Safety Evolution Guide: Safety reporting, investigation and improvement

Evolution Guide based on an SMS practice that has been recognised as Optimised by the CANSO Safety Standing Committee

1. OBJECTIVE OF GUIDE

Members of the Civil Air Navigation Services Organisation (CANSO) are committed to the improvement of their services. As part of this commitment, organisations share their practices in efforts to transfer learning across the industry.

This guide captures:

- the practices of an Air Navigation Service Provider (ANSP) in one element of the CANSO Standard of Excellence (SoE) in Safety Management Systems (SMS). The practices of this ANSP have been recognized by their peers as being an optimised practice within the industry (see Figure 1).
- the optimized practices have been selected on the basis of their novelty, innovation or the recognition of their potential to manage operational risks; or
- proposed practices that are based on contemporary thinking in the safety management sphere. These proposals have yet to be fully adopted by any ANSP, but they are viewed by the CANSO Safety Standing Committee (SSC) as having significant potential in the industry's efforts to evolve how safety is managed.

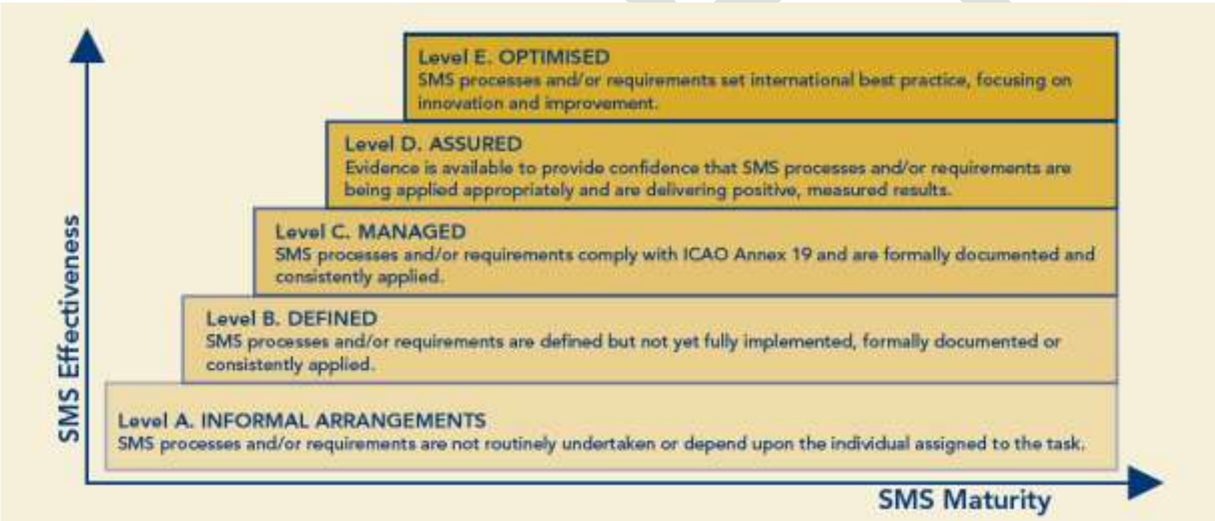


Figure 1. CANSO Standard of Excellence – Maturity Pathway

Given the dynamic nature of safety management, the practices presented in this document may be superseded. CANSO will publish updated best practice guidance.

2. APPLICATION OF THE GUIDANCE

CANSO recognizes that this guidance will not be relevant to all ANSPs. The maturity of any ANSP's Safety Management System will be dependent on their specific context. This context will be a reflection of factors including the size and complexity of the organisation, domestic regulations and the risk appetite of the organisation.

ANSPs do not necessarily need to adopt all the practices and processes promoted by CANSO, but consider the relevance of the practices promoted in this guide to their operational environment.

3. OPTIMISED PRACTICE

This guide addresses an SMS process that was identified in 2017 as being optimised. It details how one ANSP, Airservices Australia, designed and implemented a safety intelligence framework to improve safety reporting and analysis. The approach was reviewed by a panel of experts from the Future Safety Working Group of the SSC. The approach meets the CANSO standards for Safety Reporting, Investigation, and Improvement (see below).

