FLIGHT SAFETY FOUNDATION

GLOBAL SAFETY INFORMATION PROJECT

Level 2 Intensity Toolkit

DECEMBER 2017

Table of Contents

List of Figures

List of Tables

FLIGHT SAFETY FOUNDATION

Toolkit Introduction

What Is the Purpose of the Toolkits?

The Global Safety Information Project (GSIP) toolkits continue Flight Safety Foundation's leadership of innovative safety initiatives within the industry. They add to a legacy of pioneering U.S. and international aviation safety conferences, establishing formal education for accident investigation, and other consensus building on standards and guidance. We believe tomorrow's risk-mitigation advances will come from the way we use comprehensive safety data collected before accidents happen — not just isolated forensic or auditing data. We must know far more than which countries aren't passing International Civil Aviation Organization (ICAO) Universal Safety Oversight Audit Programme (USOAP) audits or what airline failed to meet standards of an International Air Transport Association (IATA) Operational Safety Audit (IOSA) audit, whether airlines appear on a blacklist, or when organizations experience a safety event that becomes headline news. Today's focus must be on combined, in-depth knowledge of both immediate and long-term risks, such as those in the safety reports that front-line operations staff are submitting to their safety departments, their analysis of routinely recorded data from all flights over time, and operational risk assessments by local and regional organizations around the world.

Aviation organizations like yours increasingly perform detailed safety studies of their operations. Their analyses of aircraft flight data re-corder parameters, for example, reveal insights that show where safety programs could be strengthened to avoid a hazard or mitigate an event. These studies are intensifying, and their pace is quickening. At the same time, given the human factors risks and the related necessity for procedural consistency, no organization should manage operations by making changes to procedures after every flight. So the longer-term trends are important, and changes need to be considered carefully — perhaps tested before they are even introduced to assure an acceptable level of risk.

Our GSIP toolkits consider critical components of the risk management process so you can make good decisions and share information among stakeholders that benefit the entire safety management system.

Who Are the Toolkits for?

We've designed the toolkits for any one of the multitude of aviation industry stakeholders.

Regulators, for example, want to make sure that the safety performance of their country steadily improves. They want to ensure that service providers are learning and applying safety insights. They want to trust that the industry is doing the right thing, while holding individuals and organizations accountable to standards that address critical risk issues. Data will help them set their priorities.

Airlines, too, want to manage their risk using the best data they can get their hands on. They realize improved safety performance is not assured solely by their compliance with standards or by creating more standards.

Air navigation service providers (ANSPs) want to ensure that hazards and risks affecting air traffic have been identified and managed to ensure safety.

Airports want to make sure their runways are in service and in a safe condition at all times for takeoff, landing and taxiing without confusion. Airport signage, marking and lighting to be clear and unobstructed, and communications must be clear to minimize the risk of runway or taxiway incursions. Preventing aircraft ground damage is critical for safe operations.

Aircraft and engine manufacturers want fleets to operate reliably and to be recognized throughout world markets as extremely safe. They perform safety analyses before any aircraft is built, and they continue to monitor operations globally to identify emerging safety challenges. They also proactively issue recommendations and respond to trends as operators report events or conditions, or ask for assistance with other technical issues.

Data Collection

Your objective in data collection at the GSIP Level 2 intensity is to collect and optimize increasingly complex data. This enables risk analysis by methods more sophisticated than those applied at Level 1 intensity. We therefore focus on external and internal information sources from which your aviation organization obtains the risk data most relevant to daily operations. We also recommend best practices to maximize the effectiveness of these data sources. For clarity and context, we've included practical examples of Level 2 best practices from three industry stakeholder groups: airlines and other aircraft operators, air navigation service providers (ANSPs) and manufacturers.

Table 1 shows the four intensity levels of data collection detailed in GSIP toolkits.

When your safety program fits the criteria of Level 1 intensity, data collection focuses on public safety information and basic observed/analyzed data from safety events. At Level 2 intensity, your program expands that data collection to include sources common to ICAO-defined safety data collection and processing systems (SDCPS) and safety data that helps you identify specific risks and causal factors involved in safety events. To expand Table 1's description, Level 2 data collection emphasizes:

- Collecting operational event data — also called safety assurance data (for example, data from flight data monitoring [FDM], flight data analysis programs [FDAP] and employee voluntary safety reporting programs [VSRP]) — from all available SDCPS sources;
- Putting into context your organization's increased reliance on internal safety data and public safety information and risks in daily operation; and,
- Collecting safety data to support your analyses of highly complex risks and causal factors.

We based our examples on commercial aviation scenarios, but you may prefer to tailor our underlying approaches to your needs.

Gathering Data to Develop a Broader Risk Picture

Level 2 data collection adds value by combining complex data, multiple sources and advanced risk analysis methods, and all these elements must work together. This toolkit focuses on applying the elements to develop a broad, relatively complete risk picture. We also provide other tools and techniques to more accurately put risk into context and identify causal factors most relevant to your daily operations.

At Level 2 intensity, we assume your organization collects safety assurance data to gain in-depth understanding of its current operations. We also assume that you already collect external public safety information in the form of official accident and serious incident reports published for anyone to use to benchmark or compare your organization's activities to others. For more details of this data collection concept, see the following hypothetical example for an airline.

A Case of Safety-Data Shortfall — The airline aims to understand the most common threats (risks and direct causal factors) at its hub airport during daily operations that could lead to a runway incursion — a hazard and undesired state.

Data Collection From Internal Sources — The airline typically draws from flight operational quality assurance (FOQA) programs, as well as FDM-FDAP data and VSRP data to better understand specific threats (performance deviations) that have led to runway incursions at a hub airport.

External Data Collection Sources — The airline collects public safety information to better understand threats and primary categories of issues known to have led to runway incursions involving comparable organizations (for example, they ask something like, "What were the primary categories of runway incursions at JFK Airport?"). This may help differentiate how many aircraft, ground equipment, pedestrian or other types of incursions have taken place.

Table 1 — Level 2 Intensity in the Data Collection Matrix

GSIP Toolkit Matrix	Level 1	Level 2	Level 3	Level 4
Data Collection	Data are collected to adequately identify and monitor the normal hazards an organization may encounter, and to support a functioning SMS.	Data are collected to understand hazards, the exposure of operations to those hazards, and primary causal factors (for example, through flight data acquisition systems).	Data are collected to advance a comprehensive understanding of causal and contributory factors (for example, data collected through LOSA).	TBD

LOSA = line operations quality assurance; SMS = safety management system; TBD = to be determined

Table 2 — Sample Data Sources for Identifying and Mapping Events to Known Industry Risks

Air Accident Investigation Bureau of Singapore	Civil Aviation Authority of New Zealand	Hong Kong Accident Investigation Division
India Directorate General of Civil Aviation	Japan Transport Safety Board	Maldives Civil Aviation Authority
Portugal Aircraft Accident and Investigation Bureau	South African Civil Aviation Authority	Transportation Safety Board of Canada

Data Application — Collecting internal data and external data enables your airline to conduct sophisticated risk analysis. Typically, these methods identify the primary causes of runway incursion threats at your hub airport of concern, and identify gaps in SDCPS risk management by comparing your internal findings to independent external findings.

Beyond the types of internal safety assurance data we've already noted, this toolkit cites global public safety information sources you could use to benchmark — that is, to compare — data results. These examples are a subset of public safety information sources covered in our Level 1 tookit; they are not prioritized.

Types of Safety Data

In our GSIP toolkit for safety programs at Level 1 intensity, we introduced root-cause diagrams (also known as Ishikawa or fishbone diagrams) as a method to identify the root causes of your organization's key safety risks. To build upon this, Level 2 data collection activities add emphasis on collecting types of data that help you validate the root causes and identify potential gaps in understanding them. As you detect gaps, your organization can use the additional data to redirect your data collection activities to address new or unforeseen threats that could lead to a specific hazard or undesired state. This section provides an overview of these types of data that your organization will collect at Level 2 intensity for the reasons noted and to support your development of a bow-tie model.

Automated or System-Based Data

In this toolkit, we frequently use the term *automated/system-based data–capture system* to describe any electronic record fitting one or more characteristics of an aviation operation (such as FDM). You'll routinely gather this type of data, on a fixed regular or occasional periodic basis (based on time intervals or frequency of an operation, for example), by designating personnel who use software and other techniques to download, decode and prepare the data for analysis. As they select and convert the data to usable formats, ensure that they continuously verify that the automated/system-based data–capture system performs as designed and intended. This verification process asks and answers the following types of questions:

- Are all the necessary operational parameters being recorded by the system?
- Are there missing data elements or pieces?
- Were the data collected in a timely fashion?
- Were any data elements lost or compromised during the collection and conversion process?

Monitoring and controlling the quality of your automated/system-based data are necessary to ensure that your safety program continually meets the evolving needs of your organization. The following sub-sections show applied automated/system-based data examples for each GSIP domain. Accompanying each applied example are opportunities for your organization to develop operational performance thresholds. We expect thresholds to support and/or drive your expansion of data collection activities.

Airline Operator Example of Automated/System-Based Data: FOQA-FDM-FDAP

FOQA, also known as FDM or FDAP, is a common automated/system-based data capture program. In commercial air transport and business aviation, operators rely on this safety data source to better understand their current operations and improve safety. FOQA-FDM-FDAP programs require two primary aircraft components: a flight data acquisition unit (FDAU) and a digital flight data recorder (FDR). The FDAU acquires aircraft flight data parameters from on-board sensors then converts and sends selected data in the required formats to the FDR and to a quick access recorder (QAR). The QAR records a subset of flight parameters, usually a minimum number established by the operator and/or the regulator for proactive safety analyses.

In some airline programs, a technician will retrieve or download raw data from the QAR. Access can involve removing a line-replaceable-unit (the QAR itself, or its memory card) or another storage device, or downloading the data using a secure, broadband wireless network. FOQA-FDM-FDAP

programs handle and maintain the flight data for set periods of time, so we recommend robust processes to prevent the irretrievable loss or corruption of any flight data.

FOQA-FDM-FDAP programs provide you with uniquely valuable and objective insights into routine operations and safety events detected outside operational limits. Analysis of the flow of data provides your analysts with a detailed understanding of specific thresholds or tolerances (called *exceedances*) during a safety event or a normal flight. Coupled with other information sources, this process can help your organization identify the primary causal factors of specific threats, hazards and undesired states. Here are our recommended sources of further information:

- European Authorities Coordination Group on Flight Data Monitoring: *Good Practice on the Oversight of Flight Data Monitoring Programmes*; and,
- U.S. Federal Aviation (FAA) Advisory Circular 120-82, *Flight Operational Quality Assurance.*

Examples of Performance Thresholds Used by Airlines. We encourage you to develop performance thresholds that will yield meaningful insights into daily operations during flight data analysis. These thresholds — based on your selected parameters and results of study — may be driven by your specific operational threats, hazards and undesired states, or ICAO safety performance indicator (SPI) metrics. If your organization detects performance threshold exceedances, collect and analyze additional data from internal and external sources. Table 3 shows examples of thresholds to consider in your FOQA-FDM-FDAP program.

