

POLITECNICO DI TORINO

Dipartimento di Ingegneria Meccanica e Aerospaziale

Corso di laurea di II Livello in Ingegneria Aerospaziale



Introduzione del Safety Management System nelle aziende CAMO

Relatore
Prof. Paolo Maggiore

Candidato
Martina Valle

Indice:

1	EVOLUZIONE DEL CONCETTO DI SAFETY	8
2	SAFETY MANAGEMENT	10
2.1	INTRODUZIONE AL SAFETY MANAGEMENT SYSTEM	10
2.2	SAFETY MANAGEMENT STRATEGIES	11
2.3	SYSTEM DESCRIPTION.....	14
2.4	GAP ANALYSIS.....	14
2.5	PIANO DI IMPLEMENTAZIONE	15
3	STRUMENTI NECESSARI PER LA GESTIONE DELLA SAFETY	16
3.1	HAZARDS.....	16
3.2	CONCETTI FONDAMENTALI DEL PROCESSO DI HAZARD IDENTIFICATION	17
3.2.1	UNDERSTANDING HAZARDS	17
3.2.2	HAZARD IDENTIFICATION	17
3.2.3	HAZARD ANALYSIS	18
3.2.4	DOCUMENTATION OF HAZARDS	18
3.3	SAFETY RISKS	20
3.3.1	SAFETY RISK MANAGEMENT	20
3.3.2	SAFETY RISK PROBABILITY	22
3.3.3	SAFETY RISK SEVERITY	23
3.3.4	SAFETY RISK TOLERABILITY	24
3.3.5	SAFETY RISK CONTROL/MITIGATION	25
4	ROOT CAUSE ANALYSIS.....	28
5	ICAO ANNESSO 19	29
6	INTRODUZIONE SMS NELLE AZIENDE CAMO.....	30
7	SISTEMA DI GESTIONE	32
7.1	ORGANISATION AND ACCOUNTABILITIES	35
7.1.1	ACCOUNTABLE MANAGER.....	35
7.1.2	SAFETY MANAGER	37
7.1.3	COMPLIANCE MONITORING MANAGER.....	38
7.1.4	SAFETY REVIEW BOARD	39
7.1.5	SAFETY ACTION GROUP	39
7.2	SAFETY POLICY AND OBJECTIVES.....	40
7.2.1	SAFETY POLICY	40

7.2.2	SAFETY OBJECTIVES	41
7.3	SAFETY MANAGEMENT KEY PROCESSES	42
7.3.1	HAZARD IDENTIFICATION PROCESSES.....	42
7.3.2	RISK MANAGEMENT PROCESSES.....	43
7.3.3	INTERNAL INVESTIGATION	44
7.3.4	SAFETY PERFORMANCE MONITORING AND MEASUREMENT.....	44
7.3.5	MANAGEMENT OF CHANGE	45
7.3.6	CONTINUOUS IMPROVEMENT	46
7.3.7	IMMEDIATE SAFETY ACTION AND COORDINATION WITH THE OPERATOR'S EMERGENCY RESPONSE PLAN (ERP).....	47
7.4	SAFETY PROMOTION	47
7.4.1	SAFETY TRAINING	48
7.4.2	SAFETY COMMUNICATION	50
7.5	MANAGEMENT SYSTEM DOCUMENTATION	51
7.5.1	CONTINUING AIRWORTHINESS MANAGEMENT EXPOSITION (CAME).....	51
7.6	COMPLIANCE MONITORING.....	54
7.6.1	COMPLIANCE MONITORING FUNCTION.....	54
7.6.2	COMPLIANCE MONITORING.....	54
7.6.3	INDEPENDENT AUDIT	55
7.6.4	FEEDBACK SYSTEM	55
8	SISTEMA INTERNO DI SEGNALAZIONE IN MATERIA DI SICUREZZA	57
9	SEGNALAZIONE DI EVENTI.....	59
10	FRAMEWORK PER L'IMPLEMENTAZIONE DEL SMS	62
10.1	SAFETY POLICY AND OBJECTIVES.....	63
10.1.1	MANAGEMENT COMMITMENT	63
10.1.2	SAFETY ACCOUNTABILITIES AND RESPONSABILITIES	64
10.1.3	APPOINTMENT OF KEY SAFETY PERSONNEL	64
10.1.4	COORDINATION OF EMERGENCY RESPONCE PLANNING (ERP)	64
10.1.5	SMS DOCUMENTATION	65
10.2	SAFETY RISK MANAGEMENT	66
10.2.1	HAZARD IDENTIFICATION	66
10.2.2	RISK ASSESTMENT AND MITIGATION	66
10.3	SAFETY ASSURANCE.....	67
10.3.1	SAFETY PERFORMANCE MONITORING AND MEASUREMENT.....	67
10.3.2	THE MANAGEMENT OF CHANGE.....	68

10.3.3	CONTINUOUS IMPROVEMENT OF THE SMS.....	68
10.4	SAFETY PROMOTION	69
10.4.1	TRAINING AND EDUCATION	69
10.4.2	SAFETY COMMUNICATION	69
11	PIANO DI IMPLEMENTAZIONE DEL SMS.....	70
11.1	FASE 1: PLANNING SMS IMPLEMENTATION.....	71
11.2	FASE 2: REACTIVE SAFETY MANAGEMENT PROCESSES.....	73
11.3	FASE 3: PROACTIVE AND PREDICTIVE SAFETY MANAGEMENT PROCESSES.....	75
11.4	FASE 4: OPERATIONAL SAFETY ASSURANCE.....	76
12	ESEMPIO: IDENTIFICAZIONE E ANALISI DEI RISCHI.....	78
13	REFERENZE BIBLIOGRAFICHE.....	80

Indice delle figure:

Figura 1 Evoluzione del concetto di safety	8
Figura 2 Safety Management Strategies	12
Figura 3 Safety Management Levels.....	13
Figura 4 Processo di documentazione degli hazard	19
Figura 5 Safety Risk Management Process	20
Figura 6 Safety Risk Probability Table.....	22
Figura 7 Safety Risk Severity Table	23
Figura 8 Safety Risk Assessment Matrix	24
Figura 9 Safety Risk Tolerability Matrix	25
Figura 10 Processo di mitigazione del rischio.....	26
Figura 11 Safety Risk Management	27
Figura 12 Training	50
Figura 13 Continuing Airworthiness Management Exposition.....	54
Figura 14 SMS Implementation-Phase Approach.....	71
Figura 15 Matrice di rischio	78

RINGRAZIAMENTI

Ringrazio coloro che mi hanno seguita durante il tirocinio presso Oxygen Labs, in particolare Enrico Foresto, per il suo supporto formativo.

Ringrazio il mio relatore Prof. Paolo Maggiore.

INTRODUZIONE

L'obiettivo di questo lavoro è quello di supportare l'implementazione del Safety Management System nelle aziende CAMO secondo *Il Regolamento (UE) 2019/1383*, che modifica e rettifica il *Regolamento (UE) n. 1321/2014* per quanto riguarda i sistemi di gestione della sicurezza nelle imprese di gestione del mantenimento dell'aeronavigabilità.

Il presente elaborato è suddiviso in due parti, la prima delle quali pone i concetti che troveranno applicazione nella parte successiva.

La prima parte, partendo dall'evoluzione del concetto di safety, introduce al Safety Management System. Vengono quindi presentati gli strumenti necessari per la gestione della sicurezza all'interno delle organizzazioni, i processi di Hazard Identification e Safety Risk Management e una classe di metodi che portano all'individuazione delle cause ultime responsabili dell'evento indesiderato.

La seconda parte è dedicata ad affrontare la gestione della compliance per l'implementazione del SMS nelle aziende CAMO.

PARTE 1

1 EVOLUZIONE DEL CONCETTO DI SAFETY

Agli albori dell'aviazione, ovvero gli anni a cavallo della Seconda Guerra Mondiale fino agli anni '70, il concetto di safety si riferiva esclusivamente a fattori tecnici: si parla di "Technical Era". In questi anni infatti, la tecnologia non era ancora a un livello tale da supportare lo sviluppo dell'aviazione, che si prestava a diventare un mezzo di trasporto di massa. I guasti tecnici erano quindi la principale causa di incidenti aerei, a cui si cercava di far fronte tramite investigazioni e miglioramento tecnologico.

A partire dagli anni '70, si entra nella cosiddetta "Human Era": si cerca quindi di garantire la sicurezza spostando l'attenzione sulle performance umane, portando alla nascita del concetto degli Human Factors. Questo non permise però nel ventennio a seguire, durante la "Golden Era", di ottenere una riduzione degli incidenti in quanto ci si focalizzò solo ed esclusivamente sull'individuo, prestando poca attenzione all'interazione tra individuo e ambiente circostante in cui esso opera. Qualcosa cambiò soltanto entrando nella cosiddetta "Organisational era", negli anni '90, in cui la safety cominciò ad essere vista da una prospettiva sistemica, che abbracciava i fattori tecnici, umani ma anche i fattori organizzativi, che scaturiscono dall'interazione dell'uomo con l'ambiente circostante.

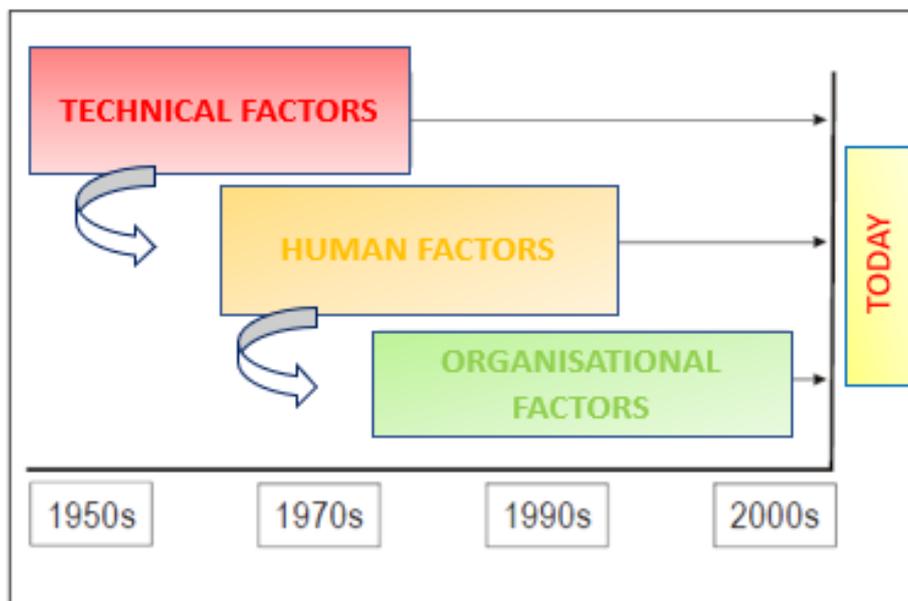


Figura 1 Evoluzione del concetto di safety

Oggi il concetto di safety viene inteso come il risultato della gestione dei processi organizzativi, il quale ha l'obiettivo di tenere sotto controllo le conseguenze dei fattori di rischio, i cosiddetti hazard.

Si giunge quindi alla seguente definizione di safety: condizione in cui la possibilità di danneggiare persone o equipaggiamenti viene ridotta e mantenuta al di sotto di un certo livello accettabile tramite il processo di Hazard Identification e Safety Risk Management.

2 SAFETY MANAGEMENT

Il Safety Management è una disciplina, basata sull'applicazione di tecniche di gestione sistematica, finalizzata all'identificazione e al controllo di eventi o condizioni indesiderate lungo tutto il ciclo di vita di un progetto, programma o attività. La prevenzione di eventi indesiderati può essere conseguita tramite l'identificazione, la valutazione, l'eliminazione o il controllo dei cosiddetti safety-related hazards fino a livelli considerati accettabili e controllabili.

2.1 INTRODUZIONE AL SAFETY MANAGEMENT SYSTEM

Per introdurre il concetto di SMS, si può utilizzare una metafora: si pensi a un contenitore, contenente tutti gli strumenti di cui l'organizzazione ha bisogno al fine di tenere sotto controllo le conseguenze dei safety-related hazards che possono nascere nel momento in cui l'organizzazione fornisce il proprio servizio. Il Safety Management System mira all'identificazione di quelle condizioni, eventi o circostanze che possono produrre o contribuire al verificarsi di un evento indesiderato con la conseguenza di ridurre la capacità di svolgere una determinata funzione. L'obiettivo del Safety Management System è quindi quello di garantire un continuo miglioramento del livello di safety di un'organizzazione.

In quanto tale consiste in un'attività non stop.

I due processi fondamentali del Safety Management sono:

- *Hazard Identification*
- *Safety Risk Management*

Il SMS non si limita a una specifica azione ma è indirizzato a tutte le attività svolte all'interno dell'organizzazione che portano con sé la possibilità di generare un hazard. Vengono incluse quindi manutenzione, operazioni, riparazioni, servizi di supporto, training e attività di controllo.

Il SMS deve essere appropriato alla dimensione e alla complessità dell'organizzazione.

Il Safety Management System deve essere:

1. *Sistematico*. Il SMS è sistematico in quanto le attività svolte rispecchiano un piano pre-determinato e applicato in modo coerente in tutta l'organizzazione. Come conseguenza della sua natura sistematica, il SMS mira a un miglioramento graduale ma costante del livello di safety e si focalizza sui processi più che sulle conseguenze.
2. *Proattivo*. Il SMS è proattivo in quanto si fonda su un approccio che enfatizza i processi di Hazard Identification e controllo e mitigazione del rischio, prima che l'evento indesiderato avvenga, anziché intraprendere azioni correttive una volta verificatosi l'evento. Questo è

reso possibile attraverso un continuo monitoraggio delle attività all'interno dell'organizzazione.

3. *Esplicito*. Tutte le attività che riguardano la gestione della safety vengono documentate.

L'implementazione di un SMS richiede il coinvolgimento dei più alti livelli gestionali al fine di perseguire un programma che assicuri:

- La definizione di una filosofia di gestione che riconosca sempre l'esistenza di potenziali criticità per la sicurezza, definisca gli standard organizzativi e confermi che la sicurezza è responsabilità di tutti.
- La determinazione di una strategia per il raggiungimento della sicurezza tramite l'identificazione di chiare responsabilità, ruoli e priorità aziendali.
- L'identificazione delle procedure da implementare dirette a tutto il personale, dei mezzi per pianificare, organizzare, monitorare e analizzare lo stato della sicurezza e i processi.
- Verifiche continue sulla realtà aziendale tramite adeguate ed efficaci procedure che valorizzino l'importanza di una cultura positiva della sicurezza e prevedano azioni correttive laddove vengono identificate eventuali criticità.

2.2 SAFETY MANAGEMENT STRATEGIES

Esistono tre tipologie di sistemi per la raccolta di dati sulla sicurezza: reattivi, proattivi e predittivi. Questi producono rispettivamente strategie di gestione della safety reattive, proattive e predittive e di conseguenza portano a metodi di mitigazione anch'essi reattivi, proattivi e predittivi.

- *Reattivi*. Questi metodi sono insufficienti per una gestione efficiente della safety in quanto permettono di intervenire dopo che l'incidente o l'evento che ha portato al degrado della safety ha già avuto modo di manifestarsi.
- *Proattivi*. Sono basati sul fatto che le failures possono essere minimizzate identificando un potenziale evento dannoso prima che esso si manifesti e prendendo le adeguate azioni di mitigazione per tenere sotto controllo tale rischio. In questo caso il processo di raccolta dei dati inizia non appena un evento, anche con conseguenze non dannose, si manifesta.
- *Predittivi*. Il processo di raccolta dati è un processo continuo che avviene in real time anche nel momento in cui nessun potenziale pericolo si manifesta. I processi predittivi si basano sul fatto che il processo di gestione della sicurezza viene migliorato cercando di trovare problemi e non solo aspettando che si quest'ultimi si presentino. Pertanto, i sistemi predittivi

di acquisizione dei dati di sicurezza cercano in modo continuativo informazioni sulla sicurezza che potrebbero essere indicative di rischi emergenti.

I sistemi di raccolta dati predittivi sono essenzialmente sistemi statistici, in cui una grande quantità di dati viene analizzata e combinata assieme a dati raccolti dai sistemi proattivi e reattivi. L'aggregazione di questi dati porta a un sistema completo che permette alle organizzazioni di minimizzare la probabilità che eventi indesiderati accadano e di mantenere alto il livello di gestione della sicurezza. Esempi di metodi predittivi sono: sistema di segnalazione dei pericoli, analisi dei dati di volo e monitoraggio delle operazioni.

Un sistema di gestione della sicurezza maturo necessita della combinazione di tutti questi sistemi di acquisizione di dati.



Figura 2 Safety Management Strategies

I metodi predittivi sono i più efficienti in quanto intervengono nella fase "infantile" degli hazard e non permettono quindi di sviluppare il loro potenziale dannoso. Le azioni di mitigazione sviluppate tramite questi sistemi di raccolta dei dati si trasformano in reti di contenimento o filtri di tale rigidità che bloccano totalmente il passaggio dei pericoli emergenti.

I metodi proattivi, anch'essi, operano nella fase iniziale degli hazard e per questo motivo anche questa strategia è molto efficiente. Nonostante ciò gli hazard hanno la possibilità di sviluppare il loro

potenziale dannoso. Per questo motivo, le mitigazioni sviluppate da dati proattivi sulla sicurezza si trasformano in reti di contenimento o filtri che, pur essendo stretti, consentono all' hazard di svilupparsi.

Per quanto riguarda invece l'approccio reattivo, questo permette ai rischi di continuare a sviluppare il loro potenziale dannoso. Le mitigazioni sviluppate tramite questo approccio di sicurezza reattiva si trasformano quindi in reti di contenimento o filtri a trama libera, che possono essere frequentemente penetrati dai pericoli. A un livello ancora più basso di sistema di raccolta reattiva dei dati, le investigazioni a seguito di incidenti funzionano in modo da riparare il danno ormai accaduto. Questo rende evidente l'inadeguatezza di questo approccio nel garantire un sistema efficiente di gestione della sicurezza all'interno delle organizzazioni.

