



Република Северна Македонија
Republika e Maqedonisë së Veriut
Агенција за цивилно воздухопловство
Agjencia e Aviacionit Civil

Бр.-Нг. 12-1351/1

03-09-2026 год.-viti

03092026



АГЕНЦИЈА ЗА ЦИВИЛНО
ВОЗДУХОПЛОВСТВО

ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА
СИСТЕМ ЗА УПРАВУВАЊЕ СО БЕЗБЕДНОСТА
(SMS) КАЈ ОРГАНИЗАЦИИТЕ

SQS-MAN-005



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

СОДРЖИНА	
ПРИЛОГ	6
КРАТЕНКИ	7
ДЕФИНИЦИИ	7
ОБЈАСНУВАЊЕ НА СИМБОЛИТЕ	9
ЛИСТА НА ИЗДАНИЈА И РЕВИЗИИ	9
СПИСОК НА ВАЖЕЧКИ СТРАНИЦИ	10
ВОВЕД СО ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ	11
ТАБЕЛА НА ОДОБРУВАЊЕ	12
СПИСОК НА ДИСТРИБУЦИЈА	12
РЕФЕРЕНТЕН ДОКУМЕНТ	12
• Опсег и намена	13
Одговорности	13
Агенцијата за цивилно воздухопловство (АЦВ)	13
Организациите	13
• Вовед	14
• Главен дел	14
1. Политика и цели за безбедност	14
1.1 Заложба на раководството (Management Commitment)	14
Применливо барање (Applicable Requirement)	14
Имплементација од страна на организацијата (Implementation by Organization)	14
Самооценување на SMS (SMS Self-Assessment)	15
1.2 Одговорност и отчетност за безбедноста (Safety Accountability and Responsibilities)	15
Применливо барање (Applicable Requirement)	15
Имплементација од страна на организацијата (Implementation by Organization)	15
Самооценување на SMS (SMS Self-Assessment)	16
1.3 Назначување на клучен персонал за безбедност (Appointment of Key Safety Personnel)	16
Применливо барање (Applicable Requirement)	16
Имплементација од страна на организацијата (Implementation by Organization)	16
Самооценување на SMS (SMS Self-Assessment)	17
1.4 Координација на планирањето на одговор во вонредни ситуации (Coordination of Emergency Response Planning)	17
Применливо барање (Applicable Requirement)	17
Имплементација од страна на организацијата (Implementation by Organization)	17
Самооценување на SMS (SMS Self-Assessment)	18
1.5 SMS документација (SMS Documentation)	18
Применливо барање (Applicable Requirement)	18
Имплементација од страна на организацијата (Implementation by Organization)	18
SMM – Прирачник за управување со безбедноста (Safety Management Manual)	18



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИЈИТЕ**
Одделение SQS и мониторинг на усогласеност

Пример на структура на SMM.....	19
SMS записи (SMS Records).....	19
Процедури (Procedures).....	19
Водење записи (Record Keeping).....	20
Управување со документацијата (Documentation Management).....	20
Надворешна документација (External Documentation).....	20
Самооценување на SMS (SMS Self-Assessment).....	20
2. Управување со безбедносниот ризик (Safety Risk Management – SRM).....	21
2.1 Идентификација на опасности (Hazard Identification).....	21
Применливо барање (Applicable Requirement).....	21
Имплементација од страна на организацијата (Implementation by Organization).....	21
Обработка на безбедносни настани (Processing of Safety Occurrences).....	22
Самооценување на SMS (SMS Self-Assessment).....	22
2.2 Проценка и намалување на безбедносниот ризик (Safety Risk Assessment and Mitigation).....	23
Применливо барање (Applicable Requirement).....	23
Имплементација од страна на организацијата (Implementation by Organization).....	23
Проценка на безбедносниот ризик (Safety Risk Assessment).....	24
Матрица на безбедносен ризик (Safety Risk Matrix).....	25
Прифатливост на безбедносниот ризик (Safety Risk Tolerability).....	25
Прифаќање и одобрување на ризикот (Risk Acceptance and Approval).....	26
Намалување на безбедносниот ризик (Safety Risk Mitigation).....	26
Самооценување на SMS (SMS Self-Assessment).....	26
3. Уверување во безбедноста (Safety Assurance).....	27
3.1 Следење и мерење на безбедносните перформанси (Safety Performance Monitoring and Measurement).....	27
Применливо барање (Applicable Requirement).....	27
Имплементација од страна на организацијата (Implementation by Organization).....	27
Индикатори за безбедносни перформанси (Safety Performance Indicators – SPIs).....	28
Внатрешни проверки (Internal Audits).....	28
Извори за следење на безбедносните перформанси (Sources for Safety Performance Monitoring).....	29
Самооценување на SMS (SMS Self-Assessment).....	29
3.2 Управување со промени (Management of Change).....	29
Применливо барање (Applicable Requirement).....	29
Имплементација од страна на организацијата (Implementation by Organization).....	30
Безбедносна студија на промена (Safety Study of Change).....	30
Преоден период и следење на промената (Transition Phase and Change Monitoring).....	31
Пуштање во употреба и документација (Commissioning and Documentation).....	31
Самооценување на SMS (SMS Self-Assessment).....	31



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ
Одделение SQS и мониторинг на усогласеност**

3.3 Континуирано подобрување на SMS (Continuous Improvement of the SMS).....	32
Применливо барање (Applicable Requirement).....	32
Имплементација од страна на организацијата (Implementation by Organization)	32
Циклус на континуирано подобрување (Plan–Do–Check–Act – PDCA).....	32
Корективни мерки (Corrective Actions).....	33
Преглед од страна на раководството (Management Review).....	33
Следење на SMS (SMS Monitoring).....	33
Самооценување на SMS (SMS Self-Assessment).....	33
4. Промоција на безбедноста (Safety Promotion)	34
4.1 Обука и едукација (Training and Education).....	34
Применливо барање (Applicable Requirement).....	34
Имплементација од страна на организацијата (Implementation by Organization)	34
Содржина на SMS обуката (SMS Training Content).....	35
Обука според функцијата и одговорностите (Role-Based Training).....	35
Евиденција за обуките (Training Records)	35
Следење и ажурирање на обуката (Training Monitoring and Update)	36
Самооценување на SMS (SMS Self-Assessment).....	36
4.2 Комуникација за безбедноста (Safety Communication).....	37
Применливо барање (Applicable Requirement).....	37
Имплементација од страна на организацијата (Implementation by Organization)	37
Внатрешна комуникација за безбедноста (Internal Safety Communication).....	37
Надворешна комуникација за безбедноста (External Safety Communication)	38
Комуникација на SMS информации (Communication of SMS Information).....	38
Самооценување на SMS (SMS Self-Assessment).....	38
5. Нивоа и критериуми за утврдување (Determination Levels and Criteria).....	39
6. Список на применливи процедури, обрасци и контролни листи.....	40
• Заклучок.....	41



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

ПРИЛОГ

Број	Ознака



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

КРАТЕНКИ

Кратенка	Значење
АЦВ / САА	Агенција за цивилно воздухопловство / Civil Aviation Agency
ICAO	International Civil Aviation Organization – Меѓународна организација за цивилно воздухопловство
SMS	Safety Management System – Систем за управување со безбедноста
SMM	Safety Management Manual – Прирачник за управување со безбедноста
SSP	State Safety Programme – Државна програма за безбедност
SRM	Safety Risk Management – Управување со безбедносен ризик
SPI	Safety Performance Indicator – Индикатор за безбедносни перформанси
SPT	Safety Performance Target – Целна вредност на безбедносните перформанси
ERP	Emergency Response Plan – План за одговор во вонредни ситуации
ATS	Air Traffic Services – Услуги во воздушниот сообраќај
ANS	Air Navigation Services – Услуги во воздушната навигација
MOR	Mandatory Occurrence Reporting – Задолжително пријавување на настани
VOR	Voluntary Occurrence Reporting – Доброволно пријавување на настани

ДЕФИНИЦИИ

Термин	Дефиниција
Систем за управување со безбедноста (SMS)	Систематски пристап кон управувањето со безбедноста, вклучувајќи ги потребните организациски структури, одговорности, политики и процедури.
Безбедност (Safety)	Состојба во која ризиците поврзани со воздухопловните активности, кои се однесуваат на или директно ја поддржуваат експлоатацијата на воздухопловите, се намалени и контролирани на прифатливо ниво.
Опасност (Hazard)	Состојба или предмет со потенцијал да предизвика или да придонесе кон воздухопловен инцидент или несреќа.
Безбедносен ризик (Safety Risk)	Предвидена веројатност и сериозност на последиците или исходите од постоечка опасност.
Управување со безбедносен ризик (SRM)	Процес кој вклучува идентификација на опасности, проценка на безбедносните ризици и определување и спроведување соодветни мерки за нивно намалување или контрола.
Безбедносни перформанси (Safety Performance)	Постигнување на безбедноста на државата или давателот на услуги, дефинирано преку неговите безбедносни цели и индикатори за безбедносни перформанси.
Индикатор за безбедносни перформанси (SPI)	Параметар базиран на податоци кој се користи за следење и оценување на безбедносните перформанси.
Целна вредност на безбедносните перформанси (SPT)	Планирана или посакувана вредност на индикаторот за безбедносни перформанси во определен временски период.
Безбедносна политика (Safety Policy)	Документирана заложба на организацијата за управување со безбедноста, со која се утврдуваат основните принципи и насоки за постигнување и одржување на прифатливо ниво на безбедност.



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**

Одделение SQS и мониторинг на усогласеност

Безбедносна цел (Safety Objective)	Кратка изјава на високо ниво за безбедносно достигнување или посакуван резултат што треба да се постигне.
Уверување во безбедноста (Safety Assurance)	Процеси и активности преку кои организацијата утврдува дали SMS функционира во согласност со очекувањата и дали воспоставените мерки за контрола на безбедносниот ризик остануваат ефективни.
Промоција на безбедноста (Safety Promotion)	Комбинација од обука и комуникација на безбедносни информации со цел развивање и одржување позитивна безбедносна култура и потребните компетенции за ефективно управување со безбедноста.
Безбедносна култура (Safety Culture)	Начинот на кој безбедноста се перципира, вреднува и практикува во организацијата и степенот до кој вработените и раководството се посветени на безбедноста.
План за одговор во вонредни ситуации (ERP)	Документиран план со кој се утврдуваат активностите, одговорностите и координацијата на организацијата при вонредна ситуација.



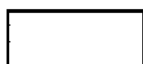
**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

ОБЈАСНУВАЊЕ НА СИМБОЛИТЕ

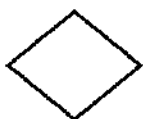
Подолу е наведено објаснување на симболите на дијаграмот на текот на процесот кои се користени во овој прирачник.



