Flight Safety Foundation
Alexandria, Virginia 22314
Tel 703 739-6700
Fax 703 739 6708
flightsafety.org

GLOBAL SAFETY INFORMATION

ADDITIONAL TOOLKIT DETAILS

Level One Intensity – Safety Data and Information for risk management within a basic Safety Management System

Draft V2.0 Mar 17, 2017

TABLE OF CONTENTS

Contents

Toolkit Introduction 5

What is the purpose of the toolkits? 5

Who are the toolkits for? 5

Data Collection 7

Using Known Industry Risks to Drive Data Collection Activities 7

Relating Safety Data to Known Industry Risks 8

Data Collection Triggers 8

Mandatory Occurrence Reporting (CAA reports) 8

Company Operational Reporting 9

Internal Safety Investigation 10

Types of Safety Data 10

Audit Data 10

Measured Data 10

Employee Safety Survey Data 11

Sources of Safety Data 11

Public Safety Information 12

Reportable Occurrences 13

Safety Assurance 13

Employee Voluntary Reporting Programs 14

Reliability and Quality of Information 15

Data Collection Map 15

Creating a Plan for Success 16

Key Terminology 17

Data Analysis 18

Optimization and Management of Safety Data 18

Assessment of Risk: Root-Cause Analyses 19

The Architecture of a Cause-and-Effect (Ishikawa/Fishbone) Diagram 19

Guide to Using Cause-and-Effect (Ishikawa) Diagrams 20

Applied Ishikawa/Fishbone Example 20

Level 1 Risk Analysis Inputs, Outputs, and Techniques 21

TABLE OF CONTENTS

Quantitative Risk Assessment 23

Risk Probability Assessment 24

Risk Impact Assessment 24

Assignment of Risk Ratings 25

Applied Examples of Probability, Impact, and Risk Category Customization 26

Documenting Risks and Top Safety Issues 29

Safety Performance Indicators 30

Controller Flight into Terrain (CFIT) 30

Loss of Control In-Flight (LOC) 30

Mid-Air Collision 31

Runway Safety 31

Monitoring Beyond SPIs and Top Safety Issues 31

Best Practices for Representing and Summarizing Data 32

Selecting Chart Types 32

Line graph 32

Bar Graph 32

Pie Graph 33

Analysis and Making Conclusions 33

Create a Plan for Success 34

Information Sharing 35

General Information Sharing Best Practices & Recommendations 35

Establishment of Safety Teams and Workgroups 36

Voluntary Safety Reporting Programs 38

Best Practices for VSRP Information Sharing – Level 1 Intensity 38

Create a Plan for Success 40

Information Protection 41

Standards and Recommended Practices on the Legal Protection of Safety Information 41

Laws, Regulations, and Policies to Protect Voluntarily Reported Safety Information – 41

Protecting the Safety Data and Safety Information Within the Organization 42

Developing and Implementing Policies Within the Organization – 42

The Role of Labor Organizations – 44

Creating a Plan for Success – 44

TABLE OF CONTENTS

Data Collection – List of Figures

Figure 1 Data Collection Level 1 Intensity Matrix 7
Figure 2 ICAO 2016 Accidents by Category. Modified for printing. 8
Figure 3 Summary of Safety Data Sources 12
Figure 4 Sample Level 1 Intensity Data Collection Map. 16
Figure 5 Data Analysis Level 1 Intensity Matrix 18
Figure 6 Ishikawa/Fishbone Diagram Architecture 20
Figure 7 Applied Runway Safety Fishbone Example 21
Figure 8 Sample Frequency-Based Analysis Results 22
Figure 9 Sample Baseline Analysis Results 23
Figure 6 ICAO Document 9859 Safety Risk Assessment Matrix. Modified for printing. 25
Figure 11 Information Sharing Level 1 Intensity Matrix 35
Figure 12 Communication Model 36
Figure 13 Sample Airline Organizational Chart / Lines of Business 37
Figure 14 Information Protection Level 1 Intensity Matrix 41

Table 1 Sample Sources for Identifying & Mapping to Known-Industry Risks 8
Table 1 Example Frequency-Based Analysis Inputs and Outputs 22
Table 2 Example Baseline Analysis Inputs and Outputs 23
Table 4 ICAO Document 9859 Safety Risk Probability 24
Table 5 ICAO Document 9859 Safety Risk Severity 25
Table 6 FAA SRM Quick Reference Guide, Hazard Severity Definitions 26
Table 7 FAA SRM Quick Reference Guide, Hazard Likelihood Definitions 27
Table 8 FSF Impact Assessment Criteria; Tailored Example 28
Table 9 Risk Register Template 29
Table 10 Example Risk Register 29
Table 11 CFIT SPI Example 30
Table 12 LOC SPI Example 30
Table 13 NMAC SPI Example 31
Table 14 Runway Safety SPI Example 31
Table 15 SPI Status Example 39

TOOLKIT INTRODUCTION

Toolkit Introduction

What is the purpose of the toolkits?

Flight Safety Foundation considers itself a leader when it comes to safety initiatives within the industry. We were the first in putting together safety conferences, safety investigation guidance, etc. We think the next biggest advances in safety come from the way we will use safety data being collected BEFORE accidents happen – not just what countries aren't passing ICAO audits, not just whether someone doesn't meet an IOSA audit, not just airlines on a blacklist, not just who had an event that hit the news, but from the combined knowledge of the long term risks, the safety reports that front line operations staff are telling their safety departments, the actual measured and recorded data on real flights over time and the operational risk assessments that are being done by many organizations around the world.

More and More organizations are doing detailed study of their operations. The flight data recorder parameters provides an abundance of information that indicates good results and where programs could be strengthened to stay away from hazards that could lead to an event. That work is happening more and more often and the pace is quickening. At the same time, because of human factors and maintaining consistency, no one would manage their business by making changes to procedures after every flight. So the longer term trends are important and changes need to be considered carefully, perhaps even tested before they are introduced. The risk of any operation today must be traded for a lower risk of tomorrow that can be assured.

The toolkits consider the components of the risk management process that are important to make good risk decisions and share information between stakeholders that will benefit the larger system.

Who are the toolkits for?

Any of a number of aviation industry stakeholders.

Regulators want to make sure that the safety performance of their country improves on a steady basis. They want to know that service providers are learning from the information they have and applying it. They want to trust that the industry is doing the right thing, but hold individuals and organizations accountable to standards that they themselves know are largely related to critical risk issues. We expect that more and more they may set the priorities for the industry on what risks are gaining the most attention and how that relates to data gathered and analyzed within the industry.

Airlines want to make sure they manage their risk using the best data they can get their hands on. Improving safety performance is not assured just because you are compliant to the standards. Besides, no one can write enough standards to guarantee this will ever happen.

TOOLKIT INTRODUCTION

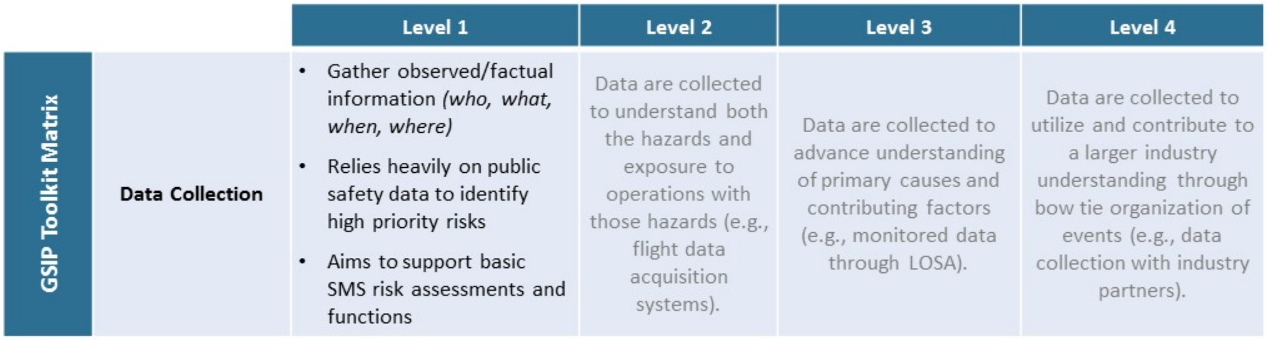
Air Navigation Service Providers want to make sure they are staying on top of all the hazards associated with air traffic flow and necessary separation standards so that pilots can do their jobs.

Airports want to make sure the runways are available and safe at all times for landing and taxing to the appropriate areas with the least amount of confusion.   Airport signage and marking has to be well understood and communications must be clear to avoid any potential runway or taxiway incursions. Avoiding any potential ground damage is critical for safe operations.

Manufacturers want to make sure their fleet is being operated and represented in the world markets as safe equipment. They regularly do their own safety analysis before the aircraft is built and continue to monitor operations and some of the biggest safety challenges. They are often involved in pushing out tips and recommendations to the operators as they may report conditions or ask for assistance on technical issues with their equipment.

Data Collection

Level 1 intensity focuses on the identification of risks (potential problems), issues (current problems), and opportunities (potential positive risk benefits) that are of the highest priority to your operation. This toolkit describes how a variety of safety data sources can be used to identify the major risk areas across your domain. It also provides best practices to assure that data collection activities address an organization's top priority risks.



		Level 1	Level 2	Level 3	Level 4
GSIP Toolkit Matrix	Data Collection	• Gather observed/factual information *(who, what, when, where)* • Relies heavily on public safety data to identify high priority risks • Aims to support basic SMS risk assessments and functions	Data are collected to understand both the hazards and exposure to operations with those hazards (e.g., flight data acquisition systems).	Data are collected to advance understanding of primary causes and contributing factors (e.g., monitored data through LOSA).	Data are collected to utilize and contribute to a larger industry understanding through bow tie organization of events (e.g., data collection with industry partners).

Figure 1 Data Collection Level 1 Intensity Matrix

While the examples provided in this toolkit focus on commercial aviation, the underlying approaches can be tailored to address your specific operational needs.

Using Known Industry Risks to Drive Data Collection Activities

To guide the development of a clear and focused risk picture, an organization must first understand the major risk areas across their domain. Identifying these risk areas is critical as they can serve as an initial guide for the prioritization of near-term safety data collection activities. Valuable sources for this type of information are global safety leaders (e.g., ICAO), regulators (e.g., FAA, ATSB, etc.), organizations that operate at higher levels of Safety Data Collection and Processing System (SDCPS) intensity (e.g., NATS UK), and/or your organization's internal operations experts. Data collected from these sources can assist an organization in the identification of top priority risks, unforeseen risks, and/or future safety enhancement opportunities. For example:

- **ICAO** publishes an annual safety report that uses multiple data sources to highlight important safety statistics and elevated risk categories. Sample categories include runway safety, loss-of-control in-flight, and controlled flight into terrain. Annually, ICAO uses these categories to present data trends, unique comparative views, and other performance-based insights.
- **Regulators** such as the FAA, publish annual safety reports that detail the health of their safety reporting programs (e.g. ATSAP, TSAP, etc.) that are used to identify and respond to top priority safety risks.
- **Organizations operating at high levels of intensity** such as NATS UK, publish annual reports that highlight strategic safety goals, their progress in achieving those goals, and recent operational safety improvements.
- **Internal operations experts** can be periodically polled to identify the most sensitive areas within your operation. These experts will have unique insight into an operation's exposure rate to certain hazards like weather, workforce skills, training, or equipment-based issues.

DATA COLLECTION

Table 1 Sample Sources for Identifying & Mapping to Known-Industry Risks

ICAO 2016 Safety Report	IATA Annual Safety Report	EASA Annual Safety Review
NATS Annual Reports & Accounts 2016: Strategic Report	FAA ATO 2015 Safety Report	Flight Safety Foundation Archived Publications
UK CAA Global Fatal Accident Review	RASG-Pan America Annual Safety Report	Aviation Safety Data Collection and Processing – Singapore's Experience

Relating Safety Data to Known Industry Risks

Major risk areas can also be used to categorize or map an organization's top priority risks. Establishing these relationships provides individual or groups of risks with valuable operational and industry-wide context. For example, an ANSP may identify Loss of Runway Separation and Runway Incursions as individual risks. When grouped, these risks can relate to or be mapped to the ICAO Runway Safety risk category.

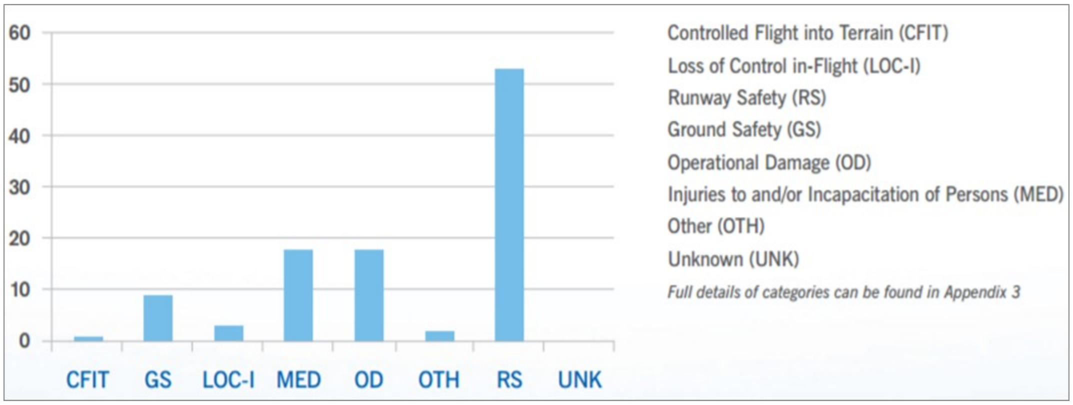


Figure 2 ICAO 2016 Accidents by Category. Modified for printing.