4. SCOPE OF GUIDE

This guide provides insight into how Airservices Australia (Airservices) integrated a safety intelligence framework; embedding the use of Threat and Error Management (TEM) and the Eurocontrol Risk Analysis Tool (RAT) to improve safety reporting and analysis. This guide outlines the approach taken in establishing the framework, the benefits achieved, as well as lessons learnt during implementation.

5. APPLICABLE STANDARDS

CANSO Standard of Excellence in Safety Management Systems

11. Safety Reporting, Investigation and Improvement

Objective	Informal Arrangements	Defined	Managed	Assured	Optimised
11.1 A continuing organisation-wide process to report and investigate safety occurrences and risks.	There is an informal system in place for reporting safety occurrences, but reports are not reviewed systematically. The reporting system is not organisation-wide. Investigation is done on an *ad hoc* basis and with little or no feedback.	The reporting system is widespread but does not yet cover the whole organisation. Feedback is given on *ad hoc* basis. There is a plan to formalise the existing reporting and investigation system. There is commitment from management to allocate resources to implement this system.	The system in place is commensurate with the size of the organisation *The organisation has a complete and formal system that records all reported information relevant to the SMS, including incidents and accidents.* Corrective and preventive actions are taken in response to event analysis.	Identified safety-related risks and deficiencies are actively and continuously monitored and reviewed for improvement.	Personnel who report safety occurrences, risks and problems are empowered to suggest corrective actions, and there is a feedback process in place.

Figure 2. Extract from CANSO Standard of Excellence in Safety Management Systems

6. ORGANISATIONAL CONTEXT

In 2016, Airservices integrated TEM as part of a safety intelligence framework to improve the organisations understanding of system safety, operational risk management, and human performance.

Prior to implementation, Airservices already had experience with the TEM model as part of completing biennial Normal Operating Safety Surveys (NOSS). The NOSS is an approach utilised by a growing number of ANSPs, which seeks to observe everyday operations; capturing the relevant threats and errors that controllers manage during normal operations. The safety intelligence framework sought to expand the use of TEM throughout Airservices, embedding an expanded version of TEM as the overarching model governing all operational safety reporting and analysis within Air Traffic Services (ATS). The key components of the Airservices safety intelligence framework detailed within this guide include:

- the expanded TEM model;
- the TEM taxonomy;
- integration of TEM and the RAT within safety reporting systems;
- end-to-end management of occurrences; and
- training & guidance materials.