Почеток/крај на процедурата



Активност



Контролна ставка, контролна активност



Документ, информација



Точка на спојување

ЛИСТА НА ИЗДАНИЈА И РЕВИЗИИ

Рев.бр.	Датум	Внесена од	Опис на ревизијата
00	27.08.2026	Кире Колевски Валерија Стрезовски	Прво издание



Страна	Издание	Рев.	Датум
2	01	00	27.08.2026
3	01	00	27.08.2026
4	01	00	27.08.2026
5	01	00	27.08.2026
6	01	00	27.08.2026
7	01	00	27.08.2026
8	01	00	27.08.2026
9	01	00	27.08.2026
10	01	00	27.08.2026
11	01	00	27.08.2026
12	01	00	27.08.2026
13	01	00	27.08.2026
14	01	00	27.08.2026
15	01	00	27.08.2026
16	01	00	27.08.2026
17	01	00	27.08.2026
18	01	00	27.08.2026
19	01	00	27.08.2026
20	01	00	27.08.2026
21	01	00	27.08.2026
22	01	00	27.08.2026
23	01	00	27.08.2026
24	01	00	27.08.2026
25	01	00	27.08.2026
26	01	00	27.08.2026
27	01	00	27.08.2026
28	01	00	27.08.2026
29	01	00	27.08.2026
30	01	00	27.08.2026
31	01	00	27.08.2026
32	01	00	27.08.2026
33	01	00	27.08.2026
34	01	00	27.08.2026
35	01	00	27.08.2026
36	01	00	27.08.2026
37	01	00	27.08.2026
38	01	00	27.08.2026
39	01	00	27.08.2026
40	01	00	27.08.2026
41	01	00	27.08.2026

[illegible]



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

ВОВЕД СО ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Прирачникот е издаден од страна на:

Агенција за цивилно воздухопловство
Даме Груев 1, 1000 Скопје, Северна Македонија

Се забранува копирање или умножување на овој материјал без претходна писмена согласност на издавачот.

Ова издание на овој прирачник влегува во сила со денот на донесувањето. Секоја понатамошна ревизија на овој прирачник влегува во сила со денот наведен во Табелата на одобрување.

За издавачот:
Драги Стојановски, директор на АЦВ





**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

ТАБЕЛА НА ОДОБРУВАЊЕ

	Име и позиција	Датум	Потпис
Подготвил:	Валерија Стрезовски, Советник за SAR и испитување на настани, Одделение SQS и мониторинг на усогласеност	27.08.2026	
Контролирал:	Кире Колевски, Раководител на Одделение SQS и мониторинг на усогласеност	27.08.2026	
Извршил проверка на квалитетот:	Кире Колевски, Раководител на Одделение SQS и мониторинг на усогласеност	27.08.2026	
Одобрил:	Драги Стојаноски, Директор	27.08.2026	

СПИСОК НА ДИСТРИБУЦИЈА

Примерок бр.	КОРИСНИК	ВИД НА ФОРМА	БРОЈ НА ПРИМЕРОЦИ
1.	Архива	Оригинал-примерок во хартиена форма	1
2.	Раководител на SQS и мониторинг на усогласеност	Оригинал-примерок во хартиена форма	1
3.	ACV-Share	Дигитален примерок	1
4.	Дигитален примерок	По електронска пошта до сите вработени	1

РЕФЕРЕНТЕН ДОКУМЕНТ

	Код на документот	Назив на документот
1.	SQS-MAN-001	Integrated Quality System Manual
2.	Службен весник на PCM (во сила)	Закон за воздухопловство
3.	ICAO Annex 19	Safety Management
4.	ICAO Doc 9859	Safety Management Manual (SMM)
5.	CB PCM бр. 67/23	Уредба за принципите по кои се води истражувањето на несреќи, сериозни инциденти, инциденти и настани на цивилни и државни воздухоплови, начинот на нивното пријавување, како и формата, содржината, начинот на водење на евиденцијата и начинот на издавањето и одземањето на службената легитимација на истражителите
6.	SSP	Национална програма за безбедност
7.	NASP / SSPI	Национален план за безбедност
8.	SQS-MAN-002	Прирачник за управување со безбедноста
9.	SQS-PRC-005	Процедура за пријавување, анализа и следење на настани поврзани со безбедноста во воздухопловството



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

• **Опсег и намена**

Овој Прирачник содржи насоки за воспоставување, имплементација, одржување и унапредување на системот за управување со безбедноста (SMS) кај организациите кои, согласно применливите прописи, имаат обврска да воспостават и одржуваат SMS.

Прирачникот е наменет за поддршка на организациите при исполнување на барањата за SMS, во согласност со применливите национални прописи, ICAO Annex 19 – Safety Management и ICAO Doc 9859 – Safety Management Manual (SMM).

Прирачникот ги опфаќа компонентите и елементите на SMS рамката утврдени во Appendix 2 на ICAO Annex 19:

- политика и цели за безбедност (Safety Policy and Objectives);
- управување со безбедносен ризик (Safety Risk Management);
- уверување во безбедноста (Safety Assurance); и
- промоција на безбедноста (Safety Promotion).

Насоките од овој Прирачник се применуваат соодветно на видот на услугите и активностите што ги врши организацијата, нејзината големина и сложеност и поврзаните безбедносни ризици. Прирачникот има карактер на упатство и не ги заменува барањата утврдени со важечките законски, подзаконски и меѓународни прописи.

Одговорности

Агенцијата за цивилно воздухопловство (АЦВ)

АЦВ е одговорна за:

- изработка, одржување и периодично ажурирање на Прирачникот за имплементација на системот за управување со безбедноста (SMS);
- обезбедување усогласеност на Прирачникот со применливите регулаторни барања, меѓународните стандарди и препорачаните практики;
- надзор над имплементацијата на SMS кај организациите, со цел обезбедување усогласеност со применливите барања и ефективност на SMS.

Организациите

Организациите се одговорни за:

- воспоставување, имплементација, одржување и континуирано унапредување на сопствениот SMS, согласно применливите барања и насоките дадени во овој Прирачник;
- изработка, одржување и ажурирање на сопствениот Прирачник за управување со безбедноста (Safety Management Manual – SMM) и другата релевантна SMS документација;
- обезбедување дека сите релевантни организациски единици и персоналот ги разбираат и применуваат своите одговорности и применливите SMS процеси и процедури;
- одржување на интерните процеси, документацијата и практиките во согласност со воспоставената рамка на SMS;
- идентификација, пријавување и управување со безбедносните ризици согласно утврдените постапки и придонесување кон континуираното унапредување на SMS;
- поддршка на надзорните активности што ги спроведува АЦВ и обезбедување на потребните податоци, повратни информации и докази за усогласеност.



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИЈИТЕ**
Одделение SQS и мониторинг на усогласеност

• **Вовед**

Системот за управување со безбедноста (Safety Management System – SMS) претставува систематски пристап за управување со безбедноста, кој ги вклучува потребните организациски структури, одговорности, политики и процедури.

SMS овозможува организацијата систематски да ги идентификува опасностите (Hazards), да ги проценува и контролира поврзаните безбедносни ризици (Safety Risks), да ги следи безбедносните перформанси (Safety Performance) и континуирано да ја подобрува ефективноста на системот.

Ефективното функционирање на SMS бара активно учество на раководството и персоналот, јасно утврдени одговорности и интегрирање на управувањето со безбедноста во редовните активности и процеси на донесување одлуки во организацијата.

Имплементацијата на SMS треба да овозможи проактивен и систематски пристап кон управувањето со безбедноста и навремено преземање мерки за спречување или намалување на безбедносните ризици.

• **Главен дел**

1. Политика и цели за безбедност

Политиката и целите за безбедност ја утврдуваат заложбата на организацијата за управување со безбедноста и начинот на кој SMS е воспоставен и управуван во рамките на организацијата.

Организацијата треба да воспостави јасни одговорности и овластувања за управување со безбедноста, да ги обезбеди потребните ресурси за функционирање на SMS и да обезбеди негово соодветно документирање.

Оваа компонента ги опфаќа следните елементи:

- Заложба на раководството (Management Commitment);
- Одговорност и отчетност за безбедноста (Safety Accountability and Responsibilities);
- Назначување на клучен персонал за безбедност (Appointment of Key Safety Personnel);
- Координација на планирањето на одговор во вонредни ситуации (Coordination of Emergency Response Planning);
- SMS документација (SMS Documentation).

1.1 Заложба на раководството (Management Commitment)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави политика за безбедност која ја одразува нејзината заложба за безбедност и претставува основа за воспоставување и функционирање на SMS.

Политиката за безбедност треба да биде одобрена и потпишана од одговорниот раководител (Accountable Executive), да биде соодветна на големината и сложеноста на организацијата и природата на нејзините активности и да биде комуницирана во рамките на организацијата.

Организацијата треба периодично да ја преиспитува политиката за безбедност за да обезбеди дека таа останува релевантна и соодветна.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба да воспостави и документира политика за безбедност која, најмалку:

- ја одразува заложбата на организацијата за безбедност;
- содржи јасна изјава за обезбедување на потребните човечки и финансиски ресурси за имплементација на политиката за безбедност;
- ја поттикнува примената на принципите на позитивна безбедносна култура;
- го поттикнува пријавувањето на прашања и настани поврзани со безбедноста;



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИЈТЕ**
Одделение SQS и мониторинг на усогласеност

- ги утврдува условите под кои нема да се преземаат дисциплински мерки за дејствија или пропусти пријавени преку системот за пријавување, освен во случаите утврдени со применливите прописи;
- ги утврдува одговорностите на раководството и вработените во однос на безбедносните перформанси на организацијата;
- содржи заложба за континуирано подобрување на SMS и безбедносните перформанси.

Политиката за безбедност треба да биде потпишана од одговорниот раководител и достапна за целиот персонал.

Политиката за безбедност треба да биде соодветно дистрибуирана и комуницирана до персоналот преку Прирачникот за управување со безбедноста (Safety Management Manual – SMM), интерни известувања, објавување во просториите и други соодветни средства. Организацијата треба да обезбеди персоналот да биде запознаен со политиката и со своите обврски во однос на безбедноста. Политиката треба да се преиспитува периодично, како и при значајни организациски или оперативни промени, за да се утврди дали останува соодветна на активностите на организацијата

Самооценување на SMS (SMS Self-Assessment)

Организацијата треба да може да одговори на следните прашања:

- Дали е воспоставена и документирана политика за безбедност?
- Дали политиката е потпишана од одговорниот раководител?
- Дали политиката ја содржи заложбата за обезбедување на потребните ресурси?
- Дали политиката ги утврдува одговорностите за безбедност?
- Дали се поттикнува пријавувањето на прашања и настани поврзани со безбедноста?
- Дали политиката ги поддржува принципите на позитивна безбедносна култура?
- Дали политиката за безбедност е вклучена или соодветно наведена во SMM?
- Дали политиката е комуницирана и достапна на персоналот?
- Дали персоналот е запознаен со политиката и своите одговорности?
- Дали политиката периодично се преиспитува и, по потреба, се ажурира?

1.2 Одговорност и отчетност за безбедноста (Safety Accountability and Responsibilities)

Применливо барање (Applicable Requirement)

Организацијата треба јасно да ги утврди одговорностите и отчетноста за безбедноста во рамките на SMS.

Одговорниот раководител (Accountable Executive) има крајна одговорност и отчетност за ефективноста на SMS и за обезбедување на потребните ресурси за негово спроведување.

Одговорностите, овластувањата и отчетноста за безбедноста треба да бидат дефинирани, документираны и комуницирани на сите релевантни нивоа во организацијата.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да го идентификува одговорниот раководител (Accountable Executive) кој, независно од другите функции, има крајна одговорност и отчетност за имплементацијата и одржувањето на SMS;
- јасно да ги дефинира линиите на одговорност и отчетност за безбедноста во целата организација;
- да ги утврди одговорностите на раководството и персоналот во однос на безбедносните перформанси на организацијата;
- да ги документа и комуницира одговорностите, овластувањата и отчетноста за безбедноста;
- да обезбеди одговорниот раководител да има соодветни овластувања за обезбедување на



ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS) КАЈ ОРГАНИЗАЦИЈТЕ

Одделение SQS и мониторинг на усогласеност

- потребните човечки, финансиски и други ресурси за ефективно функционирање на SMS;
- одговорностите, овластувањата и отчетноста за безбедноста треба да бидат документирани во соодветните документи на организацијата, вклучително во Прирачникот за управување со безбедноста (Safety Management Manual – SMM), одлуките за назначување, описите на работните места и другите релевантни документи;
- да обезбеди одговорниот раководител и другите лица со SMS одговорности да имаат пристап до потребните информации за безбедносните перформанси и функционирањето на SMS;
- да обезбеди дека одговорностите, надлежностите и линиите на известување во рамките на SMS се јасно утврдени и усогласени со организациската структура и со SMM.

