Organización de Aviación Civil Internacional
Oficina Regional Sudamericana
Reunión Virtual con los Directores de Aviación Civil de la Región Sudamericana
(Lima, Perú, abril 2020)

GUÍA DE PLANIFICACIÓN DE RESPUESTA ANTE EMERGENCIAS DE CANSO

(Preparada por CANSO)

RESUMEN

Esta nota presenta información sobre la "Guía de planificación de respuesta ante emergencias", elaborada y recientemente actualizada por CANSO, para difundir mejores prácticas sobre planificación y respuesta a emergencias que pudieran afectar a los ANSPs, en el contexto de la presente situación sanitaria global.

1. INTRODUCCIÓN

1.1 El Grupo de trabajo sobre seguridad cibernética de CANSO ha revisado la Guía de planificación de respuesta ante emergencias de CANSO, que reúne las mejores prácticas, conocimientos y experiencia relacionados con los planes y procedimientos de contingencia de los ANSPs a nivel global. Ver la precitada Guía (en idioma inglés solamente) en el Apéndice a esta Nota.

2. EXPOSICIÓN

2.1 La Guía de planificación de respuesta ante emergencias ayuda a los ANSPs a desarrollar un plan formal de respuesta a emergencias, de forma que se documente la transición ordenada y eficiente de las operaciones normales a las de emergencia y el regreso a las operaciones normales.

2.2 Esta versión actualizada, que compartimos con la reunión, contiene información sobre la gestión de incidentes de seguridad cibernética (por ejemplo, traspaso de sistemas críticos con posibilidad de propagación, bloqueo de GPS, cibersecuestro de datos - ransomware, malware), incluido el desarrollo, la capacitación y la práctica de procedimientos de emergencia / contingencia y el análisis forense digital.

2.3 La Guía tiene en cuenta los principios de la Guía de evaluación de riesgos y seguridad cibernética de CANSO y las partes del Anexo 17 de la OACI, salvaguarda de la seguridad de la aviación civil, relacionadas con la seguridad cibernética.

3. ACCIÓN SUGERIDA

3.1 Se sugiere a la Reunión virtual de Directores Generales de Aviación Civil de los Estados SAM tomar nota de la información presentada por CANSO.

canso
civil air navigation services organisation

CANSO Emergency Response Planning Guide

Acknowledgements

This publication was produced and updated by the CANSO Cyber Safety Task Force of the Civil Air Navigation Services Organisation (CANSO) Safety Standing Committee.

We particularly thank the following organisations which contributed an enormous amount of time and effort, without which this document would not have been possible.

- Avinor Flysikring AS
- Civil Aviation Authority of Singapore (CAAS)
- Aeronautical Radio of Thailand (AEROTHAI)
- Helios
- NATS
- EUROCONTROL

Contents

1. Introduction

Aviation provides a safe, reliable infrastructure to move passengers and cargo around the world. The benefits of this infrastructure are open to billions of people, connecting us more than ever before and boosting the global economy. When there are disruptions to air traffic services and related supporting services, whether the situation stems from a disruption of air traffic services or an aircraft emergency, it has a tremendous impact. Therefore, it is critical that every air navigation service provider (ANSP) is able to ensure emergency response plans are in place to quickly restore air transport services after an emergency.

The Civil Air Navigation Services Organisation (CANSO) has produced the *CANSO Emergency Response Planning Guide* to bring together best practices, knowledge and experience related to contingency plans and procedures from ANSPs around the world. This Guide helps ANSPs develop a formal emergency response plan that documents the orderly and efficient transition from normal to emergency operations and return to normal operations.