Data Collection Triggers

At level 1 intensity, an organization may be motivated to understand its top priority risks in response to a series of operational event outcomes or to simply improve their SDCPS risk management capabilities. The following sub-sections describe potential data collection triggers that may prompt an organization to gather safety data.

Mandatory Occurrence Reporting (CAA reports)

ICAO Annex 13 defines occurrence types that require mandatory personnel reporting. These occurrences are accidents and serious incidents. While this Annex defines a set of minimum mandatory occurrence reporting criteria, individual countries may have more restrictive reporting criteria in-place. For example, ICAO Annex 13 Attachment C states that "CFIT marginally avoided" is a serious incident. To clarify "marginally avoided" an individual country may define specific lateral and vertical distances by which terrain was avoided.

Company Operational Reporting

Several domains within the aviation industry (e.g. airlines, ANSPs, manufacturers, etc.) have internal mandatory reporting requirements that are more restrictive than the mandatory reporting requirements enforced by ICAO Annex 13 or by an individual country. For example, an air carrier may require mandatory event reporting for flight crews that declare minimum fuel inflight to ATC since any undue delays will cause a flight crew to use their fuel reserves. While the flight crew exercised good judgement and prevented safety from being compromised, there was no ICAO or state requirement to initiate a mandatory report for such an event. The air carrier in this scenario independently recognized that hazardous conditions may exist in an operation that might benefit from a company risk assessment.

Internal Company Audits

Internal company audit programs may be established for maximizing both internal product or process quality and operational safety outcomes. These programs may examine organizational compliance with company SOPs and/or well-established industry standards. They may also evaluate the effectiveness of an organization or process to identify improvement opportunities that have an indirect relationship to safety. These programs are a valuable source for hazard information that can be used during risk assessments.

External or 3rd Party Audits

Audits conducted by external or independent 3rd parties can significantly benefit an organization. These audits aim to examine the health and quality of an organization or process without internal organizational bias. The results of these audits offer the opportunity to understand how your organization compares against others across the industry. These results often outline findings and actionable recommendations in detailed reports. Example external auditing parties are IOSA, USOAP, ISBAO, and BARS.

Voluntary Disclosure Reporting Programs

In many countries, the regulator has offered a defined program by which a service provider may notify the regulator of a self-discovered non-compliance of either regulations or company procedures and policies. These programs offer an organization the opportunity to admit discovery and define a corrective action plan to address any known deficiencies. If accepted by the regulator, these programs can provide relief from enforcement actions. The successful characteristics of these programs include:

- A means to ensure the discovery was not already known to the regulator and under investigation.
- A safeguarding method for accepting appropriate reports while excluding those of intentional acts that disregard safety.
- A monitoring and follow-up process that ensures the corrective action addressing the root cause of the non-compliance has been successfully carried out for all conditions identified at the time of discovery and noted similar situations that could lead to future cases of non-compliance.

Internal Safety Investigation

For some events, a special investigation may be required if the severity of a discovery in any of the above data collection efforts is underway. That investigation may be conducted by an independent team to examine the circumstances that led to a negative outcome. The final report should document several findings and recommendations. For example, many organizations may decide that every mandatory occurrence report demands an investigation. Each organization may define their own threshold for initiating these investigations. Just as each of the hazards are identified in many of the other programs, each finding could be considered hazard information for future risk assessments.

Types of Safety Data

To identify major risk areas, teams within an organization will often collect and merge data from multiple information sources. This section is intended to provide an overview of the types of data that can benefit the advancement of an organization's SDCPS risk management capabilities.

Audit Data

Audit data measures an organization's compliance with a set of industry standards, regulations, or procedures. It is used to understand how an organization or a specific process performs when compared to standardized benchmarks or regulatory evaluation criteria. Outputs from an audit can reveal critical components of an operation that are vulnerable to errors or potential defects. They may also reveal findings that have indirect impacts on safety, such as operational consistency issues or process effectiveness. These deficiencies are typically documented as *findings*.

As detailed above, audits can be conducted by internal stakeholders or external parties. Examples of internal stakeholders are safety program managers and quality assurance managers. Examples of external parties are regulators and independent 3rd parties such as ICAO or IATA. Both types of audits can identify significant findings which may impact an organization. Examples of these include line operations (e.g. flight operations), operations support (e.g. maintenance, dispatch), and training (e.g. flight crew training).

To address the outcomes of an audit, findings are generally assigned to a department or an individual who then develops a corrective action and oversees its implementation. Often, the corrective action plans are meant to address the root cause of an audit finding. In short, audits are an extremely valuable source of potential hazard information, which can be used during risk assessment activities.

Measured Data

Measured data represents information collected by an observer or automated system during routine operations. The collection of measured data may be triggered by an event outcome (e.g. increased frequency of maintenance events), or it may be initiated by predetermined rates (e.g. heavy maintenance/D-checks).

Measured data often uses data sampling to limit the number of measurements needed. Data sampling is a technique used to select a representative subset of what is being measured in order to identify patterns and trends in the larger data set being examined. The subset may be defined by a specific time-period or by a select portion of an operation. For example, during an audit it may not be practical to assess every aircraft in an operator's fleet, so a select number of aircraft are chosen, possibly at random, to be assessed during the audit. When measured data using data sampling is recorded, it is intended to summarize either an entire operation (e.g. an entire flight) or a clearly defined portion of one (e.g. the approach to landing phase). Depending on how this data is recorded (e.g. by an observer versus automated system), it may be qualitative, have an element of subjectivity, and differing levels of consistency across observers. Measured data is often used to identify potential safety risks based on the frequency of leading outcomes. Historical measured data is a good source for hazard likelihood information during risk assessments.

Employee Safety Survey Data

Safety surveys are a key component to monitoring the health an integrity of an organization's safety program. They provide employees the opportunity to report their perception of an organization's safety program and their opinion of safety practices in day-to-day operations. For example, safety surveys can answer the following questions:

- Do employees feel safe?
- Are employees receiving the appropriate training and support for risk-based decision-making?
- Are employees confident that raised safety concerns are addressed by their organization?
- Are employees aware of their organization's safety performance objectives?

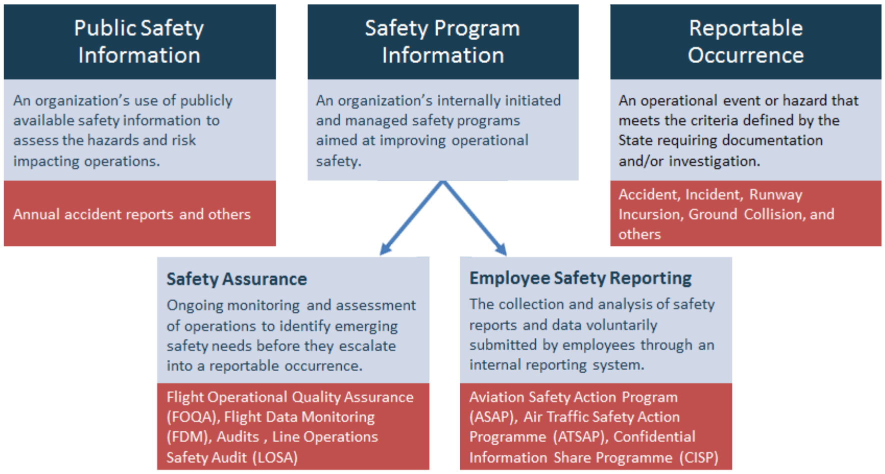
Safety surveys are helpful when working to initiate safety improvements. Surveys may also help diagnose trends in employee perceptions.

Successful management of risk depends on continuous improvement and a resolve to eliminate risk in every way possible. Perception measures gathered from employee safety surveys can indicate the degree to which the overall company has adopted an attitude of continuous improvement and risk reduction. Keep in mind that variation in responses is normal and that while some employee perceptions may not be positive, an organization as a whole can still be doing good things to improve safety.

Sources of Safety Data

Across the aviation industry, there numerous sources of safety data. For the purposes of this toolkit, these sources have been grouped into the following categories: Public Safety Information, Safety Program Information (which includes Safety Assurance, and Employee Safety Reporting), and Reportable Occurrence Data.

DATA COLLECTION



Public Safety Information

An organization's use of publicly available safety information to assess the hazards and risk impacting operations.

Annual accident reports and others

Safety Program Information

An organization's internally initiated and managed safety programs aimed at improving operational safety.

Reportable Occurrence

An operational event or hazard that meets the criteria defined by the State requiring documentation and/or investigation.

Accident, Incident, Runway Incursion, Ground Collision, and others

Safety Assurance

Ongoing monitoring and assessment of operations to identify emerging safety needs before they escalate into a reportable occurrence.

Flight Operational Quality Assurance (FOQA), Flight Data Monitoring (FDM), Audits , Line Operations Safety Audit (LOSA)

Employee Safety Reporting

The collection and analysis of safety reports and data voluntarily submitted by employees through an internal reporting system.

Aviation Safety Action Program (ASAP), Air Traffic Safety Action Programme (ATSAP), Confidential Information Share Programme (CISP)

Figure 3 Summary of Safety Data Sources

While each of these sources provide information that is unique and valuable, an organization must consider when each source is appropriate. This is typically driven by the need that an organization must address (e.g. identification of top priority risks vs. the cause of an accident). Throughout data collection, multiple data types (e.g. audit data, measured data, employee survey data, etc.) will be gathered by various teams across an organization. As this information is captured, it is important that it be recorded in a manner usable by other team members for SDCPS risk management. Furthermore, it is critical that an organization have the mechanisms in-place, whether it is manual or automated, to check and ensure that the data collected is free of errors.

The following sub-sections describe these data sources in more detail and provide level 1 intensity best practices for each.

Public Safety Information

Public Safety Information describes data that is available for unrestricted use by domains and organizations across the industry. This data is often used to identify lessons learned from historical occurrences with the intent to improve future operations and an organization's SDCPS risk management capabilities. Public Safety Information is available from many sources such as ICAO, IATA, Boeing, Airbus, and other Civil Aviation Authorities. Public Safety Information can be utilized by an organization to:

- Identify lessons learned from another organization or domain (e.g. risk mitigations)
- Develop performance benchmarks based on industry-wide Safety Performance Indicators (SPIs)
- Improve data collection processes and methods to achieve the next level of intensity
- Identify hazards from other organizations to that may impact your operation
- Develop targeted safety recommendations (e.g. investigative bodies)
- Pursue new rulemaking (e.g. Regulators)

Best Practices for Public Safety Information Data Collection – Level 1 Intensity

- Collect quality data from trusted sources. Analysis outputs will be limited by the quality and depth of data collected.

- Gather information from organizations operating at an equal or greater level of intensity. This includes accident reports, incident reports, and supporting analyses that are available for unrestricted use.
- Ensure the completeness of data collected. Analysts will require as much information as possible (e.g. context) to effectively normalize the data and apply it to your operation.

Reportable Occurrences

Reportable Occurrences include information on an operational event or hazard that meets the criteria defined by ICAO, the state, and/or organization requiring documentation and/or investigation. This information is obtained primarily through internal data sources by investigators, analysts, or by being a participating organization/party to an investigative process. Reportable Occurrence data is typically collected in response to the following events:

- Aircraft accident (e.g. controlled flight into terrain)
- Serious Incident (e.g. runway incursion)
- Significant Air Proximity (AIRPROX) Event

Best Practices for Reportable Occurrence Data Collection – Level 1 Intensity

As a level 1 intensity organization collects reportable occurrence data, it is helpful to use the following best practices:

- Develop a secure Reportable Occurrence data collection system and process with clear data access controls. It is important that this data is protected to encourage employee trust in the system. The level of employee trust will have a direct impact on your ability to collect more in-depth data.
- Introduce data collection checklists and/or procedures that aim to streamline the data gathering process and to limit variability across data sets. At this level of intensity, these should focus on meeting the requirements set by your domain and regulator.
- Avoid the collection of ambiguous or non-specific data that may not be useable or cannot be analyzed.

Safety Assurance

Safety Assurance describes the on-going monitoring and assessment of a domain’s operational performance to identify emerging safety needs before they escalate into a reportable occurrence. Safety assurance information can be collected from both internal and external data sources. Safety assurance information is well suited to support:

- Validation of operational performance targets (e.g. number of maintenance induced delays)
- Operational integration issues (e.g. reoccurring hard landings at a specific)
- Identification of emerging human-system performance needs (e.g. audit data)

Best Practices for Safety Assurance – Level 1 Intensity

As a level 1 intensity organization, it is helpful to use the following best practices for Safety Assurance:

- Develop a Safety Assurance program that fosters a positive safety culture. Data collected via this program should be used to educate employees, identify emerging risks, and assess the effectiveness of existing risk controls.
- Collect data from other internal (e.g. Voluntary Safety Reporting Program [VSRP] data, training data, etc.) and external sources (e.g. public safety trends, etc.) to provide context and deeper insights into outcome-based data.
- Establish a data storage strategy. Data collected should be stored, backed up, and archived in an organized manner that will support audits, targeted deep dives, and historical data reviews to assess short- and long-term performance (e.g. this could be used to support the identification of a risk's likelihood).
- Collect and store Safety Assurance data that is representative of the entire operation to develop a comprehensive risk picture. Avoid information biases or gathering disjointed data that may negatively impact the analysis process.