7. SAFETY INTELLIGENCE FRAMEWORK

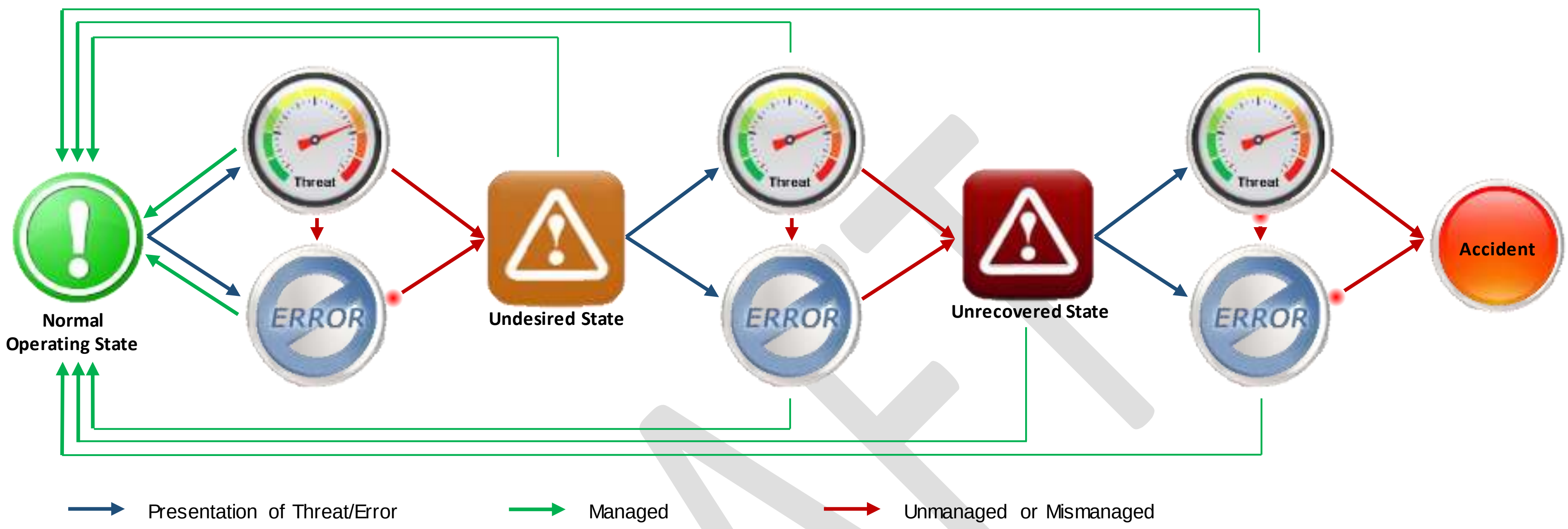
7.1. THREAT AND ERROR MANAGEMENT

TEM is a proven model within aviation, designed to better identify system and human contributors to the management of risk and shown over time to resonate with front line operational staff. TEM focuses on both the operational environment, as well as the individuals and teams discharging operational duties within that operational context.

The key components of the TEM model are threats and errors, and ultimately how these are managed to prevent undesired operating states. The expanded model implemented by Airservices further breaks down these states into undesired and unrecovered states. These components are detailed and defined in**Error! Reference source not found.**.

At its core, TEM recognises that errors and threats are an everyday part of ATS operations that need to be effectively managed by air traffic controllers in order to maintain the system within the normal operating state. To support the controller to manage these risks, a suite of controls are in place such as ATS alerting systems, airspace route structures, as well as controller training and experience.

The model depicted in Figure 3 shows how the threats and errors inherent to the normal operating state, if not effectively managed, can lead to an undesired state. In turn, undesired states present their own unique threats and errors, which must be managed effectively in order to return to the normal operating state. If these threats and errors are unmanaged or mismanaged then the system may progress to the unrecovered state, from which the threats and errors must be effectively managed in order to prevent the system progressing to a state where an accident may occur.



Threat

An event that occurs beyond the influence of the operator, increases operational complexity, and which must be managed to maintain safety.

Threats manifest as circumstances with the potential to adversely impact the integrity of controls that are in place to manage operational risk, such as:

- Exceeding a control's design limits (e.g. excessive traffic)
- Latent defects within a control (e.g. a software defect)
- Factors that increase the likelihood of potential impacts affecting controls (e.g. fatigue)
- Errors by other controllers (e.g. incomplete or incorrect coordination)

Error

An action or inaction by the operator that leads to deviation from organisational or operator intentions or expectations.

Errors manifest as the incorrect operational execution of controls that are in place to manage operational risk, such as:

- Non-execution of a control (e.g. not using a handover checklist)
- Incorrect execution of a control (e.g. entering an incorrect cleared flight level value)

Undesired State

An operational condition with the potential to reduce the margins of safety.

The point at which there is a loss of acceptable active control of operational risk (e.g. a loss of separation assurance).

Represents the failure of the suite of preventive controls to assure the safe management of operations

Unrecovered State

An operational condition in which the margins of safety have been compromised.

The point at which the acceptable margins of safety have been breached (e.g. a loss of separation).

Represents a failure of the suite of recovery controls to return an Undesired State to a situation in which operational risk is acceptable and actively managed. This failure may be due to the Undesired State not being detected or an ineffective recovery control.

Figure 3. Airservices Threat and Error Management model

7.2. BARRIER MONITORING

Within each state a suite of controls, or barriers, support the controller to maintain or return to the normal operating state by continually managing active threats and minimising the likelihood and impact of errors. Unfortunately, these barriers are not perfect, they rely on technical systems, procedures and human performance. The failure of one or more controls within these barriers may result in the threats and errors presented being unmanaged or mismanaged and the progression of the system to the next state within the model.