2. Context

The material found in this Guide is taken from the *CANSO Standard of Excellence in Safety Management Systems* (SoE in SMS) and the related *CANSO Safety Management Systems Implementation Guide* (Version 2.1). The Standard provides a framework for the implementation and continuous improvement of safety management systems within ANSPs that:

- Exceeds the existing domestic and international regulatory framework
- Allows each ANSP to build a safety management system appropriate to its size and operational complexity
- Captures and shares the knowledge of ANSPs with mature safety management systems already fully integrated into their operations

The Standard is aligned with International Civil Aviation Organization (ICAO) Annex 19, Safety Management. It emphasises a phased implementation of a safety management system (SMS), allowing the ANSP to move through five levels of maturity, from an initial, 'Informal' level to an advanced, 'Optimised' level. The five levels of maturity as they pertain to emergency response plans, and the outcomes expected for each level, are addressed on page 4.

This Guide has also taken into account principles from the *CANSO Cyber Security and Risk Assessment Guide* and the parts of ICAO Annex 17, security safeguarding civil aviation, related to cyber security.

This Guide is designed to help ANSPs in the earlier maturity phases develop these formal plans and procedures. As an ANSP matures, the objectives for emergency planning will increase. This Guide addresses outcomes for the first three phases of SMS maturity, from 'Informal' to 'Defined' to 'Managed'.

3. Objective

The *CANSO Emergency Response Planning Guide* aims to provide CANSO Members with guidance that:

- Transfers learning across the industry and builds a consistent approach to ANSP safety management practices across the globe
- Allows ANSPs to plan for a comprehensive and coordinated emergency response at the corporate, group and project levels, assuring that risks to operational service delivery are reduced to 'as low as reasonably practicable' (ALARP) levels
- Is aligned to the CANSO SoE in SMS
- Is aligned with the *ICAO Global Risk Context Statement* (RCS)

4. Guide Status

This Guide does not supersede either domestic or international regulations or regulatory guidance on SMS implementation. It draws on the experience of CANSO Members and aims to complement and supplement existing guidance. CANSO recommends the use of this guidance, but application is not binding.

5. Related Industry Guidance

This Guide provides an ANSP perspective on emergency response planning. Additional industry perspectives are available from CANSO partner organisations:

- *International Air Transport Association Emergency Response Best Practices Handbook:* www.iata.org/publications/pages/index.aspx
- *Airports Council International Emergency Preparedness and Contingency Planning Handbook:* www.aci.aero/Publications/New-Releases/Emergency-Preparedness-and-Contingency-Planning-Handbook-First-Edition-2014
- *EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services (including Service Continuity):* www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-guidelines-contingency-planning-ans-2009.pdf

6. Coordination Of Emergency Response Planning

6.1. Outcomes by Level

The following objectives for each of the five maturity levels are taken from the *CANSO Standard of Excellence in Safety Management Systems*.

Objective	Informal	Defined	Managed	Assured	Optimised
4.1 Emergency response procedures and an emergency response plan that documents the orderly and efficient transition from normal to emergency operations and return to normal operations.	The organisation has sound primary air traffic management systems but does not have redundant capabilities or back-up systems.	There are procedures and some redundant capabilities and resources to cope with abnormal and unexpected situations.	All primary systems have redundant capabilities, and emergency response procedures have been developed, documented and distributed to appropriate staff. The emergency response plan is properly coordinated with the emergency response plans of those organisations it must inter- face with during the provision of its services. (Annex 11 – 1.4)	Primary air traffic management systems are reliable and have redundant capabilities and back-up systems. The emergency response plan and procedures have been rehearsed through desktop or operational exercises.	The emergency response planning processes and emergency procedures and plans are regularly exercised and revised to keep them up- to-date.
Outcomes	No emergency response planning has been carried out. No planned redundant capabilities exist.	The primary risks to the organisation from abnormal and unexpected situations have been analysed. Emergency response procedures are documented for the most likely abnormal situations. Redundant capabilities are in place for high-risk functions.	Redundant capabilities are in place for all primary systems. Emergency response procedures have been published. An emergency response plan has been published. The emergency response plan has been coordinated with interfacing organisations.	Redundant capabilities and back-up systems exist for all primary systems. The schedule for rehearsal of the emergency response plan and procedures has been determined.	The schedule for regularly reviewing the organisation's key risks has been determined. Regular lessons learned exercises are conducted on the effectiveness of the emergency response plan.