Employee Voluntary Reporting Programs

Employee voluntary reporting programs include the collection and analysis of safety data voluntarily submitted by employees through an internal reporting system. These types of reports can provide unique insights into the safety issues and events encountered in daily operations that would otherwise go unreported. Reports can be collected through internal company reporting systems or accessed from publicly available external reporting systems.

Employee voluntary reporting programs have become more prevalent throughout the world as industry and regulators have witnessed the value of collecting safety information provided by frontline employees such as pilots, controllers, and maintenance technicians. Many safety professionals believe that the key to driving down risk is to get critical safety information from those who work in the system day-in and day-out. Data from those individuals has shown to be an effective way of detecting problems that could lead to an incident or an accident. This unique, first-hand perspective provided by employees can help an organization to do the following:

- Identify close-calls and near miss events to prioritize near-term safety needs.
- Develop and share lessons learned and best practices for managing specific types of hazards and across an organization.
- Substantiate and explain other data sources (e.g. pairing of voluntary reports with FDM data).
- Target opportunities to improve organizational safety culture (e.g. gauge program participation).

Best Practices for Employee Voluntary Reporting Programs – Level 1 Intensity

As a level 1 intensity organization, it is helpful to use the following best practices for Employee Voluntary Reporting Programs:

- Develop an Employee Voluntary Safety Reporting Program (VSRP) that is scalable to meet the immediate and long-term needs of your organization.
- Implement a VSRP that enables employees to report information in a timely manner. Critical details can often be lost or forgotten with time.

- Develop a standardized reporting form or tool that makes it easy for frontline staff to describe the nature of their discovery and details about the circumstances of what, when, where, how an event happened (e.g. factual information such as location, aircraft type, etc.).
- Establish clear expectations surrounding the types of safety events and/or issues that should be reported.
- Provide examples of safety reports through training or awareness materials to establish expectations for report quality. Materials should denote the differences between high quality and lower quality reports. Employees need to understand what information should be reported and the depth of that information.
- Clearly explain the VSRP process so that employees understand what happens after a report is filed and how they can access the status of their report. Explaining how analysts will use reports to improve organizational safety will increase the quantity and quality of the reports.
- Establish a collection agent that acts independently to receive and capture the details of each report and can perform the necessary deidentification work to protect the source.
- Establish the criterion for accepting reports into the VSRP and a process for managing reports that do not meet the criterion.
- Establish roles and responsibilities for key VSRP members. These include decision-makers and independent safety agents who may provide feedback to employees on event reports. For example, you may have a standing body of decision-makers capable of engaging the regulator as needed.

Reliability and Quality of Information

Since there is a wealth of information available, it is important to balance the quantity of data with the quality of data collected. To manage this need, it is recommended that an organization focus on the collection of high quality data that is within the agreed scope of an organization’s needs. It must also be free of errors that may impact future analysis activities. Common data quality issues include duplicative data sets, incomplete data, inconsistent data, inaccurate data, ambiguous data, and subjective data. Additional issues may be encountered if an organization uses manual processes or procedures to gather, enter, merge, and check data. To mitigate these issues, it is important that an individual be assigned the responsibility of checking your data. For example, when manual processes are used, the individual would be responsible for ensuring that fields are not left blank or that information is undecipherable.

To maintain the health and integrity of your organization’s safety program, employees must be able to trust that the data collected is of a high quality. If employees (e.g. analysts, frontline employees, managers, etc.) do not trust the data, the validity of analysis results and/or corrective actions may be questioned. Ultimately, this can erode the effectiveness of your organization’s safety program.

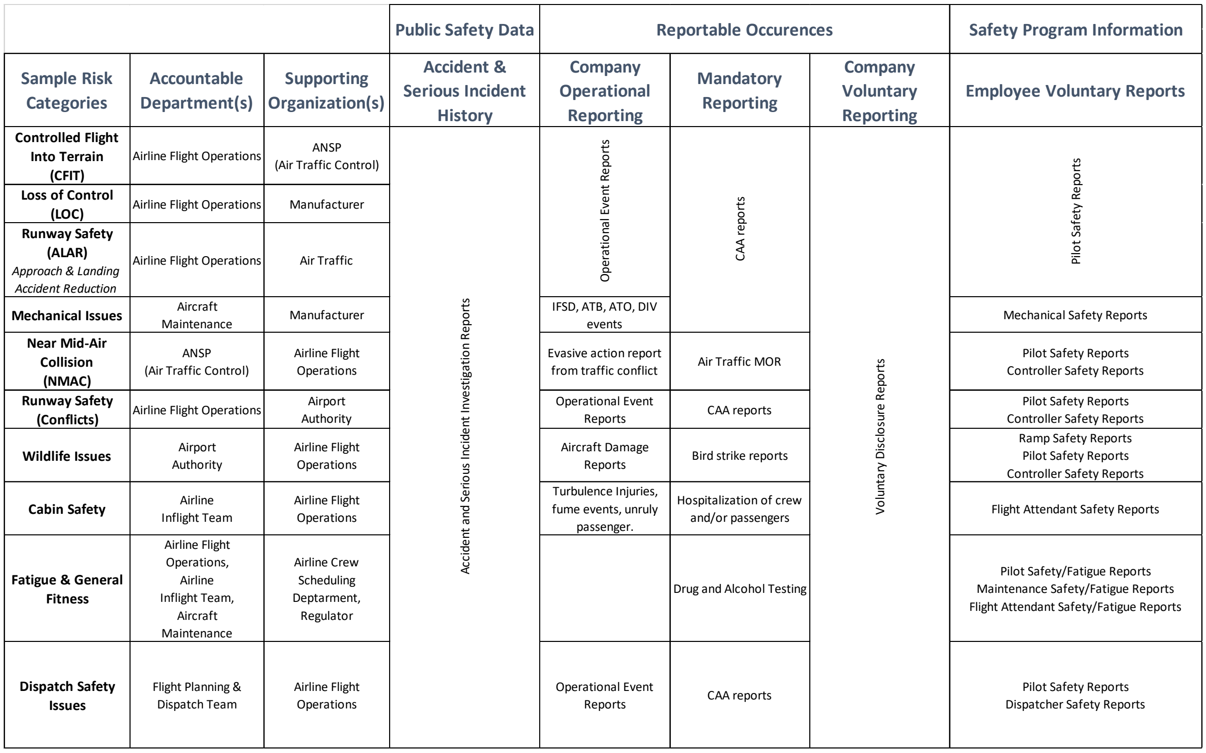
Data Collection Map

As an organization gathers and merges information from multiple safety data sources, they are encouraged to develop a safety data collection map. This map can be a valuable tool as an organization characterizes their current data collection capabilities and begins to identify opportunities to advance to the next level of SDCPS intensity. It is recommended that this map identify:

- Major risk areas that are being used to map or categorize an organization’s top priority risks,

- Sources of information that are used to gather data on each major risk area, and the
- Persons or departments that are responsible and accountable for gathering various data types from each source.

Developed by Flight Safety Foundation, Figure TBD illustrates a sample airline operator data collection map.



			Public Safety Data	Reportable Occurences			Safety Program Information
Sample Risk Categories	Accountable Department(s)	Supporting Organization(s)	Accident & Serious Incident History	Company Operational Reporting	Mandatory Reporting	Company Voluntary Reporting	Employee Voluntary Reports
Controlled Flight Into Terrain (CFIT)	Airline Flight Operations	ANSP (Air Traffic Control)	Accident and Serious Incident Investigation Reports	Operational Event Reports	CAA reports	Voluntary Disclosure Reports	Pilot Safety Reports
Loss of Control (LOC)	Airline Flight Operations	Manufacturer					
Runway Safety (ALAR) *Approach & Landing Accident Reduction*	Airline Flight Operations	Air Traffic					
Mechanical Issues	Aircraft Maintenance	Manufacturer		IFSD, ATB, ATO, DIV events			Mechanical Safety Reports
Near Mid-Air Collision (NMAC)	ANSP (Air Traffic Control)	Airline Flight Operations		Evasive action report from traffic conflict	Air Traffic MOR		Pilot Safety Reports Controller Safety Reports
Runway Safety (Conflicts)	Airline Flight Operations	Airport Authority		Operational Event Reports	CAA reports		Pilot Safety Reports Controller Safety Reports
Wildlife Issues	Airport Authority	Airline Flight Operations		Aircraft Damage Reports	Bird strike reports		Ramp Safety Reports Pilot Safety Reports Controller Safety Reports
Cabin Safety	Airline Inflight Team	Airline Flight Operations		Turbulence Injuries, fume events, unruly passenger.	Hospitalization of crew and/or passengers		Flight Attendant Safety Reports
Fatigue & General Fitness	Airline Flight Operations, Airline Inflight Team, Aircraft Maintenance	Airline Crew Scheduling Deptarment, Regulator			Drug and Alcohol Testing		Pilot Safety/Fatigue Reports Maintenance Safety/Fatigue Reports Flight Attendant Safety/Fatigue Reports
Dispatch Safety Issues	Flight Planning & Dispatch Team	Airline Flight Operations		Operational Event Reports	CAA reports		Pilot Safety Reports Dispatcher Safety Reports

Figure 4 Sample Level 1 Intensity Data Collection Map

Creating a Plan for Success

To guide the consistent collection of high quality data, it is recommended that an organization develop a data collection plan that provides a repeatable set of data collection and information management strategies. This plan may include:

☐ Data Collection Triggers – When and why data is collected from each data source
☐ Roles and Responsibilities – A matrix describing who is responsible for collecting and managing data
☐ Data Quality Management – A plan for managing the quality of collected data including data conditioning, filtering, and document change management plan
☐ Storage – Information describing where each data will be housed and who should have access to it
☐ Data Access – Describe how analysts will access each data source and who will be given access to each data source
☐ Process Improvement Plan – A plan for the organization to continually improve itself with respect to the data collection process

DATA COLLECTION

Implementing a data collection plan offers the opportunity to increase productivity, improve data consistency, and reduce potential organizational inefficiencies. A data collection plan at the first level of intensity also provides a solid foundation for achieving high levels of intensity as necessary.

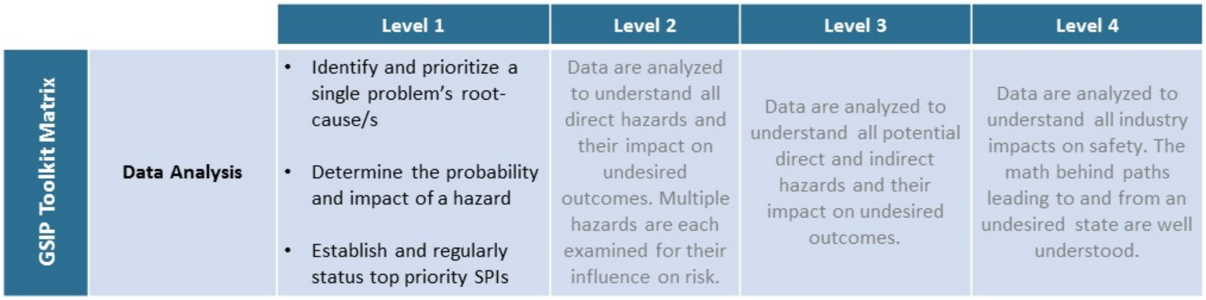
Key Terminology

<Placeholder>

DATA ANALYSIS

Data Analysis

Level 1 intensity focuses on the quantitative analysis of risks, issues, and opportunities that are of the highest priority to your operation. This toolkit describes data analysis techniques that can be used to assess those risks and begin tracking them on a Safety Management System (SMS) risk matrix. This toolkit also demonstrates how data analysis results can be applied to develop meaningful Safety Performance Indicators (SPIs).



		Level 1	Level 2	Level 3	Level 4
GSIP Toolkit Matrix	Data Analysis	• Identify and prioritize a single problem's root-cause/s • Determine the probability and impact of a hazard • Establish and regularly status top priority SPIs	Data are analyzed to understand all direct hazards and their impact on undesired outcomes. Multiple hazards are each examined for their influence on risk.	Data are analyzed to understand all potential direct and indirect hazards and their impact on undesired outcomes.	Data are analyzed to understand all industry impacts on safety. The math behind paths leading to and from an undesired state are well understood.

Figure 5 Data Analysis Level 1 Intensity Matrix

The examples provided in this toolkit will focus on commercial aviation, however the underlying approaches can be tailored to address your specific operational needs.

Optimization and Management of Safety Data

Maintaining a high level of data integrity is critical to producing analysis results that are valid and meaningful. This will require your organization to have an in-depth understanding of its safety data sources and the current health of its data collection program (e.g. employee voluntary safety reporting program, automated versus manual safety reporting systems, etc.). Continually assuring the accuracy, consistency, completeness, and timeliness of safety data can prevent low quality information from detracting from high quality information during important risk management activities.

To reduce the probability of basic data compatibility issues, it is important to normalize your organization's safety data. In other words, it is recommended to adjust your data that is measured on different scales (e.g. rates per flights conducts, findings per audit performed, issues per equipment movements, etc.) so that it is standardized and compatible for analysis. This will prevent data irregularities or redundant information from affecting the quality of key analysis inputs and outputs. This is especially true when splitting or grouping data of varying levels of significance from different domains, departments, operations, sources, time periods, issues, or deficiency types.

Not all data is created equal.

Runway safety data from a single low volume airport may not be weighted the same as runway safety data from ten of the world's busiest airports.