We encourage you to develop performance thresholds that will be consistently valid and customized to address your organization's specific operational needs. Tables 4 through 8 (p. 7) show some additional issues, discussed during 2015–2016 GSIP workshops, that may help you choose FOQA-FDM-FDAP performance thresholds.

Example of Automated/System-Based Data: CEDAR (ATC Recordings) Used by ANSPs

In the United States, the FAA monitors and stores electronic air traffic control (ATC) data (radar and voice data) for up to 45 days. These data are collected in a system called the Comprehensive Electronic Data Analysis and Reporting (CEDAR) tool. Several FAA quality assurance and quality control systems

Continued on p. 8.

Table 3 — Examples of FOQA-FDM-FDAP Performance Thresholds

		Example Performance Thresholds			
Risk Area[a]	**Hazard**	**Speed**	**Pitch**	**Bank**	**Outcome**
Runway safety	Unstable approach	Deviations outside of maximum and minimum speed thresholds below 1,000 ft: Max: V_{Ref} + 20 kt Min: V_{Ref} + 0 kt	Inconsistent angle and/or rate of descent. Glide slope exceeding ¼-scale deflection from the ILS after the final approach fix.	Excessive bank angles to maintain centerline. Localizer deflection greater than ¼-scale either side.	Unstable approach to landing is continued, resulting in a high-energy landing.
CFIT	EGPWS activation	Excessive speed deviations during arrival below 10,000 ft	Inconsistent angle and/or rate of descent. Glide slope displacement greater than ¼-scale after the final approach fix.	Excessive bank angles to maintain centerline. Localizer deflection greater than ¼-scale either side of center.	Unstable approach to landing is continued and an EGPWS alert is received by the flight crew.
LOC-I	Engine failure in flight	Airspeed below V_{MC} Note: If a critical engine becomes inoperative, this speed must be sustained to maintain positive aircraft control (per FARs 23.149, MCA)	Exceedance of aircraft pitch limitations that are deemed dangerous.	Abrupt heading changes that are greater than 20 degrees either side of center.	Critical engine failure below V_{MC} results in a temporary loss of aircraft control in flight.
NMAC	TCAS RA	Rate of closure	Compliance with TCAS RA guidance.	Compliance with collision avoidance guidance.	A near-miss in flight causes the activation of a TCAS RA.

CFIT = controlled flight into terrain; EGPWS = enhanced ground-proximity warning system; FARs = U.S. Federal Aviation Regulations; FDAP = flight data analysis program; FDM = flight data monitoring; FOQA = flight operational quality assurance; ILS = instrument landing system; LOC-I = loss of control–in flight; MCA = minimum controllable airspeed; NMAC = near-midair collision; TCAS RA = traffic-alert and collision avoidance system resolution advisory; V_{MC} = minimum control speed with critical engine inoperative; V_{REF} = reference landing speed

Table 4— Additional Ideas for FOQA-FDM-FDAP Performance Thresholds for Runway Safety

Risk Area: Runway Safety*			
Rejected takeoffs	Rate of go-arounds vs. unstable approaches	Altitude crossing runway threshold	Short landing
Runway incursions	Lateral course deviations	Point of touchdown	Hard landing
Runway incidents	Excessive bank angles	Landing pitch attitude	Late thrust reverser deployment
Taxiway excursions	Altitude deviations	Takeoff pitch attitude	Runway remaining at 80 kt
Runway excursions	Sink rate/GPWS alerts	Tail strike/scrape	Aircraft braking effort
Go-arounds	Airspeed crossing runway threshold	Long landing	Deceleration distance
Unstable approaches			Excessive taxi speeds

FDAP = flight data analysis program; FDM = flight data monitoring; FOQA = flight operational quality assurance; GPWS = ground-proximity warning system

* Some of these items may need to be derived with information from other sources

Table 5 — Additional Ideas for FOQA-FDM-FDAP Performance Thresholds for CFIT

Risk Area: Controlled Flight Into Terrain (CFIT)		
Altimeter setting errors	GPWS or EGPWS alerts	Short landings
Lateral/vertical flight path/profile deviations	Radio altimeter warnings	VFR to IFR in mountainous terrain
SID/STAR noncompliance	Unstable approaches	

EGPWS = enhanced ground-proximity warning system; FDAP = flight data analysis program; FDM = flight data monitoring; FOQA = flight operational quality assurance; GPWS = ground-proximity warning system; IFR = instrument flight rules; SID = standard instrument departure; STAR = standard terminal arrival; VFR = visual flight rules

Table 6 — Additional Ideas for FOQA-FDM-FDFAP Performance Thresholds for LOC-I

Risk Area: Loss of Control–In Flight (LOC-I)		
Pitch up greater than 25 degrees	High/low speed events	In-flight engine shutdown
Nose down greater than 10 degrees	Alpha floor activation (TOGA)	Aircraft energy management
Bank angle greater than 45 degrees	Exceedance of flight envelope/protections	Automation management error
Stall warning	Clear air turbulence encounter	Excessive flight path deviations
Stick shaker activation	Wind shear encounter	Unstable approaches
	Convective activity encounter	

FDAP = flight data analysis program; FDM = flight data monitoring; FOQA = flight operational quality assurance; TOGA = take off/go around

Table 7 — Additional Ideas for FOQA-FDM-FDAP Performance Thresholds for NMAC

Risk Area: Near-Midair Collision (NMAC)
Lateral/vertical flight path deviations
TCAS advisories
Altimeter setting error
Large height deviations
Gross navigation errors

FDAP = flight data analysis program; FDM = flight data monitoring; FOQA = flight operational quality assurance; TCAS = traffic-alert and collision avoidance system

Table 8 — Additional Ideas for FOQA-FDM-FDAP Performance Thresholds for Aircraft Maintenance

Risk Area: Aircraft Maintenance
In-flight engine shutdowns
Flight control system anomalies
Landing gear malfunctions
Overspeed conditions
Engine/compressor stalls
Rejected takeoffs
Aircraft damage

FDAP = flight data analysis program; FDM = flight data monitoring; FOQA = flight operational quality assurance

Table 9 — Example of an ANSP Performance Threshold: NMAC

		Example Performance Thresholds			
Risk Area	**Hazard**	**Lateral Separation**	**Vertical Separation**	**System Alerts**	**Outcome**
NMAC	Airprox event	Measure of compliance is less than 66% of the required lateral separation of 3 nm (6 km).	Measure of compliance is less than 66% of the required vertical separation of 1,000 ft.	Conflict alert activation	Recovery from an airprox event involving one or more aircraft.

ANSP = air navigation service provider; NMAC = near-midair collision

Table 10 — Additional Ideas for ANSP Performance Thresholds for Runway Safety

Risk Area: Runway Safety			
Runway incursions	Runway excursions	Approach altitude deviations	Runway conditions
Runway incidents	Go-arounds	Airport infrastructure status	
Taxiway excursions	Lateral course deviations	Airport weather	

ANSP = air navigation service provider

Table 11 — Additional Ideas for ANSP Performance Thresholds for CFIT

Risk Area: Controlled Flight Into Terrain (CFIT)
Altimeter setting errors
Lateral/vertical flight path/profile deviations
SID/STAR noncompliance
MSAW alerts
SOP compliance

ANSP = air navigation service provider; MSAW = minimum safe altitude warning; SID = standard instrument departure; SOP = standard operating procedures; STAR = standard terminal arrival

interact with CEDAR to monitor different aspects of daily U.S. air traffic operations.

For example, the Traffic Analysis and Review Program (TARP) automatically alerts FAA personnel if an air traffic event exceeds predetermined lateral and/or vertical thresholds (a potential loss of aircraft separation). FAA personnel then conduct a focused query within CEDAR to obtain from operations data the date and time of an event. A playback system, called FALCON, is used to help synchronize and review radar track data and air traffic voice data. Following this review, FAA personnel recommend if an event should be reviewed further. Collectively, tools such as CEDAR and FALCON provides the FAA with valuable and objective insights into routine operations and safety events.

CEDAR data can provide you're the FAA's air traffic safety analysts with a detailed understanding of an event. For example, if a specified type of event occurs, the Federal Aviation Regulations (FARs) require controller initiation of a mandatory occurrence report (MOR) and to complete an investigation. Coupled with other air traffic safety information sources, this type of operational data can help the FAA identify the primary causal factors of specific threats, hazards and undesired states.

Here are our recommended information sources for air traffic quality assurance and quality control tools:

- FAA Joint Order 7210.634: *Air Traffic Organization Quality Control*; and,
- FAA Joint Order 7210.632: *Air Traffic Organization Occurrence Reporting*.

Examples of Performance Thresholds: ANSPs. We encourage your organization to develop performance thresholds that will provide meaningful insights into your daily operations as an

Table 12 — Additional Ideas for ANSP Performance Thresholds for NMAC

Risk Area: Near-Midair Collision (NMAC)			
Airprox event	Lateral/vertical flight path deviations	Advisory of TCAS activation	Gross navigational errors
Aircraft proximity	ATC conflict alerts	Altimeter setting error	SOP compliance
Rate of aircraft closure		Large height deviations	

ATC = air traffic control; ANSP = air navigation service provider; SOP = standard operating procedure; TCAS = traffic-alert and collision avoidance system

Table 13 — Example of a Performance Threshold Used by Manufacturers

		Example Performance Thresholds	
Risk Area	Hazard	System Alerts	Outcome
Maintenance	System reliability	Conflict alert activation	Recovery from an airprox event involving one or more aircraft

ANSP. These thresholds may be driven by specific operational threats, hazards or undesired aircraft states, or by SPI metrics. If your organization detects exceedance of a performance threshold, we recommend collecting and analyzing additional data from internal and external sources. Table 9 (p, 8) shows some operational performance thresholds that you could monitor and detect via CEDAR-like safety data.

We encourage your organization to develop performance thresholds that will be valid and customized to address your specific operational needs. Tables 10 through 12 (p. 8) show additional topics identified through our GSIP workshops that may help you introduce performance thresholds to be monitored and detected using CEDAR-like tools.

Example of Automated/System-Based Data Used by Aircraft Manufacturers: ACARS

As noted, typical commercial air transport aircraft and business aircraft carry onboard sensors that monitor the real-time health, integrity and status of flight systems. These sensors continually transmit operational data to ground stations via a datalink system called the aircraft communications addressing and reporting system (ACARS). ACARS message sets contain detailed information regarding aircraft system status, engine performance, potential system abnormalities and upcoming aircraft inspection/maintenance needs. Within a ground station, ACARS data are captured, processed and stored in a secure database. This database is accessed by authorized personnel on a regular basis. The data may be collected and used to address internal maintenance needs or shared with a manufacturer to address a recurring issue.

ACARS data also can provide your safety analysts with a detailed understanding of a maintenance event. For example, system reliability data can be derived in part from ACARS data. Coupled with other safety information sources, the operational data can help your airline or manufacturing company to identify the primary causal factors associated with threats, hazards and undesired states.

