Risk-Based and Performance-Based Oversight – Guidance

May 2022

This paper was prepared by the Safety Management International Collaboration Group (SM ICG). The purpose of the SM ICG is to promote a common understanding of Safety Management System (SMS)/State Safety Program (SSP) principles and requirements, facilitating their application across the international aviation community. In this document, the term "organization" refers to a product or service provider, operator, business, and company, as well as aviation industry organizations; and the term "authority" refers to the regulator authority, Civil Aviation Authority (CAA), National Aviation Authority (NAA), and any other relevant government agency or entity with oversight responsibility.

The current core membership of the SM ICG includes the Aviation Safety and Security Agency (AESA) of Spain, the National Civil Aviation Agency (ANAC) of Brazil, the Civil Aviation Authority of the Netherlands (CAA NL), the Civil Aviation Authority of New Zealand (CAA NZ), the Civil Aviation Authority of Singapore (CAAS), Civil Aviation Department of Hong Kong (CAD HK), the Civil Aviation Safety Authority (CASA) of Australia, the Direction Générale de l'Aviation Civile (DGAC) in France, the Ente Nazionale per l'Aviazione Civile (ENAC) in Italy, the European Aviation Safety Agency (EASA), the Federal Office of Civil Aviation (FOCA) of Switzerland, the Dominican Republic Civil Aviation Institute (IDAC), the Finnish Transport Safety Agency (Trafi), the Irish Aviation Authority (IAA), Japan Civil Aviation Bureau (JCAB), the United States Federal Aviation Administration (FAA) Aviation Safety Organization, Transport Canada Civil Aviation (TCCA), United Arab Emirates General Civil Aviation Authority (UAE GCAA), and the Civil Aviation Authority of United Kingdom (UK CAA). Additionally, the International Civil Aviation Organization (ICAO) is an observer to this group.

Members of the SM ICG:

- Collaborate on common SMS/SSP topics of interest
- Share lessons learned
- Encourage the progression of a harmonized SMS/SSP
- Share products with the aviation community
- Collaborate with international organizations such as ICAO and civil aviation authorities that have implemented or are implementing SMS and SSP

For further information regarding the SM ICG please contact:

Claudio Trevisan
EASA
+49 221 89990 6019
claudio.trevisan@easa.europa.eu

Andrew Larsen
TCCA
(613) 993-9158
andrew.larsen@tc.gc.ca

Eugene Huang
FAA, Aviation Safety
(202) 267-7577
eugene.huang@faa.gov

Neverton Alves de Novais
ANAC
+55 61 3314 4606
Neverton.Novais@anac.gov.br

Charles Galea
CASA
+ 07 3144 7487
Charles.Galea@casa.gov.au

SM ICG products can be found on SKYbrary at: http://bit.ly/SMICG

Risk-based and Performance-based Oversight - Guidance Document

1. Executive Summary

Since the early stages of aviation, the civil aviation system was established on a set of prescriptive rules, designed to ensure safety. ICAO Annex 19 (Safety Management) introduces a new approach to managing safety, focused on safety performance and safety risks. As a consequence, States are putting in place risk-based oversight (RBO) and performance-based oversight strategies.

RBO is an approach where oversight activities are prioritized based on the risk profile of the organization. Performance-based oversight, on the other hand, assesses the effectiveness of the organization's management system (e.g., Safety Management System [SMS], Quality Management System [QMS]) in driving toward safety objectives. Therefore, the combination of compliance-based, risk-based and performance-based oversight should all be seen as complementary approaches.

An organization's risk profile allows Authorities to determine the appropriate surveillance, in terms of frequency and scope, in order to focus surveillance activities in the areas of greater concern or need. In addition, risk profiles may be used to plan other safety oversight activities such as rule development and safety promotion.

Risk- and performance-based oversight should consider the following:

- Gathering and analyzing safety risk information
- Grouping safety risk information into sectors with similar types of operation
- Assessing the performance of each organization to manage their safety risks
- Directing resources proportionately to oversight activity to enhance safety

The outcome of oversight activities feeds back into the risk profiles, thus affecting subsequent planning and other surveillance activities.