As your organization filters and merges raw data sources, it is important to be aware of common data analysis issues. These issues include but are not limited to the following: Lack of data traceability (understanding and documenting the original source from which data is being collected), overemphasis and/or under emphasis of outlying data points, lack of consistent data cleansing, information bias, and incorrect correlation of data. Understanding the intent, benefits, and limitations of your data will help defend against these common issues. For example, audit data is used to measure an organization's compliance with industry standards. Using audit data makes identifying non-compliance both simple and objective. Another type of data is measured data, also known as field data. Measured data can represent information collected by an observer. This type of data may be qualitative, have an element of subjectivity, and have differing levels of consistency across observers. While both data types are extremely valuable, it is important to recognize their similarities and differences to effectively guard against common data analysis issues.

Assessment of Risk: Root-Cause Analyses

Flight Safety Foundation encourages the use of Cause-and-Effect (Ishikawa) Diagrams as a part of SDCPS risk management. This valuable root-cause-analysis method provides users with a repeatable process to identify the source of risk by systematically determining the root causes of a problem.

Often organizations spend too much time focusing on the symptoms of a problem rather than the causes. The Ishikawa cause-and-effect diagram, also known as a fishbone diagram, is a tool which facilitates the uncovering of a problem's root-causes through a simple and straight-forward process. For example, fishbone diagrams are typically used in group settings. A facilitator or designated team member will be responsible for drawing the diagram and continually asking the group to brainstorm "why?" a situation, problem, and/or factor occurs. While brainstorming, it is highly recommended to use evidence, or data, to develop the fishbone rather than speculation.

The Architecture of a Cause-and-Effect (Ishikawa/Fishbone) Diagram

It is important to understand the basic architecture and terminology associated with a fishbone diagram. The **problem** is represented at the head of the fish located at one end of the diagram. Trailing from the fish head is the backbone with off-shooting ribs forming the **major factors** (major causal categories) related to the problem. Typically, there are 3 to 6 major factors per problem. Stemming from each of these ribs are the **sub-causes** that detail why a problem occurs. These sub-causes may have their own sub-causes which can be shown by adding additional levels of branching. Each level of branching is carried out as far as possible by asking "Why?" repeatedly for each cause and effect relationship to identify the root causes that lead to the main problem.

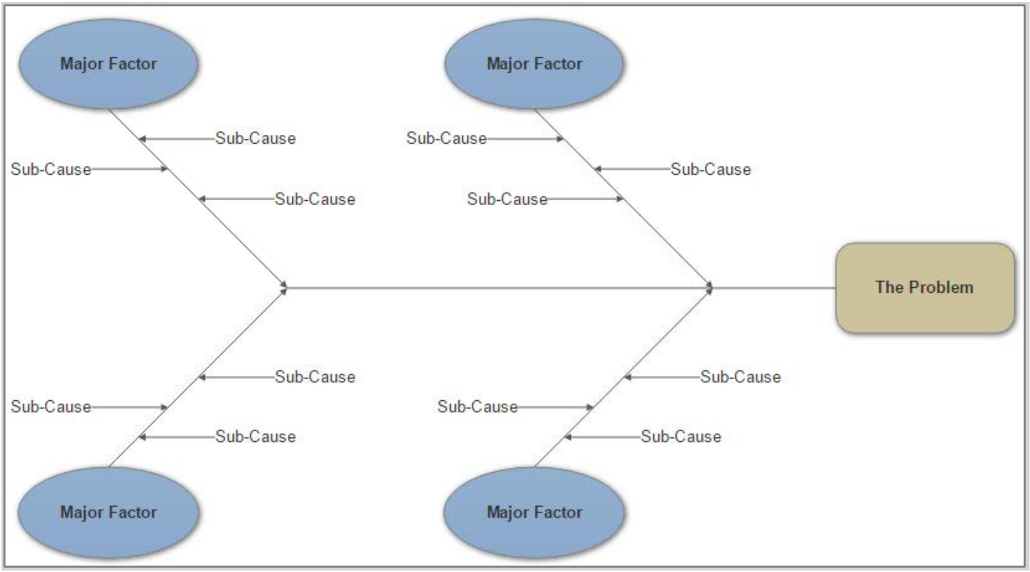


Figure 6 Ishikawa/Fishbone Diagram Architecture

When identifying root causes of very specific events, you may wish to move to a more scalable and more flexible method called cause-mapping. This method is similar the Ishikawa Diagram except it does not rely on major factors to sort causes. Instead, all causes stem directly from the problem (backbone). For each cause-effect relationship, individual pathways are shown. While cause-mapping does not usually result in a fishbone-like appearance, it accomplishes similar goals.

Guide to Using Cause-and-Effect (Ishikawa) Diagrams

To complete an Ishikawa diagram, an organization must first choose a problem to analyze. This problem can be identified by referencing recent safety data analysis outputs, an operation's risk register, or an organization's top priority risks. Once a problem is selected, it should be clearly documented in the head of the fishbone diagram (if you struggle to clearly document the problem, consider what, when, where, and why your selected problem exists). Next, you will determine the major factors, or categories, that are used to focus the development of the ribs. It may be necessary to customize the major factors to address your specific problem, but if you are having difficulty thinking of categories you may wish to use materials, machines, people, methods, and environment as a default.

Next, fill out the fishbone diagram one rib at a time. For each major factor, list the identified causes and sub-causes of the problem. This can be done by asking "why?" and listing the responses from group participants. This process should be repeated until the root causes of the problem are clearly identified. Typically, this should take no more than 5 levels of questioning ("why?"). Outputs from an Ishikawa Diagram are a list of a problem's root-causes. It is highly recommended to consider the use of other data sources and analysis techniques to help prioritize and respond to these root causes.

Applied Ishikawa/Fishbone Example

Figure TBD shows an example of an Ishikawa diagram prepared by an example organization that was experiencing issues with runway incursions. The problem identified by this organization was "Runway incursions that were affecting safety of humans and property". To focus brainstorming activities, the organization used the following major factors (categories): Methods, People, Equipment, and

Environment. Within each major factor (category), the organization identified various causes and sub-causes until the causes for each major factor were fully exhausted.

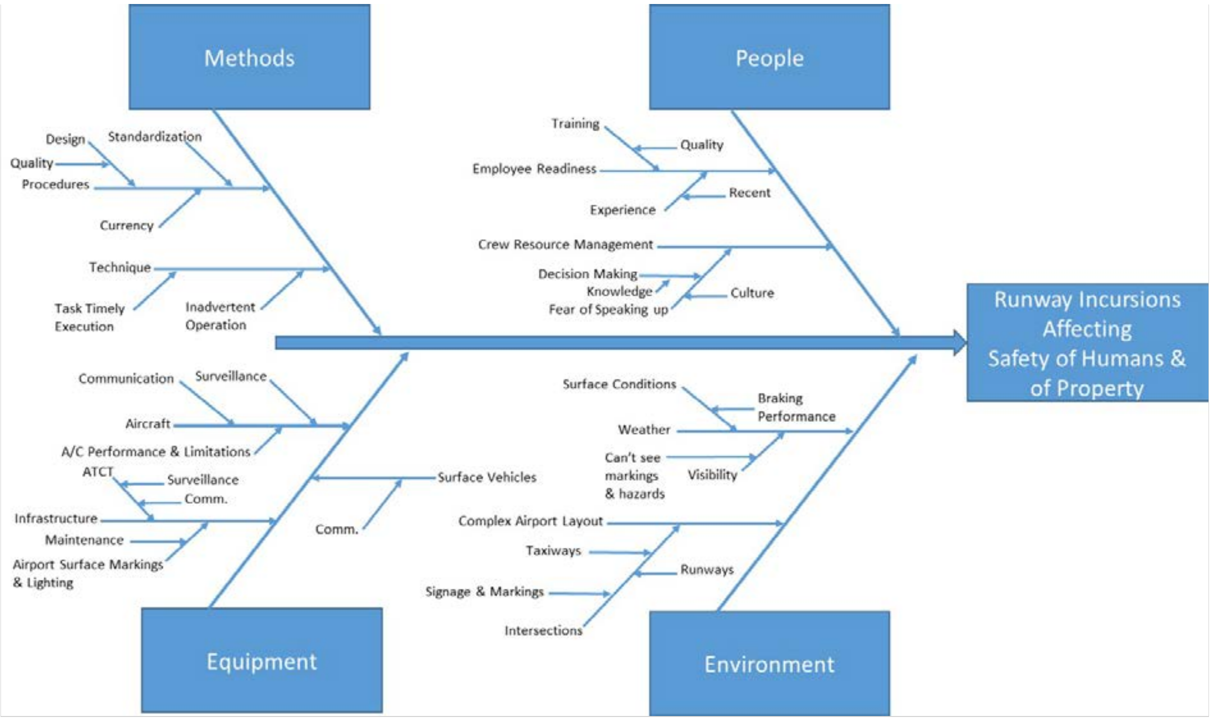


Figure 7 Applied Runway Safety Fishbone Example

After further discussion and analysis of all the root causes, the highest priority root causes were as follows: *People* - it was found that workers were not properly trained. *Environment* - it was found that signage and markings for intersections of taxiways and runways led to an overly complex airport layout. *Equipment* - it was found that communications between aircraft, ATC, and Surface Vehicles were not always successful.

Level 1 Risk Analysis Inputs, Outputs, and Techniques

At each level of intensity, the GSIP data analysis toolkits present analytical techniques that aim to increase the depth and richness of information used to populate a Cause-and-Effect (Ishikawa/Fishbone) Diagram, and at higher levels of intensity a Bowtie Model (see Level 2 Toolkits for more information on Bowties). For the purposes of this toolkit, level 1 analyses will focus on the following:

- Use of public and internal safety data to support the identification of an organization's top priority risks.
- Methods to quantify the severity and likelihood of an undesired state.
- Application of significant findings to develop meaningful SPIs.

To support the development of a level 1 intensity Cause-and-Effect (Ishikawa/Fishbone) Diagram, this section will describe sample data analysis inputs, outputs, and techniques to begin the identification of an organization's top priority risks. These analyses include a frequency-based analysis and a baseline analysis.

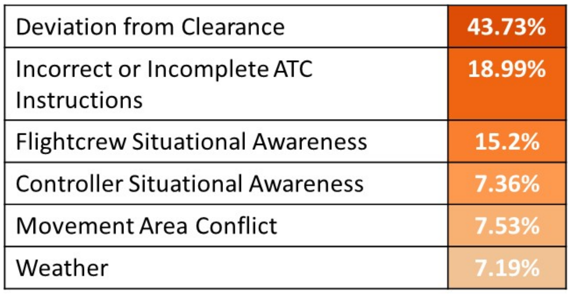
DATA ANALYSIS

Frequency-Based Analysis

Many safety analyses begin with frequency-based assessments. These assessments aim to identify the most frequently occurring hazards or safety event types (undesired states) which impact an operation. The results of a frequency-based assessment provide an organization with the data to rank and prioritize potential safety issues which require additional analysis. Below are samples of frequency-based data sources, analysis inputs, and analysis outputs.

Table 2 Example Frequency-Based Analysis Inputs and Outputs

Data Sources	Example Analysis Inputs	Example Analysis Outputs
Reportable Occurrence Data	Accident/serious incident reports describing safety event outcomes and probable causes.	Most frequently cited accident/incident outcomes and probable causes.
Employee Safety Reports	Frontline employee event narratives describing observed safety events and/or issues.	Most frequently cited event outcomes and causal factors.
Safety Assurance Data	Survey measuring employee perception of an organization's safety program.	Most frequently cited perceptions.



Deviation from Clearance	43.73%
Incorrect or Incomplete ATC Instructions	18.99%
Flightcrew Situational Awareness	15.2%
Controller Situational Awareness	7.36%
Movement Area Conflict	7.53%
Weather	7.19%

Figure 8 Sample Frequency-Based Analysis Results

At level 1 intensity, frequency-based analysis results can be used to identify the following:

- Leading negative outcomes by risk area (e.g. runway safety, CFIT, LOC, etc.).
- Most common undesired states (safety event) that led to a specific negative outcome.
- Defense patterns from public safety information (e.g. mitigations) for an undesired state.
- Top recovery measures cited by your internal organization for an undesired state.

Baseline Analysis

A baseline analysis provides an organization with performance-based reference points that can be used to assess the impact of operational changes, or to characterize current operational performance in comparison to predetermined thresholds. The results of a baseline analysis will provide an organization with detailed insights into current and historical operations data. This is especially helpful when trying to understand the health and integrity of an organization's safety program. Below are some samples of baseline data sources, analysis inputs, and analysis outputs.

Table 3 Example Baseline Analysis Inputs and Outputs

Data Sources	Example Analysis Inputs	Example Analysis Outputs
Employee Safety Reports	Frontline employee event narratives describing observed safety events and/or issues.	Most frequently cited safety events and/or issues grouped by ICAO high-risk category.
Public Safety Information	Annual safety reports detailing performance-based data.	Average number of global safety events by ICAO high-risk category.
Safety Assurance Data	Audit data describing regulatory compliance.	Internal performance-based audit data by ICAO high-risk category.
Reportable Occurrence	Accident/serious incident reports describing safety event outcomes and probable causes.	Average number of accident/serious incident outcomes by ICAO region and ICAO high-risk category.