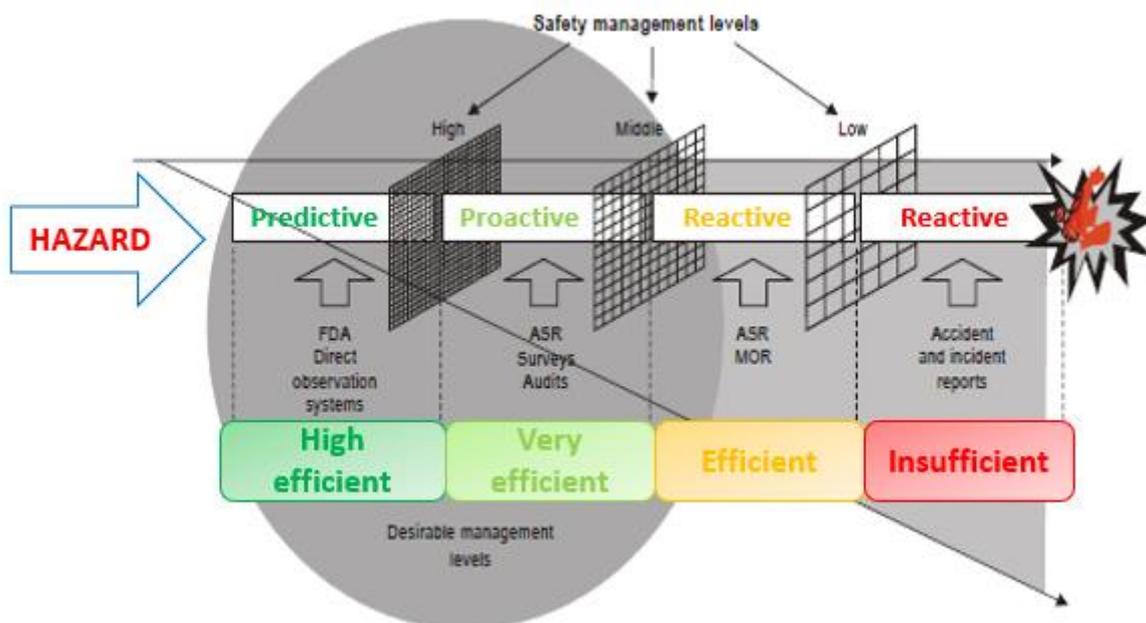


Figura 3 Safety Management Levels

2.3 SYSTEM DESCRIPTION

La descrizione del sistema è il primo passo nell'implementazione del SMS. Ogni sistema infatti, contiene una potenziale vulnerabilità per la sicurezza, quantificabile in termini di hazard. Molto spesso problemi legati alla sicurezza nascono da disallineamenti tra le interfacce tra il personale e i componenti del contesto operativo in cui le persone conducono le loro attività. Una conseguenza di questa interazione tra persone e componenti del sistema, è la nascita di potenziali hazard. Per questo motivo, i confini del sistema devono essere sufficientemente robusti per racchiudere tutti i possibili fattori di rischio che il sistema può generare. L'identificazione degli elementi dell'hazard e il loro controllo si basa su una dettagliata descrizione del sistema, che deve includere:

- Scopo del sistema.
- Modalità in cui il sistema viene utilizzato.
- Funzioni del sistema.
- Confini del sistema e interfacce esterne.
- Ambiente in cui il sistema opera.

Un modo spesso utilizzato per descrivere il sistema è il Modello Shell.

2.4 GAP ANALYSIS

Una volta che è completata la descrizione del sistema, si procede con la Gap Analysis. Quest'ultima ha un duplice obiettivo:

- Identificare eventuali disallineamenti (safety vulnerabilities) nelle interfacce tra i diversi componenti identificati durante il processo di descrizione del sistema.
- Identificare eventuali risorse aggiuntive che possono essere necessarie per definire e delineare i margini delle interfacce.

Dal punto di vista del SMS, la Gap Analysis è principalmente un'analisi delle strutture già esistenti all'interno dell'organizzazione, confrontate con quelle necessarie affinché il SMS funzioni in modo corretto. Questa analisi rileva le risorse, le strutture e le disposizioni esistenti nel sistema al fine di individuare le vulnerabilità, in termini di hazard, che derivano dall'interazione tra persone e componenti del sistema entro il quale svolgono le loro attività.

La gap analysis è quindi molto importante al fine di identificare risorse aggiuntive, strutture e disposizioni necessarie a mitigare queste vulnerabilità e aumentare la resistenza dell'organizzazione di fronte a un potenziale pericolo.

La domanda che guida questa analisi è la seguente: *“Il personale operativo è adeguatamente equipaggiato con le risorse necessarie per rendere fruibile il servizio?”* La risposta viene data sia in termini di sicurezza che di efficienza. Al fine di rispondere a questa domanda, è utile utilizzare il

Modello Shell. Una volta che questa analisi è terminata e completamente documentata, le strutture e le risorse mancanti che sono state identificate contribuiscono, assieme a quelle già esistenti, la base per l'implementazione del SMS.

2.5 PIANO DI IMPLEMENTAZIONE

Il piano di implementazione del SMS definisce l'approccio dell'organizzazione alla gestione della safety. In quanto tale, è una strategia realistica per l'implementazione di un SMS che soddisfa gli obiettivi di sicurezza dell'organizzazione, consentendo al contempo un'efficiente ed efficace fornitura del servizio. Descrive come un'organizzazione raggiungerà i suoi obiettivi di sicurezza aziendali e come soddisferà eventuali nuovi o revisionati requisiti di sicurezza, normativa o altro. Il piano di implementazione del SMS dettaglia le azioni che devono essere intraprese, fornisce informazioni su chi deve intraprenderle e fornisce informazioni sull'intervallo di tempo entro il quale queste azioni devono essere implementate in base alla dimensione dell'azienda e alla complessità delle operazioni. Il piano di implementazione può essere sviluppato da una persona o da un gruppo di pianificazione, con un'esperienza adeguata. Il gruppo di pianificazione deve incontrarsi regolarmente con il senior management per valutare il progresso del piano di implementazione e per allocare le risorse (compreso il tempo per gli incontri) commisurate al compito da svolgere.

Un tipico piano di implementazione del SMS include:

- Obiettivi e Politica di sicurezza.
- Descrizione del sistema.
- Gap Analysis.
- Componenti del SMS.
- Ruoli e responsabilità.
- Politica di hazard reporting.
- Misura delle performance in termini di sicurezza.
- Safety communication.
- Safety training.
- Gestione di revisione delle performance in ambito di sicurezza.

Una volta completato, il senior management deve approvare il piano di implementazione del SMS.

3 STRUMENTI NECESSARI PER LA GESTIONE DELLA SAFETY

I due processi fondamentali all'interno del processo di gestione della safety sono: *Hazard Identification* e *Safety Risk Management*. E' importante fare una netta distinzione tra hazard e safety risk, al fine di evidenziare le differenze necessarie per una buona riuscita del processo di gestione della sicurezza.

3.1 HAZARDS

Per capire bene il concetto generale di *hazard*, viene fatta un'ulteriore differenza tra la definizione vera e propria di hazard e le conseguenze di tale hazard.

Con hazard si intende una condizione o un oggetto con il potenziale di causare danni al personale, alle strutture o agli equipaggiamenti, una perdita di materiale o una riduzione della capacità di svolgere una determinata funzione. E' un elemento che fa parte del sistema socio-tecnologico, in cui il personale deve continuamente interagire con la tecnologia al fine di rendere fruibile un servizio. Non sempre il termine hazard ha una connotazione negativa; è solo quando quest'ultimo si interfaccia con le operazioni, che si attiva il suo potenziale diventando un rischio per la sicurezza.

Con conseguenza si intende invece il potenziale esito di un hazard. Questo si esprime attraverso una o più conseguenze. L'hazard appartiene al presente, è parte del contesto operativo, e molto spesso è identificabile attraverso audit. Le conseguenze invece, appartengono al futuro. Esse non si materializzano fino al momento in cui l'hazard non si interfaccia con le operazioni. Solo a questo punto infatti, l'hazard può manifestare il proprio potenziale danno. Questo porta a definire un aspetto fondamentale del Safety Management: le strategie di mitigazione devono mirare a contenere il potenziale dell'hazard e non aspettare che si giunga alla materializzazione della sua conseguenza. Si parla quindi di strategia proattiva e non reattiva.

Un altro punto importante è quello di descrivere la conseguenza dell'hazard in termini operativi e non assoluti, in modo da permettere di identificare delle strategie di mitigazione.

3.2 CONCETTI FONDAMENTALI DEL PROCESSO DI HAZARD IDENTIFICATION

3.2.1 UNDERSTANDING HAZARDS

Il primo passo consiste nell' identificare correttamente l'hazard e non confonderlo con una delle sue possibili conseguenze. Questo renderebbe difficile l'identificazione di altre conseguenze provocate dall'hazard stesso. Identificare correttamente l'hazard permette di capirne la natura e il suo potenziale danno e permette di valutare l'entità dei possibili effetti negativi.

Gli hazard possono essere così classificati:

- Natural hazard: sono conseguenza dell'ambiente nel quale avvengono le operazioni.
- Technical hazard: sono il risultato di fonti di energia (pressione pneumatica, pressione idraulica, elettricità, combustibile) o funzioni safety-critical (danneggiamenti hardware, anomalie nei software) necessarie per le operazioni che riguardano la fornitura di un servizio.
- Economic hazard: sono le conseguenze dell'ambiente socio-politico in cui avvengono le operazioni legate alla fornitura di un servizio.

3.2.2 HAZARD IDENTIFICATION

Come è già stato discusso precedentemente, l'hazard viene individuato tramite processi proattivi e predittivi prima che le conseguenze scaturiscano degradando la safety. Esistono diverse fonti per l'identificazione dell'hazard, esse possono essere interne o esterne all'organizzazione. Il processo di identificazione è dato da una combinazione di entrambe queste fonti. E' responsabilità di tutti, all'interno dell'organizzazione, identificare e riportare la presenza di un hazard ma esiste, all'interno dell'organizzazione, personale con il preciso compito di identificare e analizzare l'eventuale fattore di rischio.

Il processo di identificazione è un processo continuo, parte integrante dei processi e descritto nella documentazione dell'organizzazione. Le condizioni che più sono una minaccia per la safety, e che quindi necessitano di particolare attenzione durante il processo di Hazard Identification, sono:

1. Cambiamenti nel personale, nei sistemi o nell'equipaggiamento.
2. Crescita/ diminuzione rapida dell'organizzazione.
3. Casi in cui l'organizzazione vede un aumento degli eventi che portano alla riduzione della safety o infrazioni dei regolamenti.

3.2.3 HAZARD ANALYSIS

Una volta identificato l'hazard, dai dati ottenuti, devono essere ricavate delle informazioni sulla safety. Il primo passo per ottenere queste informazioni è l'Hazard Analysis.

E' un processo che si basa su tre passi:

1. Identificare il generico hazard (indicato con Top Level Hazard TLH).
2. Suddividere il THL in componenti o specifici hazard.
3. Collegare gli specifici hazard alle corrispettive potenziali conseguenze.

3.2.4 DOCUMENTATION OF HAZARDS

Un'appropriata gestione della documentazione riguardante il processo di identificazione dell'hazard è fondamentale per tradurre le informazioni riguardanti la safety in conoscenza relativa ai fattori di rischio.

La gestione della conoscenza relativa agli hazard contribuisce alla "Safety Library".

Al fine di creare la "Safety Library", bisogna ricordare che l'identificazione e l'analisi degli hazard sono facilitate da:

- Standardizzazione dei termini usati.
- Comprensione dei termini usati.
- Validazione delle informazioni raccolte.
- Reporting.
- Monitoraggio e gestione delle informazioni raccolte.

Nella figura seguente viene illustrato e spiegato il processo di documentazione dell'hazard.

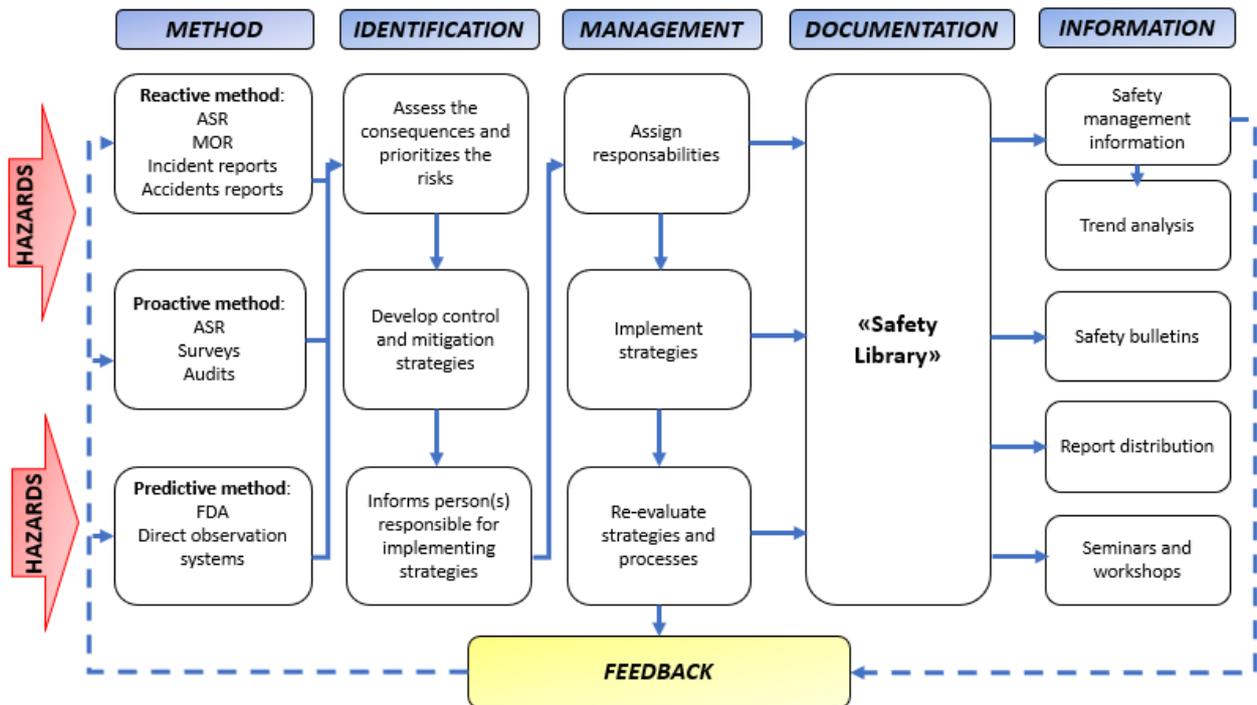


Figura 4 Processo di documentazione degli hazard

Gli hazard sono costantemente identificati tramite processi proattivi, predittivi e reattivi e vengono raccolte informazioni sulla safety. Una volta identificato l'hazard e dopo aver raccolto le informazioni, l'hazard viene valutato in termini di conseguenze e in termini di responsabilità e priorità riguardo a misure e strategie di mitigazione. Tutte queste informazioni (hazard, conseguenze, priorità, responsabilità e strategie) vengono raccolte a formare la "Safety library" dell'organizzazione.

Quest'ultima viene usata, non solo come fonte di conoscenza per quanto concerne la sicurezza, ma anche per il processo successivo di decision making al fine di attuare strategie di mitigazione, per le analisi di safety trend e per il training in materia di sicurezza.

3.3 SAFETY RISK

Il Safety Risk Management, insieme all'Hazard Identification, è una delle attività fondamentali del Safety Management System. Questo processo permette di classificare i rischi in ordine di potenziale di rischio. E' possibile in tal modo stabilire le priorità nell'allocazione delle risorse al fine di proporre strategie di mitigazione atte a contenere il potenziale dell'hazard.

Safety Risk viene definito come l'assegnazione, espressa in termini di probabilità e severità, delle conseguenze dell'hazard.

3.3.1 SAFETY RISK MANAGEMENT

Il termine Safety Risk Management comprende la determinazione e la mitigazione delle conseguenze degli hazard in termini di safety, i quali minacciano le capacità di un'organizzazione, portandole a un livello accettabile (ALARP).

La seguente figura mostra una rappresentazione del processo di Safety Risk Management.

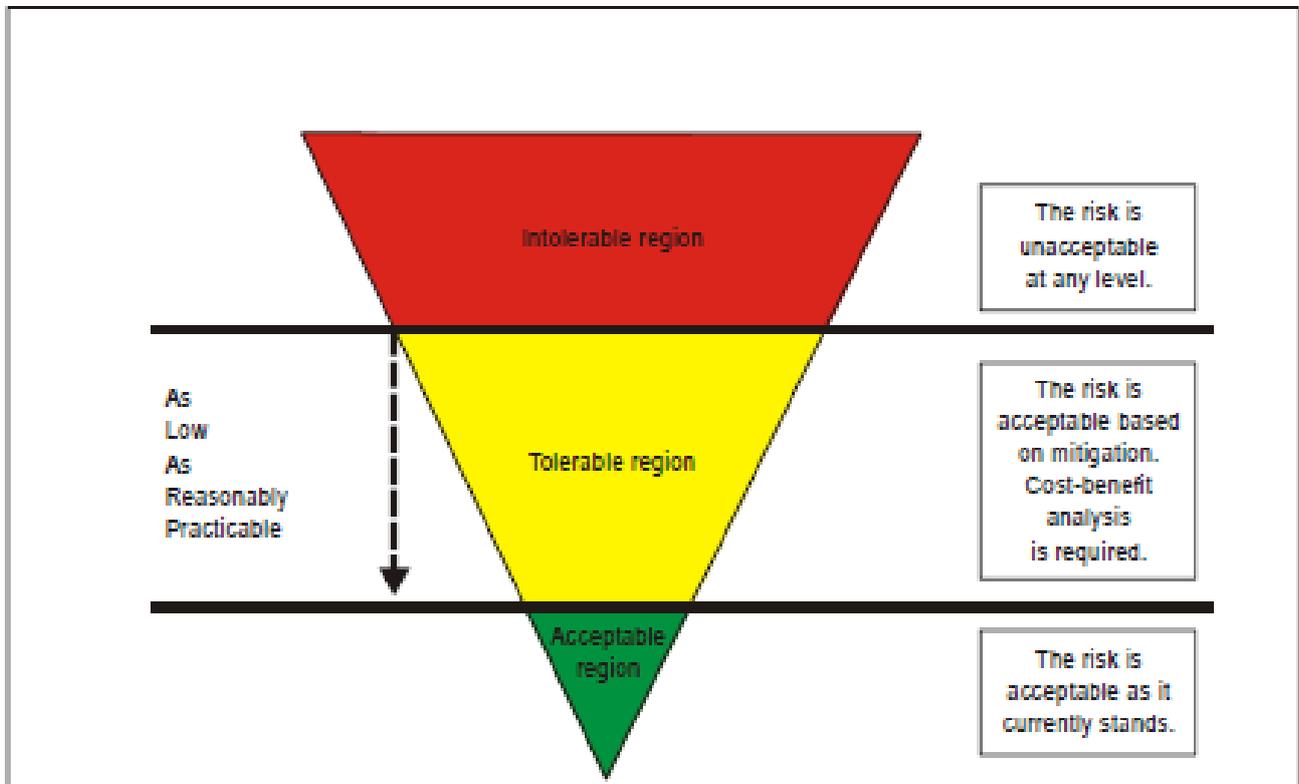


Figura 5 Safety Risk Management Process

La maggior parte delle conseguenze degli hazard cade nella regione intollerabile, un numero più piccolo ricade invece nella regione tollerabile mentre solo una piccola parte rientra nella regione di accettabilità.