Самооценување на SMS (SMS Self-Assessment)

Организацијата треба да може да одговори на следните прашања:

- Дали е формално определен Accountable Executive?
- Дали се дефинирани неговите одговорности и овластувања во однос на SMS?
- Дали Accountable Executive има крајна одговорност и отчетност за ефективност на SMS?
- Дали се јасно дефинирани и документирани одговорностите за безбедноста на релевантните раководни нивоа?
- Дали персоналот ги знае своите одговорности во однос на безбедноста?
- Дали се утврдени овластувањата за донесување одлуки во однос на безбедносните ризици?
- Дали се обезбедуваат потребните човечки, финансиски и други ресурси за SMS?
- Дали одговорностите и овластувањата се комуницирани во организацијата?
- Дали организациската структура и SMS документацијата јасно ги прикажуваат SMS одговорностите?
- Дали одговорностите, овластувањата и линиите на известување за SMS се соодветно документирани во SMM и другите релевантни документи на организацијата?

1.3 Назначување на клучен персонал за безбедност (Appointment of Key Safety Personnel)

Применливо барање (Applicable Requirement)

Организацијата треба да назначи квалификувано лице кое ќе биде одговорно за имплементацијата и одржувањето на SMS.

Назначеното лице треба да има директен пристап до одговорниот раководител (Accountable Executive) и да располага со соодветни знаења, искуство и компетенции за извршување на функциите поврзани со SMS.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да назначи лице одговорно за управување и координација на SMS (Safety Manager или соодветно назначено лице);
- да ги дефинира и документира неговите одговорности, овластувања и линии на известување;
- да обезбеди назначеното лице да има директен пристап до Accountable Executive за прашања поврзани со безбедноста;
- да обезбеди назначеното лице да ги има потребните знаења, искуство и компетенции за извршување на SMS функциите;
- да обезбеди соодветни ресурси за извршување на функциите поврзани со SMS;
- да обезбеди координација со релевантните организациски единици и персоналот вклучен во управувањето со безбедноста.



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИЈЕ
Одделение SQS и мониторинг на усогласеност**

- да обезбеди Safety Manager да учествува во изработката, одржувањето и ажурирањето на Прирачникот за управување со безбедноста (Safety Management Manual – SMM) и релевантните SMS процедури, во координација со одговорниот раководител и релевантните организациски единици и експерти;
- да обезбеди Safety Manager да го следи функционирањето и ефективноста на SMS и да го известува Accountable Executive за безбедносните перформанси и за прашањата кои бараат внимание на раководството.

Во зависност од големината, природата и сложеноста на организацијата, функцијата Safety Manager може да биде самостојна функција или да биде комбинирана со други функции, под услов да не постои конфликт на интереси и да се обезбеди ефективно извршување на SMS одговорностите.

Самооценување на SMS (SMS Self-Assessment)

Организацијата треба да може да одговори на следните прашања:

- Дали е формално назначено лице одговорно за управување и координација на SMS?
- Дали неговите одговорности и овластувања се јасно дефинирани и документирани?
- Дали има директен пристап до Accountable Executive?
- Дали се дефинирани потребните квалификации и компетенции за функцијата?
- Дали назначеното лице ги поседува потребните знаења, обука и искуство?
- Дали се обезбедени соодветни ресурси за извршување на SMS функциите?
- Дали се воспоставени соодветни линии на комуникација и координација со останатите организациски единици?
- Дали Safety Manager учествува во изработката, одржувањето и ажурирањето на SMM и релевантните SMS процедури?
- Дали Safety Manager го следи функционирањето и ефективноста на SMS и го известува Accountable Executive за безбедносните перформанси?
- Доколку функцијата е комбинирана со други должности, дали е обезбедено да нема конфликт на интереси и SMS функцијата да се извршува ефективно?

1.4 Координација на планирањето на одговор во вонредни ситуации (Coordination of Emergency Response Planning)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува План за одговор во вонредни ситуации (Emergency Response Plan – ERP), кога таков план е применлив за нејзините активности.

Планот треба да обезбеди координиран и навремен одговор во случај на вонредна ситуација и да биде усогласен со плановите и постапките на другите организации и надлежни органи со кои е потребна координација.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да воспостави и документира План за одговор во вонредни ситуации (Emergency Response Plan – ERP), соодветен на природата, големината и сложеноста на нејзините активности;
- јасно да ги утврди улогите, одговорностите и овластувањата (Roles, Responsibilities and Authorities) на персоналот при вонредна ситуација;
- да ги утврди начинот на активирање на ERP, линиите на комуникација (Communication Lines) и постапките за известување;
- да обезбеди координација на ERP (ERP Coordination) со плановите и постапките на другите организации и надлежни органи со кои е потребна соработка при вонредна ситуација;
- да обезбеди релевантниот персонал да биде запознаен со своите задачи и одговорности во случај на вонредна ситуација;



- периодично да го тестира ERP преку вежби за одговор во вонредни ситуации (Emergency Response Exercises) и да ги документа резултатите;
- да ги анализира недостатоците утврдени при вежбите или при реална вонредна ситуација и, по потреба, да презема корективни мерки (Corrective Actions);
- периодично да го преиспитува и ажурира ERP, особено по спроведена вежба, реална вонредна ситуација или значајна организациска или оперативна промена.

Самооценување на SMS (SMS Self-Assessment)

Организацијата треба да може да одговори на следните прашања:

- Дали е воспоставен и документиран План за одговор во вонредни ситуации (Emergency Response Plan – ERP), каде што е применливо?
- Дали се дефинирани улогите, одговорностите и овластувањата при вонредна ситуација?
- Дали се утврдени постапките за активирање, комуникација и известување?
- Дали ERP е координиран со плановите и постапките на релевантните надворешни организации и надлежни органи?
- Дали релевантниот персонал е запознаен со своите задачи и одговорности?
- Дали ERP периодично се тестира преку вежби (Exercises)?
- Дали резултатите од вежбите се документаат и дали се преземаат активности за отстранување на утврдените недостатоци?
- Дали ERP периодично се преиспитува и ажурира?

1.5 SMS документација (SMS Documentation)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува SMM (SMS Manual) со кој се опишуваат политиката и целите за безбедност, SMS барањата, процесите и процедурите, одговорностите и овластувањата, како и начинот на функционирање на SMS.

SMS документацијата треба да биде соодветна на големината и сложеноста на организацијата, природата на услугите и активностите што ги извршува и поврзаните безбедносни ризици.

Имплементација од страна на организацијата (Implementation by Organization)

SMM – Прирачник за управување со безбедноста (Safety Management Manual)

Организацијата треба да изработи и одржува Прирачник за управување со безбедноста (Safety Management Manual – SMM), кој покажува на кој начин организацијата ги исполнува барањата за SMS.

SMM треба да ги опфати политиката за безбедност, организациската поставеност на организацијата и поврзаноста со процесите и процедурите кои имаат влијание врз безбедноста, вклучувајќи обработка на настани поврзани со безбедноста, процена и намалување на безбедносните ризици, следење на безбедносните перформанси преку индикатори и проверки, управување со документацијата и записите, управување со компетентноста и други релевантни процеси.

Содржината на SMM треба да ја одразува реалната имплементација на SMS во организацијата. Сè што е утврдено во SMM треба да се применува и неговата имплементација да може да се докаже.

SMM треба да биде што е можно поедноставен и, секогаш кога е можно, да упатува на постојните документи на организацијата (процедури, одлуки и други релевантни документи), без непотребно повторување на нивната содржина.



Пример на структура на SMM

1. Опсег на примена
2. Мисија и дејности на организацијата
3. Организациска поставеност
4. Политика и цели за безбедност
 - 4.1 Заложба на раководството
 - 4.2 Одговорност и отчетност за безбедноста
 - 4.3 Назначување на клучен персонал за безбедност
 - 4.4 Координација на планирањето на одговор во вонредни ситуации
 - 4.5 SMS документација
 - 4.6 Управување со подизведувачи и трети страни релевантни за безбедноста
5. Управување со безбедносниот ризик
 - 5.1 Идентификација на опасности
6. Обезбедување на безбедноста
 - 6.1 Следење и мерење на безбедносните перформанси
 - 6.2 Управување со промени
 - 6.3 Континуирано унапредување на SMS
7. Промоција на безбедноста
 - 7.1 Обука и подигнување на свеста
 - 7.2 Комуникација за безбедност

SMS записи (SMS Records)

Организацијата треба, каде што е применливо, да одржува записи за:

- идентификација на опасности (Hazard Identification);
- проценка на безбедносниот ризик (Safety Risk Assessment);
- мерки за намалување/контрола на безбедносниот ризик (Safety Risk Mitigation/Control Actions);
- следење на безбедносните перформанси (Safety Performance Monitoring);
- извештаи за настани (Occurrence Reports) и преземени последователни активности (Follow-up Actions);
- обука за SMS (SMS Training);
- комуникација и промоција на безбедноста (Safety Communication and Promotion);
- SMS состаноци (SMS Meetings) и донесени одлуки;
- внатрешни безбедносни проверки/прегледи (Internal Safety Audits/Reviews);
- управување со промени (Management of Change);
- вежби за одговор во вонредни ситуации (Emergency Response Exercises);
- други записи со кои се докажува функционирањето на SMS.

Процедури (Procedures)

Организацијата треба да воспостави и одржува процедури потребни за функционирање на SMS. Тие, каде што е применливо, вклучуваат процедури за управување со документацијата, водење записи, внатрешни проверки, постапување со наоди и корективни мерки и други процедури потребни за спроведување на SMS.

Процедурите треба да бидат документирани и да ги определуваат барањата и начинот на нивна примена.



Водене записи (Record Keeping)

За SMS записите организацијата треба да воспостави соодветен начин на водење, чување и контрола со кој се обезбедува нивната идентификација, достапност и следливост. За записите треба да бидат определени најмалку:

- називот на записот;
- лицето одговорно за негово водење;
- правата на пристап;
- медиумот на кој се чува записот, во хартиена или електронска форма; и
- местото на чување.

Записите треба да се чуваат на начин што овозможува нивна идентификација, достапност и следливост.

Управување со документацијата (Documentation Management)

Организацијата треба да воспостави постапка за управување со SMS документацијата.

За секој документ, каде што е применливо, треба да бидат определени:

- лицето кое го изготвува документот;
- лицето кое го проверува;
- лицето кое го одобрува;
- периодот на важност и/или периодичниот преглед на документот;
- референтната, односно важечката верзија; и
- начинот на дистрибуција и обезбедување пристап до документот.

Организацијата треба да обезбеди дека на местата каде што документацијата се користи е достапна важечката верзија на документот (Current/Valid Version).

Надворешна документација (External Documentation)

Надворешната документација која е релевантна за SMS треба да биде идентификувана и контролирана. Организацијата треба да обезбеди следење на важечките верзии на релевантните надворешни документи.