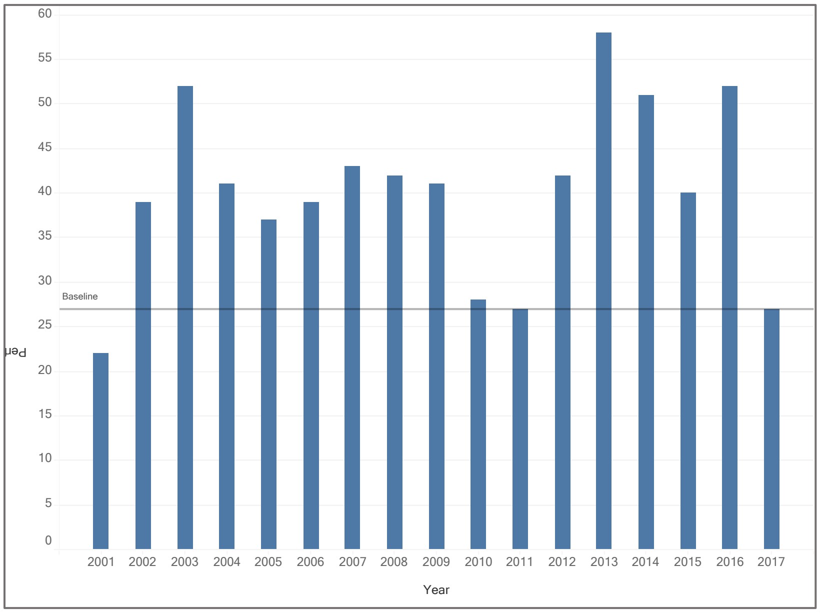


Figure 9 Sample Baseline Analysis Results

At level 1 intensity, baseline analysis results can be used to:

- Characterize current operations with performance-based reference points,
- Establish safety performance benchmarks to monitor undesired states (safety events), and
- Measure the impact of recent or proposed operational changes.

Quantitative Risk Assessment

Once a set of high priority risks, issues, and opportunities are identified, they must be further evaluated to determine their probability (likelihood) and operational impact (severity). While there are a variety of techniques that are used to assess these variables, this toolkit will reference the ICAO SMS severity and likelihood scales. Since SMS provides general definitions for each level of likelihood and severity, an organization may wish to tailor those definitions to attain a more refined level of accuracy and standardization during the risk assessment process. It is recommended that these definitions are written in plain language and are universally applied across your organization to ensure consistency.

Risk Probability Assessment

Below in Table TBD are the ICAO safety risk probability (likelihood) scale definitions. When using the probability scale during an assessment, an organization is applying their internal and external safety data (e.g. safety reports, annual reports, occurrence data, etc.) to determine the rate or frequency of exposure to a specific threat or undesired state within the context of their daily operation. The greater the rate or frequency of exposure, the greater the likelihood of a negative outcome. At level 1 intensity, it is assumed that outcome-based data (e.g. frequency of accidents, incidents, etc.) will be used to complete this assessment. At higher levels of intensity, it is assumed that more in-depth data (e.g. contributory factors, etc.) will be considered when conducting risk probability assessments.

Table 4 ICAO Document 9859 Safety Risk Probability

Likelihood	Meaning	Value
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely Improbable	Almost inconceivable that the event will occur	1

Risk Impact Assessment

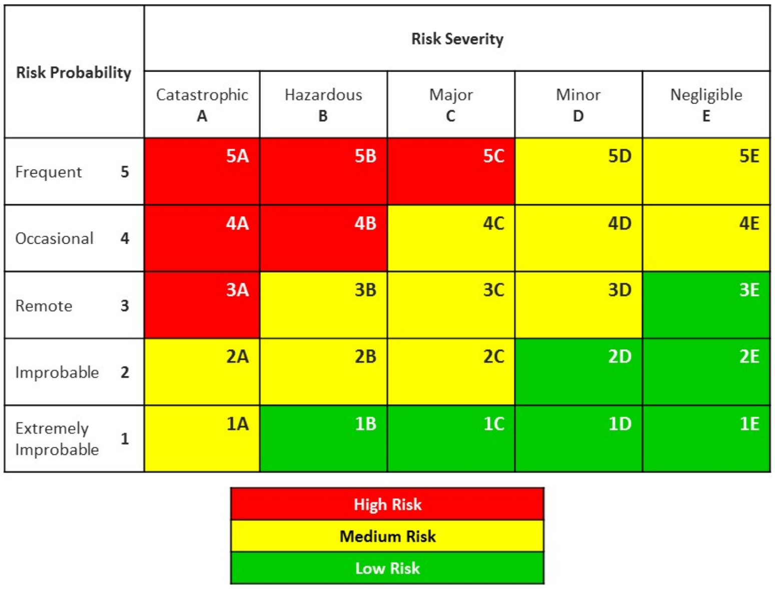
Below in Table TBD are the ICAO safety risk severity (impact) scale definitions. When applying this scale during an assessment, an organization is applying their safety data to evaluate all potential (reasonable) outcomes that may occur when exposed to an undesired state (safety event). This assessment will result in the selection and rating of the worst credible outcome within the context of an organization’s operation. At level 1 intensity, it is assumed that outcome-based data (e.g. audit data, accidents, incidents, etc.) will be used to complete this assessment. At higher levels of intensity, it is assumed that more in-depth data (e.g. close calls, etc.) will be considered when conducting risk severity assessments.

Table 5 ICAO Document 9859 Safety Risk Severity

Severity	Meaning	Value
Catastrophic	- Equipment destroyed - Multiple deaths	A
Hazardous	- A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely - Serious injury - Major equipment damage	B
Major	- A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency - Serious incident - Injury to persons	C
Minor	- Nuisance - Operating limitations - Use of emergency procedures - Minor incident	D
Negligible	- Few consequences	E

Assignment of Risk Ratings

Upon completion of both the risk probability and impact assessments, an organization must then assign a risk with a risk rating. A risk rating represents the combined values of the likelihood and severity assessment outputs. To guide risk rating assignment, it is recommended to use an SMS risk matrix (see Figure TBD).



Risk Probability		Risk Severity				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	🟥 5A	🟥 5B	🟥 5C	🟨 5D	🟨 5E
Occasional	4	🟥 4A	🟥 4B	🟨 4C	🟨 4D	🟨 4E
Remote	3	🟥 3A	🟨 3B	🟨 3C	🟨 3D	🟩 3E
Improbable	2	🟨 2A	🟨 2B	🟨 2C	🟩 2D	🟩 2E
Extremely Improbable	1	🟨 1A	🟩 1B	🟩 1C	🟩 1D	🟩 1E

🟥 High Risk
🟨 Medium Risk
🟩 Low Risk

Figure 10 ICAO Document 9859 Safety Risk Assessment Matrix. Modified for printing.

DATA ANALYSIS

In terms of risk acceptability, it is widely understood that high risks (red) are considered unacceptable and must be immediately addressed. Medium risks (yellow) may be acceptable if sufficient mitigations are in-place, however residual risk assessments are highly recommended. Low risks (green) may be deemed acceptable, however in the interest of improving safety it is still strongly recommended to thoroughly evaluate these risks either through a fishbone diagram or other assessment method.

Like the risk probability and impact scales, it is recommended that an organization tailor their high, medium, and low risk criteria as well. For example, a risk averse may consider a risk rating of 3B to be a high risk. On the other hand, an organization with a higher risk threshold may consider a 3B risk rating to be a medium risk. The criteria for high, medium, and low risks should be tailored to address your specific operational needs.

Applied Examples of Probability, Impact, and Risk Category Customization

Below are applied examples that demonstrate how an organization can tailor SMS scale definitions to address their unique operational needs. Tables TBD and TBD are customized probability and impact scale definitions that were developed by the FAA. Table TBD is a tailored impact scale that was developed by Flight Safety Foundation with the support of industry partners.

Table 6 FAA SRM Quick Reference Guide, Hazard Severity Definitions

Effect On:	Hazard Severity Classification				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
ATC Services	Conditions resulting in a minimal reduction in ATC services, or a loss of separation resulting in a Category D Runway Incursion (RI), Operational Deviation (OD), or Proximity Event (PE)	Conditions resulting in a slight reduction in ATC services, or a loss of separation resulting a Category C RI or OE	-Conditions resulting in a partial loss of ATC services, or a loss of separation resulting in a Category B RI or OE	-Conditions resulting in a loss of ATC services (ATC zero), or a loss of separation resulting in a Category A RI or OE	-Conditions resulting in a collision between aircraft, obstacles, or terrain
Flight Crew	-Flightcrew receives TCAS Traffic Advisory (TA) informing of nearby traffic, or, -PD where loss of airborne separation falls within the same parameters of a -Category D OE or PE Minimal effect on operation of aircraft	-Potential for Pilot Deviation (PD) due to TCAS Preventive Resolution Advisory (PRA) advising crew not to deviate from present vertical profile or, -PD where loss of airborne separation falls within the same parameters of Category C (OE) or, -Reduction of functional capability of aircraft but does not impact overall safety (e.g. normal procedures as per AFM)	-PD due to response to TCAS Corrective Resolution Advisory (CRA) issued advising crew to take vertical action to avoid developing conflict with traffic or, -PD where loss of airborne separation falls within the same parameters of a Category B OE or, -Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per AFM	-Near mid-air collision (NMAC) results due to proximity of less than 500 feet from another aircraft or a report is filed by a pilot or flight crew member that a collision hazard existed between two or more aircraft -Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per AFM	-Conditions resulting in a mid-air collision (MAC) or impact with obstacle or terrain resulting in a hull loss, multiple fatalities, or fatal injury

Flying Public	-Minimal injury or discomfort to passenger(s)	-Physical discomfort to passenger(s) (e.g. extreme braking action' clear air turbulence causing unexpected movement of aircraft causing injuries to one or two passengers out of their seats) -Minor injury to greater than zero to less than or equal to 10% of passengers	-Physical distress on passengers (e.g., abrupt evasive action; severe turbulence causing unexpected aircraft movements) -Minor injury to greater than 10% of passengers	-Serious injury to passenger(s)	-Fatalities or fatal injury to passenger(s)

Table 7 FAA SRM Quick Reference Guide, Hazard Likelihood Definitions

	Likelihood Definitions					
	NAS Systems & ATC Operational	NAS Systems		ATC Operational		Flight Procedures
		Qualitative				
	Quantitative	Individual System	ATC Service/NAS Level System	Per Facility	NAS-Wide	
Frequent A	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-3}$	Expected to occur about once every 3 month for an item	Continuously experienced in the system	Expected to occur more than once per week.	Expected to occur more than every 1-2 days.	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-5}$
Probable B	Probability of occurrence per operation/operational hour is less than $1x10^{-3}$ but equal to or greater than $1x10^{-5}$	Expected to occur about once per year for an item	Expected to occur frequently in the system	Expected to occur about once every month.	Expected to occur about several times per month.	
Remote C	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$	Expected to occur several times in the lifecycle of item	Expected to occur numerous times in system lifecycles	Expected to occur about once every year.	Expected to occur about once every few months.	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$
Extremely Remote D	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$	Unlikely to occur, but possible in an item's lifetime	Expected to occur several times in the system lifecycle	Expected to occur about once every 10 – 100 years.	Expected to occur about once every 3 years.	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$
Extremely Improbable E	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$	So unlikely that it can be assumed that it will not occur in an item's lifecycle	Unlikely to occur but possible in the system lifecycle	Expected to occur less than once every 100 years.	Expected to occur less than once every 30 years.	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$

1

Table 8 FSF Impact Assessment Criteria; Tailored Example

Area for Assessment	Consequences					
	Insignificant	**Minor**	**Moderate**	**Major**	**Severe**	**Catastrophic**
General	Negligible impact upon objectives	Minor effects that are easily rectified	Some objectives are affected	Some important objectives cannot be achieved	Most objectives are affected	Most objectives cannot be achieved
People/Injury	Injuries or aliments not requiring First Aid treatment	Minor injury or First Aid treatment case	Serious injury causing hospitalization or multiple medical treatment cases	Life threatening injury or multiple serious injuries causing hospitalization	Multiple life threatening injuries. Less than 10 fatalities	Multiple fatalities, 10 or more
Reputation	Internal review	Scrutiny required by internal committees or internal audit to prevent escalation	Scrutiny required by external committees or Auditor general's office, etc.	Intense public, political, and media scrutiny (e.g. inquest, front page headlines, TV, etc.)	Government inquiry or Commission of inquiry or adverse national media in excess of 1 week	Government inquiry and ongoing adverse international exposure
Airworthiness	There are no operational or safety-of-flight implications and there is suitable redundancy. The deviation can be rectified using standard procedures.	Reliability is impacted with sufficient redundancy in place and no operational or safety-of-flight implications. The deviation requires either non-standard physical rectification or extensive troubleshooting to restore to normal operations.	Reliability is impacted but there is not sufficient redundancy in place. There are small operational, or safety of flight implications (not threat). The deviation requires either physical rectification or extensive troubleshooting to restore to normal operations.	Although there is redundancy, the deviation requires non-standard measures to be taken by flight or ground crew to re-establish safe and stable operations, or to ensure the safety of crew, passengers, or the public.	There is no redundancy and the deviation presents a clear and immediate threat to aircraft safety. Emergency measures by the flight or ground crew are required to preserve aircraft integrity and the lives of crew, passengers or the public.	Potential to directly cause an aircraft accident leading to a hulls loss or affects multiple aircraft to the extent that continued safety networking operations are put into immediate jeopardy.
Environment	Minor breach in internal procedures, insignificant impact to environment	Minimal impact to environment, contained within operational area.	Medium impact to environment, possible migration outside operational area, containment required. Significant impact to environment on-site.	Significant impact to environment on-site.	Long-term impact to environment on-site.	Long-term environmental implications and potential impacts to third parties.
Organizational / Client Impact	Small delay, internal inconvenience.	May threaten an element of the service delivery function. Business objective delayed. Easily remedied, some impact on external stakeholders.	Considerable remedial action required with disruption to a group for a period of up to 1 month. Some business objectives not achieved.	Significant loss of critical information. Disruption to one or more groups for up to 3 months. Some major objectives not achieved.	Permanent loss of critical information, substantial disruption to organization or external intervention for over 3 months. Threatens existence of a group within NCAA. Major objectives not achieved.	Threatens ongoing existence of organization.
Operations	Aircraft grounded for less than 3 hours.	Aircraft grounded 3 - 48 hours.	Aircraft grounded more than 2 days.	Sub-fleet grounded up to 2 days.	Sub-fleet grounded greater than 2 days.	Complete fleet and sub-fleet grounded an extended period (greater than 3 days).
Legal	An offense which could breach a single regulation.	AN offense which breaches more than one regulation.	An offense for which company prosecution is contemplated and legal response is required.	An offense for which company prosecution is imminent and legal response is compulsory.	An offense which results in company prosecution, and/or regulatory intervention, issuance of a Notice, a substantial fine or show cause action.	An offense which results in company prosecution and may result in Directors / Executives / Senior managers jailed or loss of regulatory approval to operate.