Le conseguenze che rientrano nella zona di intollerabilità, sono inaccettabili. Ciò significa che la probabilità e /o la severità delle conseguenze rendono necessaria un'immediata azione di mitigazione. Al fine di portare il rischio nella zona tollerabile o accettabile, sono possibili due alternative:

1. Allocare risorse al fine di ridurre il potenziale dannoso della conseguenza dell'hazard
2. Se la mitigazione non è possibile, cancellare l'operazione

Il safety risk che inizialmente ricade nella zona di tollerabilità e così come quello che da intollerabile viene, tramite processi di mitigazione, a ricadere nella zona di tollerabilità, deve rimanere protetto da strategie di mitigazione che ne garantiscano il controllo. Il rischio che ricade invece nella zona di accettabilità non richiede alcuna azione per portare la probabilità e /o la severità delle conseguenze sotto controllo.

Un rischio che è stato ridotto fino a un livello "Reasonably Practicable" viene definito ALARP. Al fine di definire un rischio come "Reasonably Practicable", bisogna tenere in considerazione sia la fattibilità tecnica che il costo. Questo include un'analisi costo- benefici. Nel momento in cui un'organizzazione accetta il rischio, questo non significa che il rischio è stato eliminato ma che il rischio rimanente è sufficientemente basso e viene compensato dai benefici.

3.3.2 SAFETY RISK PROBABILITY

Il primo passo per portare il rischio delle conseguenze sotto controllo è l'assegnazione della probabilità che le conseguenze si verifichino durante le operazioni. Nell'assegnare la probabilità che un evento possa accadere, si fa riferimento ai dati storici contenuti all'interno della "Safety Library".

La probabilità che un evento indesiderato possa accadere può essere stabilito tramite una Risk Probability Table.

	MEANING	VALUE
FREQUENT	Likely to occur many times (has occurred frequently)	5
OCCASIONAL	Likely to occur sometimes (has occurred infrequently)	4
REMOTE	Unlikely to occur, but possible (has occurred rarely)	3
IMPROBABLE	Very unlikely to occur (not known to have occurred)	2
EXTREMELY IMPROBABLE	Almost inconceivable that the event will occur	1

Figura 6 Safety Risk Probability Table

Questa è una tabella a cinque punti. Essa include cinque categorie che denotano la probabilità di accadimento di un evento o di una condizione indesiderata, spiega il significato e assegna un valore a ognuna delle categorie.

3.3.3 SAFETY RISK SEVERITY

Una volta che un evento o una condizione indesiderata è stata classificata in termini di probabilità, il secondo passo nel portare le conseguenze dell'hazard sotto controllo, è quello di assegnare anche la gravità delle conseguenze.

La Safety Risk Severity è definita come la possibile conseguenza di una condizione indesiderata, prendendo come riferimento la peggior situazione prevedibile.

SEVERITY OF OCCURRENCES	MEANING	VALUE
CATASTROPHIC	<ul style="list-style-type: none"> • Equipment destroyed • Multiple deaths 	A
HAZARDOUS	<ul style="list-style-type: none"> • A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely • Serious injury • Major equipment damage 	B
MAJOR	<ul style="list-style-type: none"> • A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of increase in workload, or as result of conditions impairing their efficiency • Serious incidents • Injury to persons 	C
MINOR	<ul style="list-style-type: none"> • Nuisance • Operating limitations • Use of emergency procedures • Minor incident 	D
NEGLEGIBLE	<ul style="list-style-type: none"> • Little consequences 	E

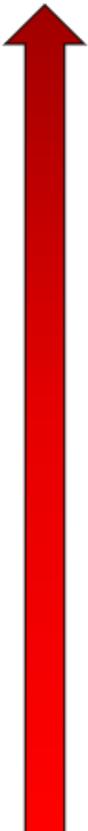


Figura 7 Safety Risk Severity Table

La tabella individua 5 categorie per indicare la gravità dell'accadimento di una condizione indesiderata, definisce il significato di ciascuna categoria e assegna un valore a ognuna delle categorie.

3.3.4 SAFETY RISK TOLERABILITY

Una volta che il rischio delle conseguenze di un evento indesiderato è stato classificato in termini di probabilità di accadimento e severità delle sue conseguenze, il terzo passo necessario per portare il rischio sotto controllo, è quello di assegnare la tollerabilità delle conseguenze dell'hazard. Il processo che porta all'assegnazione della tollerabilità, è un processo caratterizzato da due passi:

- Come primo passo bisogna ottenere un generico valore di safety risk. Questo si fa combinando la probabilità e la severità in all'interno della cosiddetta *Safety Risk Assessment Matrix*.

Risk probability	Risk severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

Figura 8 Safety Risk Assessment Matrix

Si può notare che il safety risk è un numero o una combinazione alfanumerica ma non è una componente tangibile.

- Il secondo passo consiste invece nell'esportare il safety risk index ottenuto tramite la matrice precedente, in una *Safety Risk Tolerability Matrix* che descrive i criteri di tollerabilità.

Nel caso in cui il rischio ricada nella condizione di inaccettabilità, l'organizzazione deve:

1. Allocare risorse per ridurre l'esposizione delle conseguenze.
2. Allocare risorse per ridurre l'intensità o il potenziale dannoso delle conseguenze.
3. Qualora la mitigazione non fosse possibile, cancellare l'operazione.

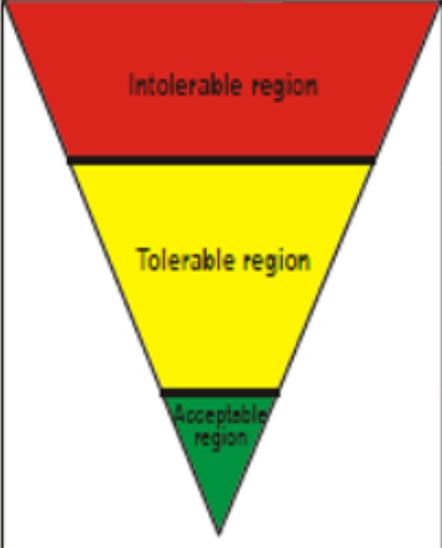
SUGGESTED CRITERIA	ASSESTMENT RISK INDEX	SUGGESTED CRITERIA
	5A, 5B, 5C, 4A, 4B, 3A	UNACCEPTABLE UNDER EXISTING CIRCUMSTANCES
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	ACCEPTABLE BASED ON RISK MITIGATION. IT MAY REQUIRE MANAGEMENT DECISION
	3E, 2D, 2E, 1A, 1B ,1C, 1D, 1E	ACCEPTABLE

Figura 9 Safety Risk Tolerability Matrix

3.3.5 SAFETY RISK CONTROL/MITIGATION

Lo step finale del processo consiste nello sviluppare strategie di controllo/ mitigazione. Con questi termini, tra loro interscambiabili, si intende indicare misure necessarie al fine di portare la probabilità delle conseguenze e la loro gravità sotto il controllo dell'organizzazione. In questa fase devono essere allocate delle risorse al fine di andare a far ricadere il rischio nella zona di accettabilità.

Se questo non è possibile, allora l'operazione deve essere annullata.

Esistono tre diverse strategie per il controllo/ mitigazione del rischio:

1. *Avoidance*. L'operazione o l'attività viene annullata o evitata perché il rischio eccede i benefici che derivano dal portare avanti l'attività.
2. *Reduction*. La frequenza dell'operazione viene ridotta oppure vengono messe in atto delle azioni per ridurre l'entità delle conseguenze.
3. *Segregation of exposure*. Vengono messe in atto delle azioni per isolare gli effetti dell'hazard oppure vengono attuati dei sistemi di ridondanza per proteggersi dalle conseguenze.

Nel valutare l'alternativa per la mitigazione del rischio, bisogna tenere in considerazione che non tutte hanno lo stesso potenziale nel ridurre il rischio. La maggior parte delle strategie di controllo e mitigazione sono basate sull'implementazione di Safety Defences o sul rafforzamento delle difese esistenti: tecnologia, training e normativa.

La figura seguente rappresenta il processo di mitigazione del rischio:

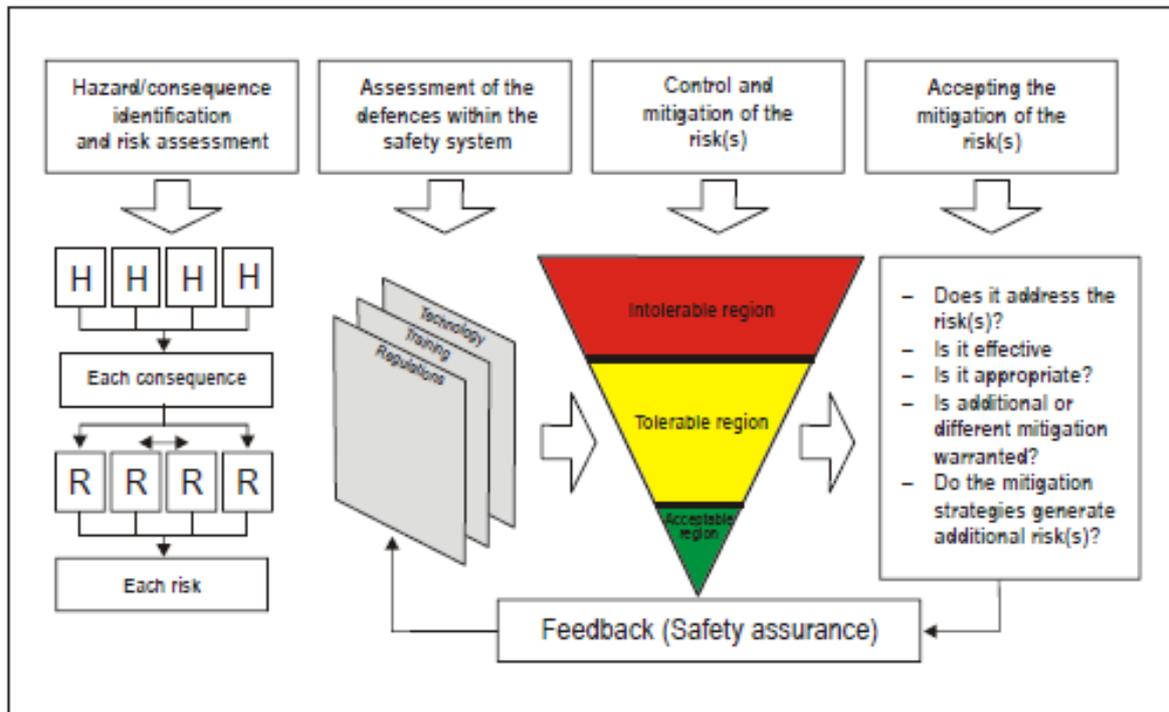


Figura 10 Processo di mitigazione del rischio

Il processo di mitigazione e controllo può essere così suddiviso:

- Identificazione dell'hazard e delle sue conseguenze e assegnazione del rischio.
- Valutazione delle difese esistenti che costituiscono il sistema.
- Attuazione delle azioni di mitigazione e controllo.
- Accettazione o no del processo di mitigazione.

Una volta che la mitigazione è stata accettata, le strategie sviluppate devono, tramite un processo di Safety Assurance, garantire integrità ed efficienza delle difese nelle nuove condizioni operative.

I concetti più significativi che riguardano il Safety Risk Management discussi in questo capitolo, possono essere schematizzati nello schema seguente:

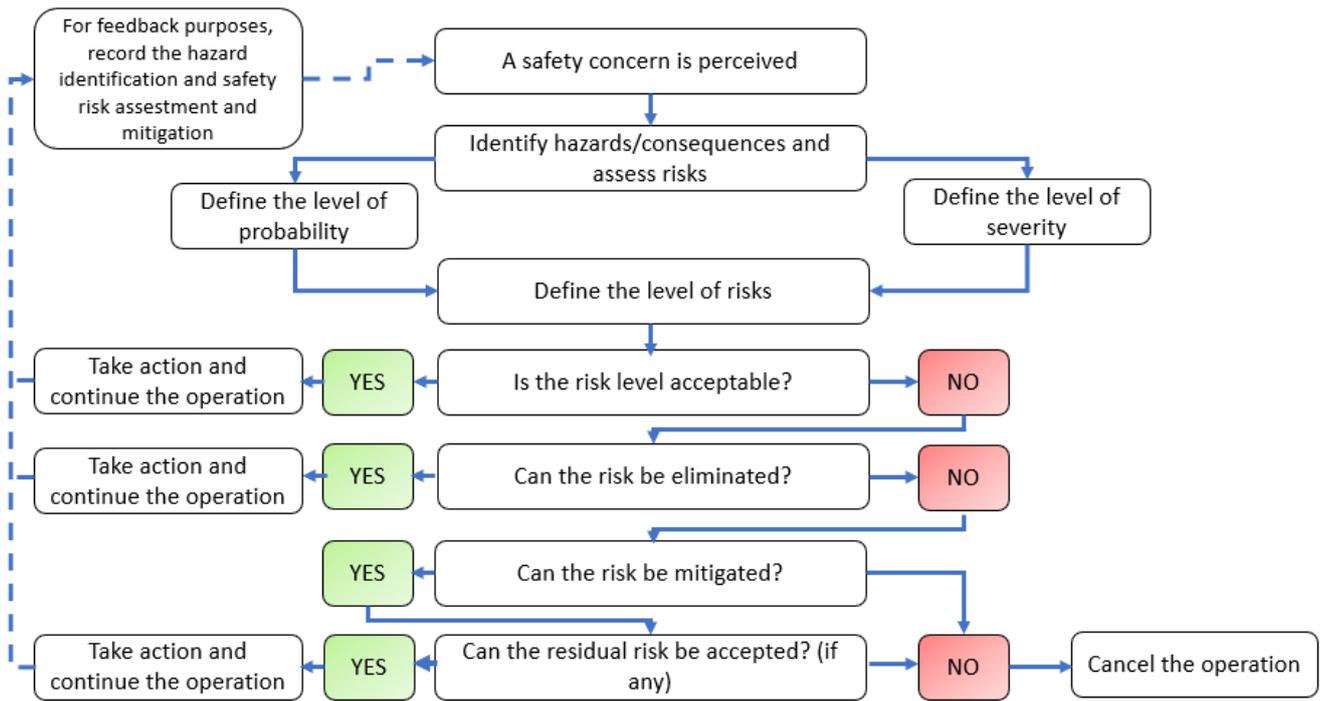


Figura 11 Safety Risk Management

4 ROOT CAUSE ANALYSIS

La Root Cause Analysis (RCA) è una classe di metodi problem solving volti a individuare le cause ultime di problemi o eventi. I principi generali per un'efficace conduzione della RCA sono:

1. Identificazione delle cause principali di un problema al fine di determinare delle azioni correttive e impedire che il problema si verifichi di nuovo.
2. Sistematicità dell'analisi ovvero deve essere considerata come un'indagine le cui conclusioni e le cause identificate devono essere sostenute da prove documentate.
3. Ci possono essere più di una causa ultima.
4. L'identificazione della causa ultima dipende da come viene definito l'evento che si deve indagare.
5. Necessità di identificare delle linee temporali per comprendere le relazioni tra i fattori contributivi, la causa ultima e l'evento principale.
6. Necessità di una politica non punitiva verso chi identifica problemi all'interno del sistema.

Passi principali nella RCA :

1. Definire il problema o descrivere l'evento.
2. Raccogliere i dati e le prove, classificandoli lungo una linea temporale degli eventi fino a giungere all'evento principale.
3. Chiedersi il "perché" e individuare le cause associate a ciascuna fase nella sequenza che ha condotto allo specifico problema o evento.
4. Identificare le cause principali che, quando rimosse, permettano di ritenere interrotta la "catena degli eventi".
5. Identificare le azioni correttive che, con certezza, evitano il ripetersi dell'evento e individuare soluzioni efficaci, controllabili e che non causino l'introduzione di ulteriori problemi per la sicurezza.
6. Implementare le azioni correttive identificate per la causa ultima.
7. Garantire l'efficacia osservando l'implementazione delle soluzioni identificate.

Esistono diverse tecniche che possono essere adottate per condurre la RCA, tra cui FMECA, Causal Factor Tree Analysis, Fault Tree Analysis, Metodo dei "5 perché" e diagramma di Ishikawa.

PARTE 2

5 ICAO ANNESSO 19

L'Annesso 19 consolida e unifica il materiale proveniente dagli Annessi esistenti riguardanti State Safety Program e sistemi di gestione della sicurezza (SMS), così come elementi correlati tra cui la raccolta e l'uso dei dati sulla sicurezza e le attività di State Safety Oversight. Il vantaggio dell'unificare questo materiale in un unico allegato è quello di focalizzare l'attenzione degli Stati sull'importanza di integrare le loro attività di gestione della sicurezza.

Facilita inoltre l'evoluzione delle disposizioni sulla gestione della sicurezza.

Gli standards e le Recommended Practices (SARPs) presenti all'interno dell'Annesso 19, hanno lo scopo di assistere gli Stati nella gestione del rischio per la sicurezza.

Data la crescente complessità del sistema globale del trasporto aereo e le attività a esso correlate, necessarie per garantire il funzionamento sicuro degli aeromobili, il presente allegato sostiene la continua evoluzione di una strategia proattiva con l'obiettivo di migliorare le prestazioni in termini di sicurezza, che si basa sull'implementazione di uno State Safety Program (SSP) che affronta sistematicamente i rischi per la sicurezza.

L'Annesso 19 è costituito da 5 capitoli:

1. Definizioni.
2. Applicabilità.
3. State safety management responsibilities.
4. Safety Management System.
5. Raccolta, analisi, protezione, condivisione e scambio di dati e informazioni sulla sicurezza.

L'Appendice II di questo Annesso, presenta il framework previsto da ICAO per l'implementazione del SMS, la cui guida approfondita è contenuta all'interno del Safety Management Manual (SMM) (*Doc 9859*) e di cui si riporta al capitolo 10 di questa tesi.

6 INTRODUZIONE SMS NELLE AZIENDE CAMO

In accordo alla EASA Policy sul Safety Management System, lo scopo principale di un SMS è assicurare che le organizzazioni, oltre a garantire la rispondenza alle normative, abbiano la capacità di identificare i rischi per la sicurezza del volo e di mitigare tali rischi.

Un SMS è un approccio sistematico e proattivo alla gestione dei rischi legati alla sicurezza che comprende strutture organizzative, politiche, processi e procedure. Le attività di gestione dei rischi sono al centro del SMS, compresa l'individuazione delle problematiche in materia di sicurezza, la valutazione dei rischi e la loro mitigazione, il tutto supportato dai processi di Safety Assurance che verificano l'efficacia delle mitigazioni, monitorano le prestazioni in termini di sicurezza e la gestione dei cambiamenti.