The type and purpose of the barriers that are designed into the system and applied by the controller differ depending on which state within the model they are employed:

- **Preventive** barriers are employed in managing the threats and errors associated with the normal operating state (i.e. to prevent progression to the undesired state);
- **Recovery** barriers are employed in managing the threats and errors associated with the undesired state (i.e. to recover from the undesired state and return to the normal operating state); and
- **Mitigation** barriers are employed in managing the threats and errors associated with the unrecovered state (i.e. to mitigate the impact of the unrecovered state and return to the normal operating state).

7.3. OCCURRENCE REPORTING

Within Airservices ATS occurrence reporting system, along with traditional occurrence data, additional TEM data reported includes:

- threats that presented to the controller(s) that contributed to the occurrence;
- errors committed by the controller(s) that contributed to the occurrence;
- failed controls, and the associated barrier, that contributed to the occurrence; and
- controls, and the associated barrier, that successfully operated to contain the occurrence and return to the normal operating state.

7.4. APPLIED EXAMPLES

Example 1 – A controller may be presented with a threat of two aircraft with similar call signs entering the same airspace. The controller may use effective communication and confirm accurate read backs, as part of the preventive barrier, to prevent this threat resulting in an undesired state (*Figure 4*).

Figure 4. Normal operating state example

In this example, there was no occurrence requiring reporting, this was simply a case of threat management within the normal operating state (i.e. the preventive barrier operating effectively).

Example 2 – Further to example 1, if the application of preventive controls fails (e.g. an incorrect read back was missed), the similar call sign threat resulted in an error and led to the undesired state of separation no longer being actively assured (due to call sign confusion) (*Figure 5*).

Figure 5. Undesired state example, part 1

Whether the undesired state is recovered from, to return to the normal operating state, or progresses on to an unrecovered state depends on how well the controller manages the undesired state. The controller may regain their situation awareness by applying the control within the recovery barrier of scanning, returning to the normal operating state (with the threat still present) (*Figure 6*).

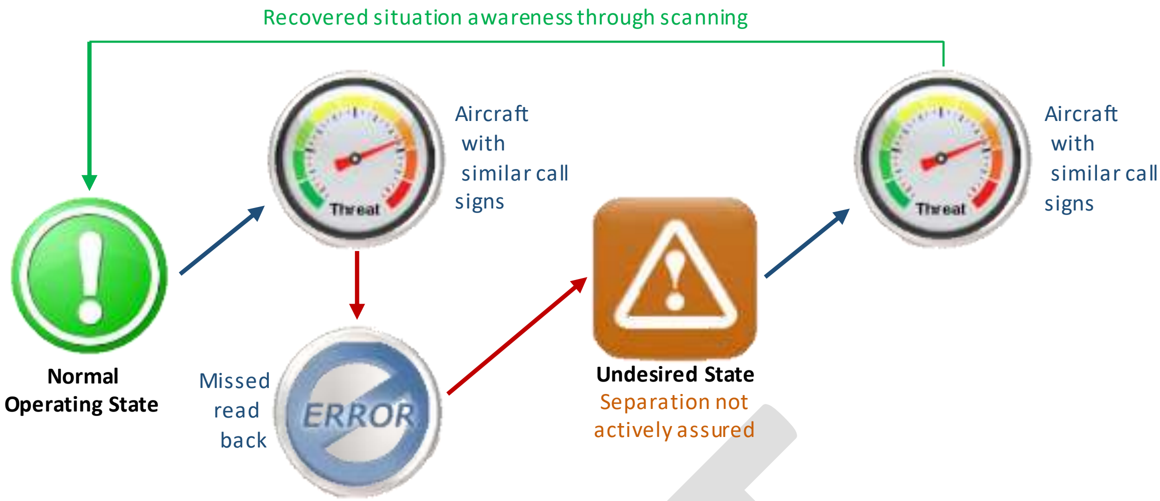


Figure 6. Undesired state example, part 2

In this example, an occurrence of the undesired state is reported along with:

- contributing threat(s): Aircraft with similar call signs
- contributing error(s): Missed read back
- control(s) that failed: Hear back / read back
  - barrier: Preventive
- control(s) that contained the occurrence: ATS action (scanning)
  - barrier: Recovery

Example 3 – In this scenario, if the controller is unable to regain their situation awareness, they may issue an instruction to an incorrect aircraft, possibly resulting in an unrecovered state of a loss of separation. At this point, controls within the mitigation barriers such as safety-net alerting may be triggered assisting the controller to act to mitigate the reduction in safety margin, restoring the normal operating state (Figure 7).