2

DATA ANALYSIS

Documenting Risks and Top Safety Issues

Once top priority risks are validated and quantified, it is important for an organization to actively track and monitor the status of these risks. The most common mechanism to do this is through a risk register. A risk register serves as a central repository that allows stakeholders within an organization to document active risks, track mitigation statuses, and monitor potential threats (watch items) that could escalate into risks. It also aids in determining when future investigations and analyses, such as cause-and-effect diagrams, may be appropriate. It should be noted that multiple lines of business within an organization, company, or domain may maintain their own risk register (e.g. maintenance, flight operations, etc.).

With the exclusion of potential threats, there should be a direct relationship between the most current version of an organization's risk matrix and the risk register. For historical and auditing purposes, it is highly recommended to maintain previous versions of your organization's risk register. For more information explaining how to develop a risk register, see Tables TBD and TBD below.

Table TBD provides a sample risk register template. Core elements to this template include risk traceability information (risk ID, risk title), descriptive risk information (IF/THEN statement), risk assessment data (severity, likelihood, risk rating, residual risk rating), and risk response plan information (mitigation strategies, current status, point of contact).

Table 9 Risk Register Template

Risk ID	Risk Title	Risk Statement	Severity	Likelihood	Risk Rating	Mitigation Strategy	Residual Risk Rating	Current Status	Point of Contact
[Develop a unique risk ID for tracking and eventual archiving purposes]	[Formulate a risk title that clearly describes the risk]	[Insert a risk IF / THEN (cause & effect) statement]	[Insert value from impact assessment results]	[Insert value from probability assessment results]	[Insert combined Severity/ Likelihood value]	[Insert each mitigation step and assign due dates]	[Insert expected level of risk after mitigations are in place]	[Document progress towards completing mitigation steps]	[Assign person(s) the responsibility for overseeing and mitigating the risk]

Table TBD is an applied risk register example that focuses on a sample airline operator training risk and their response plan.

Table 10 Example Risk Register

Risk ID	Risk Title	Risk Statement	Severity	Likelihood	Risk Rating	Mitigation Strategy	Residual Risk Rating	Current Status	Point of Contact
Training_01	Flight Crew Surface Training at Airport ABC	**IF** flight crew training is not updated to address known Airport ABC surface complexity issues **THEN** the likelihood of a runway incursion will increase	B	4	4B (High)	**Step 1:** 60 days prior to initiating service at airport ABC, update flight crew training materials **Step 2:** 45 days prior to initiating service at airport ABC, begin training flight crews **Step 3:** 10 days prior to initiating service at airport ABC, all required flight crew	1B (Low)	Step 1 completed 70 days prior to initiating service at Airport ABC. Step 2 will be started on 1-Jan 2017, 10 days ahead of schedule.	John Smith, Chief Pilot

						training must be completed			

Safety Performance Indicators

A Safety Performance Indicator (SPI) is a measure (or metric) used to express the level of safety performance achieved in a system. SPIs are linked to the safety performance targets. They enable an organization to assess current performance against the current targets. Establishing SPIs will enable your organization to ensure that the necessary mitigations or controls are being implemented to address your top priority risks. SPIs will essentially serve as a mechanism to assess the effectiveness of existing risk mitigations and controls. Not meeting an SPI target will assist your organization in identifying areas that require attention, further review, or even corrective action.

To develop meaningful SPIs an organization must agree upon its top priority issues that are relevant to daily operations. Once those issues are identified, your organization must decide on how an individual SPI will be measured (e.g. what should the metric be: lagging indicator - number of overruns/1000 takeoffs, leading indicator - % of your aircraft that have had routine maintenance inspections completed on or before their required due date, etc.). Next, your organization needs to develop measures of success to drive operational performance objectives and future data collection priorities. Below are some example SPIs that were identified during the GSIP workshops and modified for the purposes of this toolkit:

Controller Flight into Terrain (CFIT)

Table 11 CFIT SPI Example

Domain	Example Operational Performance Metric	Example SPI
ANSP	Number of Minimum Safety Altitude Warning (MSAW) Alerts per Month	Reduce the number of MSAW alerts to # per month. Regularly review ANSP safety assurance data (e.g. ATC radar feeds, etc.) to monitor progress.
Airline Operator	Number of Near-CFIT Events per Year	Reduce the number of near-CFIT events to # per year. Regularly review employee voluntary safety reports to monitor trends and progress.

Loss of Control In-Flight (LOC)

Table 12 LOC SPI Example

Domain	Example Operational Performance Metric	Example SPI
Airline Operator	Number of Stall Events per Month (stick shaker activation)	Reduce the number of stall events to # per month. Regularly review employee voluntary safety reports to monitor trends and progress.

Mid-Air Collision

Table 13 NMAC SPI Example

Domain	Example Operational Performance Metric	Example SPI
ANSP	Number of AIRPROX Events per 1,000 Flight Operations	Reduce the number of AIRPROX events to # per 1,000 flight operations. Regularly review ANSP safety assurance data (e.g. ATC radar feeds, etc.) to monitor progress.

Runway Safety

Table 14 Runway Safety SPI Example

Domain	Example Operational Performance Metric	Example SPI
Airline Operator	Number of Unstablized Approaches per 1,000 flight hours.	Reduce the number of unstablized approaches to # per 1,000 flight hours. Regularly review employee voluntary safety reports to monitor trends and progress.
Airport	Number of Runway Incursions per 1,000 flight operations.	Reduce the number of serious runway incursions to # per 1,000 flight operations. Regularly review employee voluntary safety reports to monitor trends and progress.

To ensure that your organization is meeting its safety performance targets, your organization must establish lines of accountability in each safety performance indicator by appropriately assigning departments or individuals to an SPI or set of SPIs. For example, a maintenance department would be assigned to an SPI that is related to system reliability. A flight safety department may be assigned an SPI related to runway safety. Assigning the correct organization/department to an SPI is critical to achieving your operational performance objectives. Once assigned to an SPI, a department or individual is held responsible for the relevant data collection and coordination with the safety department to calculate their SPIs. Initially an effective baseline is established in order to chart safety improvement, then once targets SPIs are set, the respective departments or individuals then work with teams to achieve their target SPIs.

Monitoring Beyond SPIs and Top Safety Issues

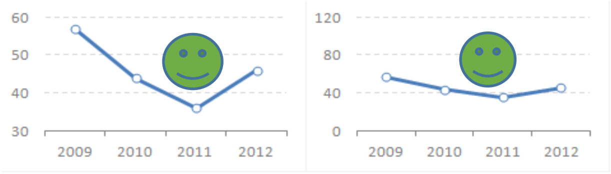
Often an organization chooses SPIs that may have deeper issues impacting top issues. Noted compliance issues and subjects that deserve increases awareness across the organization as potential root causes may be monitored separately from safety performance indicators. Maintaining this separation is critical to an employee or manager attempting to collect data unconstrained by SPIs, especially since the potential availability of system data in the digital age can be overwhelming. In an airline for example, a top safety performance indicator might be the rate of unstable approaches. Yet, the airline might also want to understand how many unstable approaches are impacted by high descent speeds. In fact, high descent speeds may be an underlying factor/root cause of unstable approaches that is worth monitoring in addition to the existing indicators which account for much of the current unstable approach performance. This additional data can continue to be collected and used where it is needed for analysis, but it does not need to be communicated with the entire organization on a regular basis if addressing unstable approaches are the objective. As the analysis capabilities of an organization improve, there may be more and more reasons to tap into sources of additional safety related monitored data.

Best Practices for Representing and Summarizing Data

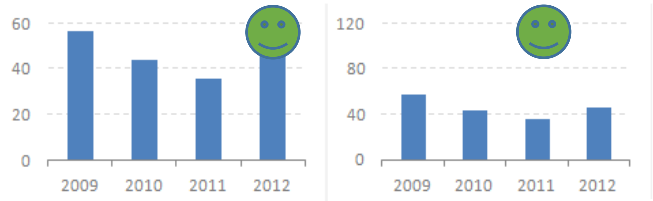
Graphics and robust data visualizations are valuable tools for messaging safety analysis results. However, it is important that these tools are correctly used so that they do not mislead decision-makers or stakeholders. To avoid common data misrepresentation errors, the following subsections will provide best practices so that an organization can maximize the effectiveness of charts, graphics, and data visualizations when summarizing key safety data analysis results.

Selecting Chart Types

Comparison:	**Distribution:**	**Trends:**	**Composition:**
Compare values such as low and high	Detect outliers, gauge range & normal tendency	Detect patterns of gradual change over time	How individual parts make up the whole
Line graphs, bar charts, scatterplots (x/y)	*Line graphs, bar charts, scatterplots (x/y)*	*Line graphs, bar charts*	*Pie charts, stacked bar charts, tree maps*

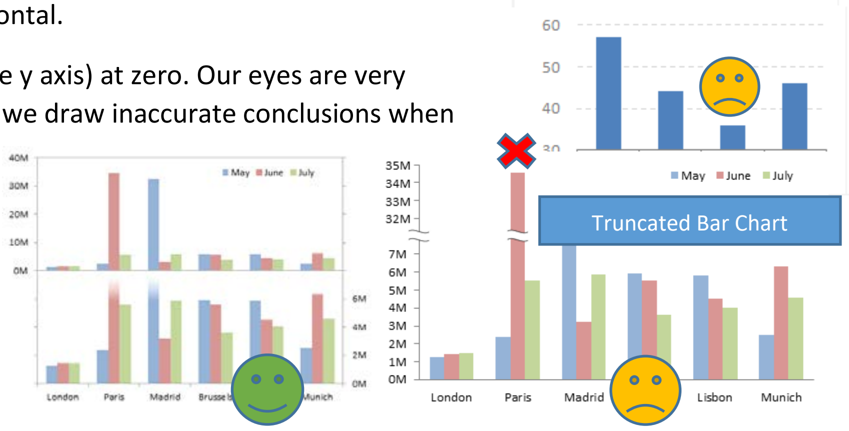


Line graph – Line graphs are used to track changes over short and long periods of time. When changes are smaller, line graphs are better to use than bar graphs. Line graphs can also be used to compare changes over the same period of time for more than one group. Use solid lines only. Avoid plotting more than 4 lines to limit visual distractions. Use the correct height so the lines take up roughly 2/3rds of the y-axis' height. For this it may be okay to start the y-axis at a value other than zero. Label the dependent axis (usually the y-axis).



Bar Graph – Bar graphs are used to compare things between different groups or to track changes over time. However, when trying to measure change over time, bar graphs are best when the changes are larger. Bars can run vertical like columns or horizontal.

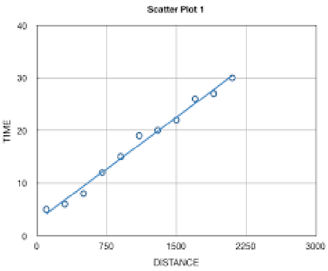
Start the numerical axis (often the y axis) at zero. Our eyes are very sensitive to the area of bars, and we draw inaccurate conclusions when those bars are cut-short/truncated. See the difference between the truncated chart and an un-truncated chart. The one on the left makes it look like the difference between the bar



Panel Chart

Truncated Chart

height much greater when in reality starting the axis at zero shows a more accurate difference. If you have one or two very tall bars, you might consider using multiple charts to show both the full scale and a "zoomed in" view - also called a Panel Chart. Breaking axis scale misrepresents the data also. Label the dependent axis. Rotate bar charts to be horizontal if the category names are long.



Scatterplot or X-Y plot – Scatterplots are used to determine relationships between the two different things.

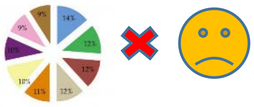
The x-axis is used to measure one event (or variable) and the y-axis is used to measure the other. If both variables increase at the same time, they have a positive relationship. If one variable decreases while the other increases, they have a negative relationship. Sometimes the variables don't follow any pattern and have no relationship. A scatterplot can also reveal the distribution trends. It should be used when there are many different data points, and you want to highlight similarities in the data set. It is also useful for identifying outliers.

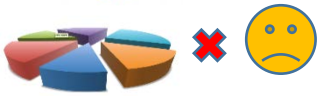
When building a scatterplot, include another variable using as mark size, shape, or color to incorporate more data. Start the y-axis at 0 to represent data accurately. If you add trend lines, only use a maximum of two to make your plot easy to understand. Label the dependent axis.

Pie Graph – Pie charts or Pie graphs are best to use when you are trying to compare parts of a whole.