Figure 1: Coordination of Emergency Response Plan from the *CANSO Standard of Excellence in Safety Management Systems*

7. Objectives

It is essential that an organisation has a clear set of actions understood by all relevant personnel in the event of an emergency. This document provides guidance on both emergency procedures and creating and maintaining emergency response plans.

With a cyber-related incident, a digital forensics capability is necessary to understand the nature and extent of the compromise, particularly with sophisticated cyber attacks. Such a capability may also be needed to successfully recover and/or support any post-incident investigation and prosecution. Digital forensics is a highly technical skill, such that an ANSP may need to establish a third-party contract prior to any incident.

7.1. Emergency Response Overview

ICAO Annex 11, Air Traffic Services, Chapter 2.30 (Amendment 46) states, inter alia, that "air traffic services authorities shall develop and promulgate contingency plans for implementation in the event of disruption, or potential disruption, of air traffic services and related supporting services in the airspace for which they are responsible for the provision of such services."

8. Emergency/Contingency Procedures

Organisations should develop emergency/contingency procedures to help maintain the safety of operations during system failures or other abnormal or unexpected situations. The emergency/contingency procedures should be based on when situations occur rather than if they occur. This will ensure that the procedures are not based on previous experience within the organisation but covers the whole threat picture.

It is essential to recognise that reacting to these kinds of failures without a plan of action is likely to result in a significant increase in risk to the organisation. Even with defined and documented procedures, the level of risk is likely to increase during such abnormal or unexpected situations as:

- Losses of major air traffic systems (e.g., communications, surveillance, flight data)
- Losses or failures in support facilities (e.g., power, air conditioning, building integrity)
- Aircraft emergencies (e.g., emergency descent, hijack, air defence security)
- Disruption of air traffic services (e.g., bomb threat or other action requiring evacuation of the operations room, emergency dispersal of traffic, closure of an adjacent air traffic centre)
- Closure or zero flow rating of traffic in national airspace as a result of adverse environmental conditions (e.g., hurricane, typhoon, volcanic activity)
- Cyber security incidents (e.g. breach of less critical systems with the possibility of propagation, GPS jamming, ransomware, malware)
  - Incident containment/quarantine: In the event of a cyber-incident, the emergency response plan should detail how best to contain that type of incident in order to minimise its impact. This is likely to include turning off communication links with non-essential services and/or third parties.
- Pandemic (e.g. spread of virus disease)

It is advisable for ANSPs to develop, document, train and practice emergency/contingency procedures for the safe handling of these types of failures.

Figure 2 provides guidance on assessing emergency scenarios.