Самооценување на SMS (SMS Self-Assessment)

Организацијата треба да може да одговори на следните прашања:

- Дали е воспоставен и одобрен Прирачник за SMS (SMS Manual/SMM) или еквивалентна SMS документација?
- Дали Прирачникот за SMS ги опфаќа сите применливи компоненти и елементи на SMS (SMS Components and Elements)?
- Дали во SMS документацијата се дефинирани политиката и целите за безбедност, организациската структура, одговорностите, процесите и процедурите поврзани со SMS?
- Дали постои план за имплементација на SMS (SMS Implementation Plan), каде што е применливо?
- Дали се воспоставени и документирани процедурите потребни за функционирање на SMS?
- Дали постои систем за водење и чување записи (Record Keeping) со кои може да се докаже спроведувањето на SMS активностите?
- Дали за SMS записите се определени одговорното лице, правата на пристап, начинот и местото на чување?
- Дали SMS записите се соодветно идентификувани, заштитени, достапни и следливи?
- Дали постои постапка за управување со документацијата (Documentation Management)?
- Дали е определено кој ги изготвува, проверува и одобрува SMS документите?
- Дали е определена важечката верзија и, каде што е применливо, периодот за преглед на документите?
- Дали измените и ревизиите на SMS документацијата се контролирани и следливи?
- Дали се обезбедува релевантниот персонал да има пристап до важечката верзија на SMS



документацијата?

- Дали е определен начинот на дистрибуција на SMS документацијата?
- Дали релевантната надворешна документација (External Documentation) е идентификувана, контролирана и ажурирана?
- Дали SMS документацијата периодично се преиспитува и се ажурира при промени во организацијата, активностите, системите или применливите барања?
- Дали организацијата може практично да покаже документи и записи како доказ дека SMS процесите навистина се применуваат?

2. Управување со безбедносниот ризик (Safety Risk Management – SRM)

Управувањето со безбедносниот ризик (Safety Risk Management – SRM) е процес преку кој организацијата ги идентификува опасностите поврзани со своите активности, ги проценува безбедносните ризици и определува соодветни мерки за нивно намалување или контрола. Процесот треба да биде соодветен на природата, големината и сложеноста на организацијата и на услугите и активностите што ги извршува.

Оваа компонента ги опфаќа следните елементи:

- 2.1 Идентификација на опасности (Hazard Identification);
- 2.2 Проценка и намалување на безбедносниот ризик (Safety Risk Assessment and Mitigation);

2.1 Идентификација на опасности (Hazard Identification)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува процес за идентификација на опасности (Hazard Identification) поврзани со нејзините услуги и активности.

Идентификацијата на опасностите треба да се заснова на комбинација од реактивни (Reactive) и проактивни (Proactive) методи за собирање и анализа на безбедносни податоци и информации.

Процесот за обработка на безбедносните настани треба да ги содржи најмалку следните чекори: пријавување, известување, анализа, проценка на ризикот според сериозност и веројатност и утврдување на причините, дефинирање и спроведување на корективни мерки, повратна информација и следење на корективните мерки.

Безбедносните настани треба да бидат обработувани од соодветно обучен персонал. Разговорот со персоналот вклучен во настанот треба да се спроведе што е можно поскоро, со цел да се обезбедат релевантните информации за контекстот на настанот.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да воспостави и документира процес за идентификација на опасности (Hazard Identification);
- да ги идентификува опасностите поврзани со услугите, системите, опремата, процедурите и активностите што ги извршува;
- да користи различни извори на безбедносни податоци и безбедносни информации (Safety Data and Safety Information), вклучувајќи, каде што е применливо:
 - o задолжително пријавување на настани (Mandatory Occurrence Reporting – MOR);
 - o доброволно пријавување на настани (Voluntary Occurrence Reporting – VOR);
 - o истраги на несреќи и инциденти (Accident and Incident Investigations);
 - o резултати од надзор и проверки (Surveillance and Audit Results);
 - o безбедносни анализи (Safety Analyses);
 - o следење на безбедносните перформанси (Safety Performance Monitoring);



ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS) КАЈ ОРГАНИЗАЦИЈИТЕ

Одделение SQS и мониторинг на усогласеност

- промени во организацијата, системите или оперативното опкружување;
- други релевантни извори на безбедносни информации;
- да обезбеди идентификуваните опасности да бидат документирани и евидентирани на начин што овозможува нивна проценка и понатамошно следење;
- периодично да ги преиспитува идентификуваните опасности и да идентификува нови опасности при промени во организацијата, услугите, системите или оперативното опкружување.

Обработка на безбедносни настани (Processing of Safety Occurrences)

Организацијата треба да воспостави процес за пријавување, евидентирање, анализа и следење на безбедносните настани и идентификуваните опасности.

Процесот треба, каде што е применливо, да ги опфати следните активности:

Пријавување (Reporting)

Персоналот треба да биде запознаен со начинот на пријавување на безбедносни настани и опасности и со каналите преку кои се доставуваат извештаите. Секој познат безбедносен настан треба да биде пријавен преку воспоставениот систем/образец за пријавување на организацијата.

Известување (Notification)

Релевантните лица и организациски единици треба навремено да бидат известени за настаните кои можат да имаат влијание врз безбедноста.

Анализа (Analysis)

Пријавените настани треба да се анализираат со цел да се утврдат причините, придонесувачките фактори и поврзаните опасности и безбедносни ризици. Анализата треба да ја опфати сериозноста (Severity), веројатноста (Probability) и причините на настанот.

Корективни мерки (Corrective Actions)

Кога анализата ќе покаже потреба од преземање мерки, организацијата треба да утврди соодветни корективни активности, одговорни лица и рокови за нивна реализација. Целта на корективните мерки е намалување на ризикот до прифатливо ниво. Корективните мерки треба да бидат насочени кон утврдените причини за безбедносниот настан и да бидат определени на соодветно раководно ниво.

Реализацијата на корективните мерки треба периодично да се следи. Треба да може да се покаже следливост помеѓу безбедносниот настан, утврдените причини и преземените корективни мерки.

Повратна информација (Feedback)

Каде што е применливо, на лицата кои пријавиле настан или опасност треба да им се обезбеди соодветна повратна информација за постапувањето по пријавата.

Следење (Follow-up)

Организацијата треба да ја следи реализацијата на утврдените активности и да обезбеди нивно затворање откако ќе се утврди дека потребните мерки се спроведени.

Евидентирање и користење на безбедносните податоци (Recording and Use of Safety Data)

Информациите добиени преку пријавувањето и анализата на безбедносните настани треба да се евидентираат и чуваат на начин што овозможува нивно понатамошно пребарување, анализа и следење.

Овие информации треба да се користат за идентификација на опасности, следење на трендови, проценка на безбедносните ризици и утврдување на потребата од дополнителни безбедносни мерки.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставен и документиран процес за идентификација на опасности (Hazard Identification)?
- Дали за идентификација на опасности се користат различни внатрешни и надворешни извори на безбедносни податоци и информации?



- Дали организацијата користи реактивни (Reactive) и проактивни (Proactive) методи за идентификација на опасности?
- Дали персоналот знае што, како и на кого треба да пријави безбедносен настан или опасност?
- Дали организацијата има воспоставен систем за пријавување, евидентирање, анализа и следење на безбедносните настани и опасности?
- Дали пријавените настани се анализираат со цел да се идентификуваат причините, придонесувачките фактори и поврзаните опасности?
- Дали по анализата се определуваат и следат соодветни мерки, кога е потребно?
- Дали се обезбедува повратна информација (Feedback), каде што е применливо?
- Дали безбедносните податоци и информации се евидентираат и се користат за идентификација на опасности и следење на безбедносни трендови (Safety Trends)?
- Дали идентификуваните опасности периодично се преиспитуваат и се идентификуваат нови опасности при промени во организацијата или оперативното опкружување?
- Дали организацијата може да покаже практични примери за идентификација и следење на опасности?

2.2 Проценка и намалување на безбедносниот ризик (Safety Risk Assessment and Mitigation)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува процес со кој се обезбедува анализа, проценка и контрола на безбедносните ризици (Safety Risk Analysis, Assessment and Control) поврзани со идентификуваните опасности.

Проценката на безбедносниот ризик треба да ги земе предвид веројатноста (Probability) и сериозноста (Severity) на можните последици од идентификуваната опасност, со цел да се утврди прифатливоста на ризикот (Risk Tolerability) и потребата од преземање дополнителни мерки.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да воспостави и документа методологија за проценка на безбедносниот ризик (Safety Risk Assessment);
- за секоја идентификувана опасност да ги утврди можните последици и да ја процени:
 - o веројатноста на ризикот (Safety Risk Probability);
 - o сериозноста на ризикот (Safety Risk Severity);
- врз основа на проценетата веројатност и сериозност да го утврди нивото на безбедносниот ризик (Safety Risk Level);
- да утврди критериуми за прифатливост на ризикот (Risk Tolerability Criteria) со кои ризиците се определуваат како прифатливи, толерантни или неприфатливи;
- кога проценетиот ризик не е прифатлив, да утврди и спроведе соодветни мерки за намалување или контрола на ризикот (Safety Risk Mitigation/Control Actions);
- да определи одговорност за спроведување на утврдените мерки и, каде што е применливо, рокови за нивна реализација;
- по спроведувањето на мерките повторно да го процени ризикот за да утврди дали преостанатиот ризик (Residual Risk) е намален на прифатливо ниво;
- да ги документа проценките на ризикот, донесените одлуки и преземените мерки и да обезбеди нивно следење.

Проценка на безбедносниот ризик (Safety Risk Assessment)

При проценката на безбедносниот ризик, организацијата треба да користи соодветна методологија која овозможува доследна проценка на:

1. Веројатност (Probability) – можноста или зачестеноста со која може да се појави одредена последица од идентификуваната опасност.

ТАБЕЛА 1. ВЕРОЈАТНОСТ НА БЕЗБЕДНОСНИОТ РИЗИК TABLE 1. SAFETY RISK PROBABILITY			
ВЕРОЈАТНОСТ PROBABILITY	ЗНАЧЕЊЕ MEANING	ОПИС DESCRIPTION	ВРЕДНОСТ VALUE
Честа Frequent	Веројатно е да се појави многу пати Likely to occur many times	Се очекува да се случува често. Expected to occur frequently.	5
Посредствена Occasional	Веројатно е понекогаш да се појави Likely to occur sometimes	Може да се случи во некои случаи. Expected to occur sometimes.	4
Оддалечена Remote	Малку е веројатно да се појави, но е можно Unlikely to occur, but possible	Може да се случи во некои случаи, но не се очекува често. Expected to occur infrequently.	3
Неверојатна Improbable	Многу е малку веројатно да се појави Very unlikely to occur	Многу ретко се очекува да се случи. Expected to occur very rarely.	2
Екстремно неверојатна Extremely improbable	Речиси е невозможливо настанот да се случи Almost inconceivable that the event will occur	Практично невозможно да се случи во исклучителни околности. Expected to occur in exceptional circumstances.	1

Извор / Source: ICAO Doc 9859 – Safety Management Manual (SMM), Fourth Edition,
Table 1 – Safety risk probability.

2. Сериозност (Severity) – степенот на штетата или последиците што може да произлезат доколку се реализира идентификуваната опасност.