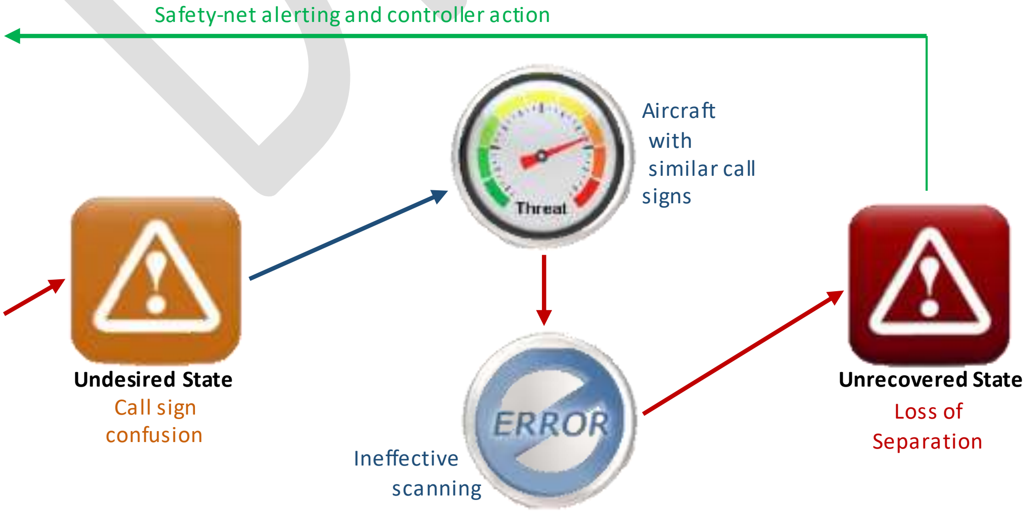


Figure 7. Unrecovered state example

In this case, an occurrence of the unrecovered state is reported along with:

- contributing threat(s): Aircraft with similar call signs
- contributing error(s): Missed read back; Ineffective scanning
- controls(s) that failed: Hear back / read back; ATS action (scanning)
    - barrier(s): Preventive; Recovery
- control(s) that contained the occurrence: Safety-net alerting
    - barrier(s): Mitigation

8. FRAMEWORK IMPLEMENTATION

In implementing TEM for ATS operations shown in Figure 3, Airservices sought to model how threats and errors are managed within a given operational context. Expanding on the data collected during biennial NOSS surveys, Airservices sought to incorporate this TEM model throughout the wider ATS safety reporting systems; capturing the threat and error data as part of each safety occurrence reported. By embedding TEM as a key facet within all ATS safety reporting, Airservices sought to:

- Provide a safety analysis framework to improve the organisation's collective understanding of system and human contributors to the management of risk;
- Support the use of a common language across processes and applications throughout ATS; and
- Enhance the quality and depth of safety data maintained by Airservices - supporting improved safety reporting, analyses, and investigation.

8.1. TEM TAXONOMY

A key component underpinning Airservices' implementation of TEM into safety reporting was the development of a comprehensive taxonomy including all threats and errors relevant to ATS. This taxonomy provides reporters with a consistent reference point to appropriately capture the relevant threats applicable to the operational context associated with a particular occurrence, as well as identify any applicable errors that contributed to the undesired or unrecovered state.

In developing this taxonomy, Airservices was able to draw on extensive experience with TEM (via NOSS and other programs) to integrate a detailed threat and error listing into the safety reporting system. The high-level threat and error categories are detailed in

Table 1 below, with more specific threats and errors able to be selected within each category. This detailed taxonomy of over 200 threats and errors is a key factor in ensuring there are valid and reliable data underpinning the TEM model. The use of these terms is further supported through a formal safety intelligence framework taxonomy, which provides a single-source of truth for the interpretation and application of the TEM model.