2. Introduction

Since the early stages of aviation, the civil aviation system was established on a set of prescriptive rules, designed to ensure safety. These rules were effective for several years and were essential to laying the foundation for the civil aviation system we know today, delivering very good safety records worldwide. With the number of air traffic operations projected to double in the next 15 years, current and emerging safety risks must be addressed proactively to ensure this significant capacity expansion is carefully and thoughtfully managed.

Recognizing that this traditional approach alone was not sufficient to improve aviation safety levels, with the focus on improving the current low level of air accident fatalities, ICAO published Annex 19 (Safety Management) consolidating a new approach focused on safety performance and safety risks. In order to implement this new approach, States are putting in place risk-based oversight and performance-based oversight strategies.

Risk-based oversight (RBO) is an approach where oversight activities are prioritised based on the risk profile of the organization. It influences the planning of oversight activities, where resources are allocated based on the organization's risk profile, so to focus on areas of greater concern. The risk profile takes into account not only the risks inherent to the organization's operations, but also the safety performance of the organization and the results of previous oversight activity. The oversight methodology may be one that is compliance-based, performance-based, or both, but is informed by the risk profile.

To understand performance-based oversight, it is useful to differentiate it from compliance-based oversight. Compliance-based oversight assesses the adequacy of the organization's compliance with regulations to achieve an intended outcome set by the regulator. This intended outcome can be contained in a prescriptive requirement or a performance-based (i.e., outcome-based) requirement.

Performance-based oversight, on the other hand, assesses the effectiveness of the organization's management system (e.g., Safety Management System [SMS], Quality Management System [QMS]) in driving toward safety objectives that were set by the organization itself and agreed to by the regulator. Performance-based oversight, focusing mainly on the achieved performance, adds another layer in the regulatory scheme, aiming to continuously improve safety. It should not be seen as a substitute for compliance-based oversight; rather both compliance-based oversight and performance-based oversight should be seen as complementary approaches.

Effective safety management, as described in ICAO Annex 19, requires that safety data and information are systematically collected, analyzed, and processed to evaluate safety risks and measure progress against expected outcomes. When conducted in a risk-based fashion, oversight results in targeted interventions, proportionate resource allocation and a focus on areas of greater concern or need.

A comprehensive safety risk profile of an organization (or of the sector the organization belongs to) and/or its safety performance allows aviation authorities to:

- Assess how an individual organization within a sector manages its safety risks, including those high-level risks identified by the Authority in its State Safety Program;
- Identify which organization or aviation sector would require more effort from the regulator;
- Determine the appropriate oversight strategy in terms of frequency and scope; and
- Agree on mitigation actions defined by the organization with associated timescales.

Although the ICAO Critical Element 7, Surveillance Obligations, is the focus of this document, it must be recognized that the principles of performance and risk addressed throughout the text may be applied for all Critical Elements.

The terminology in this document is consistent with ICAO terminology as contained in the Safety Management Manual, 4th edition (ICAO Doc 9859). Likewise, the term organization should be understood to mean service provider.

3. Developing an Organization's Risk Profile

A complete and comprehensive picture of the organization's safety risk profile allows aviation authorities to determine the appropriate surveillance, in terms of frequency and scope (including focused oversight), in order to focus surveillance activities in the areas of greater concern. In addition, the risk profile may also be used to plan other safety oversight activities such as rule development and safety promotion.

The risk profile may be made up of both qualitative and quantitative indicators, based on the availability of data. It should consist of indicators to address risks inherent to the organization, as well as indicators to address the performance of the organization.

The risk profiles should be assessed to support decision-making for oversight planning.

3.1. Risk Profile Indicators

The development of relevant indicators is an ongoing process that may take several years to mature in some domains. Indicators should be developed taking into account the relevance of the data, availability of data sources and the cost of collection of the data itself. The risk profile of an organization needs to be updated periodically as required, to support oversight planning.