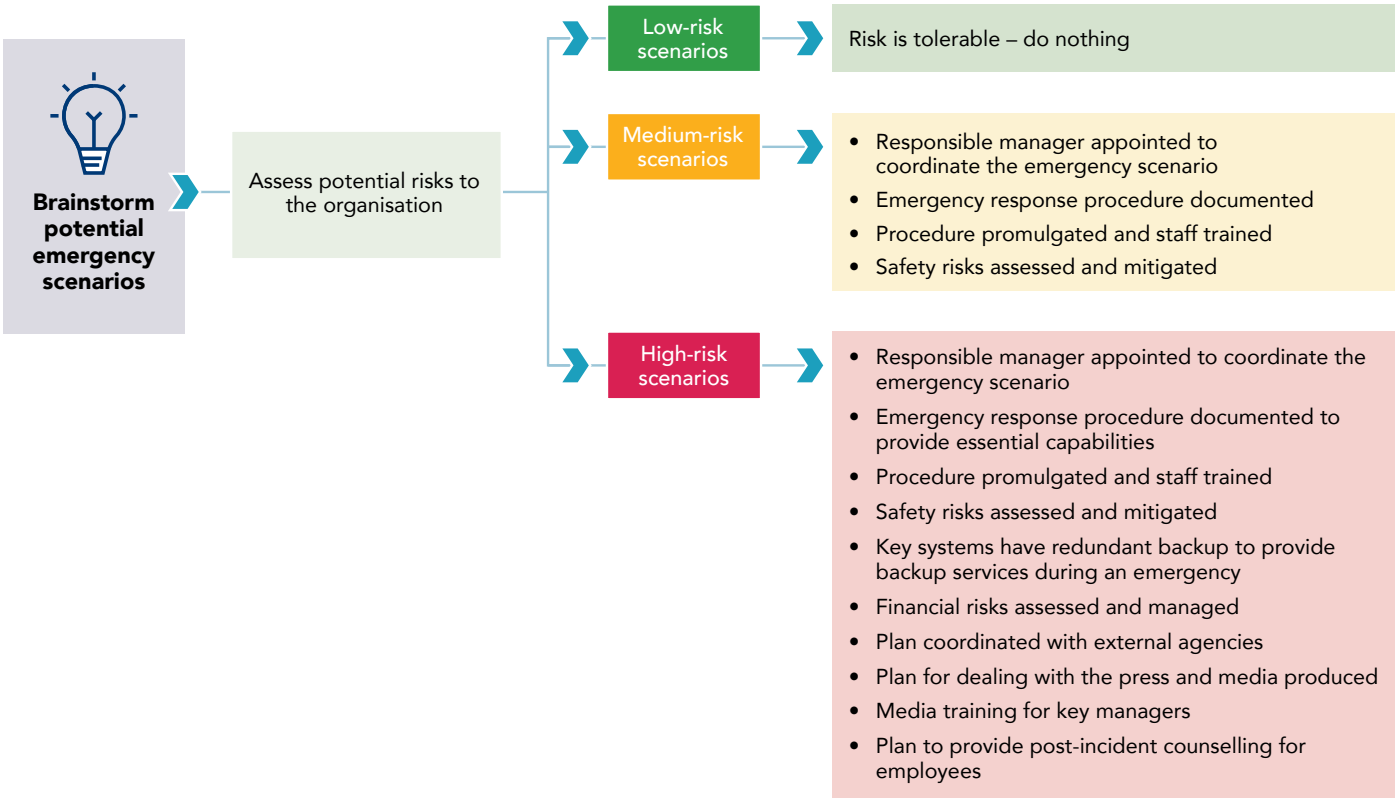

Figure 2: Assessing Emergency Scenario

In the context of ICAO obligations, contingencies can be organised along a "contingency lifecycle" (see Figure 2) composed of the following phases:

- Normal operations
- Emergency situations
- Degraded modes of operation
- Service continuity
- Recovery to normal operations
- Back to normal operations