Table 1. Threat and error categories

Threats	Errors
Airspace (5) and Aerodrome (11)	Communication (23)
ARFF / Ground Operator Threats (7)	Procedural (48)
Communication – Pilot (17)	Position Relief / Handover-Takeover (10)
Equipment and Systems (18)	
External ANSP Threat (inc. Military) (1)	
General Traffic Characteristics (12)	
Operational Demand (13)	
Other Airservices Controller (16)	
Pilot / Aircraft Performance (27)	
Weather (7)	
Workspace (Operational Context) (3)	

In addition to these categories, a category of *Other* for threats or errors can also be selected within each safety occurrence, which further prompts users to enter additional information about the relevant category. This information can then be periodically reviewed in order to determine whether additional threat or error types need to be considered or whether particular definitions need to be further updated.

8.2. TEM INTEGRATION

To ensure the TEM model was effectively implemented into all aspects of safety reporting, it was important to ensure users were equipped with the relevant support tools necessary. Rather than collecting TEM data via a separate independent mechanism, the collection of TEM data was integrated into Airservices existing safety reporting systems (namely the Corporate Integrated Reporting and Risk Information System - CIRRIS). In addition to capturing traditional safety occurrences data (i.e. occurrence type, description, aircraft details etc.) reporters are able to capture the relevant threat and error information for each applicable occurrence. Even in scenarios where there is no ATS attributable error or contribution to the occurrence, the reporter is able to capture key information about the relevant threats, selected from the categories outlined in

Table 1, to provide a more detailed picture of the operational context.

There are multiple benefits to embedding TEM into existing safety reporting mechanisms. Firstly, it allows controllers to utilise the existing safety reporting support tools they are already familiar with; minimising the time and effort required to capture data as well as working in conjunction with Airservices' existing strong reporting culture. It also serves to further embed the TEM mind set throughout occurrence reporting; whereby occurrence details and descriptions are naturally framed within the TEM model.

To further aid effective data capture, additional upgrades were also made to the CIRRIS system to ensure the threat and error categories outlined in

Table 1 are able to be easily filtered depending on the occurrence type selected. Additional links to training and guidance material referenced below is also easily accessible from within the CIRRIS interface.

8.3. RISK ANALYSIS TOOL INTEGRATION

The RAT was developed by Eurocontrol as a methodology for classification of the risk associated with air traffic management safety occurrences. Along with TEM, the RAT has been integrated into Airservices' safety reporting system with the TEM taxonomy mapped to the controllability and repeatability factors within the RAT.

This integration of TEM and RAT, and within the existing safety reporting system, allows for improved efficiency in analysis the risk bearing of occurrences and utilising these analyses within safety reporting and assurance determination and prioritisation.

9. OCCURRENCE MANAGEMENT OVERVIEW

While Airservices' approach was recognised for the way that both TEM and RAT had been integrated, an overview of the entire end-to-end occurrence management process is presented below, demonstrating how TEM and RAT are implemented in each phase of the process. The steps in the process are presented in Figure 8.

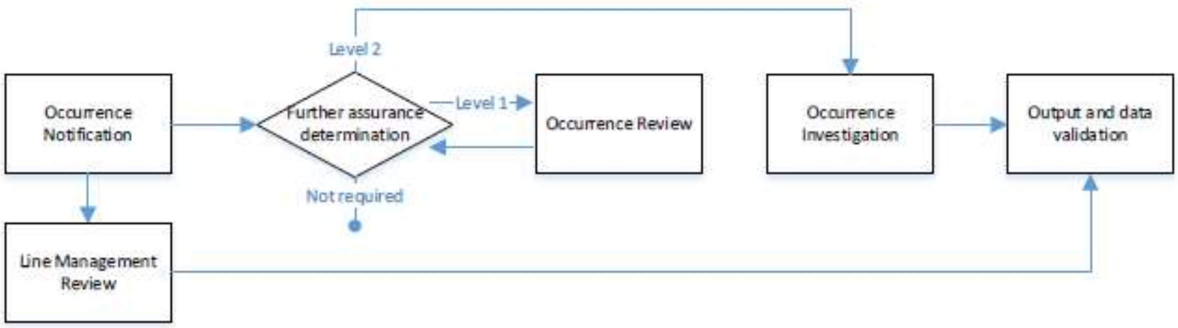


Figure 8. Occurrence management process

Occurrence Notification: Those submitting an initial occurrence report within CIRRIS are required to provide information on the 'what', 'where', 'when' and parties involved in the occurrence, along with their assessment of threats, errors, control failures, controls that identified the occurrence, and as such the barrier that contained the occurrence. Such reporting must be completed by the end of the shift in which the occurrence happened.