The inherent risk indicators relate to the following questions for the organization; where are you, who are you, and what do you do?

The inherent risk elements of the risk profile for an organization may also be available for use as part of the evaluation process for the initial certification of an organization.

<u>Sector risk profile - Where are you?</u>

See SM ICG paper Sector Risk Profile for details.

As a starting point the profile may consider the sector or sectors within which the organization intends to operate (for example, flight operations/aerodromes/airworthiness, large transport/corporate jets, passenger/cargo, fixed/rotary wing, turbojet/turboprop). State level sector risk profiles may be available which identify the specific risks in the State for the different sectors.

For example, helicopter operators would have a different sector risk profile compared to fixed wing operators. The risk profile of a helicopter operator should include the risks identified in the helicopter sector risk profile.

Nature of the organization - Who are you, and what do you do?

The risk profile may then be built by adding the indicators to address the specific nature of the organization itself and the complexity of its intended operation.

Once developed, the inherent risks of an organization should be such that it will only change in response to changes in the organization itself or its business model, changes in the intended operation, or changes to the applicable sector risk profile(s).

The list below provides examples of topics which might be considered for the development of indicators for the inherent risk section of the organization risk profile. It may be helpful to group the indicators that are developed under headers that may facilitate better understanding of the higher risk areas.

Risk Profile: Inherent Risks indicator topics

Risks inherent to the sector (where are you?)

Please refer to the SM ICG paper Sector Risk Profile for examples of types of indicators that may be appropriate for different sectors.

Risks inherent to the organization (who are you?)

Complexity of organization (who are you?)	Ownership structure (e.g., simple vs complex)
	Size of organization (e.g., number of staff, number of bases/stations, number of Air Traffic Services Units)
	Level of outsourcing (e.g., low, medium, high)
	Experience of the organization (e.g., new entrant vs experienced organization)
	Quality of supporting infrastructure (e.g., poor, adequate, good)
	Etc.

Risks inherent to the operating model (what do you want to do?)

Complexity of operations (what do you do?)	Operating environment (e.g., operations in areas such as arctic, desert, high altitude, oceanic)
	Mix of operations (e.g., cargo, passenger, scheduled, general aviation)
	Volume of operations (e.g., number of flights per year, number of revenue passenger kilometers, traffic volume)
	Air operator fleet type (e.g., single type, multi-type, mixed-types)
	Air operator special operations (e.g., low-vis, performance-based navigation [PBN])
	Airworthiness complexity (e.g., capability, specialist tasks)
	Etc.

Performance of the organization - How did you do?

The safety performance elements of the risk profile for an organization are based on the measurement of the achieved performance of the organization during the period assessed.

The safety performance risk indicators relate to the question for the organization; how did you do?

Indicators of past surveillance activities provide the most direct information available to the national aviation authority as it can be derived directly from the inspectorate staff. Comparison of even the most basic audit planning information (e.g., number of audits or findings per audit) can reveal useful information for top level audit planning purposes, but for purposes of risk-based oversight additional indicators would be required. This could include the Civil Aviation Authority's (CAA's) assessment of the organization's level of compliance as well as the organization's ability to assess its own level of compliance.

Indicators relating to the organization's safety outcomes should be used in addition to indicators arising from compliance audits. They provide information on the safety outcomes based on the organization's behavior. The SM ICG document "A Systems Approach to Measuring Safety Performance: The Regulator Perspective" provides additional guidance on this subject.

Indicators relating to the organizational health may also be used. These indicators may relate to how the organization is able to meet its objectives. In some cases, these may not be directly safety-related but could affect safety performance of the organization and the Authority's oversight activity.

It may also be useful to develop indicators based on the measure of effectiveness of the organization's safety management system.

The list below provides examples of topics which might be considered for the development of the section of the risk profile related to indicators of safety performance.

