

## Practical Safety Auditing Techniques

Sofema Aviation Services (SAS) Considers Practical Safety Auditing Techniques within an Aviation Environment – Focusing Beyond Compliance and engaging with Risk Assessment Techniques.

**Introduction** - While traditional compliance audits check whether procedures align with the regulations, practical safety audits now serve a more dynamic function – evaluating the effectiveness of the system in identifying and mitigating operational risks.

- It is no longer enough to ask, “*Are we compliant?*”  
The critical question now is, “*Are we safe, and how do we know?*”
- Safety audits provide the evidence base for effective risk assessment and control. Through structured, objective, and recurring evaluations, audits support SMS implementation by:
  - Verifying compliance with regulations and internal procedures.
  - Identifying latent conditions, organizational drift, and systemic issues.
  - Revealing ineffective mitigations or control failures.
  - Providing insight into behavioral and cultural trends that influence safety performance.

### Understanding the Shift in Audit Focus

Safety auditing under EASA must consider the intent and effectiveness of the processes, this is particularly important because a seemingly compliant system can still harbour latent or emerging risks that go undetected until a failure occurs.

For example, an organization might fully meet the requirements of its procedures, yet unsafe practices may persist due to informal workarounds, outdated assumptions, or poor safety culture. In such cases, the audit's role is to shine a light on these weaknesses before they manifest as incidents.

### Key Practical Techniques for Safety Auditing

- **Risk-Based Audit Planning** - Audits should be strategically aligned with the organization's operational risk profile.
  - This means using data such as
    - occurrence reports,
    - safety trends,
    - operational changes, and
    - human performance feedback to prioritize audit topics and areas.

- **Interviewing for Depth, Not Just Answers** - Rather than relying solely on documents or records, safety auditors must engage personnel at all levels.
  - Skilled interviewers ask open-ended questions to uncover actual practices, attitudes, and risk perceptions. For example:
    - *“Can you walk me through how you manage this process when something goes wrong?”*
    - *“What are the challenges you face when following this procedure?”*

**Take Away** - Effective auditors must go beyond compliance and ask *“Why does this issue exist?”*, linking audit findings to systemic weaknesses and opportunities for risk reduction.

**Note** - These responses can reveal hidden issues like informal workarounds, resource constraints, or communication failures.

- **Observational Techniques** - Field observation is a powerful tool. Auditors should go beyond desktop reviews and spend time on the line, in the hangar, on the ramp, or within operational control centers.
  - Observing how work is done in practice (as opposed to what procedures say) provides critical insights into human factors, workload, time pressure, and workplace ergonomics.
- **Safety Performance Trend Analysis** - Auditors should examine not just whether performance indicators are being monitored, but whether the organization understands the trends.
  - Is data being interpreted correctly?
  - Are leading indicators being acted upon?
  - How are decisions justified in relation to the organization's safety objectives?
- **Audit Trail Development** - A competent safety auditor traces how safety risks are identified, managed, and closed. This means checking whether:
  - Hazard identification feeds into the risk register
  - Risks are assessed with appropriate methodologies
  - Mitigations are implemented and monitored for effectiveness
  - Safety actions are tracked to closure, with measurable outcomes
- **Evaluating the Safety Culture** - Auditors are not culture inspectors per se, but safety audits can give insight into organizational culture by analyzing:
  - Willingness to report safety issues
  - Visibility and authority of the safety team
  - Engagement of line managers in safety processes
  - Presence of blame vs learning mindset in post-event reviews

- **Scenario-Based Auditing** - This technique involves asking “what if?” questions to explore how the system might behave under stress. For example:
  - “What would happen if a critical person was unavailable for 72 hours?”
  - “How would this process respond to a simultaneous equipment and power failure?”
- **Integration of Human Factors** - Auditors must assess how the organization manages human reliability, task complexity, fatigue, training adequacy, and interface design.
  - These factors are often the root of safety risks even when compliance is fully demonstrated.
- **Evaluation of Interfaces and Organizational Communication –**
  - Many risks emerge at interfaces:
    - Between shifts,
    - Departments,
    - Systems, or
    - Organizational levels.
    - Audits must explore whether handovers,
    - Interdepartmental processes, and
    - Safety-critical communications are effective and resilient to error.
- **Feedback Loop Assessment** - A strong SMS requires active feedback mechanisms. Auditors should evaluate whether the organization learns from audits, incidents, near misses, and safety reports – and whether this learning is systemic and continuous, not just reactive.

**Understanding Risk Assessment within EASA SMS** - Risk assessment is a core pillar of the Safety Risk Management (SRM) process, one of the four components of the ICAO-compliant and EASA-endorsed Safety Management System framework (Policy, Risk Management, Assurance, Promotion).

## **Risk Assessment Process – Step-by-Step Overview**

### **Step 1: Hazard Identification**

- Involves systematic collection of data from internal (ASR, MOR, audits, FDM) and external sources (SAFA, industry bulletins, OEM notices).
- Hazards are any condition or object with the potential to cause injury or damage.