ТАБЕЛА 2. СЕРИОЗНОСТ НА БЕЗБЕДНОСНИОТ РИЗИК TABLE 2. SAFETY RISK SEVERITY			
СЕРИОЗНОСТ SEVERITY	ЗНАЧЕЊЕ / ОПИС MEANING / DESCRIPTION	ОПИС НА ПОСЛЕДИЦИТЕ CONSEQUENCE DESCRIPTION	ВРЕДНОСТ VALUE
Катастрофална Catastrophic	Последиците се катастрофални со повреденост, смртни случаи или целосна загуба на системот, владеењето или опремата. Consequences are catastrophic with substantial fatalities or total loss of the system, aircraft or equipment.	Уништување на опрема, повреденост, смртни случаи. Equipment destroyed, injuries deaths.	A
Опасна Hazardous	Последиците се опасни. Consequences are hazardous.	Полно или делумно уништување на опремата, значителна повреденост или работна способност при што не може да се смета дека оперативниот персонал ги извршува задатите трезво или целосно, сериозни повреди, големи оштетувања на опрема. A large reduction in safety margins, physical distress of a workload with that substantial personnel safety or mind used to perform their tasks seriously or completely without effect.	B
Голема Major	Последиците се големи. Consequences are major.	Значителна намалување на безбедносните маржини, но управување со способноста на вработените персоналот да се справи со неочекувани оперативни услови како резултат на зголемено работно оптоварување или редовно што ги намалуваат маржините ефикасност; сериозен инцидент, повреда на лича. A significant reduction in safety margins, a reduction in the ability of personnel to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their effectiveness, serious incident, injury to persons.	C
Мала Minor	Последиците се мали. Consequences are minor.	Незначително ограничување на ефикасноста, употреба на ресурси за корекција ситуација, помал инцидент. Noticed, equipment impairment, use of emergency procedures, minor incident.	D
Незначителна Negligible	Последиците се незначителни. Consequences are negligible.	Мали последици. Few consequences.	E

Извор / Source: ICAO Doc 9859 – Safety Management Manual (SMM), Fourth Edition,
Table 2 – Safety risk severity.

Комбинацијата на веројатноста и сериозноста се користи за определување на индексот/нивото на безбедносниот ризик (Safety Risk Index/Level) и неговата прифатливост.

Матрица на безбедносен ризик (Safety Risk Matrix)

Организацијата треба да користи документирана матрица на безбедносен ризик (Safety Risk Matrix) со соодветни критериуми за проценка и класификација на ризикот.

Матрицата треба да овозможи утврдување на нивото на ризикот и неговата прифатливост, како основа за определување на потребата од дополнителни мерки за намалување или контрола на ризикот..

ТАБЕЛА 3. МАТРИЦА НА БЕЗБЕДНОСНИОТ РИЗИК (ПРИМЕР)
TABLE 3. SAFETY RISK MATRIX (EXAMPLE)

ВЕРОЈАТНОСТ (PROBABILITY)	СЕРИОЗНОСТ (SEVERITY)				
	A Катастрофална (Catastrophic)	B Опасна (Hazardous)	C Золема (Major)	D Мала (Minor)	E Незначителна (Negligible)
5 Честа (Frequent)	5A	5B	5C	5D	5E
4 Понекогаш (Occasional)	4A	4B	4C	4D	4E
3 Оддалечена (Remote)	3A	3B	3C	3D	3E
2 Неверојатна (Improbable)	2A	2B	2C	2D	2E
1 Екстремно неверојатна (Extremely improbable)	1A	1B	1C	1D	1E

Извор / Source: ICAO Doc 9859 – Safety Management Manual (SMM), Fourth Edition,
Table 3 – Example safety risk matrix.

Прифатливост на безбедносниот ризик (Safety Risk Tolerability)

Врз основа на резултатите од проценката, организацијата треба да утврди дали безбедносниот ризик е:

- прифатлив (Acceptable);
- толерантен/прифатлив под определени услови (Tolerable); или
- неприфатлив (Unacceptable).

За ризиците кои не се прифатливи без дополнителни мерки, организацијата треба да утврди соодветни мерки за намалување или контрола на ризикот (Safety Risk Mitigation/Control Measures) пред активноста да продолжи или промената да биде имплементирана.

ТАБЕЛА 4. ПРИФАТЛИВОСТ НА БЕЗБЕДНОСНИОТ РИЗИК (ПРИМЕР) TABLE 4. SAFETY RISK TOLERABILITY (EXAMPLE)		
НИВО НА ПРИФАТЛИВОСТ TOLERABILITY LEVEL	ИНДЕКС НА РИЗИК RISK INDEX	ПРЕПОРАЧАНА ПОСТАПКА RECOMMENDED ACTION
НЕПРИФАТЛИВ INTOLERABLE	5A, 5B, 5C, 4A, 4B, 3A	Ризикот е неприфатлив во постојните околности. Активноста не смеа да започне или мора веднаш да се запре. The risk is intolerable under the existing circumstances. The activity must not start or must be stopped immediately.
ТОЛЕРАНТЕН TOLERABLE	5D, 5E, 4C, 4D, 4E, 3B, 3C, 2A, 2B	Прифатлив врз основа на намалување на ризикот. Потребни се мерки за намалување на ризикот. Може да бара одлука на раководството. Acceptable based on risk mitigation. Risk reduction measures are required. It may require management decision.
ПРИФАТЛИВ ACCEPTABLE	3D, 3E, 2C, 2D, 2E, 1A, 1B, 1C, 1D, 1E	Прифатлив како што е. Не е потребно дополнително намалување на ризикот. Acceptable as is. No further risk mitigation required.

Извор / Source: ICAO Doc 9859 – Safety Management Manual (SMM), Fourth Edition.
Table 4 – Example safety risk tolerability.

Прифаќање и одобрување на ризикот (Risk Acceptance and Approval)

Организацијата треба да утврди соодветно ниво на овластување за прифаќање/одобрување на безбедносниот ризик (Risk Acceptance/Approval), во зависност од проценетото ниво на ризик.

Ризиците со повисоко ниво треба да бидат предмет на разгледување и одобрување од соодветно повисоко ниво на раководство.

Одлуката за прифаќање на ризикот треба да биде документирана.

Намалување на безбедносниот ризик (Safety Risk Mitigation)

Кога безбедносниот ризик е оценет како неприфатлив или кога е потребно негово дополнително намалување, организацијата треба да утврди соодветни мерки за контрола или намалување на ризикот.

Мерките може да вклучуваат промени во процедури, организација, опрема, системи, обука или други активности со кои се намалува веројатноста и/или сериозноста на можните последици.

Со повторната проценка треба да се утврди преостанатиот ризик (Residual Risk) и да се потврди дека тој е намален на прифатливо или толерантно ниво.

Доколку преостанатиот ризик и понатаму не е прифатлив, треба да се утврдат и спроведат дополнителни мерки за намалување на ризикот.

Мерките, одговорностите, роковите, резултатите од повторната проценка и одлуката за прифаќање на преостанатиот ризик треба да бидат документирани и следливи.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставена и документирана методологија за проценка на безбедносниот ризик (Safety Risk Assessment)?
- Дали за идентификуваните опасности се утврдуваат можните последици?
- Дали при проценката се утврдуваат веројатноста (Probability) и сериозноста (Severity) на можните последици?
- Дали организацијата користи документирана матрица на безбедносен ризик (Safety Risk Matrix)?
- Дали врз основа на веројатноста и сериозноста се определува индексот/нивото на безбедносниот ризик (Safety Risk Index/Level)?
- Дали се воспоставени критериуми за прифатливост на ризикот (Risk Tolerability Criteria)?
- Дали е јасно определено кои ризици се прифатливи (Acceptable), толерантни/прифатливи под определени услови (Tolerable) или неприфатливи (Unacceptable)?
- Дали е определено соодветното ниво на овластување за прифаќање/одобрување на ризикот



- (Risk Acceptance/Approval) во зависност од проценетото ниво на ризик?
- Дали одлуките за прифаќање/одобрување на ризикот се документираат?
- Дали, кога е потребно, се утврдуваат и спроведуваат соодветни мерки за намалување/контрола на ризикот (Safety Risk Mitigation/Control Measures)?
- Дали за утврдените мерки се определуваат одговорни лица и, каде што е применливо, рокови за нивна реализација?
- Дали реализацијата на утврдените мерки се следи?
- Дали по спроведувањето на мерките се врши повторна проценка на безбедносниот ризик?
- Дали по повторната проценка се утврдува и документира преостанатиот ризик (Residual Risk)?
- Дали, кога преостанатиот ризик не е прифатлив, се утврдуваат и спроведуваат дополнителни мерки?
- Дали оценките на ризикот, преземените мерки, одлуките и резултатите од повторната проценка се соодветно документирани и следливи?
- Дали организацијата може да покаже практичен пример за целосниот процес: опасност → почетна проценка на ризик → мерки за намалување/контрола → повторна проценка → преостанат ризик → прифаќање/одобрување на ризикот

3. Уверување во безбедноста (Safety Assurance)

Уверувањето во безбедноста (Safety Assurance) опфаќа процеси и активности преку кои организацијата го следи функционирањето на SMS и безбедносните перформанси и утврдува дали воспоставените мерки за контрола на безбедносниот ризик се ефективни.

Организацијата треба да воспостави механизми за следење и мерење на безбедносните перформанси, управување со промените и континуирано подобрување на SMS.

Оваа компонента ги опфаќа следните елементи:

- 3.1 Следење и мерење на безбедносните перформанси (Safety Performance Monitoring and Measurement);
- 3.2 Управување со промени (Management of Change);
- 3.3 Континуирано подобрување на SMS (Continuous Improvement of the SMS);

3.1 Следење и мерење на безбедносните перформанси (Safety Performance Monitoring and Measurement)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува процес за следење и мерење на безбедносните перформанси (Safety Performance Monitoring and Measurement) и за проверка на ефективност на мерките за контрола на безбедносниот ризик.

Безбедносните перформанси треба да се следат во однос на утврдените безбедносни цели (Safety Objectives) и индикатори за безбедносни перформанси (Safety Performance Indicators – SPIs).

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да воспостави и документира процес за следење и мерење на безбедносните перформанси;
- да утврди безбедносни цели (Safety Objectives) кои се соодветни на нејзините активности и безбедносни ризици;
- да воспостави индикатори за безбедносни перформанси (Safety Performance Indicators – SPIs) за следење на постигнувањето на безбедносните цели;
- каде што е применливо, да утврди целни вредности на безбедносните перформанси (Safety Performance Targets – SPTs);



- да собира и анализира безбедносни податоци и информации потребни за следење на безбедносните перформанси;
- да ги следи трендовите и промените во безбедносните перформанси и да идентификува области во кои е потребно преземање дополнителни активности;
- да ја следи ефективността на мерките за намалување/контрола на безбедносниот ризик (Safety Risk Mitigation/Control Actions);
- периодично да ги преиспитува безбедносните цели, SPIs и SPTs и, по потреба, да ги ажурира;
- резултатите од следењето на безбедносните перформанси да ги доставува до релевантното раководство за разгледување и преземање соодветни активности.

Индикатори за безбедносни перформанси (Safety Performance Indicators – SPIs)

Организацијата треба да воспостави индикатори за безбедносни перформанси (Safety Performance Indicators – SPIs) со кои се следи постигнувањето на утврдените безбедносни цели и безбедносните перформанси на организацијата.

SPIs треба да бидат соодветни на природата, обемот и сложеноста на активностите на организацијата и да бидат поврзани со утврдените безбедносни цели (Safety Objectives) и значајните безбедносни ризици.

При утврдување на SPIs треба да се земат предвид достапноста и веродостојноста на податоците потребни за нивно следење.

За секој SPI, каде што е применливо, треба да се определат:

- назив и опис на индикаторот;
- поврзана безбедносна цел (Safety Objective);
- извор на податоци;
- начин/метод на пресметување;
- одговорно лице или организациска единица;
- периодичност на следење;
- целна вредност (Safety Performance Target – SPT);
- ниво на предупредување (Alert Level/Trigger), каде што се користи.