Infine, le attività di Safety Promotion, garantendo il mantenimento delle competenze del personale (formazione) e la condivisione delle informazioni attinenti la safety sia all'interno delle organizzazioni che con le organizzazioni esterne con le quali l'organizzazione si interfaccia (comunicazione), svolgono un ruolo chiave nell'attuazione di un SMS efficace.

L'annesso Vc (Parte CAMO) al *Reg. (UE) N.1321/2014*, come emendato dal *Reg. (UE) 2019/1383*, contiene i requisiti per il Management System per le imprese CAMO che si applicheranno dal 24 Marzo 2020. Disposizioni in merito ai transitori per l'applicazione delle nuove previsioni e le date ultime di adeguamento stabilite per le imprese che già detengono un'approvazione CAMO in accordo alla sottoparte G della Parte M sono contenuti nell'articolo 4 del regolamento No 1321/2014 (*[.. until 24 September 2021, the organisation may correct any findings of non-compliance related to requirements introduced by Annex Vc (Part-CAMO) and not included in Subpart G of Annex I (Part-M)]*).

L'approvazione in accordo alla nuova Parte CAMO è obbligatoria sia per le organizzazioni collegate a operatori detentori di licenza di trasporto aereo rilasciata in accordo al *Reg. (EC) 1008/2008* che per le organizzazioni che gestiscono aeromobili complessi (con eccezione dei velivoli plurimotore turboelica di massa pari o inferiore a 5700kg). Nel primo caso è richiesto che il management system della CAMO sia integrato nel management system dell'operatore.

"Il Regolamento (UE) 2019/1383 modifica e rettifica il Regolamento (UE) n. 1321/2014 per quanto riguarda i sistemi di gestione della sicurezza nelle imprese di gestione del mantenimento dell'aeronavigabilità e le semplificazioni per gli aeromobili dell'aviazione generale per quanto concerne la manutenzione e la gestione del mantenimento dell'aeronavigabilità" (Rif. Gazzetta ufficiale dell'Unione Europea).

Il sistema di gestione della safety mira a identificare gli hazard e a mitigarne il rischio prima che si verifichino incidenti. La gestione della safety permette a un'organizzazione di gestire le sue attività in un modo sistematico. Quando un'organizzazione ha una chiara comprensione del suo ruolo e del suo contributo alla sicurezza dell'aviazione, può dare una priorità al rischio associato alla safety e gestire in modo efficiente le sue risorse e ottenere ottimi risultati. I principi dei requisiti espressi nei

punti *CAMO.A.200*, *CAMO.A.202*, *CAMO.A.305* e le relative AMC costituiscono il framework per la gestione della sicurezza a livello europeo.

Questo framework si rifà a quello descritto nell'appendice 2 dell'annesso 19 dell'ICAO e promuove un approccio integrato alla gestione dell'organizzazione. Questo facilita l'introduzione di nuovi componenti al sistema di gestione già esistente. Questo nuovo approccio ha l'obiettivo di introdurre la gestione della safety e il processo di decision-making basato sulla valutazione del rischio, all'interno tutte attività dell'organizzazione. Se l'organizzazione detiene più certificati nell'ambito di applicazione del *Regolamento (EU) 2018/1139*, può scegliere di implementare un singolo sistema di gestione per coprire tutte le sue attività. Il sistema di gestione integrato fa sì che si possa gestire la sicurezza tra diverse attività, rimuovendo ogni duplicazione con gli eventuali altri sistemi di gestione già implementati all'interno dell'organizzazione.

Ogni organizzazione può decidere quello che è il modo migliore per strutturare il proprio sistema di gestione, che meglio si interfaccia con i bisogni dell'organizzazione.

7 SISTEMA DI GESTIONE

CAMO.A.200 Management System

Regulation (EU) 2019/1383

(a) The organisation shall establish, implement, and maintain a management system that includes:

(1) clearly defined lines of responsibility and accountability throughout the organisation, including a direct safety accountability of the accountable manager;

(2) a description of the overall philosophies and principles of the organisation with regard to safety, referred to as the safety policy;

(3) the identification of aviation safety hazards entailed by the activities of the organisation, their evaluation and the management of associated risks, including taking actions to mitigate the risks and verify their effectiveness;

(4) maintaining personnel trained and competent to perform their tasks;

(5) documentation of all management system key processes, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation;

(6) a function to monitor compliance of the organisation with the relevant requirements. Compliance monitoring shall include a feedback system of findings to the accountable manager to ensure effective implementation of corrective actions as necessary;

(7) any additional requirements that are laid down in this Regulation.

(b) The management system shall correspond to the size of the organisation and the nature and complexity of its activities, taking into account the hazards and associated risks inherent in these activities.

(c) Where the organisation holds one or more additional organisation certificates within the scope of Regulation (EU) 2018/1139 and its delegated and implementing acts, the management system may be integrated with that required under the additional certificate(s) held.

(d) Notwithstanding point (c), for air carriers licensed in accordance with Regulation (EC) No 1008/2008, the management system provided for in this Annex shall be an integrated part of the operator's management system.

Il punto *CAMO.A.200* esprime il cuore del framework per il sistema di gestione e si focalizza sugli aspetti essenziali per la gestione della sicurezza, chiedendo all'organizzazione di:

- a) Definire in modo chiaro le responsabilità.
- b) Stabilire una politica di sicurezza e gli obiettivi in termini di sicurezza.
- c) Implementare delle procedure di safety reporting in linea con i principi di Just Culture.
- d) Garantire l'identificazione degli hazard derivanti dalle proprie attività, valutarne la loro entità, gestire il rischio a essi associato, intraprendere azioni di mitigazione e verificare l'efficacia di tali azioni.
- e) Gestire la compliance, considerando ogni requisito addizionale che può essere applicato all'organizzazione.
- f) Mantenere il personale addestrato e informato riguardo a questioni relative alla sicurezza.
- g) Documentare tutti i processi chiave di gestione.

Rispetto al sistema qualità descritto nella Subpart G della Parte M, nella nuova Part-CAMO sono stati introdotti i punti b) c) e d) di cui sopra.

Il punto *CAMO.A.200* definisce i seguenti come processi chiave nella gestione della safety:

- Identificazione dell'hazard.
- Safety Risk Management.
- Investigazioni interne.
- Misura e monitoraggio delle prestazioni di sicurezza.
- Gestione del cambiamento.
- Continuo miglioramento.
- Immediate safety action e coordinamento con l'Emergency Response Plan dell'operatore aereo (ERP).

Questi processi chiave sono supportati da una compliance monitoring function. L'effettiva conformità alla normativa durante le operazioni giornaliere e il monitoraggio indipendente delle conformità sono due aspetti fondamentali per il sistema di gestione della sicurezza. Inoltre, la compliance monitoring function, può supportare il follow-up delle azioni di mitigazione.

Nel momento in cui delle non conformità vengono identificate tramite audit, la causa viene immediatamente analizzata. Questa analisi supporta il processo di gestione del rischio nel fornire degli spunti per l'identificazione delle cause e dei fattori che hanno contribuito alla non conformità, inclusi i fattori umani, i fattori organizzativi e l'ambiente entro cui l'organizzazione opera.

Gli audit sono un metodo per informare la dirigenza del livello di compliance dell'organizzazione, dell'implementazione delle azioni di mitigazione e della necessità di azioni preventive o correttive.

Il focus primario dei processi chiave della gestione della safety è sui processi organizzativi e sulle procedure ma anche sull'essere umano, in quanto esso può contribuire sia in modo positivo che negativo ai risultati dell'organizzazione in termini di sicurezza.

L'efficacia della gestione della safety dipende dall'impegno del senior management nel creare un ambiente operativo che ottimizza le performance umane e che incoraggia il personale nel dare un contributo attivo al processo di gestione dell'organizzazione. Una cultura della sicurezza positiva si basa infatti sulla fiducia e sul rispetto tra il personale, che deve essere creata e supportata dal senior management.

Un efficiente sistema di gestione non si rivolge solo agli eventi più gravi ma anche a inefficienze nella produzione e punta al miglioramento della comunicazione, all'incentivare una cultura della safety e a un miglior controllo dei fornitori. Il fatto che il sistema di gestione della sicurezza e le corrispondenti politiche organizzative e i processi chiave non vengano implementati solo per prevenire incidenti gravi ma anche per raggiungere gli obiettivi strategici dell'organizzazione, fa sì che ogni tipo di investimento nella sicurezza venga visto come un investimento organizzativo e in termini di produttività.

I processi di Hazard Identification e Risk Assessment, mitigazione e verifica dell'efficienza delle azioni di mitigazione, creano immediati costi diretti, mentre i benefici sono spesso lenti e non tangibili.

7.1 ORGANISATION AND ACCOUNTABILITIES

Rif. CAMO.A.200 (a)(1) [The organisation shall establish, implement, and maintain a management system that includes: clearly defined lines of responsibility and accountability throughout the organisation, including a direct safety accountability of the accountable manager]

È necessario che venga definita un'architettura del SMS dell'organizzazione che corrisponda alla dimensione, alla natura e alla complessità delle operazioni ma anche ai rischi associati alle attività necessarie per la fornitura del servizio. Le responsabilità in termini di sicurezza includono anche l'allocazione di risorse tecniche, umane, finanziarie o qualsiasi altra risorsa necessaria per un'efficiente riuscita del SMS.

7.1.1 ACCOUNTABLE MANAGER

L'organizzazione deve identificare un Accountable Manager che, che in virtù della sua posizione, ha la responsabilità generale (in particolare finanziaria) della gestione dell'organizzazione. L'AM può ricoprire questo ruolo in più di una organizzazione e non gli viene richiesta una particolare conoscenza tecnica ma solo una generale conoscenza del regolamento. Solitamente l'AM è il chief executive office della CAMO ma se così non fosse, l'organizzazione deve dimostrare all'autorità competente che l'Accountable Manager ha accesso diretto nei confronti del CEO e dispone della dotazione finanziaria necessaria per le attività di gestione del mantenimento dell'aeronavigabilità.

L'Accountable Manager deve:

- Garantire la disponibilità delle risorse necessarie per condurre tutte le attività in accordo con il regolamento (EU) 2018/1139.
- Stabilire e promuovere la politica di sicurezza.
- Nominare una persona/ un gruppo di persone responsabile di garantire compliance con il regolamento. Questa persona è responsabile delle attività di gestione dell'aeronavigabilità continua, al fine di garantire che il personale dell'organizzazione lavori in accordo con le procedure e i regolamenti. Questa persona deve mostrare una conoscenza approfondita del regolamento applicabile e deve garantire che i processi e gli standards dell'organizzazione riflettano i requisiti applicabili. E' sua responsabilità garantire la gestione proattiva delle conformità, la documentazione di ogni non conformità e la conseguente implementazione di azioni di mitigazione (Rif.CAMO.A.305(a)(3)).
- Nominare una persona o un gruppo di persone con la responsabilità di gestire la compliance monitoring function in quanto parte del sistema di gestione (Rif.CAMO.A.305 (a)(4)).

- Nominare una persona o un gruppo di persone con la responsabilità di gestire lo sviluppo, l'amministrazione e il mantenimento dei processi di gestione della safety (*Rif.CAMO.A.305 (a)(5)*).
- Assicurare che una persona o un gruppo di persone, si occupino di mantenerlo informato sulla compliance e su questioni legate alla sicurezza.

Per le imprese approvate anche come vettori aerei titolari di licenza a norma del regolamento (CE) n. 1008/2008, l'Accountable Manager deve inoltre:

- Essere la persona nominata come dirigente responsabile dell'operatore aereo, come richiesto all'allegato III (parte ORO), punto *ORO.GEN.210(a)*, del regolamento (UE) n. 965/2012.
- Nominare una persona responsabile della gestione e della sorveglianza del mantenimento dell'aeronavigabilità, che non può essere dipendente di un'impresa approvata a norma dell'allegato II (parte 145) con cui l'operatore ha stipulato un contratto, salvo accordo specifico dell'autorità competente.

Quando il detentore di licenza aerea intende nominare un CAMO Post Holder che è anche dipendente di un'organizzazione approvata Part -145, deve giustificare il motivo per il quale è stata presa tale decisione e supportarla tramite una valutazione del rischio e/o azioni di mitigazione. Questo si applica solo quando l'organizzazione approvata Part 145 e l'operatore aereo titolare di licenza non sono la stessa organizzazione.

7.1.2 SAFETY MANAGER

Se più di una persona è stata identificata per lo sviluppo, l'amministrazione e il mantenimento di effettivi processi di gestione della sicurezza, l'Accountable Manager deve identificare un'unica persona a cui fare riferimento, questa persona è il Safety Manager.

Le funzioni del Safety Manger sono:

- Facilitare il processo di Hazard Identification, Risk Assessment e Risk Management.
- Monitorare l'implementazione di azioni volte a mitigare il rischio, a meno che questo non venga fatto tramite la compliance monitoring function.
- Fornire report periodici sulla performance della Safety Review Board.
- Garantire il mantenimento della documentazione riguardante la gestione della safety.
- Garantire che il training sia disponibile e che soddisfi standards accettabili.
- Fornire consulenza in materia di sicurezza.
- Garantire che vengano continuamente svolte investigazioni interne.

In base alla dimensione dell'organizzazione, alla natura e alla complessità delle sue attività, il Safety Manager può essere assistito da personale addetto alla sicurezza al fine di condurre le attività legate alla gestione della safety, come definito nella *AMC1 CAMO.A.200(a)(1)*. In ogni caso il Safety Manager deve rimanere l'unica persona di riferimento per lo sviluppo, l'amministrazione e il mantenimento dei processi di gestione della sicurezza.

Il Safety Manager deve applicare processi e procedure che permettano di adempiere le sue responsabilità, cercare opportunità per migliorare processi, misurarne l'efficienza e garantirne un continuo miglioramento. La sua posizione all'interno del SMS necessita di saper affrontare cambiamenti nelle circostanze e nelle situazioni e di agire indipendentemente dagli altri manager all'interno delle organizzazioni. E' responsabile inoltre di fornire le informazioni e avvisare l'AM per le questioni che riguardano la sicurezza delle operazioni. Questo ruolo prevede impegni con scarso preavviso e fuori dall'orario di lavoro.

Qualificazioni del Safety Manager:

- a) Buona esperienza in tutte le funzioni dell'organizzazione (gestione del training, operazioni aeree, gestione della manutenzione).
- b) Profonda conoscenza dei principi di gestione della safety.
- c) Abilità di comunicazione scritta e orale.
- d) Buone capacità relazionali.
- e) Abilità di relazionarsi a tutti i livelli sia all'interno che all'esterno dell'organizzazione.
- f) Capacità organizzativa.
- g) Capacità di leadership e approccio autorevole.
- h) Rispetto delle persone.

Data la complessità e la vastità delle materie che rientrano nelle competenze previste per questa funzione, elementi caratterizzanti della figura del Safety Manager divengono anche la capacità gestionale rivolta all'analisi e alla risoluzione dei problemi, la diplomazia e la flessibilità, tanto più estesa è la complessità del sistema aziendale. Il Safety Management Manual ICAO e le Acceptable Means of Compliance EASA dei Regolamenti Europei non prevedono per il Safety Manager né il possesso di specifici titoli scolastici o accademici, né periodi temporali minimi di esperienza; risulta però evidente che il candidato al ruolo dovrebbe avere un profilo di alta professionalità nel settore della safety aeronautica e di piena consapevolezza della realtà aziendale di appartenenza.

7.1.3 COMPLIANCE MONITORING MANAGER

Il Compliance Monitoring Manager è la persona identificata dall'AM per la gestione della Compliance Monitoring Function.

Il Compliance Monitoring Manager deve garantire che:

- Le attività dell'organizzazione siano monitorate per garantire la compliance ai requisiti applicabili e ad altri requisiti addizionali stabiliti dall'organizzazione e che le attività siano svolte sotto la supervisione delle persone nominate ai punti *CAMO.A.305 (a)(3)*, *CAMO.A.305(a)(4)* e *CAMO.A.305(a)(5)*
- Ogni contratto di manutenzione sia monitorato per garantire la compliance con il contratto/ordine di lavoro.
- Sia implementato, revisionato e applicato un piano di audit appropriato.

Il Compliance Monitoring Manager non deve essere una persona di cui al punto *CAMO.A.305(a)(3)* e deve essere in grado di dimostrare conoscenza adeguata ed esperienza riguardo le attività dell'organizzazione, inclusa un'adeguata conoscenza nel monitoraggio delle conformità. Il CMM deve anche avere accesso a tutte le parti dell'organizzazione e, dove necessario, anche alle organizzazioni subcontrattate.

Se la stessa persona viene indicata sia per la gestione della compliance monitoring function che per i processi di gestione della sicurezza, l'Accountable Manager deve garantire che adeguate risorse siano disponibili per entrambe le funzioni.

7.1.4 SAFETY REVIEW BOARD

La Safety Review Board è un comitato di alto livello che considera le questioni di sicurezza strategica a sostegno della responsabilità, in termini di sicurezza, dell'Accountable Manager.

La SRB ha le seguenti responsabilità:

- Monitorare le prestazioni in ambito di safety rispetto alla politica e agli obiettivi di sicurezza.
- Monitorare che ogni azione venga intrapresa entro i tempi stabiliti.
- Monitorare l'efficienza dei processi del sistema di gestione dell'organizzazione.
- Rivedere i risultati del monitoraggio delle conformità.
- Monitorare l'implementazione di azioni preventive e correttive .
- Garantire che vengano allocate le risorse necessarie a garantire gli obiettivi di safety che sono stati stabiliti.

Il Safety Manager, o un'altra persona indicata dal Safety Manager, può assistere ai meetings della Safety Review Board e deve comunicare all'Accountable Manager tutte le informazioni per permettere di prendere decisioni basate sui safety data.

L'organizzazione non è obbligata a istituire una Safety Review Board; questo deve essere giustificato dalla dimensione dell'organizzazione e da natura e complessità delle sue attività e deve essere soggetta a una valutazione del rischio e all'approvazione della Competent Authority. In questo caso, i compiti solitamente svolti dalla Safety Review Board, vengono svolti dal Safety Manager.

7.1.5 SAFETY ACTION GROUP

A seconda delle dimensioni dell'organizzazione, della natura e della complessità delle sue attività, un SAG può essere istituito come gruppo permanente o come gruppo ad hoc per assistere, o agire per conto del Safety Manager o della Safety Review Board. La SAG è composta da manager, supervisor e personale delle aree operative.