Risk Profile: Performance-related Risk Indicator Topics (How did you do?)

Compliance	Safety Outcomes	Organizational Health	SMS
• Audit results • Response to findings • Performance of organization • Internal compliance management /QMS	• Rate of accidents and serious incidents • Occurrence reporting rate • Rate of occurrences per occurrence category • Rate of occurrences per risk classification	• Rate of change • Staff turnover • Financial health • Industrial relations • Operational measures (e.g., on-time performance, delay rates, deferred defect rates)	• SMS maturity based on the present, suitable, operational, and effective (PSOE) methodology • Safety objectives (e.g., level of achievement) • Safety culture

For examples on how to select indicators, please refer to:

1. The ICAO SMI website, Chapter 8, Point 8.5 State Safety Assurance
2. Individual CAAs' websites, e.g., https://www.caa.govt.nz/surveillance/the-risk-indicators/
3. The SM ICG paper: A Systems Approach to Measuring Safety Performance: The Regulator Perspective

3.2. Developing the Risk Profile

The purpose of the risk profile is to facilitate safety oversight planning. It is commonly used to adjust the frequency and scope of surveillance, as well as to focus on specific areas requiring attention. The scoring of indicators allows for comparison across the organization's activities, as well as between different organizations, to facilitate the oversight planning.

In developing a scoring system, the following should be considered:

- A scoring scale (e.g., 1 to 10, or 1 to 5) provides a common basis for comparison.
- Qualitative indicators need to be scored (using the scoring scale). This will require guidelines specific to each indicator to promote consistency.
- Expert judgment involving individual inspectors or peer groups of inspectors may be used to score qualitative indicators according to the scoring guidelines. Using individual inspectors may be necessary, for example if that inspector is the only one familiar with the organization being assessed. However, peer groups are preferable, where possible, to reduce subjectivity and promote harmonization. Involving inspectors in these assessments promotes buy-in for the risk profiling methodology and may inform inspectors for their own audit preparations.
- Quantitative indicators have an individual value based on raw data. However, they could be converted into a score based on the common scale using a suitable conversion process (e.g., linear, logarithmic) as a scoring guideline.
- The preferred approach is to use quantitative data where possible to improve the accuracy of the indicator.
- Scoring allows you to compare specific indicator scores across organizations within a sector, but it is less useful for comparing across different indicators in the same organization. For example, an indicator showing an occurrence rate score of 4 in one organization would be objectively better than the same indicator score of 3 in another organization. However, an indicator showing an occurrence rate score of 4 in one organization cannot be objectively interpreted as better than a safety culture indicator score of 3 for that same organization.
- In order to compare across indicators within an organization, the indicators would have to be weighted according to their individual contribution to the risk picture. However, the process of weighing indicators is itself subject to qualitative judgments if there is no data

to support the process. The risk therefore is that the weights can be manipulated to achieve desired outcomes.

- In situations where there are a large number of indicators, it may be helpful to create clusters. This methodology may improve the ability to grasp the current risk level of a specific area within the profile.
- It may also be useful to track changes to individual indicators over time, as it would facilitate the presentation of trend information for individual indicators or groups of indicators.

Each risk profile relates to a specific organization. The risk profile of an organization is the risk indicators with scores and supporting information (for example, sources of indicators, scoring guidelines, scorer, comments, etc.). The risk profile provides the basic information and may be presented using charts, dashboards and benchmarking to support the analysis for oversight planning.

There are several options for States to present the information in the risk profile in order to suit the States specific needs. The ICAO Safety Management Implementation website may be consulted for examples used in different States.

4. Use of Risk Profiles for Surveillance

4.1. Surveillance Planning

The primary goal of surveillance is to verify that the organization continues to meet the condition of issuance of a certificate, that the services are rendered in a safe manner and are conducted in accordance with the applicable rules and regulations. A secondary goal is to acquire the safety information necessary to create and maintain the organization's risk profile. In this way surveillance and risk profiling form a closed loop process, each one building upon the other.