Example of Performance Thresholds: Manufacturers. We encourage your organization to develop performance thresholds that will provide meaningful insights into manufacturing. Your thresholds may be driven by customers' specific operational threats, hazards and undesired states, or your SPI performance metrics. If your organization or a customer detects that a threshold was exceeded, we recommend that you collect and analyze additional data from internal and external sources. Table 13 shows examples of performance thresholds that could be monitored and detected via ACARS-like data.

We encourage you to develop performance thresholds that are valid and customized to address your specific operational needs. Tables 14 through 16 show additional topics identified through our GSIP workshops that may help drive your development of ACARS-like performance thresholds.

Table 14— Additional Ideas for Manufacturer Performance Thresholds: Runway Safety

Risk Area: Runway Safety
Rejected takeoffs
Tail strike/scrape
Hard landing
Runway remaining at 80 kt
Aircraft braking effort
Deceleration distance

Table 15 — Additional Ideas for Manufacturer Performance Thresholds: CFIT

Risk Area: Controlled Flight Into Terrain (CFIT)
Altimeter setting errors
Navigational database inaccuracies
Navigational equipment errors

Table 16 — Additional Ideas for Manufacturer Performance Thresholds: ACARS

Risk Area: Loss of Control–In Flight
Exceedance of flight envelope/protections
In-flight engine shutdown
Maintenance errors
Manufacturer reports/service difficulty reports
Engine condition monitoring

ACARS = aircraft communications addressing and reporting system

Event Data

In this toolkit, the term *safety event data* most often means a narrative record of one or more characteristics of a flight operation or safety event (such as a voluntary safety report or accident report) submitted by a stakeholder who has a vested interest in improving aviation safety. This type of data is collected regularly by personnel using manual and electronic tools and all relevant sources.

Before you begin collecting in-depth causal factors and operations data, we recommend that your organization revalidate existing event-data collection tools. For example, safety programs at Level 2 intensity usually have an established employee VSRP with a form for submitting reports. Level 2 intensity involves VSRP submitters who provide detailed event context and causal factor data that exceeds Level 1 data collection. Your organization could evaluate the current submitter form's strengths and weaknesses and map the form to an established causal-factor taxonomy such as the ICAO Accident/Incident Data Reporting Taxonomy). This evaluation and mapping could add missing causal factors or other underrepresented data fields.

Highly detailed data from safety events are a key to putting into context the risks and operational outcomes that you identify through other safety data sources(including -automated/system-based data). Automated/system-based data sources provide facts and insights into normal operations and detected safety events, but they do not always address what caused the event. Therefore, you must collect event data to fill that gap and complete the risk picture.

Collecting detailed safety data from multiple internal and external sources will better position your organization to put risks into context, set meaningful performance thresholds and conduct sophisticated risk analysis. Consider, for example, annual safety reports from regulators that function at the highest levels of SDCPS intensity, and accident reports and serious incident reports from comparable stakeholders in the aviation safety community.

Data Collection Triggers

At Level 2 intensity, we assume the aviation organization is motivated to pursue the specific root-causes of all its known risks and to understand the context of those risks during daily operations. The following toolkit sub-sections describe additional data collection "triggers" (that is, prompts) that would encourage your organization to collect certain safety data in specific circumstances.

Exceedances of Operational Performance Thresholds

As already noted in this toolkit, we encourage all aviation organizations to establish minimum operational performance thresholds. Again, these thresholds may be suggested by specific operational threats, hazards or undesired states, or by ICAO's SPI metrics. Your own operations monitoring and regular data collection efforts, however, also could make you aware of exceeding performance thresholds. For example, evidence of high-energy landings, unstable approaches, near-midair collisions (NMACs) and similarly serious safety events should prompt your organization to initiate targeted data collection activities with an immediate effort to determine contexts of events and their causal factors.

System Health and Integrity Monitoring

When SPI metrics are the prominent drivers of your data collection activities — showing clearly whether you are achieving the corresponding targets — these activities must be capable of informing each SPI status update and capable of supporting "bottom-up sharing" of outcomes, focusing first on frontline staff.

Advanced SDCPS intensity levels also imply shifting your focus from only, or primarily, collecting safety data after events occur to continually enhancing your organization's self-awareness of risks. This requires collecting data primarily to monitor the overall "health" (that is, safety effectiveness) and integrity of your operation. This type of monitoring yields contextual understanding of your known risks, identifies system-wide trends and shows the effectiveness of current practices.

Risk Management Decision Strategies

Whenever you identify a safety risk, your organization must decide how to manage that risk. The alternatives typically include:

- Risk avoidance (change your course of action to completely avoid that risk);
- Risk transference (shift the risk to a third party, such as insurance);
- Risk mitigation (take control by reducing the probability and severity to an acceptable level); or,
- Risk acceptance (do nothing).

To support sound decision making, your organization's data collection must clarify the benefits and tradeoffs of alternative risk-management strategies. At Level 2 intensity, the data collection also should allow comparisons with comparable aviation organizations, substantiate your findings and justify your decisions.

Keeping Your Data Current

For analyses at Level 2 intensity, we recommend that your organization establish a quality assurance process for data

collection. This is also important to carry out at Level 3 when we discuss analysis across multiple data sources, but an emphasis here is because of the introduction of so much measured data. As a part of this process, your lines of business responsible for collecting data also will validate the currency of stored safety data. If the data are not current, updating the data will be necessary to assure high quality analysis and accurate inputs and outputs. As you collect current data, be sure to appropriately archive the older information for studying historical performance of your safety programs, auditing, benchmarking and forecasting.

Reliability and Quality of Information

At Level 2 intensity, you'll strengthen analytical conclusions and results through enhanced reliability and quality of data collection. However, you then must maintain this high level of data reliability and quality. Employee trust in your safety program will be an invaluable benefit of this long-term consistency.

As you collect, merge and store digital and paper document–based safety data, it's increasingly important to routinely check data accuracy, completeness and proper organization. Collecting and storing mixed types of data increases the opportunity for data compatibility issues and errors. To help detect potential issues, establish regular "data checks and balances." Ask the following types of questions:

- Are there gaps in data that we've decoded from an automated/system-based data capture source?
- Are there system-to-system communication gaps (that is, gaps between the sources and databases that store the decoded information)?
- Are there user-induced data translation errors?
- Do known employee safety concerns appear in our data?
- Do we see systemic data errors or incomplete data among any data we collect or store?

If so, we recommend a formal quality assurance process. This process addresses these types of divisionally cross-cutting reliability and quality issues (that is, those that occur in multiple departments of your organization). The process also will help you update the currency data, streamline quality and reliability checks, and ensure meaningful audit results. The quality assurance process also provides a sound basis during audits to compare actual data collection practices against internal quality assurance processes, external requirements and industry standards.

Safety Data Collection Map

Preparing a safety data collection map will help you gather and merge information from multiple sources. This map also can be a valuable tool to diagram and characterize your current capabilities and advance to a higher level of SDCPS intensity if that is your strategy. Your map should identify:

- Major risk areas you've selected to map or categorize top priority risks;
- Sources used to collect safety data in each major risk area; and,
- People and departments responsible and accountable for collecting specific data types from each source.

Table 17 (p. 12), prepared by Flight Safety Foundation, is an illustration of a hypothetical airline's safety data collection map. The map contains enhancements to the map in our GSIP toolkit for Level 1 intensity safety programs. Our map for Level 2 intensity adds safety data metrics from safety assurance sources. Those sources include automated/system-based data capture systems and manual data capture systems.

Creating Your Plan for Success

As a starting point or as a checklist for successful data collection, we recommend that you:

- ☐ Customize your safety program's performance thresholds to address the unique operational conditions and needs of your organization. These thresholds should make the data collection efforts precise (see "Automated/System-Based Data," p. 5).
- ☐ Periodically revalidate your data collection tools to ensure that your organization over time will gather increasingly in-depth causal factors and contextualized operations data (see "Event Data," p. 10).
- ☐ Develop a data collection quality assurance process. To reiterate, this process solves the problem of keeping safety data current and helps streamline internal data quality and reliability checks (see "Reliability and Quality of Information," p. 11).
- ☐ Document the errors, gaps and missed opportunities disclosed by your safety data collection map. Closing these gaps is essential in advancing to the next level of SDCPS intensity (see "Safety Data Collection Map," p. 11).

Table 17 — Safety Data Collection Map for Level 2 Intensity

Sample Risk Categories	Accountable Department	Supporting Organizations	Public Safety Data	Reportable Occurrences			Safety Program Information	
			Accident and Serious Incident History	Company Operational Reporting	Mandatory Regulator Reporting	Company Self-Disclosure Reporting	Safety Assurance *Measured Data*	Employee Reports
Controlled flight into terrain (CFIT)	Airline flight operations	ANSP (air traffic control)	Accident/incident investigation reports	Operational event reports	CAA reports	Voluntary disclosure reports	EGPWS warnings	Pilot safety reports
Loss of control–in flight (LOC-I)	Airline flight operations	Manufacturer					Stall and overbank warnings	
Runway safety (approach and landing accidents)	Airline flight operations	Air traffic					Stable approach Go arounds Touchdown points Rate of de-acceleration	
Mechanical issues	Airline maintenance	Manufacturer		IFSD, ATB, RTO, DIV events			Detection of structural failures	Mechanical safety reports
Near-midair collision (NMAC)	ANSP (air traffic control)	Airline flight operations		Evasive action report from traffic conflict	Air traffic MOR		TCAS warnings Loss of required separation events	Pilot safety reports Controller safety reports
Runway safety (conflicts)	Airline flight operations	Airport authority		Operational event reports	CAA reports		Runway incursions Taxiway incursions	Pilot safety reports Controller safety reports
Wildlife issues	Airport authority	Airline flight operations		Aircraft damage reports	Bird strike reports		Airport exposure information	Ramp safety reports Plot safety reports Controller safety reports
Cabin safety	Airline in-flight team	Airline flight operations		Turbulence injuries, fume events, unruly passenger	Hospitalization of crew and/or passengers		FDM turbulence detections	Flight attendant safety reports
Fatigue and general fitness	Airline flight operations, airline in-flight team, aircraft maintenance	Airline crew scheduling department, regulator		—	Drug and alcohol testing		Fatigue risk management system studies	Pilot safety/fatigue reports Maintenance safety/fatigue reports Flight attendant safety/fatigue reports
Dispatch safety issues	Flight planning and dispatch team	Airline flight operations		Operational event reports	CAA reports		Flight planning errors Load planning issues Incorrect flight plan filed MEL/CDL compliance issues NOTAM issues	Plot safety reports Dispatcher safety reports

ANSP = air navigation service provider; ATB = air turnback; CAA = civil aviation authority; CDL = configuration deviation list; DIV = diversion; EGPWS = enhanced ground-proximity warning system; FDM = flight data monitoring; IFSD = in-flight shutdown; MOR = mandatory occurrence report?; MEL = minimum equipment list; NOTAM = notice to airmen; RTO = rejected takeoff; TCAS = traffic-alert and collision avoidance system

Data Analysis

Your objective in data analysis — when your safety program functions at Level 2 intensity — is to gain a deep understanding of known safety risks and their primary causes in the context of day-to-day operations. This section of our toolkit focuses on the bow-tie model and techniques that will elevate your organization's SDCPS risk management capabilities and safety program effectiveness.