Compiti della SAG:

- Monitorare le performance in termini di sicurezza.
- Definire delle azioni correttive atte a portare il rischio a un livello accettabile.
- Valutare l'impatto sulla safety che possono avere eventuali cambiamenti all'interno dell'organizzazione.
- Garantire che le azioni riguardanti la safety vengano implementate entro i limiti di tempo previsti.
- Rivedere l'efficacia delle precedenti azioni di sicurezza e promozione della sicurezza.

Può essere istituito più di un SAG, a seconda dell'ambito dell'attività e dell'esperienza specifica richiesta.

7.2 SAFETY POLICY AND OBJECTIVES

Rif.CAMO.A.200(a)(2) [The organisation shall establish, implement, and maintain a management system that includes a description of the overall philosophies and principles of the organisation with regard to safety, referred to as the safety policy]

7.2.1 SAFETY POLICY

Il primo passo per garantire efficacia nella gestione della safety all'interno dell'organizzazione, è la definizione di una politica di sicurezza (*Safety Policy*) che deve essere comunicata a tutta l'organizzazione.

La safety policy è il mezzo tramite il quale l'organizzazione esprime la sua intenzione a mantenere e, se necessario, migliorare il proprio livello di sicurezza in tutte le attività e minimizzare il rischio che accada un incidente, portandolo a un livello accettabile. Questa politica riflette l'impegno dell'organizzazione riguardo la sicurezza e deve riflettere la filosofia dell'organizzazione in termini di gestione della sicurezza e basi su cui il sistema di gestione di fonda. Il primo passo per sviluppare una cultura della sicurezza è quello di definire una politica di sicurezza.

La politica di sicurezza deve essere approvata dall'Accountable Manager, comunicata a tutta l'organizzazione e deve essere revisionata periodicamente affinché rimanga appropriata per l'organizzazione. Il senior management deve continuamente promuovere la politica di sicurezza a tutto il personale e deve garantire la disponibilità delle risorse, sia umane che finanziarie, necessarie alla sua implementazione.

La politica di sicurezza deve riflettere l'impegno dell'organizzazione rivolto verso la sicurezza, la sua gestione proattiva e sistematica, includendo la promozione di una safety culture e deve:

- Comprendere al suo interno i principi di segnalazione interna e incentivare il personale a segnalare errori, incidenti e fattori di rischio riferiti al mantenimento dell'aeronavigabilità.
- Riconoscere il bisogno da parte di tutto il personale di cooperare con il processo di compliance monitoring e investigazione interna.
- Essere conforme alla normativa applicabile, soddisfare tutti i requisiti applicabili e adottare pratiche per migliorare lo standard di sicurezza.
- Applicare i principi degli human factors.
- Rinforzare la safety come prima responsabilità di tutti i manager.

- Applicare i principi della Just Culture durante il processo di safety reporting e non usare le informazioni per attribuire colpa o per qualsiasi altro motivo che non sia il miglioramento della sicurezza.

7.2.2 SAFETY OBJECTIVES

Una volta definita la politica di sicurezza, l'organizzazione deve definire gli obiettivi di sicurezza. Gli obiettivi devono essere alla base del processo di safety performance monitoring e measurement. Gli obiettivi devono inoltre:

- Riflettere l'impegno dell'organizzazione nel mantenere o migliorare l'efficienza del sistema di gestione.
- Essere comunicati a tutta l'organizzazione.
- Essere periodicamente revisionati affinché sia garantito che essi rimangano appropriati per l'organizzazione.

7.3 SAFETY MANAGEMENT KEY PROCESSES

Rif. CAMO.A.200 (a)(3) [The organisation shall establish, implement, and maintain a management system that includes: the identification of aviation safety hazards entailed by the activities of the organisation, their evaluation and the management of associated risks, including taking actions to mitigate the risks and verify their effectiveness]

7.3.1 HAZARD IDENTIFICATION PROCESSES

Il primo processo di cui si compone il Safety Risk Management consiste nell'identificazione dell'hazard. Questo si fonda su una descrizione delle funzioni del sistema, in cui i componenti e la loro interfaccia con l'ambiente operativo vengono analizzate, al fine di identificare la presenza di hazard o la presenza di difese già esistenti nel sistema e/o la loro mancanza.

Il processo di identificazione include sia gli hazard che possono essere generati da fattori umani, sia quelli che derivano dalla struttura organizzativa, o dalla presenza di operazioni complesse o disposizioni di manutenzione.

Gli hazard vengono analizzati all'interno del sistema di cui fanno parte, vengono identificate le loro potenziali conseguenze e valutate in termini di rischi per la sicurezza (in termini di probabilità e severità delle conseguenze discusse al capitolo 3). Quando il rischio è troppo alto per essere considerato accettabile, ulteriori controlli dei rischi devono essere inseriti all'interno del sistema.

Un sistema di segnalazione è il modo di raccogliere, registrare, analizzare, agire e generare feedback sugli hazard e sui rischi a essi associati che possono avere un effetto negativo sulla sicurezza.

Di seguito vengono riportate alcune delle tecniche usate per garantire un approccio strutturato all'identificazione dell'hazard:

- a. Checklist
- b. Group review

Il processo di identificazione dei fattori di rischio richiede personale specializzato e viene spesso condotto attraverso una discussione di gruppo, gestita da una persona che abbia esperienza in termini di tecniche di brainstorming. Solitamente questo ruolo è svolto dal Safety Manager.

A tutti gli hazard che sono stati identificati, deve essere assegnato un numero e devono essere registrati all'interno di un hazard log, il quale deve contenere la descrizione di ogni hazard, le sue conseguenze, la probabilità e la severità di quest'ultime e le misure di mitigazione adottate.

L'hazard log deve essere continuamente aggiornato non appena nuovi hazard vengono identificati e nuove misure di mitigazione introdotte.

7.3.2 RISK MANAGEMENT PROCESSES

Una volta che è stato identificato l'hazard, deve essere valutato il rischio, in termini di sicurezza, delle sue conseguenze.

Deve essere sviluppato e mantenuto un processo di gestione del rischio caratterizzato da: analisi, assessment e controllo.

L'analisi del safety risk, si basa su una ripartizione del rischio in due componenti:

- Probabilità di accadimento
- Severità dell'accadimento

Questi due aspetti vengono racchiusi all'interno della matrice di tollerabilità del rischio (capitolo 3.3).

Ogni conseguenza deve poi essere valutata in termini di tollerabilità del rischio (assessment). I livelli di management che hanno l'autorità di prendere decisioni riguardo la tollerabilità del rischio, devono essere specificati.

Il passaggio successivo consiste nell'eliminazione o nella mitigazione del rischio fino a un livello accettabile (controllo); questo viene raggiunto tramite cambi nelle procedure, modifiche delle difese esistenti o introduzione di nuove difese all'interno del sistema, cambiamenti nel training. Una volta che sono state quindi identificate le azioni di mitigazione, prima che vengano applicate, bisogna valutare se queste introducono nuovi hazard all'interno del sistema.

I processi di Hazard Identification e Risk Assessment iniziano con l'identificazione di tutte le parti interessate; è fondamentale in questa fase il coordinamento, le interfacce e la comunicazione tra le varie parti coinvolte, l'assegnazione delle task e delle responsabilità e la qualifica delle competenze del personale interessato (*Rif. CAMO.A.305*).

Il Safety Risk Management si focalizza sui seguenti aspetti:

- Chiara assegnazione delle responsabilità.
- Al fine di eliminare errori di coordinamento, ogni persona è responsabile di un solo aspetto del processo di gestione del rischio.
- Necessità di segnalare sia gli avvenimenti che possono portare a un degrado della sicurezza ma anche i progressi e i miglioramenti in termini di sicurezza.

Il processo di gestione del rischio deve inoltre garantire che vi sia un canale di comunicazione efficace tra tutte le parti coinvolte per discutere i progressi, le azioni di mitigazione, i cambiamenti nelle disposizioni e qualsiasi altra questione inerente la safety.

7.3.3 INTERNAL INVESTIGATION

Rimanendo in linea con la politica della Just Culture, l'organizzazione deve definire un modo per investigare incidenti e mancanze al fine di capire non solo ciò che è successo ma anche come è successo per evitare la possibilità che simili eventi si possano verificare nuovamente.

L'obiettivo delle investigazioni interne va oltre la segnalazione delle occorrenze (Rif. CAMO.A.160) e include segnalazioni di cui al punto CAMO.A.202(b) [*The scheme shall also enable the collection and evaluation of those errors, near misses, and hazards reported internally that do not fall under point (a)*].

7.3.4 SAFETY PERFORMANCE MONITORING AND MEASUREMENT

Il processo di misura e monitoraggio delle prestazioni in materia di sicurezza è un processo secondo il quale le prestazioni dell'organizzazione in termini di safety vengono confrontate con la Safety Policy e con gli obiettivi definiti dall'organizzazione.

In base alla dimensione dell'organizzazione, alla natura e alla sua complessità, il processo può includere:

- Safety reporting, contenenti anche lo stato di conformità con i requisiti applicabili. Solitamente, all'interno delle organizzazioni, è presente una certa riluttanza nel reporting da parte del personale. Per questo motivo è importante educare al safety reporting e garantire la protezione di chi fornisce l'informazione in materia di safety.
- Safety review, incluse le trends reviews, che vengono condotte durante situazioni di cambiamenti organizzativi o nelle procedure che possono avere un impatto sulla sicurezza, o durante l'introduzione di nuovi equipaggiamenti, componenti o tecnologie.
- Safety audits si focalizzano sull'integrità del SMS e vengono utilizzati per garantire che la struttura dell'SMS sia solida in termini di personale, di rispetto delle procedure approvate, del livello di competenza e formazione necessaria per la gestione delle attrezzature e delle strutture e per mantenere i livelli richiesti di prestazione. Periodicamente valutano lo stato dei processi di controllo del rischio.
Gli audit possono essere sia interni che esterni.
- Safety surveys che esaminano elementi o procedure di una specifica area delle attività della gestione dell'aeronavigabilità.

7.3.5 MANAGEMENT OF CHANGE

I cambiamenti nella struttura organizzativa, nel personale, nella documentazione, nelle politiche e nelle procedure, anche se vengono gestite nel modo appropriato, possono portare all'introduzione di nuovi hazard ed espongono l'organizzazione a un maggior rischio. Le implicazioni sulla sicurezza che un cambiamento può portare, sia esso di grande o piccola entità, devono sempre essere considerate in modo proattivo. In ogni processo di gestione del cambiamento, devono sempre essere valutati l'entità del cambiamento, la criticità e il potenziale impatto sulle prestazioni umane. L'organizzazione deve gestire il rischio legato a questi cambiamenti, definendo un processo documentato al fine di identificare cambiamenti interni ed esterni che possono avere delle conseguenze negative in termini di sicurezza sulla gestione delle attività di continuing airworthiness. Questo viene fatto sfruttando i processi, già implementati, di Hazard Identification, Risk Assessment e mitigazione.

Il processo di gestione del cambiamento fornisce un framework strutturato per la gestione di tutti gli aspetti che riguardano il cambiamento. Infatti un'applicazione disciplinata della gestione del cambiamento può massimizzarne la sua efficienza e minimizzare al contempo i rischi che possono derivarne.

Alcuni esempi di cambiamento sono:

- Cambiamenti nella struttura organizzativa.
- Introduzione di un nuovo tipo di velivolo all'interno delle condizioni di approvazione.
- Cambiamenti significativi nel personale.
- Nuova normativa.
- Cambiamenti nelle disposizioni di sicurezza.
- Cambiamenti nella condizione economica dell'organizzazione.
- Nuovi programmi, nuova location, nuove procedure e nuovi equipaggiamenti.
- Aggiunta di nuovi fornitori.

Un processo formale per la gestione dei cambiamenti, deve tener conto delle seguenti considerazioni:

1. *Criticità dei sistemi e delle attività.* La criticità è strettamente legata al rischio per la sicurezza e si riferisce alle potenziali conseguenze dovute all'improprio utilizzo di equipaggiamenti durante attività che non vengono svolte nel modo corretto. Durante una situazione di cambiamento si deve quindi rispondere alla seguente domanda: "Quanto è importante questo equipaggiamento/attività al fine di garantire le operazioni in sicurezza?" Sicuramente alcune attività sono più importanti di altre al fine di garantire una fornitura dei servizi in sicurezza e gli equipaggiamenti e le attività che presentano una maggiore criticità devono essere riesaminate a seguito delle modifiche per assicurarsi che possano essere intraprese le adeguate azioni correttive al fine di tenere sotto controllo i potenziali rischi per la sicurezza che possono emergere da questi cambiamenti.

2. *Stabilità del sistema e dell'ambiente operativo.* Cambiamenti di stato economico e finanziario, sciopero dei lavoratori, cambiamenti di contesto politico o normativo o cambiamenti ciclici nei modelli metereologici non sono sotto il diretto controllo dell'organizzazione ma quest'ultima deve adottare delle misure per far fronte a questi cambiamenti. Cambiamenti frequenti nell'ambiente operativo o nei sistemi fanno sì che i manager debbano aggiornare informazioni chiave più frequentemente che nelle situazioni normali.
3. *Prestazioni passate.* Le prestazioni passate dei sistemi critici sono un indicatore delle performance future. L'analisi delle tendenze del processo di safety assurance dovrebbe essere impiegato per tenere traccia delle prestazioni della safety nel tempo e usare queste informazioni durante le attività di pianificazione delle attività future in situazioni di cambiamento.

Il cambiamento inoltre può introdurre o inasprire questioni legate ai fattori umani. Infatti cambiamenti nella tecnologia, nel personale, nelle procedure, nell'organizzazione del lavoro e nei processi produttivi, possono influenzare le prestazioni. Il motivo per cui si integrano i fattori umani all'interno del processo di gestione del cambiamento è proprio quello di minimizzare il rischio considerando l'effetto dei cambiamenti sul personale interno all'organizzazione.

Una gestione efficiente del cambiamento deve essere supportata dall'implementazione di un processo di Hazard Identification e Risk Assessment. Precedentemente (Capitolo 2.2) è stata discussa l'importanza della descrizione del sistema in quanto una delle attività fondamentali nella programmazione di un SMS. Nel momento in cui il sistema evolve, bisogna che la descrizione del sistema e l'analisi dei fattori di rischio vengano riviste periodicamente.

7.3.6 CONTINUOUS IMPROVEMENT

Il SMS deve essere dinamico piuttosto che statico e puntare al miglioramento continuo delle prestazioni di sicurezza dell'organizzazione. Un miglioramento continuo può avvenire solo quando l'organizzazione garantisce un monitoraggio costante dell'efficienza delle operazioni tecniche e delle azioni correttive.

Questo può essere ottenuto tramite:

- Audit condotti da organizzazioni esterne.
- Assessment per verificare l'efficienza della safety culture e del sistema di gestione e in particolare per verificare l'efficienza del processo di gestione del rischio.
- Staff surveys, inclusa cultural survey, per avere un feedback su come il personale è impegnato all'interno del Safety Management System.
- Monitorare la ricorrenza di incidenti e avvenimenti negativi.
- Valutazione dei safety performance indicators e revisione di tutte le informazioni relative alle prestazioni in termini di safety.

- Identificazione delle lezioni imparate a seguito di incidenti.

Nel caso di prestazioni del SMS al di sotto degli standards l'organizzazione deve identificarne le cause e adottare i necessari provvedimenti per la loro eliminazione o mitigazione.

7.3.7 IMMEDIATE SAFETY ACTION AND COORDINATION WITH THE OPERATOR'S EMERGENCY RESPONSE PLAN (ERP)

È necessario implementare una procedura per consentire all'organizzazione di agire prontamente quando identifica problemi di sicurezza che potrebbero avere un effetto immediato sulla sicurezza del volo, comprese chiare istruzioni su chi contattare presso il proprietario / operatore e su come contattare queste persone, anche al di fuori del normale orario lavorativo. Un piano di risposta di emergenza (ERP) riporta le azioni che devono essere prese a seguito di un incidente e identifica chi è il responsabile per ciascuna azione. Lo scopo di un ERP è che sia assicurata una transizione ordinata ed efficiente dalle operazioni normali alle operazioni di emergenza, inclusa l'assegnazione delle responsabilità. Nel piano è anche contenuta l'autorizzazione alle azioni sia da parte del personale chiave, così come il coordinamento degli sforzi per gestire l'emergenza. L'obiettivo generale è la prosecuzione sicura delle operazioni o il ritorno quanto prima alle normali condizioni.

7.4 SAFETY PROMOTION

Le attività di safety promotion supportano:

1. Le politiche dell'organizzazione incentivando una cultura della sicurezza e creando un ambiente favorevole al raggiungimento degli obiettivi dell'organizzazione in termini di safety.
2. Organisational learning (apprendimento organizzativo).
3. Implementazione di un sistema di segnalazione in materia di sicurezza e sviluppo della Just Culture.

A seconda del particolare problema di sicurezza, la promozione della sicurezza può anche costituire o integrare azioni di mitigazione del rischio.

Il processo di safety promotion include:

- Safety training
- Safety communication.

7.4.1 SAFETY TRAINING

Rif.CAMO.A.200(a)(4) [The organisation shall establish, implement, and maintain a management system that includes: maintaining personnel trained and competent to perform their tasks]

È importante che tutto il personale abbia la necessaria competenza per lo svolgimento delle funzioni e delle responsabilità inerenti la sicurezza che gli sono state affidate. Questo risultato è ottenuto attraverso la formazione continua degli individui, indipendentemente dal loro livello all'interno dell'organizzazione.

I programmi di training devono essere adattati alla complessità e ai bisogni dell'organizzazione e devono includere la politica di sicurezza dell'organizzazione e una descrizione sui concetti fondamentali del SMS.

I requisiti del training devono essere documentati per ogni area all'interno dell'organizzazione e è necessario verificare che ogni individuo riceva il training necessario.

Il training deve essere fornito almeno nelle seguenti circostanze:

- Durante l'implementazione iniziale dei processi di gestione della sicurezza.
- A tutto il personale a cui recentemente sono state assegnati compiti riguardanti i processi di gestione della sicurezza.
- In modo regolare a tutto il personale per mantenerlo addestrato e per essere aggiornato riguardo i cambiamenti all'interno del sistema di gestione.
- Durante periodi di cambiamento di ruoli e responsabilità all'interno dell'organizzazione.

Il personale coinvolto nei processi di gestione del mantenimento dell'aeronavigabilità deve ricevere sia un training iniziale che un training periodico, appropriato alle proprie responsabilità.