Организацијата треба периодично да ги следи и анализира SPIs и SPTs со цел навремено да идентификува негативни трендови или значајни промени во безбедносните перформанси.

Внатрешни проверки (Internal Audits)

Организацијата треба да воспостави процес на внатрешни проверки (Internal Audits) како дел од уверувањето во безбедноста.

Внатрешните проверки треба да се користат за:

- проверка на усогласеноста со применливите барања;
- проверка на практичната примена на SMS процесите и процедурите;
- оценување на ефективността на SMS;
- проверка на ефективността на воспоставените мерки за контрола на безбедносниот ризик;
- идентификување на области во кои е потребно подобрување.

Организацијата треба да има документирана програма/план за внатрешни проверки и да обезбеди соодветна независност и објективност на лицата кои ги спроведуваат проверките.

Утврдените наоди треба да бидат документирани, а кога е потребно треба да се определат корективни мерки (Corrective Actions), одговорни лица и рокови за нивно спроведување.

Реализацијата на корективните мерки треба да се следи до нивно затворање и да се обезбеди следливост помеѓу наодот, преземената мерка и резултатот од нејзиното спроведување.



Извори за следење на безбедносните перформанси (Sources for Safety Performance Monitoring)

Организацијата може да користи различни извори на безбедносни податоци и информации, вклучувајќи:

- системи за пријавување на безбедносни настани;
- безбедносни анализи и студии;
- тренд анализи;
- внатрешни проверки;
- безбедносни прегледи и анкети;
- резултати од истраги;
- резултати од надзор;
- оперативни податоци и други релевантни извори.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставен процес за следење и мерење на безбедносните перформанси (Safety Performance Monitoring and Measurement)?
- Дали се утврдени безбедносни цели (Safety Objectives)?
- Дали се воспоставени SPIs поврзани со безбедносните цели и значајните безбедносни ризици?
- Дали SPIs ги опфаќаат оперативните безбедносни перформанси и функционирањето на SMS?
- Дали за секој SPI се определени изворот на податоци, начинот на пресметување, одговорноста и периодичноста на следење?
- Дали се утврдени SPTs, каде што е применливо?
- Дали се утврдени alert levels/triggers, каде што се користат?
- Дали SPIs и SPTs редовно се следат и анализираат?
- Дали се следат трендовите и значајните промени во безбедносните перформанси?
- Дали организацијата ја следи ефективноста на мерките за контрола на безбедносниот ризик?
- Дали е воспоставена програма/план за внатрешни проверки (Internal Audits)?
- Дали внатрешните проверки ја опфаќаат ефективноста на SMS и мерките за контрола на ризикот?
- Дали се обезбедува соодветна независност и објективност на внатрешните проверувачи?
- Дали наодите и корективните мерки се документираат и следат до затворање?
- Дали постои следливост наод → корективна мерка → реализација → затворање?
- Дали резултатите од safety performance monitoring и internal audits се разгледуваат од раководството?
- Дали SPIs, SPTs и другите механизми за следење периодично се преиспитуваат и, по потреба, се ажурираат?
- Дали организацијата може да покаже практични примери на SPI → monitoring/trend → утврдено отстапување → преземена активност → резултат?

3.2 Управување со промени (Management of Change)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува процес за идентификација и управување со промените (Management of Change) кои можат да влијаат врз безбедноста на нејзините услуги и активности.

Пред воведување на значајна промена, организацијата треба да ги идентификува опасностите поврзани со промената, да ги процени безбедносните ризици и да утврди соодветни мерки за нивно намалување или контрола.



Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да воспостави и документа процес за управување со промени (Management of Change);
- да ги идентификува промените кои можат да влијаат врз безбедноста, вклучувајќи, каде што е применливо, промени во:
 - o организациската структура и одговорностите;
 - o персоналот и потребните компетенции;
 - o услугите и оперативните активности;
 - o системите, опремата и технологијата;
 - o инфраструктурата;
 - o процедурите и работните процеси;
 - o регулаторните барања;
 - o оперативното опкружување;
 - o договорните односи и интерфејсите со надворешни организации;
- пред имплементација на промената да изврши идентификација на опасности (Hazard Identification) и проценка на безбедносниот ризик (Safety Risk Assessment);
- да ги земе предвид постојните мерки за контрола на безбедносниот ризик (Existing Safety Risk Controls) и да утврди дали тие остануваат соодветни и ефективни по воведувањето на промената;
- кога е потребно, да утврди и спроведе дополнителни мерки за намалување/контрола на безбедносниот ризик (Safety Risk Mitigation/Control Actions);
- да ги утврди одговорностите и роковите за спроведување на активностите поврзани со промената;
- да ја документа проценката на промената и донесените одлуки;
- по имплементацијата да го следи влијанието на промената врз безбедноста и, по потреба, да преземе дополнителни мерки.

Безбедносна студија на промена (Safety Study of Change)

Кога природата, обемот или сложеноста на промената го бара тоа, организацијата треба, пред нејзината имплементација, да спроведе и документа безбедносна студија (Safety Study).

Безбедносната студија треба да се изработува со учество на експерти од областа на која се однесува промената и лице кое ја познава применливата методологија и го координира процесот на идентификација и проценка на ризиците.

Организацијата треба да ја дефинира методологијата за изработка на безбедносната студија. Целта на студијата е да се минимизира влијанието на промената врз нивото на безбедност и да се покаже дека со воведувањето на промената нивото на безбедност нема да се намали.

Безбедносната студија треба, каде што е применливо, да содржи:

- опис и цел на предложената промена;
- опсег на промената;
- засегнати системи, процеси, услуги и организациски единици;
- идентификувани опасности поврзани со промената;
- проценка на безбедносните ризици, вклучително сериозноста (Severity) и веројатноста (Probability);
- мерки за намалување и контрола на ризиците;
- потребна внатрешна и надворешна координација;
- преоден период (Transition Phase), каде што е применливо;
- одговорности и рокови за спроведување на мерките;
- начин на следење на имплементацијата;
- услови за прифаќање и пуштање на промената во употреба;
- следливост на активностите поврзани со промената.



Проценката на безбедносниот ризик треба да се спроведе согласно методологијата утврдена во **2.2 Проценка и намалување на безбедносниот ризик (Safety Risk Assessment and Mitigation)** од овој прирачник.

Мерките за намалување на ризикот треба да бидат спроведени пред имплементацијата на промената. По нивното спроведување, за секој ризик повторно се определуваат сериозноста (Severity) и веројатноста (Probability) и се врши повторна проценка со цел да се утврдат преостанатиот ризик (Residual Risk) и неговата прифатливост.

Преоден период и следење на промената (Transition Phase and Change Monitoring)

Во текот на преодниот период (Transition Phase) организацијата треба да ги следи безбедносните ризици поврзани со преминот од постојната кон новата состојба и да обезбеди дека утврдените мерки за контрола на ризикот се соодветно спроведени.

По имплементацијата на промената треба да се провери дали:

- промената е спроведена согласно планираните активности;
- утврдените мерки за контрола на ризикот се имплементирани и ефективни;
- не се појавиле нови или претходно неидентификувани опасности;
- промената не влијае негативно врз постојните мерки за контрола на ризикот;
- преостанатиот ризик е на прифатливо ниво;
- се потребни дополнителни безбедносни мерки.

Пуштање во употреба и документација (Commissioning and Documentation)

Каде што е применливо, промената треба да биде пуштена во употреба (Commissioning) откако ќе се потврди дека утврдените безбедносни барања и мерки се исполнети и дека преостанатиот ризик е прифатлив.

Одлуката за пуштање на промената во употреба треба да биде документирана и следлива и, каде што е применливо, да се заснова на одобрение од АЦВ и на референца кон соодветната безбедносна студија (Safety Study).

Документацијата поврзана со управувањето со промената, вклучително безбедносните студии, проценките на ризик, утврдените мерки, одобрувањата и доказите за нивната имплементација, треба соодветно да се чува и да биде следлива.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставен и документиран процес за управување со промени (Management of Change)?
- Дали е јасно определено кои промени се предмет на овој процес?
- Дали потенцијалното влијание врз безбедноста се оценува пред имплементацијата на промената?
- Дали пред имплементацијата на значајна промена се врши идентификација на опасности (Hazard Identification) и проценка на безбедносниот ризик (Safety Risk Assessment)?
- Дали се оценува влијанието на промената врз постојните мерки за контрола на безбедносниот ризик?
- Дали се определуваат и следат потребните мерки за намалување на ризикот, одговорностите и роковите?
- Дали за значајните промени се изготвува безбедносна студија (Safety Study), каде што е применливо?
- Дали по спроведувањето на мерките се врши повторна проценка и се утврдува преостанатиот ризик (Residual Risk)?
- Дали се управува со безбедносните ризици во преодниот период (Transition Phase)?
- Дали пред пуштањето во употреба се проверува имплементацијата и ефективноста на утврдените безбедносни мерки?
- Дали по имплементацијата се проверува дали промената создала нови опасности или влијаела врз постојните ризици?

- Дали, каде што е применливо, промената формално се пушта во употреба (Commissioning)?
- Дали документацијата поврзана со управувањето со промените се чува и е следлива?
- Дали организацијата може да покаже практичен пример за управувана промена од нејзиното иницирање до имплементацијата и следењето?

3.3 Континуирано подобрување на SMS (Continuous Improvement of the SMS)

Применливо барање (Applicable Requirement)

Организацијата треба континуирано да ја следи и оценува ефективноста на системот за управување со безбедноста (Safety Management System – SMS) и да ги идентификува областите во кои е потребно подобрување.

Континуираното подобрување треба да се заснова на резултатите од следењето на безбедносните перформанси, внатрешните проверки, анализата на безбедносните податоци и информации, управувањето со ризиците, корективните мерки и прегледите од страна на раководството.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- периодично да ја оценува ефективноста на SMS и неговите процеси;
- да ги користи резултатите од следењето и мерењето на безбедносните перформанси (Safety Performance Monitoring and Measurement) за идентификување на области во кои е потребно подобрување;
- да ги зема предвид резултатите од:
 - o внатрешните проверки (Internal Audits);
 - o анализата на безбедносните настани;
 - o идентификацијата на опасности и проценката на ризиците;
 - o следењето на SPIs и SPTs;
 - o безбедносните анализи и трендови;
 - o корективните и превентивните мерки;
 - o управувањето со промени;
 - o повратните информации од персоналот и други релевантни извори;
- да утврдува и спроведува соодветни активности за отстранување на утврдените недостатоци и подобрување на SMS;
- да определува одговорни лица и рокови за спроведување на активностите;
- да ја следи реализацијата на утврдените активности до нивно затворање;
- да ја оценува ефективноста на преземените активности;
- кога преземените активности не се доволно ефективни, да утврди и спроведе дополнителни мерки.

Циклус на континуирано подобрување (Plan–Do–Check–Act – PDCA)

Континуираното подобрување на SMS може да се спроведува преку принципот Планирај – Спроведи – Провери – Подобри (Plan–Do–Check–Act – PDCA):

- Планирај (Plan) – идентификување на потребата за подобрување и планирање на потребните активности;
- Спроведи (Do) – спроведување на планираните активности;
- Провери (Check) – следење и оценување на резултатите и ефективноста на преземените активности;
- Подобри (Act) – преземање дополнителни активности, кога е потребно, и вградување на постигнатите подобрувања во SMS.



Корективни мерки (Corrective Actions)

Кога преку внатрешни проверки, анализа на безбедносни податоци, следење на безбедносните перформанси или други SMS активности ќе се идентификува недостаток, организацијата треба да утврди соодветна корективна мерка (Corrective Action).