The planning function is implemented in accordance with the States safety oversight policy and consequently may vary from State to State. Equally, the implementation of surveillance activities may vary from sector to sector within a given State. This means that there is no one size fits all solution available for the use of organizations risk profiles for all sectors and States.

Another consideration in surveillance planning is to determine the surveillance cycle. The surveillance cycle is the interval of time within which compliance with specified requirements is verified by the Regulator. The surveillance cycle might be stipulated in the national regulations and may vary between one and several years. Typically, a surveillance cycle is associated with each organization and, in some cases, the organization must meet certain conditions in order to be granted an extended cycle.

Surveillance cycles allow for surveillance activities to be performed at different intensities based on the following:

- Frequency corresponds to the number of planned activities within a given cycle. It is normally determined through the analysis of the risk profile, and any additional intelligence identified since the last risk profile was generated. Frequency may also be increased or decreased depending on the demonstrated safety performance of the organization. In addition, non-periodic out-of-schedule surveillance activities can be performed in response to events or changes that might take place within the cycle.

- Scope corresponds to the breadth of planned activities that need to be addressed during each surveillance activity. Areas of greater attention may be identified on the basis of the risk profile. Likewise, the information can indicate areas not deserving to be surveyed. The scope is also determined through analysis identified since the last risk profile was generated. Moreover, developing scope allows for an efficient breakdown of activities within the given surveillance cycle. Typically, the scope is decided in a qualitative/tailored manner to make surveillance effective and efficient and can be adapted shorty before the activity takes place.

However, it is also possible for a State to use other methods, not requiring on-site surveillance, supporting verification of effective compliance, such as increased communication, meetings, data review desktop reviews, etc. These options can be used in particular to efficiently assess management of changes in the organization and contributes to updating the risk profile.

4.2. Risk Profile Analysis

There are several techniques to use the outcomes of the risk profile for oversight planning. The grouping of safety information about organizations into industry sectors with similar types of operation (for example, small aerodromes, offshore helicopters, large airlines), creates commonality amongst safety risk profiles. This facilitates the promotion of good practices to manage identified risks, including those where new business models and practices are being applied.

Analyzing the risk profile of a specific organization holding approvals in multiple sectors can help the CAA identify risks that affect these various approvals. An outcome of the oversight planning for such organizations could include integrated audits of the multiple approvals that the organization holds, with focus on cross-domain risks. Planning of such activities could also be used to inform surveillance team composition.

In addition, analyzing the risk profile of an organization may identify common risks that affect that organization, multiple organizations within a sector or even multiple sectors. For example, risk related to runway safety may have an impact on flight operations, aerodromes and air navigation services. In this case, the CAA may decide to plan targeted oversight activities focusing on runway safety issues across all affected sectors and domains.

The organization's risk profiles may also vary in maturity between sectors and possibly may not yet be developed, in some sectors. The individual State's overall surveillance planning must adopt the most appropriate use cases in the application of risk-based oversight, within each individual sector. The following use cases provide a "menu" of options that must be tailored for use within each specific sector and possibly within sub-sectors as necessary.

One use case for a risk profile is to compare an aggregate of all indicators in the risk profile across multiple organizations. This will result in the aggregation of each organization's risk profile indicators into one overall score. Although this may be an appealing approach, such a broad aggregation of the scores could produce an overall score that has a high level of uncertainty. Such an aggregation process may run the risk of reaching erroneous conclusions unless the State has established a method to determine the contribution of each indicator to the total risk picture. In that case, weighting factors could be applied to account for the contribution of each risk factor to the total risk profile. Assigning weighting factors without such a determination would require subjective judgment, which may result in a bias toward a desired outcome.

A second use case is to compare the individual indicators for a single organization. This can highlight individual risks to be addressed as part of focused oversight (i.e., used to adjust the scope of an audit). The integrity of this approach is high because individual indicators can be compared directly. This use case could result in supplemental checklists that probes deeper into single risks.