Il training deve essere fornito al seguente personale:

- Line managers.
- Persone coinvolte in attività legate ai processi di monitoraggio delle conformità e/o gestione della sicurezza, inclusa l'applicazione dei fattori umani e investigazioni interne. Il personale dedicato alla gestione della compliance monitoring function deve ricevere un training adeguato a questo ruolo, che comprenda i requisiti di compliance monitoring, manuali e procedure, tecniche di audit, di reporting e recording.
- Personale di supporto tecnico come pianificatori, ingegneri e personale addetto alla documentazione tecnica.
- Airworthiness review staff.
- Personale dedicato allo sviluppo, alla revisione, alla valutazione dell'efficienza dell'AMP e al programma di affidabilità. Il personale dedicato a queste attività deve ricevere training riguardante analisi statistica e metodi affidabilistici e la metodologia usata nello sviluppare il programma di manutenzione raccomandato dal costruttore, come parte delle istruzioni per il mantenimento dell'aeronavigabilità (ICA).

Lo scopo del training in materia di sicurezza e il relativo programma di training dipende molto dalla dimensione e dalla complessità dell'organizzazione. Il training deve riflettere l'evolvere del sistema di gestione compresi i cambiamenti di ruolo del personale.

Il training iniziale deve coprire tutti gli aspetti contenuti nel syllabus di cui alla *GM2 CAMO.A.305(g)*, che però possono essere adattati per meglio riflettere il bisogno della singola organizzazione.

Il training iniziale deve essere fornito al personale entro i sei mesi dall'entrata del personale all'interno dell'organizzazione. Il personale reclutato da un'altra organizzazione deve ricevere training aggiuntivo.

Il training periodico ha invece l'obiettivo di garantire che il personale rimanga aggiornato per quanto riguarda i principi del SMS e degli human factors e per raccogliere feedback su questioni legate al SMS. Deve essere coinvolto il compliance monitoring staff e il personale chiave nella gestione della safety per facilitare il processo di feedback.

La formazione periodica sulla sicurezza deve essere erogata come corso dedicato o integrato nell'ambito di altra formazione. Dovrebbe avere una durata adeguata all'interno di un periodo di due anni, in relazione ai risultati dell'audit indipendente e di altre fonti interne / esterne di informazioni in materia di sicurezza e questioni legate agli HF.

L'organizzazione dovrebbe valutare la necessità di una formazione specifica; per esempio, per quanto riguarda gli standards di competenza stabiliti nella *AMC 20-22 "Electrical Wiring Interconnection System"* (EWIS), e nella *AMC 20-20 "Continuing Structural Integrity Programme"* o "Critical Design Configuration Control" (CDCCL).

Fa parte del training specifico anche il fuel tank safety training, di cui si riporta una guida nell'Appendice III alla *AMC4.CAMO.A.305(g)*.

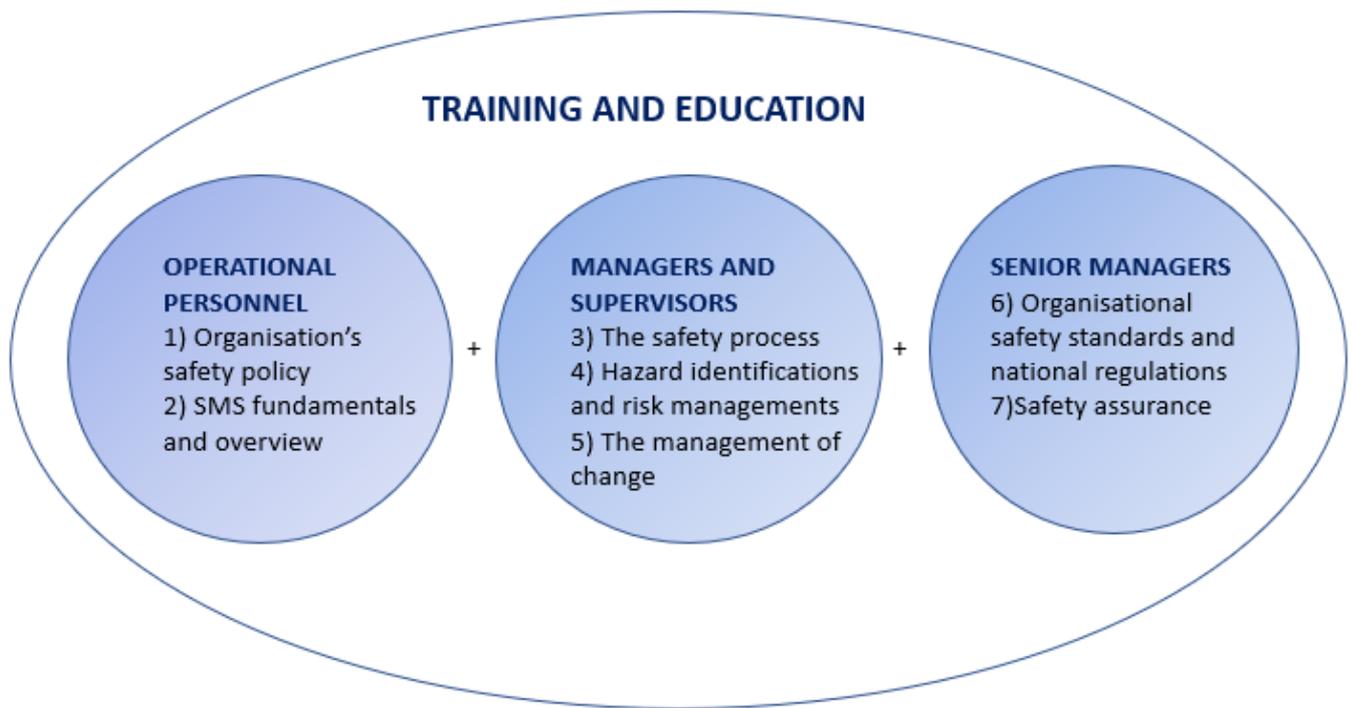


Figura 12 Training

7.4.2 SAFETY COMMUNICATION

L'organizzazione deve stabilire un sistema di comunicazione riguardo alle questioni di sicurezza, che:

- Garantisca che tutto il personale sia consapevole delle attività della gestione della safety e delle proprie responsabilità.
- Trasmetta informazioni safety-critical, soprattutto relative alla valutazione del rischio e all'analisi dei fattori di rischio.
- Spieghi il motivo per cui determinate azioni sono state messe in atto.
- Spieghi perché alcune procedure sono state introdotte o modificate.

Un modo per comunicare questioni di sicurezza è lo svolgimento di incontri regolari con il personale durante i quali vengono discusse azioni, procedure e informazioni raccolte. Altri esempi di comunicazione includono, newsletter, bollettini, email o siti web.

7.5 MANAGEMENT SYSTEM DOCUMENTATION

Rif. CAMO.A.200 (a)(5) [The organisation shall establish, implement, and maintain a management system that includes: documentation of all management system key processes, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation]

L'organizzazione deve documentare la sua politica di sicurezza, gli obiettivi e i processi del sistema di gestione all'interno di un manuale (come SMSM O MSM) o nel CAME (Parte 2 "Management System Procedures").

Le organizzazioni che sono in possesso di più certificati nell'ambito di applicazione del regolamento (EU)2018/1139 possono scegliere di usare un manuale separato per evitare duplicazioni. Questo manuale o il CAME è lo strumento principale per comunicare a tutta l'organizzazione il proprio approccio al sistema di gestione.

Nel caso in cui l'organizzazione scelga di documentare alcune delle informazioni richieste in modo separato, il CAME deve contenere riferimento a queste informazioni separate. Tutti questi documenti sono parte integrante della documentazione del sistema di gestione.

7.5.1 CONTINUING AIRWORTHINESS MANAGEMENT EXPOSITION (CAME)

L'obiettivo del CAME è quello di:

- Specificare lo scope of work e indicare come l'organizzazione è organizzata per essere conforme ai requisiti dell'annesso Vc (Part CAMO).
- Fornire tutte le informazioni e le procedure necessarie al personale dell'organizzazione per svolgere le proprie attività.

Il rilascio iniziale del CAME deve essere soggetto all'approvazione dell'autorità competente e deve essere continuamente modificato e aggiornato affinché resti conforme con le eventuali modifiche fatte all'interno dell'organizzazione.

Di seguito si riporta un esempio di CAME. Laddove un'organizzazione utilizzi un formato diverso, ad esempio, per consentire al CAME di essere utilizzato per più di un'approvazione nell'ambito del regolamento (UE) 2018/1139, l'esposizione deve contenere un cross-reference Annex che utilizza questo elenco come indice, con una spiegazione di dove un determinato argomento può essere trovato all'interno dell'esposizione.

Part 0	GENERAL ORGANISATION, SAFETY POLICY AND OBJECTIVES
0.1	Safety policy, objectives and accountable manager statement
0.2	General information and scope of work
0.3	Management information
0.4	Management organisation chart
0.5	Procedure for changes requiring prior approval
0.6	Procedure for changes not requiring prior approval
0.7	Procedure for alternative means of compliance (AltMoC)
Part 1	CONTINUING AIRWORTHINESS MANAGEMENT PROCEDURES
1.1a	Use of aircraft continuing airworthiness record system and if applicable, aircraft technical log (ATL) system
1.1b	MEL application
1.2	Aircraft maintenance program (AMP)- development amendment and approval
1.3	Continuing airworthiness records: responsibilities, retention and access
1.4	Accomplishment and control of airworthiness directives
1.5	Analysis of the effectiveness of the maintenance programme(s)
1.6	Non-mandatory modifications and inspections
1.7	Repairs and modifications
1.8	Defect reports
1.9	Engineering activity
1.10	Reliability programmes
1.11	Pre-flight inspections
1.12	Aircraft weighing
1.13	Maintenance check flight procedures
Part 2	MANAGEMENT SYSTEM PROCEDURES
2.1	Hazard identification and safety risk management schemes
2.2	Internal safety reporting and investigations
2.3	Safety action planning
2.4	Safety performance monitoring
2.5	Change management
2.6	Safety training and promotion
2.7	Immediate safety action and coordination with operator's Emergency Response Plan (ERP)
2.8	Compliance monitoring

2.8.1	Audit plan and audit procedure
2.8.2	Monitoring of continuing airworthiness management activities
2.8.3	Monitoring of the effectiveness of the maintenance programme(s)
2.8.4	Monitoring that all maintenance is carried out by an appropriate maintenance organisation
2.8.5	Monitoring that all contracted maintenance is carried out in accordance with the contract, including subcontractors used by the maintenance contractors
2.8.6	Compliance monitoring personnel
2.9	Control of personnel competency
2.10	Management system record-keeping
2.11	Occurrence reporting
Part 3	CONTRACTED MAINTENANCE-MANAGEMENT OF MAINTENANCE
3.1	Maintenance contractor selection procedure
3.2	Product audit for aircraft
Part 4	AIRWORTHINESS REVIEW PROCEDURES
4.1	Airworthiness review staff
4.2	Documented review of aircraft records
4.3	Physical survey
4.4	Additional procedures for recommendations to competent authorities for the import of aircraft
4.5	ARC recommendations to competent authority
4.6	Issue of ARC
4.7	Airworthiness review records, responsibilities, retention and access
4.8	ARC extension
Part 4B	PERMIT TO FLY PROCEDURES
4B.1	Conformity with approved flight conditions
4B.2	Issue of the permit to fly under the CAMO privilege
4B.3	Permit to fly authorised signatories
4B.4	Interface with the local authority for the flight
4B.5	Permit to fly records, responsibilities, retention and access
Part 5	SUPPORTING DOCUMENTS
5.1	Sample documents, including the template of the ATL system
5.2	List of airworthiness review staff
5.3	List of subcontractors as per point <i>CAMO.A.125(d)(3)</i>

5.4	List of contracted maintenance organisations and list of maintenance contracts as per point <i>CAMO.A.300(a)(13)</i>
5.5	Copy of contracts for subcontracted work (Appendix II to <i>AMC1 CAMO.A.125(d)(3)</i>)
5.6	List of approved maintenance programme as per point <i>CAMO.A.300(a)(12)</i>
5.7	List of currently approved alternative means of compliance as per point <i>CAMO.A.300(a)(13)</i>

Figura 13 Continuing Airworthiness Management Exposition

Il personale deve essere familiare con le parti del CAME che sono importanti per le proprie attività.

La CAMO deve indicare una persona responsabile per monitorare il CAME, inclusi eventuali manuali delle procedure associati, in accordo con il punto *CAMO.A.300(c)*.

Per la pubblicazione del CAME, la CAMO può utilizzare l'elaborazione elettronica dei dati (EDP), prestando però attenzione alla compatibilità dei sistemi EDP con la diffusione, sia interna che esterna, del CAME.

7.6 COMPLIANCE MONITORING

7.6.1 COMPLIANCE MONITORING FUNCTION

La funzione di compliance monitoring è uno degli elementi necessari per soddisfare i requisiti applicabili. La funzione di compliance monitoring stessa deve essere soggetta a monitoraggio indipendente delle conformità e deve essere indipendente dalla funzione di gestione della aeronavigabilità continua.

7.6.2 COMPLIANCE MONITORING

Gli obiettivi primari del monitoraggio della conformità sono quelli di fornire una funzione di monitoraggio delle conformità dell'organizzazione ai requisiti applicabili, alle politiche e alle procedure e richiedere delle azioni correttive laddove vengano identificate delle non conformità. L'indipendenza del compliance monitoring viene garantita facendo sì che audit e ispezioni vengano svolte da personale che non è responsabile delle funzioni, delle procedure o dei prodotti che vengono auditati o ispezionati.

7.6.3 INDEPENDENT AUDIT

L'audit indipendente è un elemento essenziale del monitoraggio delle conformità. E' un processo oggettivo di controllo dell'abilità della CAMO nel portare avanti la gestione dell'aeronavigabilità continua soddisfacendo gli standard richiesti dalla normativa.

L'organizzazione può stabilire un audit plan per organizzare il processo di audit. Il piano di audit dovrebbe garantire che tutti gli aspetti della conformità riferiti alla Parte-CAMO siano verificati ogni anno, comprese tutte le attività subcontrattate; l'audit può essere effettuato come un singolo esercizio o suddiviso nel periodo annuale. Se una procedura è in comune a più linee di produzione, non è necessario che venga verificata per ogni linea nel caso in cui, durante gli audit precedenti, non sia stato evidenziato alcun finding.

Laddove l'organizzazione abbia più di una sede approvata, il piano di audit dovrebbe garantire che ogni sede sia sottoposta ad un audit annuale o ad un intervallo di tempo determinato attraverso una valutazione del rischio concordata dall'autorità competente ma che non superi il ciclo di pianificazione dell'audit.

Ogni volta che viene effettuato un audit deve essere fatto un report che descrive ciò che è stato verificato e i finding di non conformità emersi rispetto ai requisiti e alle procedure applicabili.

Le relazioni di independent audit di cui all'*AMC2 CAMO.A.200 (a) (6)* devono essere inviate ai relativi dipartimenti per l'implementazione delle azioni correttive, fornendo le date entro cui queste azioni devono essere implementate.

Se viene utilizzato personale esterno per eseguire audit indipendenti, tali audit vengono eseguiti sotto la responsabilità del Compliance Monitoring Manager e l'organizzazione rimane responsabile di garantire che il personale esterno disponga delle conoscenze e delle esperienze appropriate alle attività oggetto di audit, comprese le conoscenze e l'esperienza nel monitoraggio della conformità. L'organizzazione mantiene la responsabilità ultima per l'efficacia della funzione di monitoraggio delle conformità, in particolare per l'effettiva implementazione di tutte le azioni correttive.

7.6.4 FEEDBACK SYSTEM

Un elemento importante per la gestione delle conformità è il sistema di feedback. La principale funzione del sistema di feedback è garantire che tutti i finding risultanti dall'audit indipendente siano propriamente investigati e corretti entro i tempi previsti. Nel momento in cui viene identificata una non conformità, la compliance monitoring function deve garantire che le cause e i fattori che hanno contribuito alla non conformità vengano identificati e che vengano definite delle azioni correttive. Il sistema di feedback deve definire chi è tenuto a risolvere eventuali non conformità e la procedura da seguire se l'azione correttiva non viene completata entro il periodo di tempo

definito. I dipartimenti designati all'implementazione delle azioni di mitigazione, devono fornire alla compliance monitoring function delle informazioni sullo stato di implementazione di queste azioni.

L'Accountable Manager deve tenere meetings periodici con lo staff per controllare il progresso di ogni azione correttiva; questi meetings possono essere delegati al Compliance Monitoring Manager a condizione che l'Accountable Manager incontri lo staff almeno due volte l'anno per monitorare le prestazioni della compliance monitoring function e che riceva un report semestrale dei finding individuati.

Tutti i record relativi all'audit indipendente e al sistema di feedback devono essere conservati per un periodo di cinque anni o per un periodo tale da supportare le modifiche al ciclo di pianificazione dell'audit.

8 SISTEMA INTERNO DI SEGNALAZIONE IN MATERIA DI SICUREZZA

(Rif. CAMO.A.202 *Regulation (EU) 2019/1383*)

Nell'ambito del suo sistema di gestione, l'organizzazione deve istituire un sistema interno di segnalazione in materia di sicurezza che consenta di rilevare e valutare gli eventi da segnalare di cui al punto CAMO.A 160. Avvalendosi di tale sistema l'organizzazione deve:

- Individuare le cause e i fattori che hanno contribuito a eventuali errori, incidenti, e pericoli segnalati e affrontarli nell'ambito della gestione del rischio di sicurezza in conformità al punto CAMO.A.200 (a)(3).
- Garantire la valutazione delle informazioni note e pertinenti agli errori, all'incapacità di seguire le procedure e ai pericoli.

L'organizzazione deve consentire l'accesso al proprio sistema interno di segnalazione in materia di sicurezza a qualsiasi impresa subcontrattata e deve cooperare nelle inchieste di sicurezza con qualsiasi altra impresa che contribuisca in modo significativo alla sicurezza delle sue attività di gestione nel mantenimento dell'aeronavigabilità.

L'obiettivo generale dello schema interno di segnalazione della sicurezza è quello di raccogliere informazioni fornite dal personale e usarle per migliorare il livello di compliance e performance in materia di sicurezza all'interno dell'organizzazione. Lo scopo non è quello di attribuire una colpa o individuare un colpevole.

Ciascun sistema interno di segnalazione della sicurezza dovrebbe essere riservato e consentire e incoraggiare la comunicazione libera di qualsiasi evento potenzialmente correlato alla sicurezza, compresi incidenti, problemi di sicurezza e hazard identificati. Ciò sarà facilitato dalla creazione di una Safety Culture.

Gli obiettivi sono:

- Consentire una valutazione delle implicazioni per la sicurezza di ciascun incidente, problema di sicurezza e hazard, in modo che possano essere intraprese tutte le azioni necessarie.
- Assicurare che la conoscenza degli incidenti rilevanti, dei problemi di sicurezza e degli hazard sia condivisa in modo che altre persone e organizzazioni possano imparare da essi.