Корективни мерки треба да се утврдуваат и спроведуваат, особено, за причините за безбедносните настани, наодите од проверките и кога индикаторите за безбедносни перформанси покажуваат незадоволителни резултати.

За корективните мерки треба да бидат определени:

- утврдениот недостаток или наод;
- потребната корективна мерка;
- одговорното лице или организациска единица;
- рокот за реализација;
- статусот на реализација;
- начинот на проверка на ефективноста.

Организацијата треба да има документирана процедура за управување со корективните мерки, која го опфаќа нивното утврдување и следење и обезбедува поврзаност помеѓу утврдениот наод (безбедносен настан, наод од проверка или друг релевантен извор) и соодветната корективна мерка.

Корективните мерки треба да се следат до нивното затворање. Треба да постои следливост помеѓу наодот → корективната мерка → реализацијата → проверката на ефективноста → затворањето.

Следливоста на корективните мерки треба да биде обезбедена, да може да се докаже и соодветно да се евидентира и чува.

Преглед од страна на раководството (Management Review)

Раководството треба периодично да ја разгледува соодветноста и ефективноста на SMS.

Прегледот треба, каде што е применливо, да ги земе предвид:

- безбедносните цели и нивното остварување;
- SPIs и SPTs и нивните трендови;
- значајните идентификувани опасности и безбедносни ризици;
- резултатите од внатрешните проверки;
- статусот и ефективноста на корективните мерки;
- значајните промени кои можат да влијаат врз SMS;
- резултатите од безбедносните анализи;
- потребата од дополнителни ресурси или подобрувања.

Резултатите од прегледот треба да бидат документирани, а утврдените активности да се следат до нивна реализација.

Следење на SMS (SMS Monitoring)

Организацијата треба континуирано да го следи функционирањето на SMS со цел да утврди дали системот останува соодветен и ефективен и дали ги постигнува утврдените безбедносни цели.

Следењето треба да овозможи навремено идентификување на слабости, негативни трендови и области во кои се потребни дополнителни активности или подобрувања.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставен и документиран процес за континуирано подобрување на SMS (Continuous Improvement of the SMS)?
- Дали ефективноста на SMS и неговите процеси периодично се оценува?
- Дали резултатите од следењето на безбедносните перформанси (Safety Performance Monitoring), внатрешните проверки (Internal Audits), анализата на безбедносните настани (Occurrence Analysis) и другите SMS активности се користат за идентификување на области



- и можности за подобрување?
- Дали утврдените недостатоци резултираат со соодветни корективни мерки (Corrective Actions)?
- Дали за корективните мерки се определуваат одговорни лица и рокови за нивна реализација?
- Дали реализацијата на корективните мерки се следи до нивното затворање?
- Дали се проверува и документира ефективностa на преземените корективни мерки?
- Дали се утврдуваат и спроведуваат дополнителни мерки кога првично преземените мерки не се доволно ефективни?
- Дали постои следливост наод → корективна мерка → реализација → проверка на ефективностa → затворање?
- Дали раководството периодично спроведува преглед на SMS (Management Review)?
- Дали прегледот од страна на раководството (Management Review) ги опфаќа безбедносните цели, SPIs/SPTs, значајните идентификувани опасности и безбедносни ризици, резултатите од внатрешните проверки, статусот и ефективностa на корективните мерки, значајните промени и потребата од дополнителни ресурси или подобрувања?
- Дали резултатите, одлуките и утврдените активности од Management Review се документираат и следат до нивна реализација?
- Дали организацијата континуирано го следи функционирањето на SMS со цел да утврди дали системот останува соодветен и ефективен и дали ги постигнува утврдените безбедносни цели?
- Дали организацијата може да покаже практичен пример за процесот: утврден недостаток → корективна мерка → реализација → проверка на ефективностa → затворање/дополнителна мерка?

4. Промоција на безбедноста (Safety Promotion)

Промоцијата на безбедноста (Safety Promotion) е важен дел од системот за управување со безбедноста (Safety Management System – SMS) и има за цел да обезбеди персоналот да ги поседува потребните знаења и компетенции за извршување на своите безбедносни одговорности и да биде информиран за прашањата поврзани со безбедноста.

Оваа компонента ги опфаќа следните елементи:

- 4.1 Обука и едукација (Training and Education);
- 4.2 Комуникација за безбедноста (Safety Communication);

4.1 Обука и едукација (Training and Education)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува програма за обука за безбедност (Safety Training Programme) со која се обезбедува персоналот да биде обучен и компетентен за извршување на своите должности поврзани со SMS.

Обемот и содржината на обуката треба да бидат соодветни на улогата, одговорностите и вклученоста на персоналот во функционирањето на системот за управување со безбедноста (Safety Management System – SMS).

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да ги утврди потребите за SMS обука за различните категории на персонал;
- да воспостави и документира програма и план за обука (Training Programme and Training Plan);
- да обезбеди обуката да биде соодветна на улогите и одговорностите на персоналот во SMS;



ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS) КАЈ ОРГАНИЗАЦИИТЕ

Одделение SQS и мониторинг на усогласеност

- да обезбеди почетна обука (Initial Training) за персоналот кој има должности и одговорности поврзани со SMS;
- да обезбеди периодична/обновувачка обука (Recurrent/Refresher Training) со цел одржување и ажурирање на потребните знаења и компетенции;
- да обезбеди соодветна SMS обука за раководниот персонал, вклучително и за одговорниот раководител (Accountable Executive/Manager);
- да обезбеди соодветна обука за раководителот за безбедност (Safety Manager) и други лица со специфични SMS одговорности;
- да обезбеди персоналот да биде запознаен со измените на SMS, релевантните процедури и новите или изменетите безбедносни барања;
- да ја следи реализацијата на планираните обуки и, кога е потребно, да ја ажурира програмата и планот за обука;
- да води и чува соодветна евиденција за завршените обуки.

Содржина на SMS обуката (SMS Training Content)

Содржината и нивото на SMS обуката треба да бидат приспособени на функциите и одговорностите на персоналот.

Обуката, каде што е применливо, треба да ги опфати:

- политиката и целите за безбедност (Safety Policy and Objectives);
- организацијата, улогите и одговорностите во SMS;
- принципите и компонентите на SMS;
- идентификацијата на опасности (Hazard Identification);
- проценката и намалувањето на безбедносниот ризик (Safety Risk Assessment and Mitigation);
- системите за пријавување на безбедносни настани;
- следењето и мерењето на безбедносните перформанси (Safety Performance Monitoring and Measurement);
- индикаторите и целите за безбедносни перформанси (SPIs/SPTs);
- управувањето со промени (Management of Change);
- уверувањето во безбедноста (Safety Assurance);
- промоцијата на безбедноста (Safety Promotion);
- релевантните процедури и документација на организацијата.

Обука според функцијата и одговорностите (Role-Based Training)

Организацијата треба да обезбеди различно ниво и содржина на обуката во зависност од функцијата и SMS одговорностите на персоналот.

Особено треба да се земат предвид потребите за обука на:

- одговорниот раководител (Accountable Executive/Manager) и високото раководство;
- раководителот за безбедност (Safety Manager) и персоналот кој непосредно работи на SMS;
- раководителите на организациските единици;
- оперативниот и техничкиот персонал;
- персоналот вклучен во идентификација на опасности (Hazard Identification), проценка на безбедносниот ризик (Safety Risk Assessment), пријавување на безбедносни настани (Occurrence Reporting) и уверување во безбедноста (Safety Assurance);
- друг персонал чија работа може да има влијание врз безбедноста.

Евиденција за обуките (Training Records)

Организацијата треба да воспостави и одржува евиденција за спроведените SMS обуки.

Евиденцијата треба, каде што е применливо, да содржи:



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИЈИТЕ**
Одделение SQS и мониторинг на усогласеност

- име и функција на учесникот;
- назив и содржина на обуката;
- датум на одржување;
- вид на обука;
- давател/инструктор на обуката;
- доказ за завршена обука;
- датум или период за следна обука, кога е применливо.

Евиденцијата треба да овозможи организацијата да го следи статусот на обученост и компетентност на персоналот и навремено да ги планира потребните периодични или дополнителни обуки.

Следење и ажурирање на обуката (Training Monitoring and Update)

Програмата и планот за обука треба периодично да се преиспитуваат и, кога е потребно, да се ажурираат, земајќи ги предвид:

- промените во SMS;
- промените во организацијата и нејзините активности;
- измените на применливите барања;
- резултатите од safety performance monitoring;
- резултатите од проверки и проценки;
- идентификуваните потреби за дополнителна обука;
- lessons learned од безбедносни настани и други релевантни безбедносни информации.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставена и документирана програма за SMS обука (SMS Training Programme)?
- Дали организацијата има воспоставен план за реализација на SMS обуките (SMS Training Plan)?
- Дали потребите за обука се утврдени според функциите, улогите и SMS одговорностите на персоналот?
- Дали се обезбедува почетна обука (Initial Training) за персоналот кој има должности и одговорности поврзани со SMS?
- Дали се обезбедува периодична/обновувачка обука (Recurrent/Refresher Training) со цел одржување и ажурирање на потребните знаења и компетенции?
- Дали одговорниот раководител (Accountable Executive/Manager) и раководниот персонал добиваат SMS обука соодветна на нивните улоги и одговорности?
- Дали раководителот за безбедност (Safety Manager) има соодветна обука и компетентност за извршување на својата функција?
- Дали персоналот вклучен во идентификација на опасности (Hazard Identification), проценка на безбедносниот ризик (Safety Risk Assessment), пријавување на безбедносни настани (Occurrence Reporting) и уверување во безбедноста (Safety Assurance) е соодветно обучен?
- Дали содржината и нивото на SMS обуката се соодветни на функциите, должностите и одговорностите на персоналот?
- Дали програмата и планот за обука периодично се преиспитуваат и, кога е потребно, се ажурираат?
- Дали организацијата води и чува соодветна евиденција за обуките (Training Records)?
- Дали евиденцијата овозможува следење на статусот на обученост и компетентност на персоналот и навремено планирање на потребните периодични или дополнителни обуки?
- Дали организацијата ја оценува потребата од дополнителна обука врз основа на промени во SMS и организацијата, изменети барања, наоди, безбедносни настани, резултати од следењето на безбедносните перформанси (Safety Performance Monitoring) и поуки од



искуството (Lessons Learned)?

- Дали организацијата може да покаже практичен пример за следливост: Training Programme → Training Plan → спроведена обука → Training Records → следење/обновување на обуката?

4.2 Комуникација за безбедноста (Safety Communication)

Применливо барање (Applicable Requirement)

Организацијата треба да воспостави и одржува формални средства за комуникација за безбедноста (Safety Communication) со кои се обезбедува релевантниот персонал да биде информиран за SMS, значајните безбедносни прашања и безбедносните ризици поврзани со активностите на организацијата.

Комуникацијата треба да придонесува за развој и одржување на позитивна култура на безбедност (Safety Culture) и да обезбеди навремено споделување на релевантните безбедносни информации.