Table 18 summarizes GSIP levels of intensity in data analysis.

Expanding the idea in Table 18, Level 2 data analysis emphasizes:

- Validating the root causes of threats and undesired states you identified during Level 1 data analysis;
- Analysis at level 2 applies to measured data in Flight Data Monitoring Programs. Where Level 1 focuses on investigations and fishbone diagrams for potential causes, Level 2 analysis advances the understanding of those causes;
- Developing a deeper understanding of the direct causal factors of undesired states and residual risks; and,
- How to apply focused risk analysis methods to create a bow-tie model.

Although our toolkits focus on commercial air transport and business aviation, you can tailor the underlying approaches to other operational needs if necessary.

Using Complex Safety Data for Analysis

In your data analysis at Level 2 intensity, you'll have the advantages of increasingly complex safety data that enable robust, advanced and clear understanding of risk. You'll be able to leverage data collection from multiple internal and external sources. This sub-section of our toolkit:

- Recommends how to identify and refine problems that can be evaluated using the previously introduced cause-and-effect diagram;
- Supports your efforts to understand the magnitude and influence of each identified threat so that the relationship between threats and undesired states can help you set priorities; and,
- Reinforces bow-tie model elements with quantitative and qualitative safety data.

Bow-Tie Model Introduction

Flight Safety Foundation encourages wide use of the bow-tie model as a key part of aviation risk management. This valuable risk-assessment method provides you with a repeatable process to identify and document multiple risk scenarios and causal factors in a consolidated view. The following subsections introduce the model's architecture and the bow-tie method, a step-by-step guide on how to populate a bow-tie model, and an example of practical application.

Architecture of the Bow-Tie Model

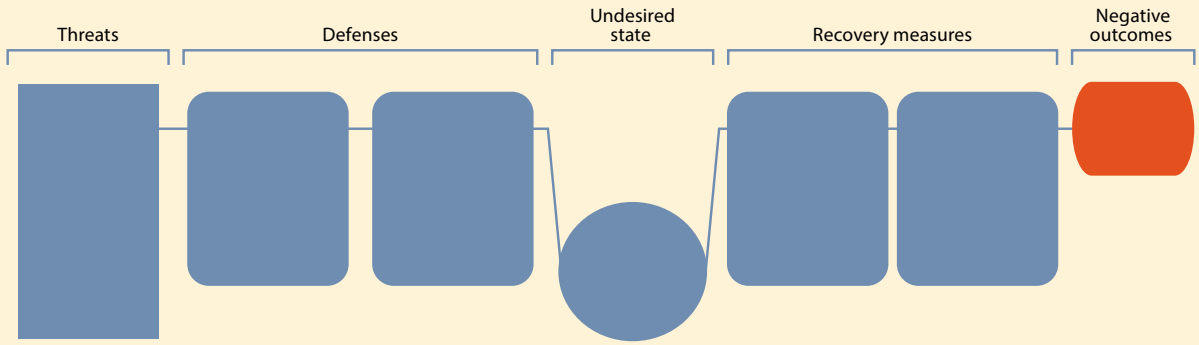
Here's the basic architecture and terminology you'll need to use with bow-tie models if you're not already familiar with them. At the position of the "bow-tie knot," or center of the model's diagram, you'll insert the *undesired state* you are studying. An undesired state is an critical condition that could lead to a negative outcome (that is, the worst credible outcome/-consequence) within the context of your operation. Forming the left side of the bow-tie are individual *threats* and a set of related *defenses*. Threats would become the primary causal factors of an undesired state if not managed. Defenses are proactive protections that you'll implement to prevent a threat from leading to an undesired state (such as loss of control–in flight [LOC-I]).

Table 18 — Data Analysis Matrix at Level 2 Intensity

GSIP Toolkit Matrix	Level 1	Level 2	Level 3	Level 4
Data Analysis	Data are analyzed to determine acceptable risks. Safety performance indicators are monitored regularly to display status against objectives.	Data are analyzed to understand all direct hazards and their impact on undesired outcomes. Multiple hazards are examined for their influence on risk.	Data are analyzed to understand all potential direct and indirect hazards and their impact on undesired outcomes.	TBD

TBD = to be determined

Figure 1 — Bow-Tie Model Architecture



Forming the right side of the bow-tie are sets of *recovery measures* and *negative outcomes*. Recovery measures are reactive protections that could prevent an undesired state from escalating into a negative outcome or reduce the consequences of risk associated with that outcome. Here again, we define negative outcomes as the worst credible outcome resulting from an unmanaged undesired state. A negative outcome typically is loss of life, injury or damage to property.

Guide to Using a Bow-Tie Model

Bow-tie models are used by aviation safety managers, internal and external auditors, and other stakeholders who need to conduct robust risk analyses. To complete the diagram of your bow-tie model, you'll first identify a set of undesired states that plausibly could lead to a corresponding set of undesired outcomes. The set of undesired states can be selected by reference to known predictors of negative outcomes (including the aircraft accident scenarios you've analyzed using a cause-and-effect diagram) or adapting your organization's top priority risks. You can derive negative outcomes from your organization's safety performance goals (the SPI targets) or by analyzing public safety information, primarily accident data and serious incident data in reports.

Starting with a single undesired state, clearly name and describe the hazard of interest in the center of the bow-tie. Next, insert a plausible negative outcome that could occur if that undesired state is not managed.

On the far left side of your bow-tie, name and describe the leading threats (direct causes) that can result in an undesired state. Internal threats in your organization can be taken from cause-and-effect diagrams, analysis of public safety information or your safety assurance data (comprising, as noted, audit data, data from automated/system-based data capture sources and event data). Subsequent sections of this toolkit propose data analysis techniques to identify and prioritize threats.

Next, list defenses that could prevent the undesired state from occurring. You can identify defenses by interviewing your operational subject matter experts and line employees, or by analyzing public safety information (specific examples include post-accident recommendations and recovery measures after a serious incident).

On the right side of the bow-tie, insert the individual recovery measures that could be taken to prevent an undesired state from escalating into the stated negative outcome or reduce the consequences of the risk associated with that outcome. You can easily list relevant recovery measures by analyzing internal safety assurance data (specific examples include your employee VSRP, automated/system-based data capture sources and standard operating procedures).

Example of Practical Application of a Bow-Tie Model

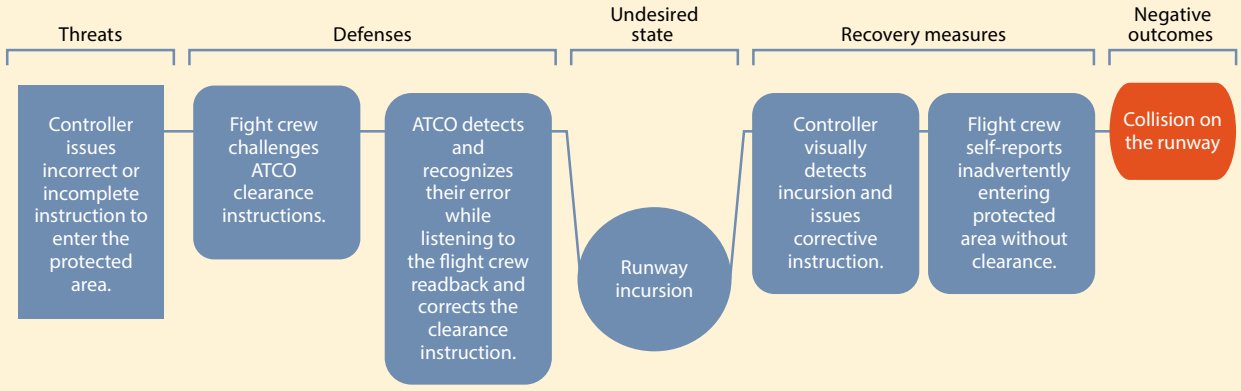
Figure 2 (p. 15) shows a bow-tie model diagram prepared by a de-identified organization that shared its runway incursion experiences with the U.K. Civil Aviation Authority (CAA). The organization completed the following steps:

Step 1, Undesired State — To name and describe the undesired state of interest, the organization reviewed its set of top priority risks. They selected "Runway Incursion" for further evaluation. They added this at the center of the bow-tie diagram.

Step 2, Negative Outcome — They then reviewed runway safety accident reports and serious incident reports to select a set of worst credible outcomes that could result from not managing this undesired state. They chose just one negative outcome — "Collision on the runway." They added this on the far right side of the bow-tie diagram.

Step 3, Threats — To identify certain runway incursion causal factors as threats, the organization prepared a cause-and-effect diagram. For the bow-tie diagram, they chose just one causal factor — "Controller issues incorrect or incomplete

Figure 2— Practical Application of the Bow-Tie Model to Runway Safety



ATCO = air traffic control officer

Source: Adapted from the U.K. Civil Aviation Authority's Bowtie Library

instruction to enter the protected area." This causal factor was added, as a threat, to the far left side of the bow-tie diagram.

Step 4, Defenses — To understand proactive measures that line employees could use to prevent that threat from leading to a runway incursion, the organization interviewed internal subject matter experts. These interviews resulted in a set of protections added to the left side of the bow-tie diagram as two defenses. These were: "Flight crew challenges [the air traffic controller's] clearance or instructions." and "[The air traffic controller] detects and recognizes their error while listening to the flight crew readback and corrects the clearance/instruction."

Step 5, Recovery Measures — Finally, the organization conducted an in-depth review of its employee VSRP. The purpose was to understand the reactive measures used by line employees to prevent the undesired state on the bow-tie diagram from escalating into the negative outcome. The review specifically found VSRP safety event reports that documented a prior operational response to runway incursions. The reviewers added the results from this review to the right side of the bow-tie diagram as recovery measures. These were: "Controller visually detects incursion and issues corrective instructions" and "Flight crew self-reports inadvertently entering protected area without clearance."

The practical application in Figure 2 demonstrates the value of using the bow-tie method. The method gives you a repeatable process of robust risk assessments, and lets you consolidate the results in an easy-to-understand bow-tie diagram. We strongly recommend using only validated safety data to populate elements of your bow-tie diagrams. Additionally, you must continually reassess probability and severity after finishing the model — as discussed in our Level 1 toolkits — to ensure you're directing analytical efforts to your organization's most critical risk areas. As the bow-tie modeling gets more complete, new potential paths towards the undesired state will be discovered along with new barriers to contain the threat. The following toolkit sections introduce Level 2 tools and techniques, including further uses of bow-tie models.

How to Refine Safety Problems for Analysis: Cause-and-Effect Diagram

You'll typically need robust forms of risk data to develop a bow-tie model at Level 2 intensity. Readily available sources, as noted, include your safety assurance data, which will reveal relatively substantive and detailed events (undesired states), and causal factors (threats) that enable deeper analysis. We want to bridge the gap in sophistication between the cause-and-effect diagrams (also called Ishikawa diagrams and fishbone diagrams, as noted), that we recommended in our Level 1 toolkits, and the bow-tie models that we recommend in our GSIP Level 2 toolkits.