A third use case is to compare clusters of aggregated indicators within an organization. This can highlight risk areas within a single organisztion for focused oversight. This approach may be more useful than comparing individual indicators especially in instances where there is a large number of indicators in the risk profile. In order to compare clusters of indicators, it will be necessary to aggregate the score of the individual indicators within the cluster. Aggregation could involve a mathematical formula such as taking the average, or by some other means. Due to the aggregation process, the level of uncertainty of the group score would naturally be higher. This level of uncertainty can be reduced by careful selection of indicators for the cluster. This use case could inform the audit focus for an individual organization and consequently the makeup of the audit team for that organization.

A fourth use case is to compare a single indicator across multiple organizations. This approach can provide information on the risk picture related to that indicator across a group of organizations (for example within a sector). This can identify if an individual risk should be subject to focused oversight for an individual organization only, or for an entire sector. If the indicator shows an elevated risk for an entire sector, other mitigating means (e.g., safety promotion) may be appropriate. This could also inform the sector risk profile. The integrity of this approach is high as individual indicators can be compared directly across organizations.

A fifth use case is to compare clusters of indicators across multiple organizations. The purpose of selecting a cluster of indicators is to focus on a particular need. Various clusters of indicators may be selected for different purposes (i.e., to support frequency and/or scope adjustment). As with the second use case, it will be necessary to aggregate the score of the individual indicators for each of the groups. Again, the level of uncertainty can be reduced by careful selection of indicators within each group.

The outcome of the analysis of risk profiles need not be limited only to surveillance activities. The analysis may also identify systemic risks that may be better addressed through other means

available to the CAA such as review of policy and regulations, or through safety promotion and education efforts. This may be very useful when safety risks of the organization.

4.3. Conducting Surveillance

The purpose of surveillance activities is to verify compliance, as well as to understand how an organization manages its own risks and whether the safety management system, when required, is effective in delivering the expected results. Surveillance activities may be addressed at two levels: systemic and output. For the first, the ICAO definition of audit applies, while for the latter, the one of inspection applies. However, compliance verification remains the primary method for ensuring legal validity of the certificates and licences issued.

If an SMS is in place, an assessment tool can be used, that differs from the compliance checklist, as it allows to rate on a scale the level of maturity of each area of the SMS.

When it comes to assessing safety performance, the Authority should:

- Review the indicators and targets defined by the organizations, including assessing their suitability to describe the effectiveness of the risk management process in place. This may include challenging the appropriateness of both.
- Verify whether the organization has met its own targets and what it has done when it realized that the targets were not or would not be achieved. Assessment of targets' effectiveness is also done at this stage.
- Ensure that the organization's safety indicators and targets are aligned with the safety objectives of the organization and consider the safety objectives in the State Safety Program.

The outcome of surveillance activities typically results in two distinct, yet linked, feedback loops. The first relates to the follow-up of the identified issues with the organization, which may imply further interaction with the organization. The second relates to feeding back the identified issues into the risk profile of that organization, as well as tailoring the scope and frequency of subsequent surveillance activities, without necessarily needing to re-assess the risk profile.

The activities above are giving shape to a performance assessment, which complements the previously described audits and inspections. This performance assessment may take the form of an open conversation with the organization where the points above are reviewed in a structured manner and duly documented. It is highly desirable that the accountable executive of the organization attends this conversation in order to take ownership and to exercise accountability. The outcome of the conversation may be an action plan aimed at enhancing the effectiveness of the safety management process.

An organization's willingness or unwillingness to take appropriate corrective action, when non-compliances are identified, may also be seen as an indication of their attitude towards regulatory requirements. The organization's ability to address identified safety issues can be considered in the context of effective safety performance.

All results of surveillance activity will be fed back into the organization's risk profile in order to maintain confidence on the organization's risk profile. If the result of past surveillance activities indicate compliance is being maintained and the system is performing well within an area, the frequency of future surveillance activities could be decreased.