Questo sistema è una parte fondamentale della funzione di monitoraggio e deve essere complementare alle procedure giornaliere e ai sistemi di controllo, ma non deve sostituirli.

Lo schema deve contenere i seguenti elementi:

- a) Obiettivi chiaramente identificati e obiettivi con impegno aziendale dimostrabile.

- b) Una politica di Just Culture, come parte della Safety Policy, e le sue relative procedure di implementazione.
- c) Un processo per identificare quelle segnalazioni che richiedono ulteriori investigazioni e, in questo caso, indagare su tutti i fattori causali, inclusi fattori tecnici, organizzativi, manageriali e fattori umani che contribuiscono all'incidente o al fatto identificato. Inoltre analizzare i dati raccolti per mostrare gli andamenti e la frequenza dei fattori identificati.
- d) Azioni correttive appropriate basate sui finding.
- e) Cooperazione tra organizzazione e proprietario/operatore nelle indagini sugli eventi scambiando informazioni pertinenti per migliorare la sicurezza aerea.

E' importante che il sistema interno di segnalazione garantisca riservatezza nei confronti di chi fa la segnalazione e sia un sistema closed-loop, per garantire che vengano intraprese azioni interne per affrontare eventuali problemi di sicurezza.

9 SEGNALAZIONE DI EVENTI

CAMO.A.160

Regulation (EU) 2019/1383

- (a) As part of its management system the organisation shall implement an occurrence reporting system that meets the requirements defined in Regulation (EU) No 376/2014 and Implementing Regulation (EU) 2015/10181.
- (b) Without prejudice to point (a), the organisation shall ensure that any incident, malfunction, technical defect, exceeding of technical limitations, occurrence that would highlight inaccurate, incomplete or ambiguous information contained in data established in accordance with Annex I (Part-21) to Regulation (EU) No 748/2012 or other irregular circumstance that has or may have endangered the safe operation of the aircraft and that has not resulted in an accident or serious incident are reported to the competent authority and to the organisation responsible for the design of the aircraft.
- (c) Without prejudice to Regulation (EU) No 376/2014 and Implementing Regulation (EU) 2015/1018, the reports referred to in points (a) and (b) shall be made in a form and manner established by the competent authority and shall contain all pertinent information about the condition known to the organisation.
- (d) Reports shall be made as soon as possible, but in any case within 72 hours of the organisation identifying the condition to which the report relates, unless exceptional circumstances prevent this.
- (e) Where relevant, the organisation shall produce a follow-up report to provide details of actions it intends to take to prevent similar occurrences in the future, as soon as these actions have been identified. This report shall be produced in a form and manner established by the competent authority.

L'organizzazione deve, all'interno del sistema di gestione della sicurezza, introdurre un sistema di segnalazione di eventi, basato su un approccio proattivo e basato sulle evidenze. Al fine di migliorare la sicurezza, informazioni relative alla safety devono essere raccolte, mantenute, protette scambiate e analizzate e sulla base di queste, devono essere messe in atto delle azioni adeguate.

Il sistema di segnalazione deve essere adeguato alla dimensione dell'organizzazione e allo scopo della sua attività. Nel caso di piccole organizzazioni è possibile unire alcune funzioni riguardanti la segnalazione di eventi all'interno dell'organizzazione, condividere attività di occurrence reporting con altre organizzazioni o delegare i processi di raccolta dei dati a enti specializzati approvati dall'autorità competente dello stato membro.

(Rif. Regulation (EU)No 376/2014 [*..It should therefore be possible, in particular for smaller organisations, to decide to join or merge functions related to occurrence handling within the organisation, to share occurrence reporting tasks with other organisations of the same nature or to outsource the collection, evaluation, processing, analysis and storage of details of occurrences to specialised entities approved by the competent authorities of the Member States..*])

Esistono due tipologie di reporting:

- Mandatory reporting
- Voluntary reporting

La prima tipologia consiste nel segnalare eventi che possono rappresentare un rischio significativo per la sicurezza dell'aviazione mentre i secondi riguardano tutte le altre informazioni che si pensa possano essere un potenziale pericolo per la sicurezza. Il sistema di segnalazione volontario deve essere complementare al sistema di segnalazione obbligatorio ed entrambi devono permettere all'individuo di riportare dettagli delle situazioni che possono avere un impatto sulla safety.

Per le organizzazioni che hanno il loro principale place of business in uno stato membro, il regolamento (EU) 2015/1018 presenta una lista di occorrenze che devono essere riportate obbligatoriamente. Questa lista non deve essere considerata una raccolta esaustiva di tutte le questioni che possono risultare un rischio per la sicurezza e per questo motivo il report non deve essere limitato a tale lista (Rif. GM.CAMO.A.160).

Le organizzazioni devono analizzare le informazioni raccolte al fine di identificare potenziali hazard e mettere in atto appropriate azioni correttive o preventive. I risultati di queste analisi devono essere mandati all'autorità competente dello stato membro o all'Agenzia.

(Rif. Regulation (EU)No 376/2014 [*..Organisations should send the preliminary results of their analyses to the competent authority of their Member States or to the Agency and should also send them the final results if those results identify an actual or potential aviation safety risk.*])

E' importante che i dati raccolti siano completi e precisi, in quanto informazioni poco corrette potrebbero portare a risultati sbagliati e a una perdita dell'affidabilità del sistema di segnalazione. Al fine di garantire la qualità dei report, essi devono contenere alcune informazioni minime, che dipendono dal tipo di avvenimento per il quale si sta facendo la segnalazione.

Tutte le informazioni contenute nei report devono essere appropriatamente protette e usate esclusivamente al fine di mantenere o migliorare la sicurezza. Questo obiettivo è raggiunto tramite il concetto di "Just Culture", il cui obiettivo è il perseguimento della sicurezza e non quello di individuare un colpevole e attribuire una colpa. La persona che effettua la segnalazione o una persona menzionata nel report deve essere adeguatamente protetta. Il concetto di "Just Culture" è un elemento essenziale per la "Safety Culture" che permette di creare le basi per un solido sistema di gestione della sicurezza. Il concetto di "Just Culture" deve incoraggiare gli individui a riportare informazioni sulla safety. Il personale deve essere protetto e non deve essere soggetto a nessuna

colpa o pregiudizio, ad eccezione del caso in cui sia manifestata la volontà di causare eventi che possono compromettere il livello di sicurezza.

(Rif. Regulation (EU) No 376/2014 [..except in cases of wilful misconduct or where there has been manifest, severe and serious disregard with respect to an obvious risk and profound failure of professional responsibility to take such care as is evidently required in the circumstances, causing foreseeable damage to a person or to property, or seriously compromising the level of aviation safety.])

(Rif AMC1.CAMO.A.160)

Nel caso in cui l'organizzazione sia in possesso di più certificati nell'ambito di applicazione del regolamento (EU) 2018/1139, l'organizzazione può stabilire un sistema di occurrence reporting integrato che copra tutti i certificati posseduti, mentre report singoli devono essere fatti se:

- Il report include tutte le informazioni pertinenti dal punto di vista dei diversi certificati di organizzazione posseduti.
- Il report affronta tutti i campi di dati obbligatori e identifica chiaramente tutti i titolari di certificati per i quali è stato presentato il report.
- L'autorità competente per tutti i certificati è la stessa e il report singolo è stato concordato con tale autorità.

L'organizzazione deve assegnare la responsabilità a una o più persone qualificate per coordinare le azioni sulle airworthiness occurrences e per avviare ogni investigazione necessaria e le attività di follow up. Se vengono identificate più persone per questo ruolo, l'organizzazione deve identificare una persona di riferimento per garantire che venga istituito un singolo canale di segnalazione verso l'Accountable Manager.

L'organizzazione dovrebbe condividere i report relativi alle occorrenze che hanno un impatto sulla safety con il design approval holder del velivolo al fine di consentirgli di fornire istruzioni e raccomandazioni di servizio appropriate a tutti i proprietari o operatori. Questo è necessario per avere un feedback riguardo le azioni di mitigazioni proposte o per ottenere una soluzione a uno specifico problema.

10 FRAMEWORK PER L'IMPLEMENTAZIONE DEL SMS

Il framework proposto da ICAO per lo sviluppo e l'implementazione del SMS consiste in 4 componenti e 12 elementi, e la sua implementazione deve essere commisurata alla dimensione dell'organizzazione e alla complessità dei servizi forniti.

Rif. CAMO.A.200(b) *[The management system shall correspond to the size of the organisation and the nature and complexity of its activities, taking into account the hazards and associated risks inherent in these activities]*

1. Safety policy and objectives

- 1.1 Management commitment
- 1.2 Safety accountability and responsibilities
- 1.3 Appointment of key safety personnel
- 1.4 Coordination of emergency response planning
- 1.5 SMS documentation

2. Safety risk management

- 2.1 Hazard identification
- 2.2 Safety risk assessment and mitigation

3. Safety assurance

- 3.1 Safety performance monitoring and measurement
- 3.2 The management of change
- 3.3 Continuous improvement of the SMS

4. Safety promotion

- 4.1 Training and education
- 4.2 Safety communication

Le due attività principali sono il Safety Risk Management e la Safety Assurance. Queste sono condotte grazie al supporto della politica e degli obiettivi di sicurezza e della promozione della safety.

10.1 SAFETY POLICY AND OBJECTIVES

Rif.CAMO.A.200(a)(2) [The organisation shall establish, implement, and maintain a management system that includes a description of the overall philosophies and principles of the organisation with regard to safety, referred to as the safety policy]

10.1.1 MANAGEMENT COMMITMENT

L'organizzazione deve definire una Safety Policy in accordo con i requisiti nazionali e internazionali. La Safety Policy, firmata dall' Accountable Manager, deve:

- Riflettere l'impegno organizzativo in materia di sicurezza, compresa la promozione di una Safety Culture.
- Includere una chiara dichiarazione sulla fornitura delle risorse necessarie per l'attuazione della politica di sicurezza.
- Includere procedure di safety reporting.
- Indicare chiaramente quali tipi di comportamenti sono inaccettabili in relazione alle attività di trasporto aereo del service provider e includere le circostanze in cui non sarebbe applicabile un'azione disciplinare.
- Essere comunicata, con visibile approvazione, a tutta l'organizzazione.
- Essere periodicamente revisionata per garantire che rimanga pertinente e appropriata all'organizzazione.

Tenendo conto della politica di sicurezza, devono essere definiti anche gli obiettivi. Gli obiettivi di safety indicano ciò che l'organizzazione vuole raggiungere in termini di sicurezza e deve definire gli step necessari a raggiungere tali obiettivi. Sia gli obiettivi di safety che gli standard di safety performance devono essere collegati agli indicatori di safety performance, ai safety performance targets e ai piani d'azione del SMS.

Gli obiettivi devono:

- Riflettere l'impegno del service provider a mantenere o migliorare costantemente l'efficacia complessiva dell'SMS.
- Essere comunicati a tutta l'organizzazione.
- Essere periodicamente rivisti per garantire che rimangano pertinenti e appropriati.

10.1.2 SAFETY ACCOUNTABILITIES AND RESPONSABILITIES

Il service provider deve:

- Identificare il dirigente responsabile che, indipendentemente da altre funzioni, è responsabile per conto dell'organizzazione per l'implementazione e il mantenimento di un SMS efficace.
- Definire chiaramente le linee di responsabilità sulla sicurezza all'interno dell'organizzazione.
- Identificare le responsabilità di tutti i membri dell'organizzazione, indipendentemente dal ruolo, riguardo le prestazioni di sicurezza dell'organizzazione.
- Documentare e comunicare la responsabilità in materia di sicurezza a tutta l'organizzazione.
- Definire con l'autorità livelli di gestione che possano prendere decisioni in merito alla tollerabilità del rischio di sicurezza.

10.1.3 APPOINTMENT OF KEY SAFETY PERSONNEL

Il service provider deve indicare un Safety Manager che è responsabile per l'implementazione e il mantenimento del SMS. In base alla dimensione dell'organizzazione e alla complessità delle sue attività, queste responsabilità possono essere assegnate a una o più persone adempiendo al ruolo del Safety Manager, quale sua unica funzione o combinato con altri compiti, a condizione che questi non comportino conflitti di interessi.

(Rif. ICAO Annex 19 Appendix 2 [Depending on the size of the service provider and the complexity of its aviation products or services, the responsibilities for the implementation and maintenance of the SMS may be assigned to one or more persons, fulfilling the role of safety manager, as their sole function or combined with other duties, provided these do not result in any conflicts of interest.])

10.1.4 COORDINATION OF EMERGENCY RESPONSE PLANNING (ERP)

L'organizzazione deve stabilire un piano di risposta alle emergenze da utilizzare in caso di incidenti o altre emergenze e deve essere coordinato con gli ERP delle organizzazioni con le quali ci si deve interfacciare durante lo svolgimento delle proprie attività.

10.1.5 SMS DOCUMENTATION

E' necessario che tutti gli aspetti del SMS siano chiaramente documentati in modo da mantenere un'accurata registrazione delle ragioni per cui le decisioni sono state prese e deve far riferimento, alla normativa applicabile, nazionale e internazionale. L'organizzazione deve sviluppare un manuale del sistema di gestione della sicurezza che deve includere:

- Politica e obiettivi di sicurezza.
- Requisiti del SMS.
- Processi e procedure del SMS.
- Responsabilità per i processi e le procedure del SMS.

L'organizzazione deve sviluppare dei record riguardanti le attività del SMS. Manuali e record, in base alla dimensione dell'organizzazione e alla complessità delle sue attività, possono essere sotto forma di documenti autonomi o possono essere integrati con altri documenti organizzativi (o documentazione) gestiti dal service provider.

10.2 SAFETY RISK MANAGEMENT

Un'organizzazione gestisce la sicurezza garantendo, attraverso il sistema di gestione della sicurezza, che i rischi delle conseguenze di un hazard, vengano mantenuti sotto un livello accettabile definito ALARP.

10.2.1 HAZARD IDENTIFICATION

L'organizzazione deve sviluppare e mantenere un processo finalizzato all'identificazione degli hazard associati alle attività dell'organizzazione. Questo processo deve essere basato su una combinazione di metodi reattivi e proattivi.

I metodi per l'identificazione degli hazard, sono stati già presentati nel capitolo 3.2.2.

10.2.2 RISK ASSESTMENT AND MITIGATION

L'organizzazione deve sviluppare e mantenere un processo che garantisca l'analisi, la valutazione e il controllo del rischio per la sicurezza derivante dagli hazard identificati. Questo processo deve includere un metodo predittivo di analisi dei dati sulla sicurezza.

10.3 SAFETY ASSURANCE

La Safety Assurance è l'insieme dei processi e attività con cui l'organizzazione verifica le prestazioni e l'efficacia del SMS, determina se esso è conforme agli obiettivi e ai requisiti di sicurezza e ne assicura il suo miglioramento continuo.

Il processo di Safety Assurance è complementare a quello di compliance monitoring, entrambi comprendono analisi, documentazione, auditing e valutazioni per assicurare che gli obiettivi e i criteri di sicurezza siano soddisfatti. Mentre il secondo si concentra sulla conformità dell'organizzazione ai requisiti normativi, la Safety Assurance monitora in maniera specifica l'efficacia delle mitigazioni dei rischi (safety controls) sulla safety.

Le safety performance devono essere verificate facendo riferimento ai safety performance indicators e ai safety performance targets.

10.3.1 SAFETY PERFORMANCE MONITORING AND MEASUREMENT

Il primo compito della safety assurance è il controllo. Questo viene raggiunto tramite il monitoraggio e la misura delle prestazioni in termini di sicurezza, processo tramite il quale queste ultime vengono confrontate con la politica e gli obiettivi di sicurezza. Di seguito una lista dei generici aspetti che devono essere considerati per assicurare la safety, attraverso il monitoraggio e la misura delle prestazioni.

- Responsabilità. Colui che risponde della gestione delle attività operative (planning, organizing, directing, controlling).
- Autorità. Chi dirige, controlla, cambia le procedure e chi prende la decisione in materia di accettabilità del rischio.
- Procedure. Modalità per svolgere le attività al fine del raggiungimento di un obiettivo.
- Controlli. Elementi del sistema inclusi hardware, software, procedure speciali al fine di mantenere le attività nella giusta direzione.
- Interfacce. Comunicazione, consistenza delle procedure, definizione delle responsabilità all'interno dell'organizzazione.
- Misure del processo. Modalità per fornire dei feedback ai responsabili sul fatto che le azioni necessarie sono in svolgimento, sugli output ottenuti e sul raggiungimento dei risultati prefissati.

10.3.2 THE MANAGEMENT OF CHANGE

Le attività di un'organizzazione possono essere soggette a frequenti variazioni. E' pertanto necessario implementare un processo di identificazione dei potenziali pericoli che possono derivare da questi cambiamenti e valutare l'impatto sulla sicurezza degli eventuali cambiamenti apportati.

Un processo formale di gestione del cambiamento deve identificare i cambi nell'organizzazione che possono avere delle conseguenze su processi stabiliti, procedure, prodotti e servizi. Prima di implementare i cambi, un processo di gestione del cambiamento deve descrivere le modalità attuate per garantire le performance dal punto di vista della sicurezza. Il risultato di questo processo è la riduzione, fino a un livello accettabile (ALARP), dei rischi per la sicurezza, derivanti da cambiamenti nella fornitura di servizi da parte dell'organizzazione.

10.3.3 CONTINUOUS IMPROVEMENT OF THE SMS

L'organizzazione deve continuamente migliorare le prestazioni in ambito di safety e l'efficienza del sistema di gestione.

10.4 SAFETY PROMOTION

10.4.1 TRAINING AND EDUCATION

L'organizzazione deve sviluppare un programma di training che garantisca che il personale sia sempre addestrato e pronto per svolgere i propri doveri all'interno dell'organizzazione.

10.4.2 SAFETY COMMUNICATION

L'organizzazione deve comunicare gli obiettivi del SMS e le procedure a tutto il personale. Il Safety Manager deve comunicare le prestazioni del SMS attraverso bollettini o briefing e deve anche far sì che le lezioni imparate da investigazioni vengano distribuite a tutti. La comunicazione deve avvenire attraverso tutta l'organizzazione e deve:

- Garantire che tutto lo staff sia consapevole del SMS.
- Trasmettere informazioni safety-critical.
- Spiegare il perché vengano intraprese certe azioni.
- Spiegare perché certe procedure di safety vengano introdotte o cambiate.

11 PIANO DI IMPLEMENTAZIONE DEL SMS

L'implementazione del SMS deve essere sostenuta dal senior management dell'organizzazione e sviluppata sulla base della normativa nazionale, degli International Standards and Recommended Practices (SARPs) e sulla base della descrizione del sistema e dei risultati della gap analysis.