They are often overused and can be made difficult to interpret. They do not show changes over time. Only use them for a percentage breakdown where each slice represents a certain percentage out of 100%. Alternative charts to show parts of the whole are stacked bar charts, tree maps, and area charts.

Avoid illustrating too many categories to ensure differentiation between the pie slices. Avoid using a pie chart if it has more than 5 slices, and never make it 3D. Three-Dimensional effects reduce comprehension and make it difficult to compare and judge area. Ensure the slice values add up to 100% and order the slices according to their size for readability.





Analysis and Making Conclusions

Be careful with averages – mean/median/mode. Often only showing the mean average will hide or misrepresent overall distribution. Avoid basing conclusions on small sample sizes or when using a very narrow or controlled data set. A good way of testing your sample is to check the statistical significance of findings. In any experiment or observation that involves drawing a sample from a population, there is always the possibility that an observed effect would have occurred due to sampling error alone. But if the finding is statistically significant, an analyst may conclude that that effect reflects the characteristics of the whole population. Beware of unchecked extrapolation (assuming that a trend based on a small set of data will continue in the future). Avoid generalizing findings when comparing elements that are by nature, scale, and context very different (i.e., comparing apples and oranges). For example, avoid comparing small samples with large samples then expect them to behave the same. Avoid basing conclusions on data that are irrelevant. Avoid Confirmation bias which is the tendency to interpret information in a way that confirms one's preexisting beliefs or hypotheses, while giving disproportionately less consideration to alternative possibilities.

Understand that a **correlation** alone is not enough to prove **causation**. Causation is often confused with correlation, which indicates the extent to which two variables tend to increase or decrease in parallel. However, correlation by itself does not imply causation. There may be a third factor, for example, that is responsible for the fluctuations in both variables. One example is as ice creams sales increase, so do drownings. Ice cream sales do not cause drownings, but a third factor warm summer weather increases both ice cream sales because people want to enjoy eating a cold treat and to cool off by swimming.

- Correlation could hint at actual causation: A causes B
- Correlation could be reverse causation: Windmills doesn't cause wind although both are correlated.
- Correlation could be common-cause causation: Ice cream sales and drownings are correlated but a common-cause (warm summer months) increases both.
- Correlation could be indirect causation: A causes C and C causes B.
- Correlation may be coincidence. If you look for patterns in random samples you can find something.

Finally **validate your findings**. Do not assume your findings are correct. Use additional tests, or other measures to help confirm your findings to ensure they are correct.

Create a Plan for Success

The following items can be used as a starting point or checklist when creating a plan for successful data analysis.

☐ Develop a process to cleanse, check, and prepare safety data for analysis. It is important to prevent data irregularities or redundant information from affecting key safety analysis inputs and outputs.

☐ Educate employees on the benefits and limitations of individual data sources. This can serve as a safeguard to common data analysis issues (e.g. causation vs. correlation).

☐ Establish an internal process to guide employees in the development of a cause-and-effect diagram (Fishbone). This includes facilitator and participant roles, responsibilities, expectations, and key outputs.

☐ Develop customized SMS severity, likelihood, and risk classifications scales. These scales should be compliant with ICAO guidance while addressing the specific needs of your organization.

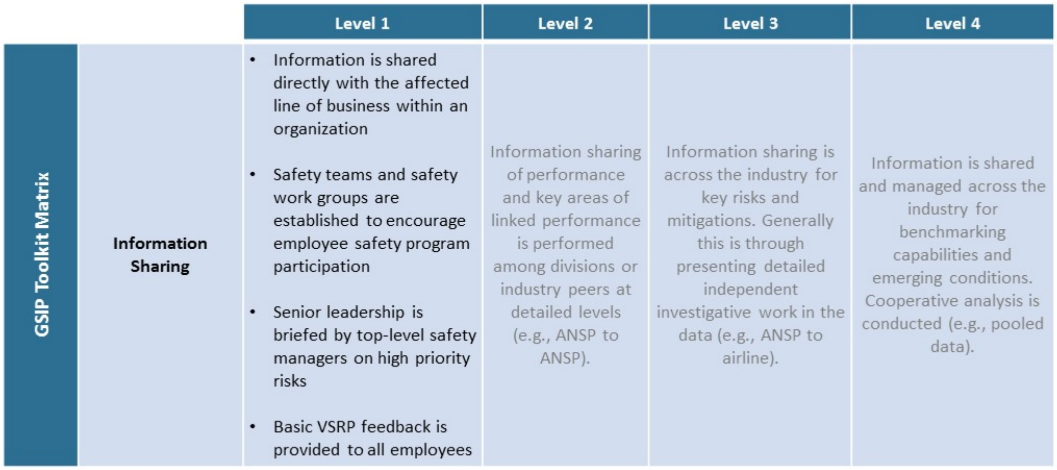
☐ Develop a standardized risk register template that can be used by the various lines of business within your organization. Accompanying this template should be an applied, operation-specific example.

☐ Implement and regularly status Safety Performance Indicators (SPIs) that are meaningful and an accurate representation of your operational safety priorities.

INFORMATION SHARING

Information Sharing

Level 1 Intensity focuses on the exchange of high priority safety information with organizations that are directly impacted by data collection and analysis findings. This toolkit describes information sharing best practices that promote increased safety program engagement, and techniques to improve the health and integrity of your organization's Safety Data Collection and Processing System (SDCPS) risk management capabilities.



		Level 1	Level 2	Level 3	Level 4
GSIP Toolkit Matrix	Information Sharing	• Information is shared directly with the affected line of business within an organization • Safety teams and safety work groups are established to encourage employee safety program participation • Senior leadership is briefed by top-level safety managers on high priority risks • Basic VSRP feedback is provided to all employees	Information sharing of performance and key areas of linked performance is performed among divisions or industry peers at detailed levels (e.g., ANSP to ANSP).	Information sharing is across the industry for key risks and mitigations. Generally this is through presenting detailed independent investigative work in the data (e.g., ANSP to airline).	Information is shared and managed across the industry for benchmarking capabilities and emerging conditions. Cooperative analysis is conducted (e.g., pooled data).

Figure 11 Information Sharing Level 1 Intensity Matrix

The examples provided in this toolkit will focus on commercial aviation, however the underlying approaches can be tailored to address your specific operational needs.

General Information Sharing Best Practices & Recommendations

The health and integrity of a safety program is dependent on the consistent engagement of all employees. This includes frontline employees (controllers, pilots, etc.), operations support employees (aircraft mechanics, airport operations employees, etc.), supervisors and managers, executives, and other relevant stakeholders across your organization or domain.

At level 1 intensity, this toolkit focuses on the exchange of safety information within a single organization (e.g. flight operations, maintenance) with the intent to increase safety program participation, safety data quality, and operational performance. This toolkit provides various information sharing methods and techniques so that employees understand the health of their organization's data collection mechanisms (e.g. Voluntary Safety Reporting Program [VSRP] participation levels), the results of their organization's data analysis efforts (e.g. the relationship between voluntary employee safety reports and an organization's top priority risks), and their organization's plan(s) to integrate and use its safety program data (e.g., storage of data, use of analysis results, relationship between safety program data and daily operations).

INFORMATION SHARING

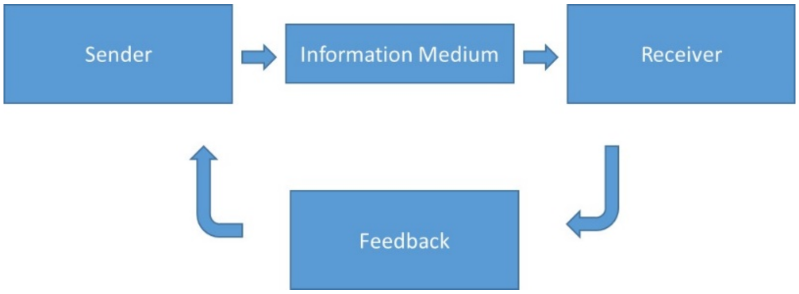


Figure 12 Communication Model

In order to build employee trust in your organization's safety program, the use of effective communication is critical. If a safety program poorly messages or inadequately shares high priority safety information, it can quickly result in the erosion of employee confidence in the program.

- **Examples of good communication** are the presentation of focused information, the use of employee inputs to reflect upon safety program information, the engagement of the correct audience, the use of clear mediums to message high priority information, and the praise of employee participation when demonstrating the applied value of a safety program.
- **Examples of poor communication** are the presentation of irrelevant information (e.g. emphasizing outlying data points from analyses rather than the major takeaways), the lack of clarity in safety data (e.g. use of overly complex materials to message simple points), the engagement of the wrong audience (e.g. an airport authority would not take interest in an ANSP's AIRPROX rates), and the use of safety program information for the purpose of being critical or negative when describing performance (i.e. you catch more flies with honey than with vinegar).

The following sections detail specific techniques and best practices to effectively share high priority safety information within an organization.

Establishment of Safety Teams and Workgroups

Safety teams are a valuable component of an organization's overall safety program. They encourage employee engagement and the bottom-up awareness of top priority issues. Safety teams are an effective mechanism to exchange safety information within an organization. These teams typically include representatives from each of an organization's major lines of business (e.g. flight operations, maintenance, ground operations, etc.) and are expected to meet on a regularly scheduled basis. During their meetings, representatives often discuss an organization's general safety performance and most current safety needs. These needs can be derived from all available SDCPS sources (Public Safety Information, Reportable Occurrence Data, and Safety Program Information).

At level 1 intensity, safety teams are expected to focus on the development and monitoring of an organization's key objectives and top priority risks. Safety teams are also expected to serve as a forum for brainstorming (e.g. where new audits or investigations might be needed to determine practices instead of relying on standard policies and procedures). Safety teams also serve as a forum for identifying emerging safety issues and reviewing the status or progress made on existing mitigation plans.

Airline Safety Team Example – Large airlines may have safety teams for each operational unit. Each of these units may have a different set of safety metrics, safety performance indicators, and priorities. The common objective across these teams is that they make measurable safety improvements to achieve their operational safety performance targets. When the representatives from these teams meet (individually and as a group), they are likely to engage in the following activities: discuss new hazards that require mitigation, review the progress made on existing mitigations (e.g. their effectiveness in reducing risk), and examine safety data that could provide insight into levels of organizational compliance and safety culture.

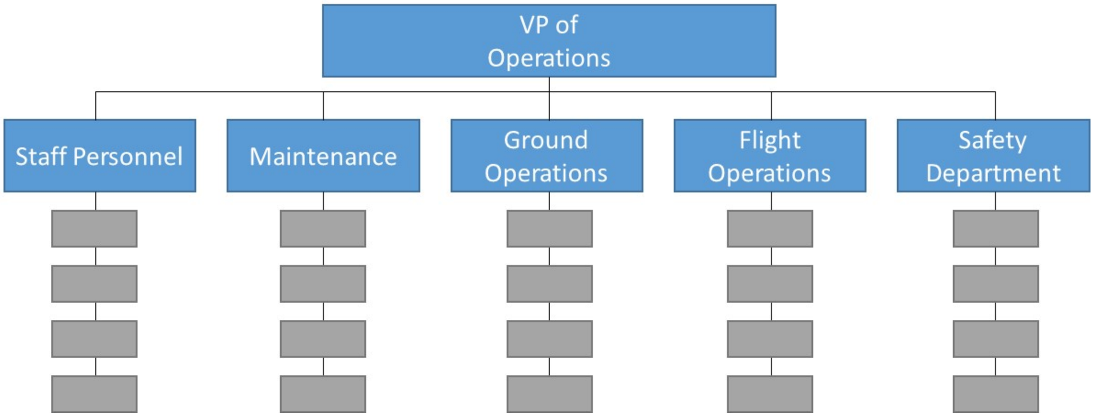


Figure 13 Sample Airline Organizational Chart / Lines of Business

As an organization grows in size and complexity, there may also be a need to establish safety workgroups. These workgroups can assist in addressing safety needs at the local facility- or operations-level. For example, ANSPs may establish safety workgroups at individual facilities. Airlines however may establish safety workgroups for each line of business (e.g. flight operations, maintenance, ground, dispatch, etc.). As these workgroups are formed, they often serve as the focal point for monitoring the achievement of specific performance metrics or SPIs. Typically, each safety workgroup will have a designated representative that is responsible for communicating the status of these metrics or SPIs to management and potentially senior leadership.

While level 1 information sharing focuses on the exchange of safety information within a single organization (either through safety teams, safety workgroups, etc.), higher levels of SDCPS intensity will focus on the exchange of information with additional safety program stakeholders.

Coordination with Senior Leadership

It is important that senior leadership establish and share a strategic safety vision which promotes increased safety program participation by all employees. This vision may be shared through regularly scheduled meetings, engagement with an organization's safety team, or other direct modes of communication. While working towards this vision, it is important that senior leadership recognize safety program accomplishments, provide feedback based on significant safety program findings, and consistently uphold safety program accountability.

To build bottom-up safety program credibility and employee trust, top-level safety managers should regularly engage with senior leadership. During these engagements, top-level safety managers should inform senior leadership of their safety program's on-going status. This status report includes what safety program metrics they are using, the status of their safety performance objectives, and the names of the designated person(s) who are accountable and/or responsible for their achievement. Depending on the size and needs of an organization, the interval (e.g., monthly, quarterly) and format (e.g., formal presentations with slides, email exchange with a written report attached) of these engagements may vary. For example, large organizations may require safety programs to engage with senior leadership on a quarterly basis. This could permit larger organizations to implement various course corrections and/or measurable changes over time. On the other hand, smaller organizations may engage with senior leadership more frequently. These engagements might be completed alongside other performance reviews due to their frequency.