Thirty-five occurrence categories ranging from circumstances where an information error has been made (e.g. ATC said FL370 when the clearance was to FL390) to Accidents are recognised within the system. Weather, ATIS information, details from the Australian Aircraft Register, flight plan among other information sources that relate to the occurrence are automatically uploaded into CIRRIS. Dependent on the type of occurrence being reported, elements of the RAT will also be populated by the reporter.

Post notification processing: All occurrences and technical system failures are automatically emailed to relevant managers, and requirements for immediate notification of significant occurrences to external agencies are enacted. Senior managers receive text messaging when more serious events occur. This practice ensures visibility of events and means that any immediate necessary action can be taken.

Line Management must review each less significant occurrence within 72 hours to ensure the accuracy of reporting ahead of reports being emailed directly to the Australian Transport Safety Bureau (the investigatory agency) and the applicable airlines, aerodromes, flying schools etc. whose operations were impacted.

Assurance Determination: All occurrences are reviewed within the first 24 hours by the Occurrence Safety Assurance Panel (OSAP), a cross service and group decision making body, who use investigation commencement criteria, which include consideration of TEM and RAT data, as a guide to determining the level of further review/investigation that is warranted and whether the investigation should be independent of the service delivery group.

Occurrence Review: Reviews are always required for certain occurrence types and demand that additional information is entered into CIRRIS to facilitate trend monitoring. Those completing a review must also attach a completed document that presents factual information and analysis that support their coding of the occurrence.

Investigation: Similar investigation protocols are used regardless of whether a first or second level assurance investigation is being undertaken. Airservices has adopted a three line of defence model in its assurance activities, details of this governance model can be found in the public domain, with the foci of lines one and two in relation to investigations discussed in Table 2.

Table 2. Assurance delivery focus and provision

Assurance Level	First Line of Defence (Level 1)	Second Line of Defence (Level 2)
Focus	Defined processes have been effectively applied by staff	Systems are fit for purpose, current risk controls are effective and regulatory obligations were met
Assurance Provider	Service Delivery Group	Party independent of service delivery.

The investigation builds on the information that the reporter provided, supplementing and providing more detail as to:

- why the threats and errors occurred and were or weren't appropriately managed;
- how risk controls performed;
- how our barriers worked to constrain the incident trajectory; and
- validation and confirmation of entries that support the RAT assessment.

As an investigation proceeds, managers of the investigatory areas may determine that the type of assurance being delivered is inappropriate for the occurrence, and the group undertaking the investigation may change. Core data collection, investigatory techniques and report templates allow this to occur with ease and standardise how information is fed back to the accountable manager, involved staff and, when the report is finalised, the wider organisation.

Data Validation: before a record can be closed, the data is verified to ensure that all relevant fields are completed.

10. TRAINING & GUIDANCE MATERIAL

As with any Safety Management System change, ensuring that key stakeholders are actively engaged throughout the change process is critical to success. This was an important component of ensuring TEM was fully embraced as the overarching model governing operational safety reporting and analysis within ATS. While ATS staff already maintained a level of understanding and experience with TEM as part of conducting NOSS surveys, it was important to extend and expand this understanding across the organisation.

A communication strategy and awareness campaign was developed to distribute information and guidance on how TEM would be incorporated into Airservices' safety reporting and data management systems. This included a series of videos distributed throughout the organisation outlining the benefits of the safety intelligence framework, TEM, and how TEM data captured within CIRRIS can be utilised by Airservices and the broader aviation industry.