Lo sviluppo di un piano di implementazione serve per:

- Aiutare nella preparazione di una strategia per l'implementazione di un SMS che soddisfa i requisiti di sicurezza dell'organizzazione.
- Fornire una serie di passaggi da seguire durante il processo di implementazione del SMS.
- Fornire un quadro di responsabilità per l'attuazione del SMS.

L'implementazione del SMS dipende da molti fattori e è quindi conveniente un approccio detto *Phased Approach*, secondo il quale l'implementazione del SMS viene fatta in più step. Questo permette una migliore disponibilità di risorse, una riduzione del carico di lavoro associato all'implementazione e soprattutto garantisce un robusto sistema di gestione della sicurezza. Il tempo per l'implementazione di ciascuna fase deve essere commisurato alla dimensione dell'organizzazione.

Di seguito si riporta un piano per l'implementazione del sistema di gestione riferito al framework ICAO descritto al capitolo 10.

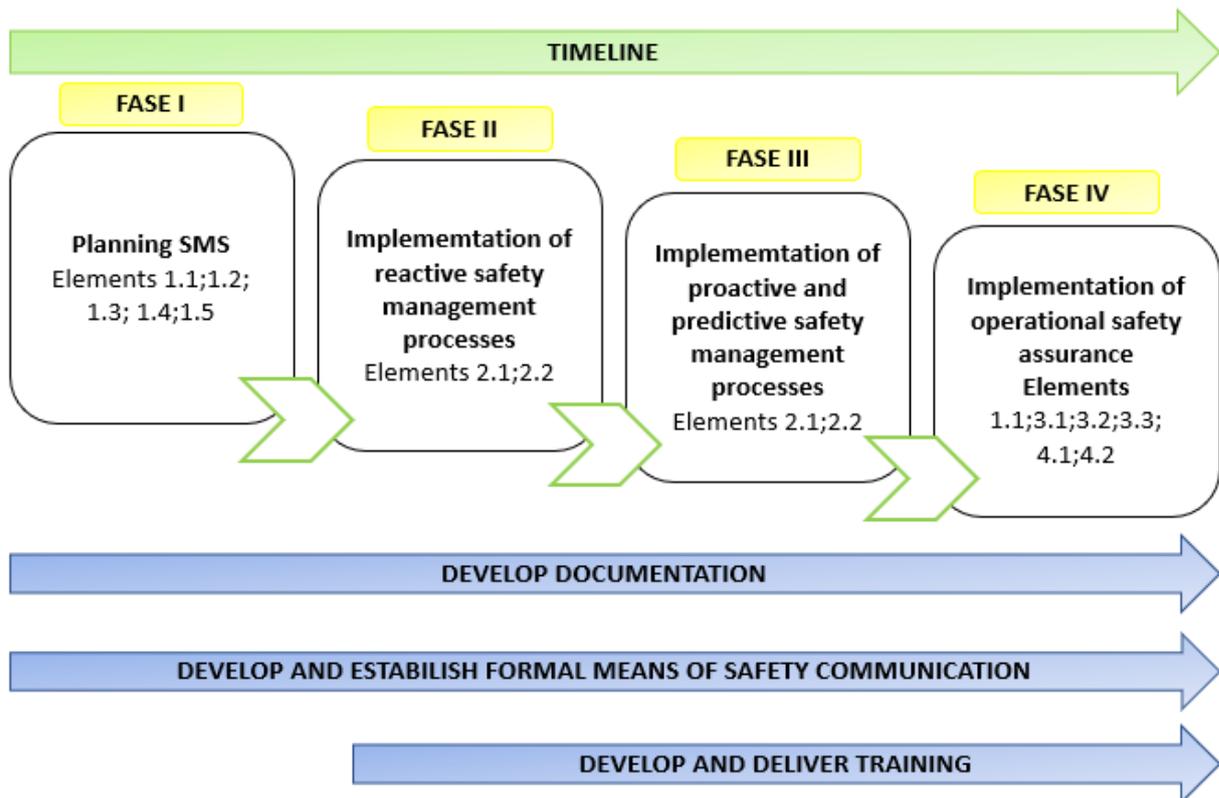


Figura 14 SMS Implementation-Phase Approach

11.1 FASE 1: PLANNING SMS IMPLEMENTATION

Gli obiettivi della fase 1 consistono sia nella definizione della modalità in cui i requisiti del SMS verranno raggiunti e integrati nelle attività dell'organizzazione, che nell'assegnazione delle responsabilità del SMS. Fondamentale in questa prima fase è la gap analysis, tramite la quale si può determinare lo stato dei processi di gestione della sicurezza già implementati nell'organizzazione e programmarne di nuovi.

Elementi che caratterizzano questa prima fase sono:

- *Accountable Manager*
Bisogna identificare l'AM e la persona o il gruppo di persone all'interno dell'organizzazione responsabili dell'implementazione del sistema di gestione della sicurezza e assegnare le responsabilità dei manager in materia di sicurezza.
- *System description e gap analysis*
La descrizione del sistema è la prima attività necessaria per lo sviluppo del SMS all'interno dell'organizzazione. La descrizione deve includere le interfacce interne al sistema, così come quelle con altri sistemi.

Condurre una gap analysis serve per identificare le risorse e le disposizioni presenti all'interno dell'organizzazione, confrontarle con i requisiti necessari per un SMS e identificare quelle mancanti. Svolta la gap analysis, tenendo conto dei requisiti nazionali e delle SARPs internazionali, si può sviluppare un piano di implementazione che spiega come verrà implementato il sistema di gestione all'interno dell'organizzazione. Quest'ultimo deve tenere conto di potenziali lacune che possono ostacolare l'implementazione del SMS e sviluppare strategie per affrontarle.

- *Politica e obiettivi di sicurezza*

E' necessario sviluppare una documentazione riguardante la politica di sicurezza e comunicarla a tutta l'organizzazione. Bisogna inoltre stabilire un programma di revisione della politica di sicurezza per garantire che rimanga, nel tempo, pertinente e adeguata all'organizzazione.

Per quanto riguarda gli obiettivi dell'organizzazione in termini di sicurezza, è importante sviluppare degli standard di prestazione espressi in termini di indicatori di prestazioni, obiettivi di prestazione e piani di azione.

- *Responsabilità in materia di sicurezza e nomina del personale addetto alla sicurezza*

La struttura del SMS viene definita nella prima fase e consiste nel definire un Safety Service Office e nominare un Safety Manager, responsabile dello sviluppo e del mantenimento di un sistema di gestione efficiente. Sempre in questa fase devono essere stabilite le linee di comunicazione tra AM, Safety Action Group (SAG) e il Safety Review Board (SRB). Senior manager devono essere nominati per far parte della SRB, presieduta dall'AM.

Le linee di comunicazione devono essere commisurate alla dimensione dell'organizzazione e alla complessità dei servizi.

L'assegnazione di queste responsabilità deve essere documentata e comunicata a tutta l'organizzazione, includendo una definizione dei livelli di gestione che possano prendere decisioni riguardanti la tollerabilità di un rischio per la sicurezza.

- *Documentazione del SMS*

Bisogna sviluppare delle linee guida per la raccolta e la gestione di tutta la documentazione riguardante il SMS e la sua implementazione facendo riferimento alla normativa nazionale e agli standard internazionali. Definire un SMSM tramite il quale si comunica l'approccio dell'organizzazione verso la sicurezza; questo deve essere revisionato e aggiornato durante le fasi di implementazione del SMS.

- *Training*

Bisogna sviluppare sia un documento contenente i requisiti del training che un processo che ne misuri l'efficacia e identifichi i costi associati. Il training deve essere appropriato al personale in base al ruolo e alla responsabilità all'interno del SMS.

Al termine di questa fase, l'organizzazione ha a disposizione gli strumenti necessari per condurre un'analisi sulla sicurezza, sulla base delle informazioni ottenute attraverso la raccolta dei dati.

Il tempo di implementazione stimato per questa prima fase può variare da 1 a 6 mesi in base alla dimensione e alla complessità dell'organizzazione.

Al termine di questa fase, l'organizzazione deve aver raggiunto i seguenti obiettivi e condotto le seguenti attività:

- a) Definizione della Safety Policy firmata dall'Accountable Manager.
- b) La politica di sicurezza deve essere stata comunicata a tutto lo staff.
- c) Descrizione completa del sistema.
- d) Gap analysis.
- e) Definizione della struttura organizzativa del SMS.
- f) Approvazione del piano di implementazione del SMS.
- g) Erogazione del training sulla pianificazione del SMS.
- h) Pubblicazione di una prima bozza del SMSM.
- i) Definizione dei mezzi per comunicare informazioni relative alla sicurezza.

11.2 FASE 2: REACTIVE SAFETY MANAGEMENT PROCESSES

L'obiettivo di questa seconda fase è quello di implementare processi essenziali riguardanti la gestione della safety e allo stesso tempo correggere le carenze presenti nei processi già esistenti all'interno dell'organizzazione. Infatti spesso le organizzazioni hanno già implementato attività di gestione della sicurezza come audit, investigazioni interne e report da parte del personale. L'obiettivo di questa fase è quello di implementare i processi già esistenti e svilupparne di nuovi qualora non fossero mai stati implementati all'interno dell'organizzazione. Per questo motivo questa fase viene considerata con un approccio reattivo.

La seconda fase è caratterizzata da:

- *Analisi e identificazione dei fattori di rischio basata su processi reattivi*
E' necessario a questo punto dell'implementazione del SMS identificare le fonti necessarie per raccogliere informazioni reattive che riguardano gli hazard e implementare un approccio strutturato per l'identificazione reattiva di questi ultimi.
- *Safety risk management basato su processi reattivi*
Bisogna sviluppare una matrice di rischio al fine di poter implementare quelle attività presenti nel piano di implementazione, che riguardano la gestione del rischio tramite un processo reattivo.

- *Training*
Fornire un training adeguato sia rivolto al personale, che ai manager e ai supervisori riguardante l'implementazione delle componenti del SMS, la gestione del processo di gestione del rischio basato su un approccio reattivo e le modalità tramite le quali effettuare la segnalazione di hazard.
- *Documentazione di processi reattivi*
Bisogna definire una Safety Library, inserire informazioni all'interno del SMSM relative alla gestione reattiva della safety e inserire i requisiti per i processi di Hazard Identification e Safety Risk Management all'interno della documentazione.
- *Safety promotion -Safety communication*
Bisogna sviluppare mezzi di comunicazione efficaci come newsletter, avvisi e bollettini per diffondere all'organizzazione le informazioni ricavate durante la fase 2.

Il tempo di implementazione richiesto per la fase 2 può variare tra i 9 e i 12 mesi, in base alla dimensione dell'organizzazione e alla complessità dei servizi forniti.

In sintesi, al termine della fase 2 devono essere concluse le seguenti attività:

- a) Definizione della Safety Library.
- b) Implementazione di un processo reattivo di gestione della sicurezza.
- c) Erogazione del training riguardante l'implementazione delle singoli componenti del SMS e della gestione dei rischi per la safety.
- d) Distribuzione a tutta l'organizzazione delle informazioni safety-critical raccolte.

11.3 FASE 3: PROACTIVE AND PREDICTIVE SAFETY MANAGEMENT PROCESSES

A differenza della fase precedente, nella quale i processi di gestione della safety prevedono un approccio reattivo, in questa fase si cerca di definire dei processi lungimiranti, caratterizzati quindi da un approccio proattivo e predittivo nella raccolta dei dati sulla sicurezza.

Questa fase è caratterizzata da:

- *Analisi e identificazione dei fattori di rischio basata su processi proattivi e predittivi*
E' necessario in questa fase identificare le fonti interne ed esterne usate per ottenere informazioni proattive e predittive sui fattori di rischio e implementare un approccio strutturato per l'identificazione proattiva e predittiva degli hazard.
- *Gestione del rischio basata su processi proattivi e predittivi*
Per fare questo è necessario sviluppare una matrice di rischio e includere l'utilizzo di quest'ultima all'interno del programma di training.
- *Training*
Fornire un training adeguato all'implementazione delle componenti del SMS e alla gestione del processo di risk management basato su approccio proattivo e predittivo.
- *Documentazione di processi proattivi e predittivi*
Sviluppare documentazione che riguarda sia l'implementazione delle componenti del SMS che la gestione del rischio basata su un approccio proattivo e predittivo.
Per far questo bisogna inserire le informazioni all'interno della Safety Library, aggiornare il SMSM con informazioni relative al processo di gestione del rischio proattivo e predittivo, sviluppare safety performance indicators e safety standard e scrivere requisiti per i processi di Hazard Identification e gestione del rischio basata su processi proattivi e predittivi all'interno della documentazione.
- *Safety promotion*
Analogamente alla fase precedente, bisogna sviluppare mezzi di comunicazione efficaci per trasmettere le informazioni riguardanti questa fase a tutta l'organizzazione. Questo viene fatto tramite newsletter, bollettini, avvisi, siti web ed email.

Il tempo stimato per l'implementazione di questa fase va dai 12 ai 16 mesi in base alla dimensione dell'azienda e alla complessità dei servizi forniti.

Prima di implementare l'ultima fase, l'organizzazione deve aver svolto le seguenti attività:

- a) Aver stabilito un periodo iniziale di test per l'identificazione degli hazard in modo proattivo e predittivo.
- b) Implementato processi proattivi e predittivi di gestione della safety.

- c) Completato un training riguardante le componenti del piano di implementazione del SMS e del processo di gestione del rischio basato su un approccio proattivo e predittivo.
- d) Distribuito a tutta l'organizzazione informazioni safety-critical raccolte per mezzo di processi proattivi e predittivi.

11.4 FASE 4: OPERATIONAL SAFETY ASSURANCE

L'ultima fase del processo di implementazione del SMS si basa sul processo di Safety Assurance, attraverso l'implementazione di un processo di monitoraggio periodico, feedback e azioni correttive al fine di mantenere l'efficacia del sistema di controllo del rischio sotto mutevoli esigenze operative. Alla fine di questa fase, la gestione delle informazioni sulla sicurezza e i processi analitici garantiscono la sicurezza dei processi organizzativi nel tempo e durante i periodi di cambiamento all'interno dell'ambiente operativo.

Quest'ultima fase di implementazione del SMS pone l'attenzione su:

- *Prestazioni del SMS in materia di sicurezza*
Bisogna sviluppare indicatori di prestazioni della sicurezza, target di prestazioni in termini di safety, stabilire piani di azione e definirne misure di affidabilità, disponibilità e accuratezza.
- *Misura e monitoraggio delle prestazioni in materia di sicurezza*
Bisogna in questa fase finale di implementazione definire un sistema di monitoraggio delle prestazioni.
- *Gestione dei cambiamenti*
Stabilire un processo formale per la gestione dei cambiamenti che consideri la criticità dei sistemi e delle attività, la stabilità dei sistemi e degli ambienti operativi e le prestazioni passate. Inoltre bisogna identificare quei cambiamenti che possono avere conseguenze su processi, procedure, prodotti e servizi già implementati. Prima di effettuare un cambiamento bisogna definire le misure adottate per garantire le prestazioni in materia di sicurezza.
- *Miglioramento continuo del SMS*
Al fine di garantire un continuo miglioramento del sistema di gestione, è necessario:
 - Sviluppare forms per valutazioni interne e garantire che queste valutazioni vengano fatte in modo indipendente dai processi tecnici che devono essere valutati.
 - Sviluppare un processo di audit interno.
 - Sviluppare un processo di audit esterno.

- Definire un piano organizzato per la valutazione proattiva di facilities, equipaggiamenti, documentazione e procedure; questo piano deve essere completato tramite indagini e audit.
 - Sviluppare documentazione adeguata.
- *Training*
Sviluppare training mirato al miglioramento continuo in termini di safety.
 - *Safety promotion- safety communication*
Sviluppare e stabilire mezzi di comunicazione per divulgare le informazioni ottenute in questa fase, tramite newsletter, bollettini, siti web, avvisi ed email.

Il tempo ipotizzato per l'implementazione di questa fase varia dai 9 ai 12 mesi in base alla dimensione dell'azienda e alla complessità dei servizi forniti.

Terminata l'ultima fase del processo di implementazione del SMS è necessario che:

- Sia stato raggiunto un accordo con l'autorità statale per quanto riguarda indicatori e target di prestazioni in materia di sicurezza.
- Sia stato completato il training per personale operativo, manager e supervisori.
- La documentazione sia stata integrata all'interno della Safety Library.

12 ESEMPIO: IDENTIFICAZIONE E ANALISI DEI RISCHI

Di seguito si riporta il processo di identificazione e analisi dei rischi legato all'emergenza COVID-19.

Descrizione del possibile fattore di rischio: contagio del personale operativo CAT per il trasporto di persone non sospette, ma che potrebbero essere contagiate da Coronavirus.

Tramite il processo di Hazard Analysis, si individuano le possibili conseguenze dell'hazard:

- Malattia da Coronavirus.
- Contagio di altro personale in ambito lavorativo.
- Quarantena e assenza dal lavoro.
- Riduzione delle capacità operative CAT.
- Danno di immagine.

Con il processo di Safety Risk Management, le conseguenze del fattore di rischio vengono valutate in termini di probabilità di accadimento e gravità delle conseguenze. Questo porta alla definizione della tollerabilità del rischio, espressa con la seguente matrice:

			Severità delle conseguenze				
			Catastrofica A	Pericolosa B	Maggiore C	Minore D	Trascurabile E
Probabilità evento	Frequente	5	5A	5B	5C	5D	5E
	Occasionale	4	4A	4B	4C	4D	4E
	Remota	3	3A	3B	3C	3D	3E
	Improbabile	2	2A	2B	2C	2D	2E
	Estremamente Improbabile	1	1A	1B	1C	1D	1E

Figura 15 Matrice di rischio

Il caso in esame presenta una probabilità occasionale e una severità pericolosa → 4B e ricade pertanto nella zona di non tollerabilità.

Inizia quindi il processo di Safety Risk Control and Mitigation, durante il quale vengono adottate delle misure di mitigazione per portare il rischio a un livello di accettabilità.

Le barriere introdotte sono:

- Applicazione delle disposizioni del Ministero della salute, delle disposizioni Enac e delle direttive aeroportuali per il trasporto dei passeggeri.
- Sanificazione dell'aeromobile.

Con queste barriere, il rischio va a ricadere all'interno della zona di accettabilità → 2D, presentando quindi un rischio improbabile e con severità minore.

13 REFERENZE BIBLIOGRAFICHE

- Safety Management Manual (SMM) Doc.9859
- Consolidated Regulation (EU) No 1321/2014 on Continuing Airworthiness (applicable from 24 March 2020)
- Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Annex Vc (Part CAMO) to Commission Regulation (EU) No 1321/2014
- ICAO Annex 19 Second Edition
- EASA Regulation (EU) No 376/2014
- ENAC Circolare NAV-75 A