Voluntary Safety Reporting Programs

The success of a Voluntary Safety Reporting Program (VSRP) relies heavily on employee buy-in and consistent employee participation. To increase the use and bottom-up support of a VSRP, it is essential to provide employees with feedback which promotes engagement throughout all SDCPS activities including data collection, data analysis, and the applied use of safety program data in day-to-day operations.

Best Practices for VSRP Information Sharing – Level 1 Intensity

Provide Feedback to Individual Employees. Successful communication is a two-way street. In other words, employees who submit safety reports should receive direct feedback regarding their report. Feedback should be delivered with respect, without bias, and with clear communication. While individual programs may have different feedback approaches (e.g. confirmation that a report was received, a notice that risk assessment is in-process, or a notification when a report is closed), the common goal is to assure a strong safety culture through open communication and employee engagement. When providing feedback, it is recommended to do the following:

- Acknowledge the successful receipt of a safety report (e.g. verbally, through a website or portal, etc.).
- Provide employees with an updated status of their safety report (e.g. review in-progress, additional information needed, report closed, etc.). This will increase employee confidence in the system.
- Educate submitters on the quality and completeness of their safety report to refine future report quality.
- Describe the positive contributions that a submitter's safety report made to a VSRP (e.g. identified an emerging safety issue). While not all reports lead to changes in processes or procedures, they can still be rich in information.
- As a part of the report closing process, provide a submitter with the corrective actions that will be further explored to address the safety need described in their report, explaining any caveats such as necessary approvals and processes that could affect the ultimate decision to implement various corrective actions. Depending upon the size of an organization, this may be through an automated process or through one-on-one verbal communication.

Provide Constructive Feedback about Safety Report Quality to Employees. Programs are encouraged provide constructive feedback to employees regarding the depth, consistency, and usability of their safety report(s). To encourage future reporting and the quality of those reports, one-on-one feedback is extremely valuable. The following is an example of how report quality can impact potential analyses and corrective actions.

☹ **Pilot Submits a Vague Safety Report:** A pilot submits a safety report that states “Better taxiway signage is needed at the Amsterdam airport”. While this report is valuable, it is not actionable due to the lack of clarity and detail.

☺ **Pilot Submits a Detailed Safety Report:** A pilot submits a safety report that states “Mandatory signage near runway 36 at the Amsterdam airport was obstructed by tall grass”. This report is extremely valuable as it is clear and specific. This report can easily be assigned to the correct depart for corrective action.

Provide Feedback to All Employees within an Affected Organization. To increase employee participation and VSRP buy-in, it is important to provide aggregate feedback to all employees within an affected organization. This feedback could be delivered through a variety of mediums (team meetings, safety memos, online web portals, newsletters, etc.) and should occur over regularly scheduled time intervals (e.g. monthly, quarterly, and annually). When providing group feedback, the following activities are recommended:

- Provide periodic VSRP summaries (e.g. monthly, quarterly, annually) that detail things like key issues, levels of participation, significant outcomes, corrective actions, or long term trends.
- Convey the status of the VSRP’s health and integrity (detail the number of reports received, number of open/in-progress reports, closed reports, etc.).
- Contextualize VSRP findings so that employees understand the applied value of VSRP participation.
- Describe how an organization’s VSRP has impacted or changed daily operations (e.g. training, rest requirements, etc.).
- Report the progress on achieving organizational safety performance indicators (SPIs) or metrics.

Flight Safety Foundation believes that an organization’s safety performance indicators and their current SPI status should be directly communicated with all employees. When providing an SPI status, an organization should include the risk area (for context), the SPI target, the organization’s current performance, and actions any that are underway to improve performance and or close any potential performance gaps. In some organizations, this can be communicated with a simple chart or even verbally during regularly scheduled safety meetings.

Table 15 SPI Status Example

Risk Area	Example Safety Performance Indicator	Example Performance	Status/Comments
CFIT	1.0 Minimum Safety Altitude Warning (MSAW) Alerts per Month	1.1 per month	SPI metric not achieved. Reviewing data from recent events to understand the cause.
LOC In-Flight	1.0 Number of Near-Stall Events per Month (stick shaker activation)	1.9 per month	Exceeding the SPI metric. Reviewing employee inputs on how to sustain this performance.

Runway Safety	1.0 Runway Incursions per 10,000 flight operations.	3.5 per 10,000	SPI metric not achieved. Reviewing causal factors and implementing corrective actions.
NMAC	1.0 AIRPROX Events per 100,000 flight operations.	2.1 per 100,000	SPI metric not achieved. Reviewing data from recent events to understand the cause and develop corrective actions.

Create a Plan for Success

The following items can be used as a starting point or checklist when creating a plan for successful information sharing.

- □ Educate employees through memos or other training materials on effective communication best practices. Effective communication is critical to building employee trust in your safety program.
- □ Establish safety teams from each line of business to encourage employee participation in safety program objectives.
- □ Develop safety workgroups to address local safety needs or risks. These workgroups are an effective mechanism to develop bottom-up safety solutions.
- □ Develop a high-level schedule that promotes the regular engagement of top-level safety managers and senior leadership. This schedule can add a layer of top-down safety program accountability.
- □ Establish a plan to provide individual and groups of employees with constructive feedback on voluntary safety reports. This will assist in demonstrating the value of their inputs to your VSRP.
- □ Consider including your regulator in safety program meetings or updates to give them insight into routine safety issues.

INFORMATION PROTECTION

Information Protection

Level 1 Intensity focuses on the key policies, laws and internal company policies necessary for effective protection and sustained use of this information while ensuring the trust of the participants in the voluntary programs.

	Level 1	Level 2	Level 3	Level 4
Information Protection	Individuals and organizations are protected against disciplinary, civil, administrative and criminal proceedings, except in case of gross negligence, willful misconduct or criminal intent.	The protection extends to certain mandatory safety reporting systems. In Annex 13, the protection extends to final reports and investigation personnel.	Further protection mechanisms may be in place to implement just culture principles and cross-industry support for strong safety reporting cultures.	Protection is formalized at the highest level between countries through memorandums of understanding or similar agreements.

Figure 14 Information Protection Level 1 Intensity Matrix

Standards and Recommended Practices on the Legal Protection of Safety Information –

Main Concepts: ICAO Annex 19 on *Safety Management* ("Annex 19") includes principles of safety information protection, principles of exception to such protection, guidance for public disclosure, responsibilities of persons that have safety information, and the protection of recorded information. ICAO Annex 13 on *Aircraft Accident and Incident Investigation* requires the de-identification of investigation records and limits use for purposes other than safety.

Laws, Regulations, and Policies to Protect Voluntarily Reported Safety Information –

Main Concepts: Mechanisms—including laws, regulations and policies—to protect voluntarily reported safety data and safety information in the aviation industry at both the organizational and state levels, with the use of a balancing test that takes into account safety and the need for the proper administration of justice. The protection would not extend to acts that violate state criminal laws or demonstrate a serious disregard for safety.

Example: Safety reports are a good source of hazard information to use in a safety program within any aviation-related entity. At the company level, if employers want to encourage the voluntary disclosure of safety data by employees who are in the best position to identify safety threats, policies and procedures should be developed and implemented, including in the Safety Management Systems ("SMS"). Together, these programs may result in the suspension of operations if the compliance issue is related to:

- Airworthiness Directives;
- Performance/Life Limitations; and
- Any threat indicating an unsafe condition on current operations.

INFORMATION PROTECTION

SMS should incorporate voluntary safety reporting programs within the company as well as to the regulator. These complementary levels of reporting ensure potential safety risks are shared and addressed within the industry and the appropriate civil aviation authorities along with applicable safety assurance monitoring of implemented corrective actions.

Example: Regulators in various states have implemented laws, regulations, and policies to allow notification of regulators when a discovery is made on non-compliance the protection of person reporting the information. These programs allow aviation stakeholders to conduct their own investigation and determine potential findings and root causes of safety threats, and propose corrective actions to maintain and improve safety.

Protection of information through safety programs at the state is successful in situations that include:

- A regulator or judicial officer protecting the use or disclosure of safety data or information collected through a safety program in enforcement proceedings against an individual or an organization;
- A regulator or judicial officer takes part in the safety mitigation discussion to address safety issues.

Protecting the Safety Data and Safety Information Within the Organization –

Main concepts: De-identification mechanisms (names, dates, etc.) are key to protect safety data and safety information.

Examples: When voluntary safety reports are collected, the data or information may need to be distributed for analysis and safety threats identification. De-identification will protect the reporter or the person related to the report, while allowing aviation stakeholders to assess and address potential safety issues. For example, de-identification could be deleting personal information from printed or copied report via a marker or printing only the relevant excerpts from a report through a template that is designed to omit certain fields.

The larger the organization, the more formal these protective methods may need to be. In large organizations, information can be passed easily from one group to another and a recipient may not be aware of existing protection mechanisms within the organization. If the identifying information is not contained in a released copy, the lower the likelihood the information could be used against the individual.

In small organizations, the protection of safety reports may be more challenging. For example, efforts to restrict the release of identified risks and related information may be unreasonable with the close relationships between management and employees. Such circumstances require particular and special attention to the protection of safety data and information, as well as those persons sharing the information. Thus, those in charge of the organization's SMS, and specifically the report of safety information, must develop policies and training to raise awareness among employees of the need to protect persons that report safety data and safety information.

As mechanisms and systems become more sophisticated, technical solutions to de-identify safety reports and ensuring protection through software and password controlled methods may be developed.

Developing and Implementing Policies Within the Organization –

INFORMATION PROTECTION

Purpose: The purpose of developing policies within the organization is to achieve the highest level of commitment to safety and protection of individuals and organizations who report safety data and information.

Main concepts: Safety mechanisms to protect data and information within the organization may include:

- Developing safety policies to implement within the organization with the support of labor groups and management department;
- Encouraging the de-identification of voluntary safety reports;
- Training accountable representatives to hold safety meetings on specific events; and
- Implementing de-brief meeting with crew members submitting safety reports.

Other examples to encourage the reporting of safety data and information, while protecting the reporter include:

- Safety posters and other regular means of communication to employees on opportunities for safety reporting; and
- The publication of reported issues that led to corrective actions.

One method to implement a safety program is a written policy to establish a voluntary reporting system for all employees. Appendix 2 to Annex 19 mandates organizations to "define its safety policies in accordance with international and national requirements." This includes indicating "which types of behaviours are unacceptable related to the service provider's aviation activities and include the circumstances under which disciplinary action would not apply." This means that persons that report safety data or information will be protected from disciplinary actions when carrying out their job in an acceptable manner.

Managers should be the first to implement the policy. Top level managers must remind their employees of the provisions of the policy and how it apply to current events within the organizations. The manager's leading role in implementing the safety policies are key to build a trust environment between managers and employees. This results in a trusting environment also called Just Culture.

Most of Annex 19 provisions are based on Just Culture principles. Some aviation organizations define Just Culture as "a culture in which front-line operators and others are not punished for actions, omissions or decisions taken by them which are commensurate with their experience and training, but where gross negligence, willful violations and destructive acts are not tolerated." If the organization's culture reflect the belief that all employees perform their duties to the highest standards of professionalism, this create an environment of trust, and encourage the reporting of safety information to maintain or improve aviation safety. If the evidence points to a serious disregard for safety and actions that fall outside of acceptable behaviors, then employees should be held accountable.

The boundaries of acceptable and unacceptable behavior should be defined by the regulators and the companies. The regulator—through laws, regulations, and policies—may adopt a specific language to define the boundaries of a behavior. Concurrently, aviation companies should draw from these definitions to further explain and clarify the regulator's language, and adapt those definitions to their own culture and industry practices.

The decision to pursue disciplinary action remains with the supervisors, the regulator, or the judicial officer implementing the language and principles of the state or organization's rules or policies. Disciplinary actions generally includes time-off without compensation, loss of employment, restriction of duty or assignments, certificate action, or a record in an employee's personnel file that may impact future career opportunities.

The Role of Labor Organizations –

Main concepts: Labor organizations can play an important part in helping protect safety data and information through their participation in safety teams.

Examples: In many organizations throughout the world, labor associations are involved with supporting SMS. When a company creates a safety policy, the company may address the interests of the labor association that were discussed during the labor contract negotiations. Both labor and management should support SMS, including the protection of safety data and information reported within the organization, as well as the implementation of policies to maintain the flow of safety reports and ensure the highest level of safety.

At times it may be necessary to de-brief directly with a reporter to ensure all the information contained in a report is well understood. These briefings should be handled with great care, discretion, and confidentiality to ensure a report is not used against an employee or the organization. The greater the protections in place, the greater the trust between the employers and employees.

Creating a Plan for Success –

☐ At the state level, laws and regulations that facilitate voluntary reporting within companies and to the regulator, including protection of individuals and companies.

☐ A state-established balancing test to determine whether the data and information should be protected for safety reasons or may be used for the proper administration of justice.

☐ State policies that encourage the reporting of safety data and information from the company to the appropriate civil aviation authority.

☐ Defining and explaining of acceptable and unacceptable behaviors by states and organizations.

☐ Internal company policies to develop a Just Culture environment that highlight the commitment and need for voluntary safety reports from employees to identify safety hazards in daily operations, as well as protecting individuals.

☐ Developing an efficient de-identification process of voluntary safety reports at the state and organization levels.

☐ Ensuring continued understanding of the importance to collect data and information to identify safety threats, but not to apportion blame or liability.

☐ Involving labor organizations in the company's safety programs where labor agreements exist.