annual management review meeting is scheduled and called by the Director of Safety to review elements and processes within Your Company's Safety Management System. The Director of Safety is authorized to call a management review meeting at any time, and to measure SMS processes at any time during the course of his duties. The [REDACTED] information of a sensitive nature regarding potential violations and the names of those involved.

1.12.3 MANAGEMENT REVIEW BOARD MEMBERS' RESPONSIBILITIES

- (A) Each member of the Management Review Board or Safety Action Group (MRB / SAG) shall attend the meeting with suggestions and ideas for improvement of the various elements that comprise YCO's Safety Management System.
- (B) MRB / SAG members are authorized to bring to the attention of the Accountable Executive any issue or concern they may have regarding the SMS and its many elements, or any other loss prevention program.
- (C) Due to the possibility of sensitive personal information being discussed, the annual SMS management review meeting is closed to all personnel other than members of the MRB / SAG and other persons as approved by senior management. MRB / SAG members **are not authorized** to share any information presented or discussed during any [REDACTED] report errors or violations under YCO's Employee Reporting System are protected from disclosure of sensitive information to outside parties.

1.13 MANAGEMENT REVIEW PROCESS

- (A) Annual review of the SMS is performed systematically by reviewing the various programs, processes and sources of guidance that comprise the Safety Management System. Each manual, program, process and tool is reviewed for currency, clarity, ease of use, effectiveness, and cost-benefit.

1.13.1 MANAGEMENT REVIEW QUESTIONNAIRE

- (A) As a starting point for the review, MRB and [REDACTED] questions, changes in policy, procedures and communications may be necessary to improve the effectiveness of YCO operational processes and safety / quality management processes.
- (B) This exercise is designed to stimulate thought processes and remind participants of where work is needed with regard to YCO management systems. Individual questions should not be debated at length, as many of the areas covered will be reviewed in more detail as the review progresses.

1.13.2 SYSTEM DESCRIPTION REVIEW AND UPDATE

- (A) Within the OmniSMS application, YCO's *initial system description* is updated each year during annual management review. As the description is updated, changes in YCO's operational environment may be identified and new hazards found that warrant the creation of new safety issues.
- (B) Review the existing description, make changes as necessary, and provide comments as desired. Create new issues in OmniSMS as necessary for further study:
- (1) Create a **Safety Assessment** (issue [REDACTED] factors / errors, or reported occurrences that are discovered during the review;
 - (3) Create a **Significant Safety Issue** if the issue is to be added to the company's Safety Risk Profile.
- (C) Record the date of the review and persons involved in the **System Review** panel within OmniSMS.

1.13.3 SAFETY RISK PROFILE REVIEW

- (A) Each Significant Safety Issue that comprises the current Safety Risk Profile should be reviewed for accuracy and completeness, including risk analysis / assessment processes and the issue's Corrective Action Plan (CAP):
- (1) Review each identified hazard and its associated risk(s) for continued applicability, and to ensure that any associated courses of action were followed, and continue to be followed;
 - (2) Evaluate for effectiveness, any controls in place to preclude identified top events from occurring in each area of moderate or high risk;
 - (3) Review safety communications and [REDACTED].
- (B) Based on these studies, review and revise as necessary the overall level of risk associated with each hazard's consequence (a hazard may have one or more consequences associated with it, from previous risk analysis and assessment processes).

1.13.4 OPERATIONAL PERFORMANCE REVIEW

- (A) Review flight operations performance, maintenance performance, production performance, and the operational performance of other departments as desired. Contributing factors and root causes of performance failures should be identified within OmniSMS.

1.13.5 KEY SAFETY PERFORMANCE INDICATOR REVIEW

- (A) This area of management review looks at the past 12 months of high-level and low-level KSPIs, and measures them against the previous year's objectives and goals. Target thresholds are adjusted accordingly, and further risk mitigation strategies are applied as necessary:

- (1) For high-level KSPI events:

- (a) Confirm [redacted] performed, root causes identified, and risk mitigating strategies applied;
- (b) Review implemented risk controls for continued applicability, suitability, and effectiveness.

- (2) For low-level KSPI events:

- (a) Confirm a Safety Trend (Issue type) was [redacted]
[redacted] trend for continued applicability, suitability, and effectiveness.

1.13.6 SMS PERFORMANCE REVIEW

- (A) Form **OM-01 Org SMS Performance** is used to determine if the SMS is conforming to its expectations and objectives at the organizational level and to assess performance of the SMS within various departments. Refer to the SMS Manual **Section 1, paragraph 1.5.4 – SMS Performance Indicators** for various SMS performance indicators that may be reviewed.

1.13.7 REVIEW OF OPEN EMPLOYEE REPORTS

- (A) Each functional area manager should provide a brief synopsis of the status of all open reports within the respective manager's area of [redacted] synopsis should include the initial risk assessment and level of risk, any immediate actions taken, how each report is being handled, status of investigation(s), CAP development, etc.

1.13.8 REVIEW OF VIOLATIONS AND SELF-DISCLOSURES

- (A) Any violations discovered by regulatory authorities, reported by employees, or revealed by Departmental Audits or Internal Evaluations should be reviewed. These reviews should evaluate whether:

- (1) The IEP is discovering violations or other instances of non-regulatory compliance;

- (2) Employees are utilizing the [redacted]
[redacted], and whether it is effective in:

- (a) Collecting safety data;
- (b) Avoiding certificate action;

- (4) ASRS (NASA reports) are being utilized, and whether they are effective in avoiding certificate action;

- (5) Any self-disclosures submitted are effective in avoiding:

- (a) Civil penalties and/or certificate action for YCO;
- (b) Civil penalties and/or certificate action for individual airmen.