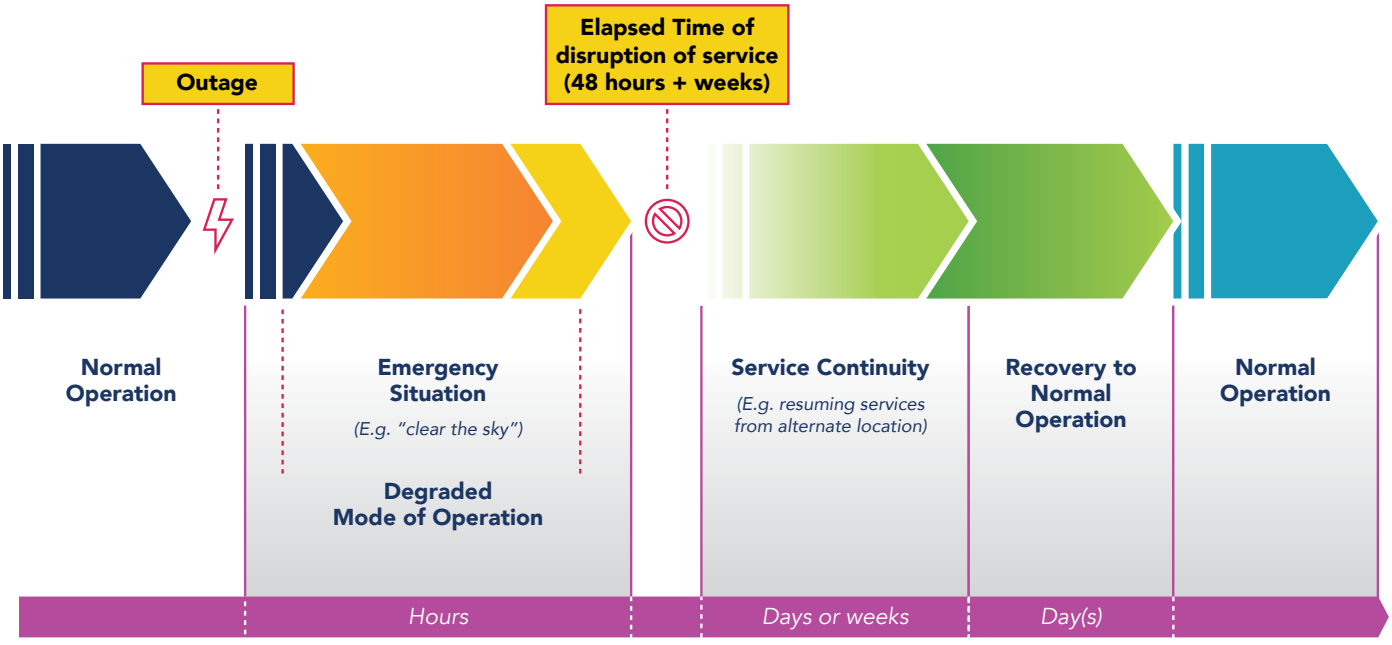

Figure 3: Generic Contingency Lifecycle

In figure 3, the durations of the various phases shown are not necessarily representative of the length of those phases; durations will differ from one event and environment to another. The lifecycle illustration should also not necessarily be understood as a strict sequence of modes of operation. For instance, depending on the cause/type of disruption:

- A system (technology, people and procedures) working in normal operations can evolve directly into an emergency situation.
- A system can deteriorate into a degraded mode of operation that further deteriorates into an emergency situation.
- An emergency situation can be followed by a service continuity mode of operation.
- In some situations, it might be necessary to move straight from normal operations into a service continuity mode of operation.
- An emergency situation can start when all parts of the functional system (technology, people and procedures) are working but the integrity of the data cannot be guaranteed.
- The outage may lead to a disruption of days or weeks.

In addition, it is desirable for primary air traffic systems to have back-up or redundant capabilities. This can be achieved by:

- Engineering a high-integrity system in a main and standby redundant configuration. In these circumstances, common-cause failures (where the standby system fails at the same time and from the same cause as the main system) are a major problem and are difficult to design out.
- Providing a high-integrity architecture using several lower-integrity systems on different operational platforms. This methodology is typically employed in the aircraft industry. It may appear to be more expensive upon first inspection, but it is likely to be cheaper in the long run.
- Ensuring geographical separation of critical physical infrastructure so that power outrage and tele-communication line failure is less likely to affect the entire delivery of ATS. Geographical separation also complicates malicious acts (e.g. terror) intended to take out the ATS function.

Chapter 9 of the *CANSO Safety Management System Implementation Guide* provides additional guidance on various risk mitigation and management strategies.