At Level 2 intensity, you'll collect case-by-case safety event data with a relatively high degree of detail and have access to comprehensive, automated/system-based data from routine operations. As your organization's entire set of safety data grows in quantity, quality, depth and complexity, you must have tools and techniques ready to maximize the utility of the entire set.

For example, to complete a cause-and-effect diagram as explained earlier, you'll first choose a high-priority safety problem to analyze (such as a threat or undesired state). At Level 1 intensity, the choice of this problem is predicated largely on known industry risks. At Level 2 intensity, the problem derives from internal safety assurance data. When evaluating safety assurance data to identify hazards (undesired states) and causal factors (threats), you may need further

organizational guidance to break this down into discreet elements and their logical connections.

Preparing a casual factors checklist also helps to focus your data analysis activities. This checklist provides a repeatable set of questions to guide your evaluation of event data and automated/system-based data. The checklist serves as a foundation to put into context findings during initial data analysis.

We recommend that your causal factors checklist have four primary categories of questions for evaluating a safety event. They are: people/operator; methods; tools and techniques; and operations environment. These categories help ensure compatibility of your work across risk assessment methods and tools, including the cause-and-effect diagram and the bow-tie model-diagram method.

Table 19 (p. 17) shows a hypothetical causal factors checklist prepared by Flight Safety Foundation. Your organization should tailor your causal factors checklist to apply to your operational needs.

A tailored causal factors checklist will be an especially valuable tool for the safety analysts who review and evaluate safety data. The use of a checklist focuses an analyst's work on the identification of hazards and direct causal factors. The checklist use also encourages:

- Refined definitions of problems for analysis (for example, refinements derived from a cause-and-effect diagram or the bow-tie model/method);
- Deeper understanding of your organization's safety data, which helps you target corrective actions and/or mitigations for root causes of a threat or undesired state;
- Support for validation of root causes that previously were identified; and,
- Increasingly complex SDCPS risk management tools, such as the bow-tie model/method.

Your causal factors checklist also helps identify multiple causes of a safety event. Understanding those causes is a key to the next level of SDCPS intensity.

Addressing Residual Risks

Risk management in aviation typically has four phases: identify hazards; assess risk; develop and implement risk responses or mitigations; and monitor and control risk. In the third phase, we assume that resultant actions reduce risk but cannot eliminate risk. Any risk that remains after you introduce a risk response/mitigation plan is called *residual risk.*

Your organization should determine the probability and severity of residual risk in basically the same manner as when you conduct your initial qualitative and quantitative assessment of risk. Understanding residual risk enables your organization to decide whether a proposed risk response/mitigation plan is adequate.

If assessment reveals that event probability and severity will not fall to an acceptable level, you must revise your risk response/mitigation plan. In the opposite situation, you probably can proceed as planned.

Assessing residual risk requires the same methodology followed during your initial risk assessment. For example, if your organization tailors the ICAO safety management system (SMS) probability and severity scales to your operation, then use the same tailored scales (see the *GSIP Level 1 Data Analysis Toolkit*). Also, remember to save residual risk assessments in your risk register.

As you manage safety at Level 2 intensity, periodically apply automated/system-based data to revise and revalidate your tailored (customized) scales developed for Level 1 purposes. Using these data will provide more accuracy and traceability of differences compared with ICAO's established scale (in other words, you'll have more accurate probability and severity scales for your operations). If your organization updates its tailored scales, be sure to reevaluate the probability and severity of all your active risks, residual risks and related mitigation strategies.

Identifying Threats and Undesired States in Context

Automated/system-based data sources help your organization to more clearly understand risks in the context of daily operations. Data collected from these sources clarify your exposure (rate or frequency) to a threat or undesired state. For example, FOQA/FDM/FDAP, ATC recordings and ACARS maintenance data help your organization:

- Understand and highlight frequently recurring threats and undesired states;
- Compare actual operational performance to desired performance targets; and,
- Contrast operational outcomes with aggregated trends within your organization or across the aviation industry.

You also can apply automated/system-based data to:

- Validate your organization's tailored SMS scales;
- Focus root-cause analysis and safety event investigations;
- Identify SDCPS risk management gaps; and,
- Develop a baseline understanding of normal operations (for example, aircraft braking performance on a dry runway versus braking performance on a snow-covered runway).

Your reliance on automated/system-based data often yields valuable insights. However, if used in isolation, you may have difficulty understanding the root causes of an event. In that

Table 19 — Proposed Causal Factors Checklist

Identification of Potential Causal Factors	Applicability		Comments Describing the Context of a Causal Factor
	Yes	No	
People/Operator			
Did the operator's inadequate readiness, preparedness or fitness for duty cause the threat or undesired state?			
Did procedural or SOP nonconformance cause a threat or undesired state?			
Did intentional deviation from procedures or SOPs cause a threat or undesired state?			
Did the complexity of a procedure or SOP cause the threat or undesired state?			
Did the complexity of one or more tasks cause a threat or undesired state?			
Did operator timeliness (that is, a delay in identifying a threat) cause an undesired state?			
Was the threat or undesired state reported to the CAA by the operator? If yes, how?			
Methods			
Did the lack of procedures or SOPs (such as failure to conduct a position relief briefing) cause the presence of a threat or the occurrence of an undesired state?			
Did the lack of compliance with a procedure or SOP (such as noncompliance with an approach procedure or a FOD-inspection procedure) cause the introduction of a threat or the occurrence of an undesired state?			
Tools and Equipment			
Did faults in equipment or tools cause the threat or undesired state?			
Did the equipment and/or tool detect the cause of a threat or undesired state (for example, in a TCAS RA or radar traffic conflict alert)?			
Did the incorrect use of tools or equipment cause the event (for example, automation error)?			
Did the tool and/or equipment readiness cause the event (for example, was it turned on, was there a compatibly issue)?			
Did known tool and/or equipment design issues cause the event (for example, was there a usability issue)?			
Was the threat or undesired state automatically reported by a tool or other equipment? If yes, which tool or piece of equipment?			
Operations Environment			
Did the location of the operator's work environment (for example, an excessively loud or poorly lighted workstation) cause the event?			
Did adverse weather conditions (such as reduced visibility) cause the event?			
Did unplanned environmental conditions (such as clear air turbulence) cause the event?			
Did environmental complexity (such as airport layout or complex airspace design) cause the event?			

CAA = civil aviation authority; FOD = foreign object damage; SOP = standard operating procedure; TCAS = traffic-alert and collision avoidance system; RA = traffic collision alert system resolution advisory

case, add sources of safety event data (such as VSRP data and audit data) to gain a clearer, more complete grasp of root causes.

The following toolkit sections describe in detail the inputs, outputs and techniques that add context about risks and enable sophisticated risk analysis methods, such as the bow-tie model.

Level 2 Risk Analysis Inputs, Outputs and Techniques

For all levels of intensity that we recognize in safety programs, GSIP data analysis toolkits recommend analytical techniques aimed at increasing the depth and richness of information you use to populate your cause-and-effect diagrams and your bow-tie model diagrams . Our Level 2 recommendations focus on your use of internal safety assurance data and public safety information for deep understanding of undesired states, causal factors and residual risks. Remember, risk is the product of a hazard's frequency and severity.

This toolkit also presents examples of inputs, outputs and techniques that show the influence/magnitude of relationships and opportunities. The examples reinforce our recommendations of cause-and-effect diagrams and the bow-tie models, both using quantitative and qualitative data.

Heat Map Analysis

A heat map analysis visually summarizes the results of frequency-based data analysis. In other words, we typically rely upon software assigning colors to the frequency of occurrence of one or more variables. This type of analysis provides you with a concise, easy-to-understand view of a large data set. An example of a variable in aviation safety could be a set of threats or a set of undesired states. Note, however, that some factors naturally occur more frequently in your data or taxonomies. Therefore, you must keep the broader context in mind when you review any heat map analysis.

Figure 3 — Example of Highlight Table Analysis Results

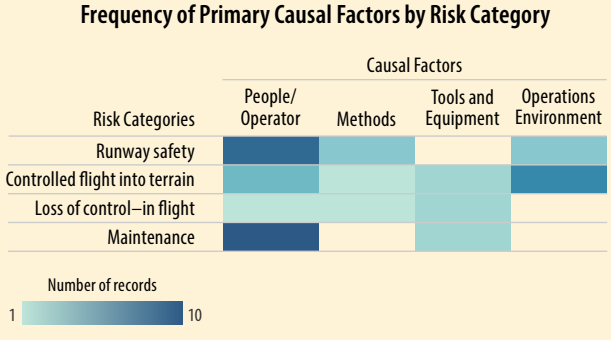


Figure 4 — Example of Geographic Hot Spot Analysis Results

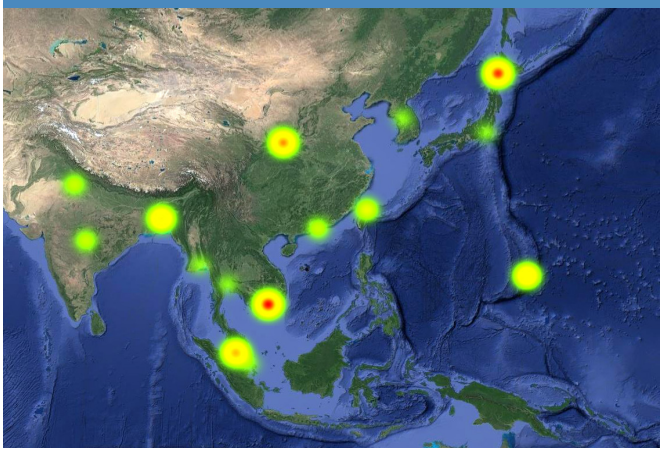


Figure 5 — Example of Highlight Table Analysis Results

Frequency of Primary Causal Factors by Risk Category

Risk Categories	Causal Factors: People/ Operator	Methods	Tools and Equipment	Operations Environment	Total Number of Factors	Total Number of Events
Runway safety	9	3		3	15	10
CFIT	4	1	2	7	14	5
LOC-I	1	1	2		4	2
Maintenance	10		2		12	7

Number of records: 1 – 10

CFIT = controlled flight into terrain; LOC-I = loss of control–in flight

Geographic Hot Spot Analysis

A geographic hot spot analysis highlights the overlapping data elements or the most frequently occurring data elements by geographical location. The results of a hot spot analysis provide your organization with appropriate data to identify targeted locations that may be more prone than others to a specific operational risk. A unique feature of this analysis is the two-dimensional or three-dimensional (2-D or 3-D) mapping of analysis results. These maps are extremely valuable when you are ready to communicate the outputs of your analyses. Figure 4 shows geographic hot spot analysis generated by software from a fictitious data set solely for educational purposes.

Highlight Table Analysis

A highlight table analysis summarizes large sets of frequency-based data and includes specific types of values that are not

Table 20 — Examples of Different Analysis Inputs and Analysis Outputs

Data Sources	Example Analysis Inputs	Example Analysis Outputs
Employee safety reports	Frontline employee event narratives describing observed safety events	Most frequently cited: • Location of safety events/issues, and • Event causal factors
Public safety information	Accident/serious incident reports from other organizations operating at higher levels of SDCPS intensity	Most frequently cited threats that have led to a specific undesired state
Safety assurance data	Automated/system-based data capture sources (for example, FOQA)	Location of most frequent performance deviations

FOQA = flight operational quality assurance; SDCPS = safety data collection and processing system

part of a heat map analysis. A highlight table analysis labels the value of each shaded area and shows specific values while drawing your viewer's eye to hot spots.