Имплементација од страна на организацијата (Implementation by Organization)

Организацијата треба:

- да воспостави соодветни формални канали и средства за комуникација за безбедноста;
- да обезбеди персоналот да биде запознаен со политиката и целите за безбедност (Safety Policy and Objectives) и своите улоги и одговорности во рамките на SMS;
- да обезбеди комуникација на релевантните безбедносни информации до персоналот кој има потреба од нив;
- да ги комуницира значајните идентификувани опасности, безбедносните ризици и релевантните мерки за нивно намалување или контрола;
- да обезбеди персоналот да биде информиран за причините за воведување или изменување на SMS процедурите и другите активности поврзани со безбедноста;
- да ги комуницира релевантните промени во SMS документацијата и процедурите;
- да споделува релевантни поуки од искуството (Lessons Learned) од безбедносни настани, анализи, истраги и други извори на безбедносни информации, каде што е применливо;
- да обезбеди комуникацијата за безбедноста да биде двонасочна и да овозможува персоналот да доставува повратни информации и безбедносни прашања;
- да ја оценува соодветноста и ефективноста на средствата за комуникација и, по потреба, да ги подобрува.

Внатрешна комуникација за безбедноста (Internal Safety Communication)

Внатрешната комуникација треба да обезбеди релевантниот персонал да добива навремени и соодветни информации за прашањата кои можат да влијаат врз безбедноста.

За таа цел, организацијата може да користи:

- билтени за безбедност (Safety Bulletins);
- известувања за безбедност (Safety Notices);
- состаноци и безбедносни брифинзи (Safety Briefings);
- електронска пошта и интерни информациски системи;
- интранет;
- презентации и обуки;
- постери и информативни материјали;
- резултати од безбедносни анализи (Safety Analyses);
- поуки од искуството (Lessons Learned);
- други соодветни средства за комуникација.



Надворешна комуникација за безбедноста (External Safety Communication)

Каде што е релевантно, организацијата треба да воспостави соодветна комуникација за безбедноста со надворешни организации и други заинтересирани страни со кои постојат оперативни или безбедносни интерфејси.

Надворешната комуникација може да вклучува размена на релевантни безбедносни информации, координација во однос на идентификувани опасности и ризици и споделување информации за промени кои можат да влијаат врз безбедноста.

При размената на безбедносни информации треба да се почитуваат применливите барања за заштита и доверливост на безбедносните податоци и информации (Protection and Confidentiality of Safety Data and Safety Information).

Комуникација на SMS информации (Communication of SMS Information)

Организацијата треба да обезбеди персоналот да биде информиран за функционирањето и развојот на SMS.

На персоналот треба да му бидат достапни релевантните SMS информации и документација, вклучително SMM, процедурите, извештаите од безбедносни прегледи, извештаите од проверки и другите релевантни SMS документи. Овие информации треба да бидат лесно достапни за персоналот.

Комуникацијата за безбедноста треба да обезбеди персоналот да биде информиран за главните безбедносни проблеми идентификувани во рамките на организацијата, како и за релевантните безбедносни проблеми и информации кои потекнуваат од други организации.

Организацијата треба да го информира релевантниот персонал за преземените активности по пријавени безбедносни настани, вклучително корективните мерки и повратните информации (Feedback), со цел да се поттикне пријавувањето на настаните.

Комуникацијата треба, исто така, да објасни зошто се преземаат определени активности за подобрување на безбедноста и зошто се воведуваат или менуваат определени процедури за безбедност.

Комуникацијата треба, каде што е применливо, да опфати:

- политика и цели за безбедност (Safety Policy and Objectives);
- SMS улоги и одговорности (SMS Roles and Responsibilities);
- значајни опасности (Hazards) и безбедносни ризици (Safety Risks);
- мерки за намалување/контрола на безбедносниот ризик (Safety Risk Mitigation/Control Actions);
- релевантни SPIs/SPTs и безбедносни трендови;
- промени во SMS и релевантните процедури;
- резултати од активностите за уверување во безбедноста (Safety Assurance Activities);
- релевантни поуки од искуството (Lessons Learned);
- други информации потребни за ефективно функционирање на SMS.

Самооценување на SMS (SMS Self-Assessment)

- Дали организацијата има воспоставен и документиран процес за комуникација за безбедноста (Safety Communication)?
- Дали персоналот е запознаен со политиката и целите за безбедност (Safety Policy and Objectives) и со своите улоги и одговорности во рамките на SMS?
- Дали релевантните безбедносни информации навремено се доставуваат до персоналот кој има потреба од нив?
- Дали се комуницираат значајните идентификувани опасности (Hazards), безбедносните ризици (Safety Risks) и релевантните мерки за нивно намалување или контрола?
- Дали персоналот се информира за причините за воведување или изменување на SMS процедурите и другите активности поврзани со безбедноста?



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИИТЕ**
Одделение SQS и мониторинг на усогласеност

- Дали релевантните промени во SMS документацијата и процедурите соодветно и навремено се комуницираат?
- Дали организацијата споделува релевантни поуки од искуството (Lessons Learned) од безбедносни настани, анализи, истраги и други извори на безбедносни информации?
- Дали се користат различни и соодветни средства за комуникација, како билтени за безбедност (Safety Bulletins), безбедносни брифинзи (Safety Briefings), состаноци, електронска пошта, интранет, презентации и други соодветни средства?
- Дали комуникацијата за безбедноста е двонасочна и дали персоналот има можност да доставува повратни информации и прашања поврзани со безбедноста?
- Дали, каде што е применливо, се разменуваат релевантни безбедносни информации со надворешни организации и други заинтересирани страни со кои постојат оперативни или безбедносни интерфејси?
- Дали при надворешната комуникација се почитуваат применливите барања за заштита и доверливост на безбедносните податоци и информации (Protection and Confidentiality of Safety Data and Safety Information)?
- Дали организацијата периодично ја оценува соодветноста и ефективноста на средствата за комуникација за безбедноста и, кога е потребно, ги подобрува?
- Дали организацијата може да покаже практични докази за комуникација за безбедноста (Safety Communication), како билтени за безбедност, презентации, записи од состаноци, безбедносни брифинзи, електронска пошта или други објавени безбедносни информации?
- Дали SMS информациите и документацијата (SMM, процедури, извештаи од Management Review, извештаи од проверки, годишен акциски план, корективни мерки и др.) се достапни на персоналот?
- На кој начин и од кого се обезбедува нивната достапност?
- Дали индикаторите за безбедносни перформанси се објавуваат/комуницираат и на кој начин?
- Дали релевантниот персонал се информира за безбедносни проблеми идентификувани во други организации и на кој начин?

5. Нивоа и критериуми за утврдување (Determination Levels and Criteria)

Организацијата треба, каде што е применливо, во рамките на своите SMS процеси да воспостави, документира и применува соодветни критериуми и нивоа за донесување одлуки и преземање активности.

Критериумите и нивоата, каде што е применливо, треба да опфатат:

- класификација и прифатливост на безбедносниот ризик (Safety Risk Classification and Tolerability);
- нивоа на овластување за прифаќање/одобрување на ризикот (Risk Acceptance/Approval Levels);
- критериуми за определување, спроведување и следење на мерките за намалување/контрола на безбедносниот ризик (Safety Risk Mitigation/Control Measures);
- критериуми за следење на безбедносните перформанси, вклучително SPIs, SPTs и нивоа на предупредување/активирање (Alert Levels/Triggers), каде што се применуваат;
- класификација и следење на наодите од внатрешните проверки (Internal Audits), каде што се применува;
- рокови за спроведување на корективните мерки (Corrective Actions), соодветни на значењето на утврдениот недостаток или наод;
- критериуми за проверка на ефективноста и затворање на корективните мерки;
- нивоа на одговорност и овластување за донесување одлуки поврзани со безбедноста.

Критериумите, нивоата и роковите треба да бидат соодветни на природата, обемот и сложеноста на активностите на организацијата и да бидат утврдени во SMS документацијата или во соодветните процедури.



**ПРИРАЧНИК ЗА ИМПЛЕМЕНТАЦИЈА НА СИСТЕМ ЗА
УПРАВУВАЊЕ СО БЕЗБЕДНОСТА (SMS)
КАЈ ОРГАНИЗАЦИЈИТЕ
Одделение SQS и мониторинг на усогласеност**

6. Список на применливи процедури, обрасци и контролни листи

Организацијата треба да воспостави, одржува и ажурира список на процедурите, обрасците, контролните листи и другата документација што се користи за спроведување и одржување на SMS. Во рамките на SMS, организацијата треба да воспостави и одржува документираните процедури за процесите за кои е потребно да се обезбеди стандардизиран начин на постапување, одговорности, следливост и евиденција.

Како минимум, каде што е применливо, SMS документацијата треба да вклучува процедури за:

- управување со документацијата (Document Management);
- управување и чување на записи (Record Keeping);
- внатрешни проверки (Internal Audits);
- управување со наоди и корективни мерки (Findings and Corrective Actions).

Покрај наведените, организацијата треба да воспостави и други процедури потребни за функционирање на SMS, во зависност од природата, големината и сложеноста на нејзините активности и применливите барања.

Списокот треба да овозможи идентификација на важечката верзија на секој документ и, каде што е применливо, да ги содржи кодот, називот, видот на документот, бројот на издание/ревизија и датумот на важечката ревизија.

Табелата е дадена како пример и треба да се дополни со сите применливи процедури, обрасци, контролни листи и други контролирани документи што организацијата ги користи во рамките на SMS.

Бр.	Код Code	Назив на документот Document Title	Вид Type	Издание/Ревизија Edition/Revision	Датум Date
1.			Процедура Procedure		
2.			Процедура Procedure		
3.			Образец Form		
4.			Образец Form		
5.			Контролна листа Checklist		



- **Заклучок**

Овој прирачник обезбедува насоки за воспоставување, имплементација, одржување и континуирано подобрување на системот за управување со безбедноста (Safety Management System – SMS) кај организациите, во согласност со применливите национални барања и стандардите и препорачаните практики на ICAO.

Ефективното функционирање на SMS бара систематски пристап кон управувањето со безбедноста, кој ги опфаќа политиката и целите за безбедност (Safety Policy and Objectives), управувањето со безбедносниот ризик (Safety Risk Management), обезбедувањето на безбедноста (Safety Assurance) и промоцијата на безбедноста (Safety Promotion).

Организацијата е одговорна да обезбеди SMS да биде соодветен на природата, обемот и сложеноста на нејзините активности и да биде интегриран во нејзините редовни процеси на управување и донесување одлуки.

SMS треба да биде соодветно документиран преку Прирачникот за управување со безбедноста (Safety Management Manual – SMM), применливите процедури, записи и друга релевантна SMS документација. SMM треба да го прикажува начинот на кој организацијата ги исполнува применливите SMS барања и да упатува на постојните процедури и други контролирани документи, каде што е применливо.

Воспоставувањето на SMS не треба да се смета за еднократна активност. Организацијата треба континуирано да ги следи своите безбедносни перформанси, да ги идентификува опасностите, да ги проценува и управува безбедносните ризици, да ја следи ефективната на преземените мерки и да го подобрува SMS врз основа на добиените резултати.

Промените кои можат да имаат влијание врз безбедноста треба да се управуваат на систематски начин, а кога природата, обемот или сложеноста на промената го бара тоа, организацијата треба да спроведе и документира безбедносна студија (Safety Study), да ги утврди и спроведе потребните мерки за намалување на ризикот и да ја следи нивната ефективност.

Корективните мерки утврдени врз основа на безбедносни настани, проверки, следење на безбедносните перформанси и други SMS активности треба да бидат документирани, следливи и следени до нивното затворање и проверка на нивната ефективност.

Соодветната обука, комуникацијата за безбедноста и активното учество на раководството и персоналот се неопходни за одржување на ефективен SMS и за развивање и одржување на позитивна култура на безбедност.

Организацијата треба да може да обезбеди соодветни и следливи докази дека барањата, процесите и процедурите утврдени во нејзиниот SMS и SMM се применуваат во пракса и континуирано се одржуваат и подобруваат.