Note that a cyber-incident might lead to particular challenges when it comes to proving that the system, network and/or wider infrastructure is “clean” (i.e. no longer compromised) as some cyber-threats are highly persistent and a high level of safety assurance evidence will be needed before operations can resume.

8.1. Development and Assurance

The techniques used to develop and assure emergency/contingency procedures are similar to those used to develop standard operating procedures. Figure 3 shows a process that organisations may follow to develop, document, train and assure a set of emergency response procedures.

For emergency procedures, it is advisable to establish an ongoing programme of desktop reviews, table top exercises or simulations to assure that everyone involved understands what is required of them. It is also advisable to run a full-scale simulation for major incident procedures to help identify potential shortcomings. In combination, these simulations provide assurance that the procedures are fit for their intended purpose and will help to restore safe air traffic services. Below are some examples of scenarios that can be include as annual table top exercises or as full-scale simulations.

- Contamination of airspace
- Pandemic
- Total loss of critical ATM system
- Partial loss of critical ATM system
- Mid-air collision
- Drone incidents
- Distribution of security sensitive information (e.g. information marked CONFIDENTIAL or SECRET)
- GPS jamming
- Malicious act (Insider, bomb threat, hijack, cyber security)

It is important that the whole organisation is prepared to act according to emergency/contingency procedures (e.g. ATCOs, ATSEPs, HR, IT, PR, safety, security, management). As such the scope of the exercises and simulations should over a period of time cover all relevant areas and representative risk/threats to the organisation.

Once documented, emergency procedures must be readily available at operational units and other relevant parts of the organisations so that they can easily access them in stressful situations. If these procedures are documented in a larger manual for example, it is less likely that they will be consulted in an emergency.

It is important that no matter the emergency, procedures are available in situations with no access to ATM systems, internet, mobile network etc. This can be done by printing hardcopies or using platforms that work independently (e.g. tablet). This is to ensure that the response is resilient to loss of communications as attacking communications infrastructure in parallel is a good way of aggravating a cyber-incident.

9. Emergency Response Plan

Emergency response plans assist ANSPs in providing for the safe and orderly flow of air traffic in the event of disruptions to air traffic services and related supporting services. They are aimed at preserving the availability of major air routes within the air transportation system where ANSPs are designated to provide services, and to assure access to designated aerodromes for humanitarian reasons. An ANSP, like any organisation supporting flight operations, should have an emergency response plan to complement its contingency procedures.

An emergency response plan:

- Provides for the orderly and efficient transition from normal to emergency/contingency operations and the subsequent return to normal operations
- Must be properly coordinated with the emergency response plans of those organisations that it must interface with during the provision of its services (see page 9 below)
- Outlines what actions should be taken following an accident and who is responsible for each action

An emergency response plan may address procedures for avoiding airspace; current and alternative routes; simplified route networks; procedures to cope with degraded navigational capability; and/or procedures to cope with degraded communications or surveillance capability. Appendix B of the *ICAO Safety Management Manual* provides detailed guidance concerning the specific areas that should be included in an emergency response plan:

- Governing policies
- Affected organisations
- Notifications
- Initial response
- Additional assistance
- Crisis management centres
- Records
- Accident sites
- News media
- Formal investigations
- Family assistance
- Post–critical incident stress counselling
- Post-occurrence reviews

Training and exercises are necessary to assure that capabilities match the plan and to reveal any gaps or deficiencies. The plan should be assigned an owner within the organisation, and the owner should regularly review the plan to assure that employees are aware of and trained on the actions to take in the event of an emergency. An organisation may have one or more response plans that cover specific areas such as cyber-incident, degraded equipment, natural disasters etc. These plans should be aligned to reflect the overall principles in the emergency response procedure.