Table 20 shows data sources, analysis inputs and analysis outputs for heat map, geographic hot spot and highlight table analyses.

Safety Performance Indicators

ICAO-defined safety performance indicators enable your organization to specify desired safety outcomes and to measure the effectiveness of the day-to-day actions you take to address causal factors or risks. While SPIs can vary in detail and completeness, every robust Level 2 SPI has the following attributes:

- Risk category (scope);
- Objective (desired result/outcome);
- Performance metric target (evaluation criteria); and,
- Action plan (response to the challenge).

With your safety program functioning at Level 2 intensity, you'll have access to greater amounts and a higher quality of information than at Level 1. You can apply data derived from Level 2 analyses to refine or revalidate your existing SPIs. For example, introducing automated/system-based data opens possibilities for your organization to have refined metrics based on in-depth knowledge of your day-to-day operations. Highly detailed event data also enable you to develop SPI action plans through clearer understanding of causal factors of your primary risks.

Tables 21, 22, 23 (p. 20) and 24 (p.20) show examples prepared by Flight Safety Foundation to illustrate Level 2 SPIs with sample data/metrics for each risk category. Our data

Table 21 — Example of a Safety Performance Indicator: Runway Safety

Domain	Risk Category	Objective	Performance Metric Target or SPT	Action Plan
Airport	Runway safety	Reduce the number of runway incursions.	Reduce the number of serious runway incursions to 0.4 per million operations.	Establish minimum surface marking and signage quality requirements. Improve airport operations awareness of those requirements through recurrent training and outreach materials.

SPT = safety performance target

Table 22 — Example of Safety Performance Indicator: CFIT

Domain	Risk Category	Objective	Performance Metric Target or SPT	Action Plan
ANSP	CFIT	Reduce the number of CFIT events.	Reduce the number of near-CFIT events to 0.05 per million operations.	Provide aircraft with consistent lateral and vertical flight paths to reduce the opportunity for near-CFIT events. Improve airspace procedure awareness requirements to enhance individual and team performance.

ANSP = air navigation service provider; CFIT = controlled flight into terrain; SPT = safety performance target

Table 23 — Example of Safety Performance Indicator: LOC-I

Domain	Risk Category	Objective	Performance Metric Target or SPT	Action Plan
Airline operator	LOC-I	Reduce the number of LOC-I events.	Reduce the number of LOC-I events to 0.05 per million operations.	Improve flight crew training and evaluation criteria to emphasize pilot recognition and response to LOC-I events.

LOC-I = Loss of control–in flight; SPT = safety performance target

Table 24 — Example of Safety Performance Indicator: NMAC

Domain	Risk Category	Objective	Performance Metric Target or SPT	Action Plan
ANSP	NMAC	Reduce the number of airprox events.	Reduce the number of airprox events to 0.05 per million operations.	Improve controller awareness of potential level-bust leading indicators.

ANSP = air navigation service provider; NMAC = near-midair collision; SPT = safety performance target

collection map, introduced in the "Data Collection" section of this toolkit, shows potential automated/system-based data sources useful for developing your SPIs.

Runway Safety

See Table 21.

Controlled Flight into Terrain (CFIT)

See Table 22.

Loss of Control–In Flight (LOC-I)

See Table 23.

Near-Midair Collision (NMAC)

See Table 24.

Create Your Plan for Success

We recommend these ideas as your starting point or checklist as you create a plan for successful data analysis.

- ☐ Create and customize a causal factors checklist to focus your data analysis activities. Your tailored checklist will provide a repeatable guide to identify multiple causal factors while analyzing safety events and automated/system-based data (see "How to Refine Safety Problems for Analysis: Cause-and-Effect Diagram," p. 15).
- ☐ Apply your automated/system-based data to revalidate your organization's tailored ICAO SMS scales (the probability and severity scales). These data will provide the most reliable tools for assessing risk in your daily operations (see "Addressing Residual Risk," p. 16).
- ☐ Revalidate and refine your organization's SPIs so that they include the most robust information available, such as risk categories, SPIs, detailed performance metrics and targeted action plans (see "Safety Performance Indicators," p. 19).

Information Sharing

Level 2 Information Sharing

GSIP Level 2 intensity includes information sharing to broaden your initial exchanges of safety data across multiple lines of business within your organization. In level 1 we focused on sharing this information back with the direct frontline staff that would be submitting the safety reports. At this level the sharing within the organization is broadened. This toolkit introduces communication tools, techniques and opportunities that will promote cross-organizational safety program support and increase employee participation.

Table 25 shows the GSIP information sharing intensity levels.

In Table 25, the Level 2 information sharing aims to improve:

- Effectiveness of automated/system-based data capture programs (such as FOQA, FDAP and FDM);
- Awareness of your organization's operational performance thresholds;
- Cross-organizational understanding of risks and causal factors; and,
- Bottom-up employee engagement in SPI action plans.

The examples in this toolkit focus on commercial air transport and business aviation; however, the underlying approaches can be tailored to address operational needs in other aviation segments.

Managing Stakeholder Perceptions

Enhancing your safety program's effectiveness requires bridging the gap between your safety program and the lines of business that comprise your organization. The lines of business may have different levels of expertise, influence and interest in your SDCPS. To overcome any gaps, consider all the employee perceptions about your:

- Automated/system-based data capture programs;
- Event data collection and analysis programs and activities;
- SPI action plans; and,
- Proposed safety partnerships with your regulator.

We recommend researching these perceptions through organizational safety surveys (see details in the GSIP Level 1 toolkits), informal one-on-one and/or group discussions, and/or through other internal feedback mechanisms. How your safety program manages these perceptions could have a direct impact on the effectiveness of your safety program's activities, and the overall safety culture.

In high-risk domains like aviation, you must address sensitivity and confidentiality challenges associated with all operational safety data. This is especially true as you introduce automated/system-based data capture methods into flight operations. Regularly communicating how your safety program addresses those needs will increase the transparency of the overall program, and support your infusion of just culture principles.

As your organization grows in size and complexity, continually manage the interests of each line of business in your safety program. To guide this work, we recommend creating a formal strategy to manage your internal safety program communications. This strategy should identify:

- Safety program stakeholders within each line of business;
- Specific safety interests of each stakeholder;

Table 25 — Level 2 Intensity Matrix for Information Sharing

GSIP Toolkit Matrix	Level 1	Level 2	Level 3	Level 4
Information Sharing	Information sharing of performance results is performed within an organization (for example, within one organization).	Information sharing of performance and key areas of linked performance is comprehensive within an organization.	Information sharing is across the industry for key risks and mitigations. Generally, this is through presenting detailed independent investigative work in the data (for example, airline to airline, ANSP to airline).	TBD

ANSP = air navigation service provider; TBD = to be determined

- What safety information is required to address each stakeholder's needs;
- The necessary frequency of safety program communications or updates;
- How safety information will be communicated to each stakeholder (for example, in a formal memo and an informal briefing); and,
- How your safety program will address information-sensitivity issues when coordinating safety information with one or more stakeholders (for example, whether nondisclosure agreements will be required and what action will be required to de-identify data).

The following toolkit sections identify tools, techniques and opportunities to increase bottom to top–level employee support for your overall safety program, starting with robust safety information sharing at the front lines.

How to Build Trust in Automated/System-Based Data Capture Programs

Automated/system-based data capture programs can provide unique insights into routine operations, safety events and event outcomes. Without such programs, critical information often would go unreported or undetected by your safety program. The legitimacy and success of the programs also hinge on employee buy-in and ongoing support.

At Level 2 intensity, your organization will see the results of these programs across all relevant lines of business. This includes sharing information to support any potential safety partnerships established with your organization's civil aviation authority and other regulators. To manage employee perceptions and expectations of an automated/system-based safety data capture program, we recommend that your safety program:

- Clearly identify the scope and objectives of the automated/system-based data capture program;
- Develop a process to provide employees with regular program updates (for example, link to safety communications management strategy, memos and meetings);
- Establish information protection measures to promote fairness within a just culture (see the "GSIP Information Protection" section of this toolkit;
- Define and coordinate operational performance thresholds;
- Define and regularly communicate about program boundaries, basically who is working which aspects of safety, to reduce the likelihood of negative or inaccurate safety program perceptions; and,
- Leverage program outputs to promote a unified safety message across your organization.

When sharing program results, closely adhere to your communications management strategy — especially the parts that identify information-sensitivity needs and stakeholder-coordination plans. For example, when you share results of automated/system-based data capture, they should be de-identified so that no event details can be linked to a person or specific group of employees.

Regularly communicate the results from your automated/system-based data capture program so that employees' confidence in the program increases and they fully understand its added value in reaching your safety goals and objectives. For example, you might detail how the findings from one department (for example, flight operations) impact the cross-organizational practices in another department (for example, aircraft maintenance). Through your communication and outreach process, reaffirm that automated/system-based data capture programs are not intended to be used as a means of triggering punitive action. Rather, they solely provide deeper insights into routine operations so that known risks can be more effectively managed, and emerging risks can be identified before an accident or serious incident occurs.

To enhance employee buy-in, offer your employees the opportunity to provide constructive safety-program feedback. When you respond to employee feedback, notice and address any potential barriers that could limit or impact your safety program's success. Possible barriers include, but are not limited to:

- Information confidentiality concerns (who will see the recorded data);
- Concerns about retaliatory action (fear of punishment); and,
- Information bias (personnel acting without understanding the full context of an operation).

Actively sharing results from your automated/system-based data capture program helps you maintain a high level of employee trust, leading to credibility and acceptance of your safety data collection and analysis tools.

Sharing Event Data and Causal Factors

Event data collection and analysis tools offer the opportunity to identify both positive and negative risk causal factors. However, the depth of information gathered and the success of those tools are contingent upon employees understanding their value and how to use them. For example, at Level 2 intensity, we assume that you'll refine your VSRP submitter form to collect detailed, robust data suitable to determine causal factors. Unless your organization clearly informs employees about reasons for such changes, your context and motivation, and provides detailed

instructions on how they are expected to use the revised form, your success in gaining full cooperation could be limited.

At Level 2 intensity, we also expect your organization will share risk data and causal factor data (derived from safety event data) with all relevant lines of its business.

To reiterate, as when handling any safety data source, we recommend that you de-identify event data characteristics that can identify any person or group of employees. While communicating across your lines of business, encourage employees to provide constructive feedback on your safety data collection and analysis findings. Their opportunities to share event data, risk factors and causal factors should include, but not be limited to:

- Formal safety meetings with program stakeholders;
- Safety program memos;
- Employee training; and,
- Safety program educational and outreach materials.

To maximize the effectiveness of sharing safety event data, we recommend, at a minimum, that you cover:

- Relevant historical performance in the given risk category;
- Forecasts of future performance and/or goals;
- Status of current risks, issues, opportunities and mitigations;
- Safety program progress accomplished during a given work period (such as the past month or the previous quarter);
- Major changes and/or positive effects related to your safety program; and,
- Applicability to each employee within your organization (to help them to answer the question "Why are the data important to me?").