Additional modules were also added to the existing CIRRIS ATS Occurrences online training program - a mandatory program for all staff responsible for entering ATS safety occurrences. These training modules detailed the safety intelligence framework taxonomy as well as relevant worked occurrence examples; outlining the relevant threats and errors that should be captured. Additional supporting guidelines also included a series of help cards for both reporters of occurrence and supervisors reviewing occurrences.

Additional specific online training courses are continuing to be developed and implemented for ATS operational staff. Current TEM online training courses include modules exploring:

- cognitive processing in ATS;
- effective scanning; and
- operations below Lowest Safe Altitude

11. CONTINUAL IMPROVEMENT

Since TEM was formally implemented into Airservices safety reporting, it has become a central component of the Airservices Safety Management System. TEM has provided a common safety language throughout ATS and improved the organisation's understanding of the complex interplay between system and human performance factors and how they contribute to safety.

Capturing TEM data within safety reporting has also served to improve safety performance analysis. Data is now available to analyse occurrence trends based not only on occurrence type or location, but the specific threats and errors managed during the occurrence. Importantly, this has also provided more detailed information regarding the effectiveness of preventive and recovery controls involved in managing threats and errors back to a normal operating state. Crucially as the Airservices TEM database continues to grow, the potential for more complex modelling and statistical analysis is significant; further enhancing Airservices understanding of the operational environment.

Moving forward, Airservices will continue to evolve and expand the use of TEM as the overarching safety analysis framework. Key future activities include:

- continuing to improve the integration between TEM occurrence reporting, investigations and operational risk management;
- analysis of TEM occurrence data in concert with data collected as part of ongoing safety surveys – in particular the NOSS;
- utilisation of TEM data to support more in depth safety analysis and investigations; including analysis of the effectiveness of existing controls, as well as proposed future controls; and
- further embedding the TEM framework within initial controller training and education; shifting controller understanding of TEM from an implicit awareness to a more explicit recognition of their role as proactive threat and error managers.

11.1. LESSONS LEARNT

Throughout the implementation of Airservices' safety intelligence framework, the following lessons have been learnt:

- *Training and awareness programs:* The major benefits of capturing TEM data within safety occurrences can only be achieved if the data collected is valid and reliable. It is worth noting that during implementation Airservices did not mandate the input of TEM data as part reporting safety occurrences. While this serves to minimise reporting times for frontline ATS personnel and helps maintain Airservices' strong reporting culture, it means that communication and training programs are critical to ensure consistent occurrence data entry is maintained across the business. While significant TEM data continues to be captured within safety reporting, there remains scope to improve the consistency and quality of TEM data recorded. For this reason, training and awareness programs should not be considered as initial activities to be completed during implementation, but seen as ongoing requirements necessary to support the continued integration of TEM.

- *Feedback to frontline operators:* Capturing TEM data provides a wealth of information to support more detailed safety performance analysis. For Airservices, it is typically the frontline ATS staff that are responsible for capturing this data and as such, it is important to ensure that the value of this data collection is fed back to those frontline staff. Not only does this serve to encourage continued data collection, but also helps to further embed the TEM context relevant to a particular airspace sector or tower location.

- *Simple & Intuitive TEM Taxonomy:* Maintaining a centralised taxonomy is recognised as a central tenant to the successful implementation of TEM within occurrence reporting. However, it is also critical that this taxonomy is readily accessible and embedded within occurrence reporting tools to support the ease, quality, and consistency of reporting by frontline staff. While steps have already been taken to ensure TEM reporting is supported through CIRRIS, this is an ongoing process with further improvements underway to help simplify the TEM taxonomy within the reporting processes and make it more intuitive for reporters to capture data.

12. SUMMARY

This guide provides an example of how one ANSP has sought to improve safety reporting and analysis through the integration of TEM within safety reporting, investigation and improvement.

Like all safety management practices, approaches to safety reporting must be tailored to the specific operations and requirements of the ANSP and the program outlined within this guide may not be appropriate for all ANSPs. This guide seeks to provide practical guidance and lessons learnt for ANSPs seeking to improve their safety reporting systems.

The primary keys to the success of this program were the adaptation of a recognised model for threat and error management, active use of effective training and communication strategies as well as the provision of appropriate tools to support efficient capture of TEM and RAT data as part of existing safety reporting processes.