10. Coordination

Since disruptions in one portion of airspace affect adjacent areas, it is advisable to develop an emergency response plan in conjunction with other agencies, such as airlines, airport operators, police, military entities, security services, CERT (cyber incidents), regulators and the State (see Figure 4). In addition to containing individual emergency response plans, the SMS manual of each organisation should outline the coordination of these plans across the industry during emergency situations. When international coordination is required, it is the responsibility of ICAO to facilitate or initiate the necessary coordination, while international organisations such as the International Air Transport Association (IATA). EUROCONTROL and the International Federation of Airline Pilots' Associations (IFALPA) serve as valuable advisors.

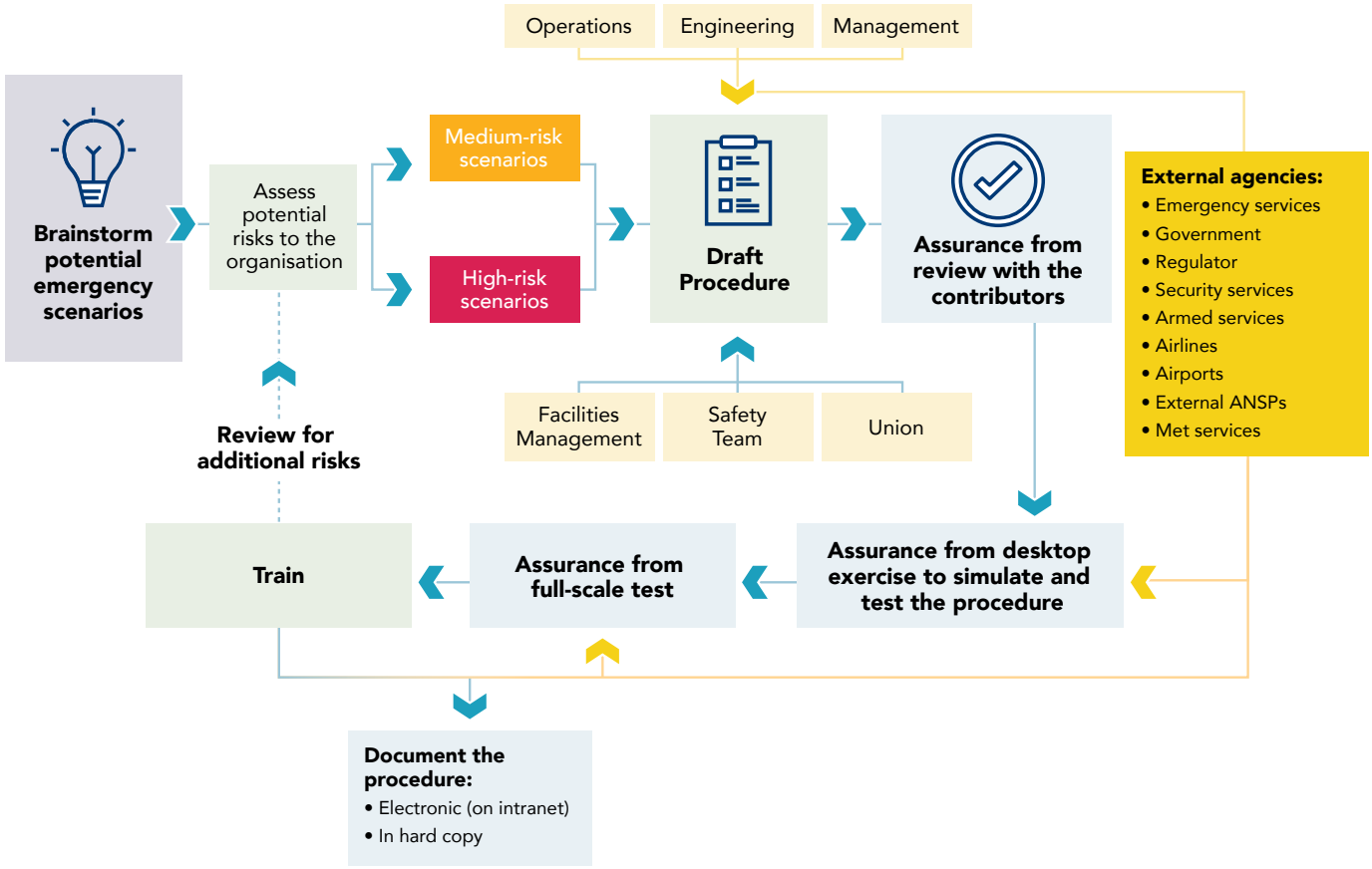

Figure 4: Emergency Response Plan Coordination

11. Occurrence Response Hierarchy

Some organisations provide a hierarchy for response during a safety occurrence, such as the following command structure:

11.1. Strategic

The strategic staff is in overall control of the organisation's resources at the incident. The staff remains away from the scene of the incident and formulates the strategy for dealing with the emergency. If the strategic staff members for various organisations are not co-located at an incident, they will remain in contact with one another via other communication methods. For the purposes of this guide, the strategic staff is likely to be the head of the organisation and other top management.

11.2. Tactical

The tactical staff is the tactical level who manages the strategic direction set out by the strategic staff and consequently converts it to actions completed by the operational team. Tactical staff should be located away from the immediate scene of the incident and work closely with tactical staff from other agencies. They will not become directly involved in dealing with the incident itself. For the purposes of this guide, the tactical staff is likely to be the manager directly in charge of an operational air traffic service unit or level 3 managers at the area affected by the incident.

11.3. Operational

The operational staff directly controls the organisation's resources at the incident and will be found with his/her staff working at the scene. If an incident is geographically widespread, different operational level managers may assume responsibility for different locations. If the incident is of a complex nature, as is often the case, operational managers are given individual tasks or responsibilities at an incident. For the purposes of this guide, the operational manager is likely to be the operational manager dealing with the air traffic or engineering incident.