Building SPI Action Plan Support

ICAO safety performance indicators, as noted, enable your organization to define desired safety outcomes and to measure the effectiveness of related day-to-day actions. SPIs vary in detail and completeness, but every robust SPI has these attributes:

- Risk category (scope);
- SPI objective (desired result/outcome);
- Performance metric (evaluation criteria); with safety performance target (SPT) and,
- Action plan (response to the challenge).

SPI action plans help you increase the safety awareness and engagement of your employees. Action plans also must be clear about employees' roles. Table 26 shows an example of practical application:

At Level 2 intensity, your organization first would be expected to share safety information across all lines of business. This includes SPI action plans. The difficulty we've noted, however, is that each line of business may have different levels of expertise, influence and interest in your safety program.

Therefore, your outreach to individual lines of business likely will need to be tailored. For example, expanding the idea in Table 26, the SPI action plan would state, "Establish runway incursion awareness materials. Improve organizational awareness of material contents through recurrent training."

To fully execute this action plan, all the lines of business will need to be engaged. One of them would need to develop runway incursion awareness materials. Another would modify training plans to use those materials. Every contribution must be clearly defined and coordinated.

Like other safety activities and programs, the status of SPI action plans should be communicated regularly so that employees build continued confidence in their organization's safety program, and understand an SPI's added value. Throughout this process, employees should also be given the opportunity to provide constructive SPI action plan feedback.

Building Cross-Organizational Safety Teams

Safety teams are a valuable component of your safety program. They encourage employee engagement and their bottom-up awareness of key issues. Safety teams are one of the most effective ways to exchange safety information within your organization. Teams typically include representatives from each of your organization's major lines of business (such as flight operations, aircraft maintenance and ground operations). You'll typically expect them to meet on a regular schedule. During meetings, representatives often will discuss general safety performance and current safety needs.

Table 26— Example of Practical Application of an SPI: Runway Safety

Risk Category	Objective	Performance Metric Target or SPT	Action Plan
Runway safety	Reduce the number of runway incursions.	Reduce the number of serious runway incursions to 0.4 per million operations.	Establish runway incursion awareness materials. Improve organizational awareness of material contents through recurrent training.

SPI = safety performance indicator; SPT = safety performance target

Briefings can be derived from all available SDCPS sources (including public safety information, reportable occurrence data and safety program information).

At Level 2 intensity, your safety team meetings also will be a forum for brainstorming and sharing safety information in a just culture environment. Brainstorming, for example, could help you determine where new audits or investigations are needed. They help you closely monitor practices instead of relying on policies and standard operating procedures. Safety team meetings also serve as a forum for reviewing results from the risk mitigation plans already in place.

Airline Example — Large airlines often create a safety team for each operational unit. Each of the units may have a different set of safety metrics, safety performance indicators and priorities. The common objective among these teams is making measurable safety improvements to achieve their operational safety performance targets. Team members, individually and as a group, should discuss new hazards, review the effectiveness of mitigations in reducing risk and seek insights into regulatory compliance and safety culture.

Safety teams establish a strong framework to regularly share safety and risk information across lines of business. As your organization grows in size and complexity, the teams will serve as your main way to unite employees around their common cause.

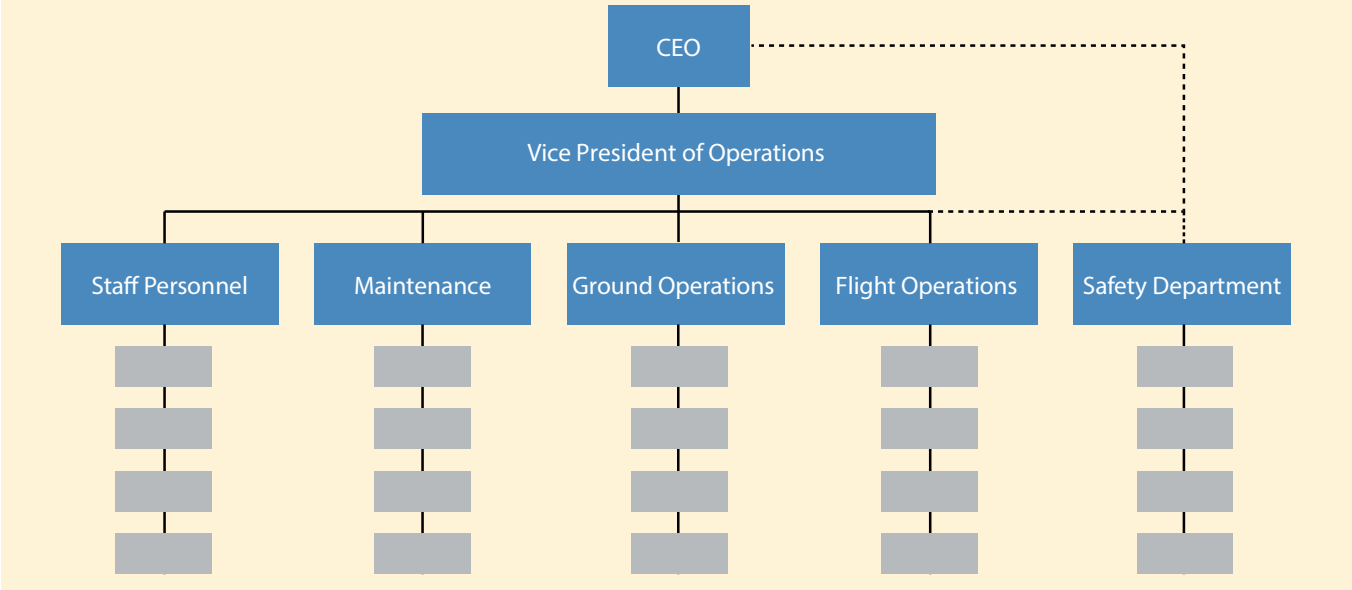
Establishing Safety Partnerships With CAAs

We highly encourage your organization to establish a safety partnership with your CAA and possibly other regulators. Historically, we've seen these relationships prove to be mutually beneficial. The intent is to provide the regulator with in-depth perspective of your routine operations and safety issues, and to build good faith that rarely makes punitive action necessary. The types of information often shared today include top-level organizational priorities, SPIs, SPTs, risks, operational issues and strategic safety opportunities.

In this kind of partner relationship, the parties essentially agree that their motivation to improve safety outweighs potential safety benefits of punitively addressing problems. That eliminates any need for punitive repercussions from routinely exposing operational errors or noncompliance to the regulator. Access to direct insights also positions your regulator to share information with you from different organizations experiencing issues similar to yours. From the regulator's standpoint, these relationships are beneficial because they can help to set and achieve broad safety goals with potential benefits for government and industry.

To initiate a safety partnership, we recommend inviting your regulator to participate in a routine event, such as a regularly scheduled internal safety team meeting, or signing a memorandum of understanding to develop the formal framework for the partnership. Further logistical steps you take to initiate the partnership will depend on a variety of factors, including the existing relationship between your organization and your regulator. Advance discussions on how the regulator intends to respond to the enhanced data view in these team meetings are important. A joint interpretation on what evidence requires immediate action may be a critical point for understanding before participating in these meetings.

Figure 6 — Sample Airline Organizational Chart by Lines of Business



Regardless of the initial method, we recommend focusing on the following areas:

- Providing your regulator with day-to-day insight into your routine operations and safety issues without fear of punitive consequences or repercussions;
- Developing a shared/common safety vision for your organization;
- Establishing a just culture for fairness between the participating organizations; and,
- Implementing clear boundaries between the expectations of your organization and those of your regulator in the partnership agreement.

Fostering and balancing this relationship positions both parties to advance their larger safety goals and helps both to elevate their SDCPS risk management capabilities to the next level of intensity.

Create a Plan for Success

In summary, we recommend the following actions as a starting point or checklist as you create or improve your plan for successful information sharing:

- ☐ Develop a management strategy for your internal safety program communications. The intent is to bridge the gap between your safety program and the lines of business across your organization (see "Managing Safety Stakeholder Perceptions," p. 21).
- ☐ Establish a strategy to share results from your automated/system-based data capture program. This strategy should help you manage employee perceptions and expectations (see "How to Build Trust in Automated/System-Based Data Capture Programs," p. 22).
- ☐ Identify opportunities to share safety analysis results and enable employees to provide regular feedback. To maximize the effectiveness of information sharing, we recommend that you address the minimum criteria in this toolkit (see "Sharing Event Data and Causal Factors," p. 22).
- ☐ Develop internal infrastructure to establish cross-organizational safety teams. These teams encourage bottom-up employee engagement and awareness of key safety issues (see "Building Cross-Organizational Safety Teams," p. 23).
- ☐ Establish a safety partnership with your regulator. These relationships have proven to be mutually beneficial for commercial aviation organizations as well as regulators (see "Establishing Safety Partnerships With CAAs," p. 24).

Information Protection

In this toolkit, the term *safety information protection (SIP) at GSIP Level 2 intensity* means that you and your organization focus on introducing or supporting laws, agreements, policies and practices that ICAO and Flight Safety Foundation recommend. We believe these measures enhance SIP and, in employee voluntary safety reporting programs, increase each participant's confidence and willingness to continue.

Level 1 intensity focuses on internal policy within organizations for information protection on voluntary programs. Level 2 intensity includes compliance with recommended policies and practices that extend protections by creating advance arrangements and by restricting the use of information obtained by a CAA's mandatory reporting system. We also urge states to extend protections within their jurisdiction by restricting the use of information published in final reports on aviation accidents, and through inter-state cooperation on protection of these final reports.

ICAO's Recommended Practices for Safety Information Protection

Let's begin with a main concept from ICAO Annex 19, *Safety Management*, which recommends that states and aviation organizations protect mandatory safety reporting systems and related sources; adjust applicable laws, regulations and policies to facilitate and promote voluntary reporting of safety information; and use advance arrangements for SIP.

ICAO Annex 13, *Aircraft Accident and Incident Investigation,* recommends that states determine whether additional records obtained or generated by their accident investigation authority (such as records in the U.S. National Transportation Safety Board's [NTSB's] public dockets) need to be protected. The annex also makes the following related recommendations:

- Only the accident investigation authority should retain copies of its records.
- Official participants (also called parties) in accident investigations should cooperate to determine the limitations on disclosure or use of information before information is exchanged.
- The authority should record the reasons for its determination of whether to protect or disclose these types of information.
- Authorities should take steps to limit the use of final reports of aviation accidents for a purpose other than the prevention of accidents and incidents.
- Laws on judicial procedures may not compel accident investigation personnel to give an opinion in court proceedings on matters of blame or liability for an aviation accident.

Advance Arrangements

Our second main concept deals with how to ensure that states apply ICAO's *principles of protection* and *principles of exception* as part of SIP, and do so in a comprehensive and consistent way. These principles should be applied whenever we disclose or share safety information. Advance arrangements between stakeholders, as noted, facilitate the parties' understanding of their rights and obligations to protect safety data and safety information.