1.13.9 REVIEW OF AUDIT FINDING REPORTS

- (A) The previous 12 months' Audit finding Reports (AFRs) and associated OmniSMS records should be reviewed. This includes AFRs generated as a [REDACTED] [REDACTED] Corrective Action Plans implemented by external providers.

1.13.10 REVIEW OF THE INTERNAL EVALUATION PROGRAM

- (A) A review of YCO's Internal Evaluation Program should include past and current performance as well as opportunities for improvement. The review should include:
- (1) Follow-up actions from previous management reviews, including progress reports on the status of previously established improvement objectives;
 - (2) A report on significant or systemic deficiencies, with associated status reports detailing corrective actions and planned follow-up [REDACTED]
[REDACTED]
 - (5) Recommendations for improvement and required resources.

1.13.11 REVIEW OF THE EMERGENCY RESPONSE PLAN

- (A) The YCO ERP should be reviewed annually and coordinated wherever possible with other agencies to ensure the plan is compatible, and to provide a coordinated response. Review of the ERP with local airport and other organizations before it is needed will permit deficiencies to be discovered and corrected before a response is necessary. When the YCO ERP is updated, a copy of the plan should be forwarded to appropriate coordinating agencies.
- (B) Any resources identified in the YCO emergency plan should be available in a timely manner, and have the capability to perform their intended function. Restrictions or limitations on the use of the resource should be evaluated before implementation. Any cooperative assistance agreements or mutual aid agreements referenced in the YCO ERP should be reviewed by legal counsel and signed by a responsible YCO official.
- (C) The YCO Emergency Response Plan should also be re-evaluated when any of the following occur:
- (1) Regulations change;
 - (2) New hazards are identified [REDACTED]
[REDACTED];
 - (5) After disaster/emergency responses; and after
 - (6) Infrastructure, economic, or geopolitical changes.

1.13.12 MANAGEMENT REVIEW COMMUNICATIONS

- (A) Results of YCO's safety efforts, achievement of objectives and goals, safety culture enhancements, etc. can be summarized and presented to all interested parties in the form of an annual report, newsletter, or at company-wide gatherings. Bulletin boards and electronic reporting through the YCO web site or emails of SMS results are also effective means of communication.

1.14 DOCUMENTING MANAGEMENT REVIEWS

1.14.1 MANAGEMENT REVIEW FORM QA-017

- (A) The annual Management Review is documented using **Management Review Form QA-017**, and updating the organization's System Description and Analysis in the OmniSMS application. As a result of these processes, Finding [REDACTED] actions by managers and personnel.

1.14.2 AUDIT FINDING REPORT QA-010

- (B) Management Review findings are documented in :
- (1) The completed audit checklist's **Findings / Concerns** area; and
 - (2) For all valid findings, **Audit Finding Report (AFR) Form QA-010**.
- (C) When a management review reveals findings, they are entered into OmniSMS by responsible managers, and the SRM process is utilized to manage the findings in accordance with procedures in the SMS Manual.

1.15 EMERGENCY RESPONSE EXERCISES

1.15.1 ACCIDENT RESPONSE

- (A) At least once annually, YCO conducts an aircraft accident simulation in order to exercise the duties and responsibilities of all personnel and to measure the effectiveness of ERP processes. All managers should be involved. At the discretion of management, federal, state, and local airports may also be involved.

1.15.2 MINOR EXERCISES

- (A) At least once every two years, YCO shall conduct a simulation of an emergency response (other than an aircraft accident) in order to exercise the duties and responsibilities of all personnel and to examine and measure the effectiveness of the processes established in this ERP. All managers need not be present. At the discretion of management, federal, state, and local airports may also be involved.

1.15.3 LOCAL EXERCISES

- (A) Local exercises consist of those sections of the ERP as they pertain to YCO's operations and maintenance activities at different locations. Contact lists of local resources and emergency response agencies should be updated, confirmed and applied during simulation exercises.

1.15.4 SPECIALTY EXERCISES

- (A) Specialty exercises comprise a review of certain sections of the ERP which may include:
- (1) Ground Facility Bomb Threat procedures;
 - (2) Aircraft Bomb [REDACTED]
[REDACTED] from Overseas Locations;
 - (4) Abduction/Kidnapping of Company Employees; and
 - (5) Suspicious Items/Vehicles and Explosions.

1.15.5 PRE-EXERCISE BRIEFING

(A) All managers and employees

implementation of the ERP. Each manager should collect all notes and discuss concerns with their respective employees immediately after the exercise for process measurement.

1.15.6 POST-EXERCISE DEBRIEFING

(A) Upon completion of a response exercise, the Director of Safety will discuss exercise results with department managers. Managers should bring to this in the plan, as well as provide suggestions for improvement.

(B) Results will be reported to the Safety Action Group after each exercise, and process deficiencies recorded in the OmniSMS database as Finding Reports for corrective action(s).

1.15.7 SIMULATION SCHEDULING

(A) When possible, simulation exercises should be scheduled and conducted just prior to the Safety Action Group's annual **Management Review**. This will facilitate a timely review of accident simulation results and enable the Safety Action Group to accurately measure the effectiveness of the Emergency Response Plan.