- Methods include:
  - Reactive (occurrence reports)
  - Proactive (audits, surveys)
  - Predictive (trend analysis, FDM)

## **Step 2: Risk Analysis**

- Evaluates the likelihood (frequency or probability) and severity (consequence) of the hazard materializing into an unsafe condition.
- Uses risk matrices (5x5 or similar) to assess risk exposure levels.
- Risk level = Likelihood × Severity

## **Step 3: Risk Evaluation**

- Compares risk levels against the organization's risk tolerability criteria or Safety Risk Acceptability Matrix.
- Decisions:
  - Accept the risk (if low)
  - Monitor the risk (if medium)
  - Mitigate the risk (if high or intolerable)

## **Step 4: Risk Mitigation**

- Developing controls or barriers to reduce either the likelihood or the severity.
- Controls can be technical, procedural, training-related, or behavioral.
- Follow the bow-tie model logic: prevention, detection, and recovery.

## **Step 5: Risk Acceptance & Follow-Up**

- Accountable Executive or Safety Review Board (SRB) makes final risk acceptance decision.
- Tracking via Safety Action Plan and monitoring effectiveness.
- Ensure feedback loop into Safety Assurance processes.

**Best Practices for Risk Assessment - Define Clear Roles and Responsibilities**

- Designate responsible persons for risk assessment and approval.
- Use structured Safety Committees and Safety Review Boards (SRB).

**Use a Calibrated Risk Matrix** - Establish standardized definitions for severity and likelihood across the organization.

- Avoid subjective scoring—train assessors to use consistent criteria.

**Implement a Multi-Disciplinary Approach** - Include cross-functional teams (flight ops, maintenance, ground handling, etc.) to ensure diverse perspectives.

**Integrate into Daily Operations** - Embed the risk assessment into operational decision-making (e.g., change management, SOP development, maintenance planning).

**Ensure Traceability and Documentation** - Maintain comprehensive risk registers.

- Each risk entry should show: hazard, risk statement, assessment, mitigation, responsible party, and monitoring.

**Feedback Loop and Continuous Monitoring** - Validate mitigations and track residual risk.

- Use Safety Performance Indicators (SPIs) to monitor trends and trigger re-assessment.

**Apply Risk-Based Thinking Beyond Safety** - Integrate SMS with QMS and Emergency Response Planning (ERP) for organizational resilience.

### Typical Behaviour – Observed Trends & Challenges

**Over-Reliance on Reactive Data** - Many organizations struggle to proactively identify risks.

- Heavy dependence on mandatory reports (e.g., MORs), underutilization of FDM, surveys, or internal audits.

**Inconsistent Risk Ratings** - Without standardization, different assessors rate similar risks differently.

- Risk ratings often influenced by emotional or hierarchical bias.

**Poorly Defined Mitigations** - Controls often vague or generic (e.g., “review SOPs”) rather than SMART (Specific, Measurable, Achievable, Realistic, Time-bound).

**Lack of Risk Ownership** - Risk actions often assigned to departments instead of individuals, weakening accountability.

**Ineffective Integration with Change Management** - Safety assessments often performed *after* a change, rather than as part of the change planning process.

**Neglect of Cultural Influences** - Reporting culture, trust in just culture processes, and understanding of SMS vary across departments, impacting the accuracy and utility of assessments.

### **Advanced Practices for Mature EASA SMS Environments**

- Quantitative Risk Models - Using statistical tools for risk assessment in complex operations.
- Scenario-Based Risk Workshops - Use facilitated group sessions to assess risk for major projects or operational changes.
- Linking to Financial Exposure - Assigning cost implications to risk severity to aid prioritization.

### **Risk Assessment within EASA SMS & Practical Safety Auditing Techniques**

Within the EASA framework for Aviation Safety Management Systems (SMS), Risk Assessment and Safety Auditing are interlinked and essential components of a proactive safety environment.

Risk assessment is used to evaluate and manage hazards, while safety auditing serves as a key mechanism for identifying those hazards, verifying mitigations, and ensuring the SMS is functioning effectively.

#### **Common Audit Techniques Include:**

- Interviews and Observations – Assess alignment between documented procedures and actual behaviors.
- Document Review – Examine SMS records, training files, MORs, and risk assessments.
- Checklists and Process Walkthroughs – Structured tools to assess consistency and conformance.
- Thematic Sampling – Deep dives into specific safety topics (e.g., fatigue management, change control).
- Trend Analysis – Audit findings fed into the SMS to support predictive risk modelling.

### **Best Practices in Risk Assessment and Auditing**

**For Risk Assessment** - Use a calibrated risk matrix and standard definitions.

- Maintain a central risk register accessible to all departments.
- Conduct multi-disciplinary reviews for operational changes.

- Regularly review and revalidate risk assessments after audits or significant events.

**For Auditing** - Train auditors in system thinking and bias-free investigation.

- Use evidence-based conclusions—not assumptions.
- Link audit scope to SMS priorities and known risk areas.
- Embed risk-based audit planning (focusing on high-risk or weak-performing areas).

**Conduct Risk-Informed Audits and Audit-Informed Risk Assessments**

- Plan audit scopes using outputs from the risk register.
- Use audit findings to prioritize or reclassify risks.
- Cross-reference Safety Performance Indicators (SPIs) with audit results.

**Common Pitfalls and Cultural Trends** - Observed Challenges in Risk and Audit Environments:

- **Superficial Risk Assessments:** Tick-box exercises with vague mitigations (“SOP updated”) rather than operationally meaningful controls.
- **Non-closure of Findings:** Open findings without timely resolution dilute SMS credibility.
- **Defensive Behaviour:** Line managers may resist findings out of fear of blame or reputational risk.
- **Overconfidence in Documentation:** Belief that having procedures equals safety, while real performance issues go unnoticed.