Advance arrangements are valuable tools. They enable you to implement mechanisms and procedures to ensure that safety information will not be used for purposes other than safety.

Table 27 — Information Protection Level 2 Intensity Matrix

GSIP Toolkit Matrix	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.	Protection is formalized at the highest level between countries through memorandums of understanding or similar agreements.	TBD

TBD = to be determined

Advance arrangements increase your confidence and the confidence of other stakeholders. They ensure that entities responsible for collecting and sharing the safety information already have embraced SIP.

At the company level, you should formally create advance arrangements with appropriate levels of stakeholders, such as labor unions, third parties and CAAs. In one example of such advance arrangements — titled the *Memorandum of Understanding (MOU)* — entities sign the document to participate in the FAA Aviation Safety Action Program (ASAP), a government-industry partnership for nonpunitive handling of virtually all employee voluntary safety reports.

The MOU specifies which reports are covered under the program's nonpunitive provisions. The document explicitly states that ASAP reports will not be used to initiate or to support any company disciplinary action or used as evidence in FAA regulatory enforcement actions, subject to limited exceptions (such as criminal activity). Parties to an ASAP agreement include the aviation operator (or a government employer such as the FAA Air Traffic Organization), the FAA and the labor association of a specified employee group (such as airline pilots, air traffic controllers, flight attendants and maintenance technicians).

At the state level, inter-agency advance arrangements protect safety information shared within the government, including among agencies whose primary function is not aviation safety. ICAO specifically recommends that your state's CAA enter into advance arrangements with the government department, ministry or other entity responsible for the administration of justice.

The United Kingdom offers another example. The U.K. Air Accidents Investigation Branch (AAIB) agreed to several MOUs to ensure its independence and to protect safety information collected during accident investigations. One of these advance arrangements took effect in 2008, when the Crown Prosecution Service (CPS) entered into an MOU with the AAIB.

This MOU was designed to ensure effective investigations and maintain the independence of all parties, including a provision on confidentiality of information shared by the AAIB. This MOU provides for the sharing of evidence and information, specifically prohibiting the AAIB from disclosing a witness's confidential statement or declaration to "any other party, including the police and the CPS." The AAIB also agreed to advise the CPS of any evidence or information that cannot be disclosed without a court order.

In 2012, the AAIB signed an MOU with the Association of Chief Police Officers (ACPO) to comply with the requirements of European Union (EU) Regulation 996/2010. This MOU aims to maintain the independence of all parties and reinforce principles of cooperation. For example, the AAIB will advise the police if evidence suggests that a criminal act has been committed.

In 2013, the AAIB signed an MOU with the Coroner's Society of England and Wales. This document lays out the principles of cooperation and independence accepted by each party. The MOU stresses the importance of "trust and confidence" between the AAIB and witnesses, and the need to keep confidential the details of interviews, statements or declarations. Disclosure of such information can only occur if the AAIB and the coroner can maintain confidentiality, or if the coroner makes a request to the U.K. High Court.

In Australia, the Australian Transport Safety Bureau (ATSB) and the Civil Aviation Safety Authority (CASA) signed an MOU for cooperation between the two agencies for sharing and protection of safety information. Under this MOU, the ATSB and CASA disclose and use safety information in accordance with their *Safety Information Policy Statement.* The statement details the principles and limits on the use and sharing of safety information — particularly mandatory reports of safety occurrences — between the agencies.

Advance arrangements may be necessary for you to consider, especially if existing state laws, regulations or policies require — in typical circumstances unrelated to aviation situations — a high degree of government transparency and disclosure after public inquiries through *right-to-know* laws (also called *freedom of information* laws) or other constitutional requirements.

SIP Involving Mandatory Reporting Systems

Our main concept in this GSIP toolkit subsection is a recommendation to harmonize the level of SIP applied to your employees' voluntarily submitted safety reports with the level of SIP applied to safety data or safety information collected by your state's mandatory reporting systems. This extension of SIP may help protect information that is subject to right-to-know laws, as noted, or other rules that may result in the information being used for reasons other than aviation safety.

As an aviation service provider (such as an airline), functioning at Level 2 intensity, you already work to protect the information that you require employees to report for aviation safety purposes. That practice enhances employees' confidence that, with few exceptions, no report they submit will result in adverse employment actions. This is an example of applying the principle of protection and the principle of exception.

These principles should not interfere with your company's rights and obligations to take disciplinary action against an employee in cases in which specified facts and circumstances are involved. Typically, those facts and circumstances must indicate that the safety occurrence involved gross negligence,

willful misconduct or criminal activity. Moreover, your company also should comply with applicable privacy laws when disclosing or sharing the information, including de-identifying the information used.

At the state level, SIP similarly encourages and facilitates safety reports from aviation professionals under the CAA's mandatory reporting systems. Without adequate SIP, however, industry stakeholders may be conflicted or reluctant to comply with this system because they have ongoing concerns that the safety data or safety information they submit, including their identity, may be disclosed to the public under right-to-know laws.

In Australia, the mandatory reporting scheme under the Transport Safety Investigation Act 2003 (TSI Act) requires "responsible persons" — defined as including aircraft crewmembers, aircraft owners, aircraft operators, air traffic controllers, aircraft maintenance engineers and ground crew operators — to report aviation accidents and incidents to the ATSB.

The TSI Act provides protection for the mandatory reports. The ATSB also ensures that reports are used for safety purposes only and, when made available to the general public, are kept confidential through de-identification.

Similarly, the ATSB recognizes that CASA needs to access information from these mandatory reports. Therefore, the ATSB takes steps to keep confidential the sensitive information such as operators' names, aircraft registration numbers, and event times, dates and locations. Combining these steps with other authority to use safeguards such as protective orders, closed proceedings, in-camera review (that is, private review by judges or magistrates) and de-identification, the ATSB has been able to increase stakeholders' confidence in mandatory reporting systems, despite the risk of potential information use or disclosure for purposes other than aviation safety.

Accident Investigation Reports and Information

The next main concept in this Level 2 toolkit is how to use SIP to overcome possible reasons why aviation stakeholders could be reluctant to cooperate with accident investigation authorities. Essentially, we set rules or policies for the authority's internal and external handling of information derived from an accident investigation. They cover final reports and other related information shared among states by accident investigation personnel. The rules or policies then reassure the people who have accident information. They know their cooperation will not result in criminal, civil, administrative or disciplinary proceedings, unless warranted or determined appropriate after the administration of a *balancing test,* as briefly described in the following key recommendations.

Key Recommendations

ICAO recommends that states take the following actions to encourage aviation stakeholders (such as parties, witnesses and others who may be the only source of critical facts) to fully cooperate with accident investigators:

- Determine whether existing SIP extends to records obtained by or generated by accident investigation authorities, although these records are not required to be protected under Annex 13;
- Cooperate to determine the limitations on disclosure or use before exchanging the information;
- Record the reasons for the determination when administering the balancing test (in other words, require the appropriate authority [a judicial authority or a non-judicial authority with safety expertise] to state why the value of disclosing confidential safety information in the case at hand outweighs the likely adverse impact that the action will have on aviation safety);
- Make advance arrangements regarding state authorities' final reports on accident investigations to prevent the use of the final report as evidence to apportion blame or liability, but to allow the use of factual information from the investigation; and,
- Prevent the accident investigation personnel who testify from stating opinions — and prohibit any requirement that they state opinions — on matters of blame or liability in civil, criminal, administrative or disciplinary hearings.

At the company level, your accident investigation participants, such as witnesses or other employees providing technical expertise, should become familiar with the precedent of your state's competent authority. That authority is responsible for administering the state's balancing test and protecting against disclosures of information until the information is released by the accident investigation authority.

Specifically, as an investigation participant, you should become familiar with the available judicial procedures that impose safeguards for safety information. These may include the previously noted in-camera review or de-identification of records. Also become familiar with the state and federal law setting forth the elements of *torts* or the elements of crimes that may result in the disclosure of protected safety information and the use of that information for purposes other than aviation safety. (The term *tort* refers to a wrongful act or to an infringement of a right [excluding rights created under a contract] that leads to civil legal liability.)

At the state level, several countries — including Australia, France and the United Kingdom — have entered into MOU-type agreements to ensure cooperation and assistance between the

independent accident investigation authority (or CAA) in charge of the safety investigation of an aviation accident, and the authority in charge of the judicial investigation of the accident.

The pre-exchange cooperation and the pre-determination of protections that these authorities will apply in sharing information reassure witnesses and other involved aviation stakeholders that protected safety information will not be used in other jurisdictions for purposes other than aviation safety.

In 2011, the French Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA) signed a memorandum of agreement with NTSB to define cooperation between their respective countries for accident investigations. The agreement covers the treatment of protected safety information with the same rules of confidentiality as those to which the providing agency is itself bound.

Although both the NTSB and the BEA conduct safety investigations, the agreement emphasizes the need to keep confidential some specified sensitive information — such as data from cockpit voice recorders and cockpit image recorders, including readouts, examinations and analyses of their data.

Promoting a Just Culture

Eurocontrol, Europe's intergovernmental organization for the safety of air navigation, defines *just culture* as "a culture in which frontline operators and others are not punished for actions, omission 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."

When you and your organization adopt these recommended practices for GSIP Level 2 intensity in SIP at either the company level or the state level, you demonstrate a full commitment to aviation safety. Experience shows that, in joining other individuals and organizations that routinely share safety information, you'll develop increased trust in the reporting system and in the people collecting, analyzing and sharing their information.

At times, you'll need to re-evaluate the laws, regulations, policies and practices that underlie so many invaluable sources. Our attention to the details of SIP, in turn, builds our confidence that safety information will be protected. Any action or decision contrary to these protection principles should prompt us to continue pursuing changes to laws, regulations and policies.

Your Plan for Success

- ☐ Enter into advance arrangements with labor organizations, CAAs and other agencies and organizations that collect and share safety data and safety information (see "Advance Arrangements," p. 26).
- ☐ Ensure that formal cooperation exists between authorities in charge of the safety investigation and those in charge of the judicial investigation to protect sensitive safety data and safety information collected following an aviation accident or incident (see "Advance Arrangements," p. 26).
- ☐ Consider extending the protections found in voluntary safety reporting systems to also cover mandatory occurrence reporting systems. Applying the principles of protection and the principles of exception ensures that information is used for aviation safety without interfering with the proper administration of justice (see "SIP Involving Mandatory Reporting Systems," p. 27).
- ☐ Establish a precedent in your jurisdiction by introducing the administration of the balancing test. Also establish a framework of rules and policies to improve protection of aviation accident information (see "Accident Investigation Reports and Information," p. 28). The balancing test referred in level 1 may need to be broadened as Level 2 addresses enhanced data sources and mandatory reporting.
- ☐ Prevent the use of final reports of aviation accidents to assign blame or liability in criminal, civil, administrative or disciplinary proceedings (see "Accident Investigation Reports and Information, Key Recommendations," p. 28).
- ☐ Adjust laws, regulations, policies and practices to ensure that just culture prevails and influences how you protect aviation safety information (see "Promoting a Just Culture," p. 29).