For strategic and tactical levels there should be an appointed 'lead' of staff. For the purpose of this guide, the 'lead' of the strategic level is likely to be head of the organisation and for the tactical level it is likely to be crisis incident manager on duty or relevant level 3 manager.

12. Lessons Learned

Below are some lessons learned by ANSPs pertaining to coordination of emergency response planning.

1. Assure that there is a manager responsible for the coordination of emergency response planning, and that the manager has the resources and seniority necessary to create, test and, where necessary, put into practice the emergency response plan.
2. A dedicated meeting room to coordinate the emergency response plan, with plentiful telephone, internet and video conference facilities, will help to move the focus of senior managers and the press away from the operations room, and will allow operational staff to manage air traffic services without interference.
3. A conference call facility with 100 or more lines proves highly valuable when managing a large-scale emergency. The ability for the moderator to mute all incoming lines can also prove invaluable when managing a large telephone conference.
4. It is essential to have sufficient staff to manage an emergency that might last for several days. This means establishing a shift system and an effective hand-off process. On-call arrangements for the staff involved are also essential. Operational staff must be supported by senior managers, lawyers, media specialists and safety professionals.
5. With a view to possible litigation, it is important to maintain a log of events and decisions made throughout the emergency and recovery processes.
6. If the emergency involves fatalities, it may be necessary to move air traffic control staff to a safe house for their protection for the duration of the emergency.
7. Critical Incident Staff Management processes may help to speed the recovery of any staff involved in the emergency.
8. It is essential to coordinate plans with external emergency services and to establish how to control access to operational sites that may be surrounded by the media.
9. For large-scale emergencies, media training for senior staff is essential to assure that the appropriate messages are delivered to a news-hungry public. Organisational internet and social media sites can also provide effective distribution of internal information.
10. It is essential to have a room approved for managing security restricted information – both verbal exchange of security restricted information and storage of such information.
11. It is essential to have appointed stakeholder roles such as head of external communications (media), CISO (Chief Information Security Officer) and Head of Human Resources as part of the core team when managing emergency situations.

Visit us:
canso.org