МЕТОДИЧЕСКО УКАЗАНИЕ

Внедряване на Част-IS (Информационна сигурност), съгласно Регламент за изпълнение (ЕС) 2023/203 и Делегиран регламент (ЕС) 2022/1645

	Име	Длъжност	Дата
Изготвил	Николай Николов	и.ф. Н-к отдел ЛГЛ	06.02.2026
Изготвил	Валентин Тодоров	и.ф. Н-к отдел ЛЕЛ	06.02.2026
Изготвил	Емилия Георгиева	Н-к отдел ЛЛНО	06.02.2026
Проверил	Христо Щерионов	Директор АОЛАС	06.02.2026
Проверил	Надя Тотева	Директор АБ	06.02.2026
Съгласувал	Васил Цолов	Гл. секретар ГД ГВА	06.02.2026
Одобрил	Анелия Маринова	Гл. директор ГД ГВА	06.02.2026

А. Списък на изданията/измененията

Издание	Дата	Изменение	Дата	Описание на изменението
001	06.02.2026	00	06.02.2026	Този документ има за цел да предостави насоки, относно внедряването на Част-IS (Информационна сигурност)

Б. Въведение

Съгласно чл. 13, ал. 3, т. 10 от „Устройствен правилник на ГД ГВА“, издаден на основание на чл. 8, ал. 3 от „Закона за гражданското въздухоплаване“, Дирекция „Авиационна безопасност“ и Дирекция „Аеронавигационно осигуряване, летища и авиационна сигурност“ изготвят и издават бюлетини по безопасност, заповеди и други документи, които подпомагат дейността на ГД ГВА и авиационната индустрия.

Настоящото „Методическо указание“ се явява част от изпълнението на задълженията на ГД ГВА по тази точка. Този документ дава насоки, относно внедряването на Част-IS (Информационна сигурност).

1. СЪДЪРЖАНИЕ

2. ТЕРМИНИ И СЪКРАЩЕНИЯ

АБ	АВИАЦИОННА БЕЗОПАСНОСТ
ГД ГВА	ГЛАВНА ДИРЕКЦИЯ ГРАЖДАНСКА ВЪЗДУХОПЛАВАТЕЛНА АДМИНИСТРАЦИЯ - Р. БЪЛГАРИЯ
ЕААБ	ЕВРОПЕЙСКА АГЕНЦИЯ ЗА АВИАЦИОННА БЕЗОПАСНОСТ
РУИС	РЪКОВОДСТВОТО ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ
СУБ	СИСТЕМА ЗА УПРАВЛЕНИЕ НА БЕЗОПАСНОСТТА
СУИС	СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ
AMC	ACCEPTABLE MEANS OF COMPLIANCE
AMO	APPROVED MAINTENANCE ORGANISATION
CCL	CYBERSECURITY CONTROL LIBRARY
EASA	EUROPEAN AVIATION SAFETY AGENCY
GM	GUIDANCE MATERIALS
SMS	SAFETY MANAGEMENT SYSTEM
ISMS	INFORMATION SECURITY MANAGEMENT SYSTEM
ISMM	INFORMATION SECURITY MANAGEMENT MANUAL
KPI	KEY PERFORMANCE INDICATOR

ИНФОРМАЦИОННА СИГУРНОСТ ОЗНАЧАВА ЗАПАЗВАНЕ НА КОНФИДЕНЦИАЛНОСТТА, ЦЕЛОСТТА, АВТЕНТИЧНОСТТА И НАЛИЧНОСТТА НА МРЕЖОВИ И ИНФОРМАЦИОННИ СИСТЕМИ

РИСК ЗА ИНФОРМАЦИОННА СИГУРНОСТ ОЗНАЧАВА РИСКЪТ ЗА ОРГАНИЗАЦИОННИТЕ ОПЕРАЦИИ НА ГРАЖДАНСКАТА АВИАЦИЯ, АКТИВИТЕ, ФИЗИЧЕСКИТЕ ЛИЦА И ДРУГИ ОРГАНИЗАЦИИ, ДЪЛЖАЩ СЕ НА ПОТЕНЦИАЛА НА СЪБИТИЕ, СВЪРЗАНО С ИНФОРМАЦИОННАТА СИГУРНОСТ. РИСКОВЕТЕ ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ СА СВЪРЗАНИ С ВЕРОЯТНОСТТА ПРИ ДАДЕНА ЗАПЛАХА ДА ИМА ВЪЗПОЛЗВАНЕ ОТ УЯЗВИМОСТИТЕ НА ДАДЕН ИНФОРМАЦИОНЕН АКТИВ ИЛИ ГРУПА ИНФОРМАЦИОННИ АКТИВИ.

ПОДИЗПЪЛНИТЕЛ – ОРГАНИЗАЦИЯ, НА КОЯТО СЕ ВЪЗЛАГА, КОЯТО И ДА Е ЧАСТ ОТ ДЕЙНОСТИТЕ ПОСОЧЕНИ В ТОЧКА IS.I/D.OR.200 Т.Е. ДА СЕ ИМА ПРЕДВИД ВЪЗЛАГАНЕ НА ДЕЙНОСТИ ПО УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ПО СМИСЪЛА НА IS.I/D.OR.235.

3. ОБХВАТ И ПРИЛОЖИМОСТ

ГД ГВА е компетентният орган за организациите, чиито одобрения е издала и като такава е отговорна за крайното решение за валидността на тези одобрения и за установяване на процедури, описващи как ГД ГВА управлява заявленията и одобренията на тези организации.
Указанията в тази методика дават насоки за внедряването на Част-IS за организации посочени в член 2 на Регламент (ЕС) 2023/203 и член 2 на Регламент (ЕС) 2022/1645 (виж т. 5 от настоящата методика).

4. ЦЕЛ

Това методическо указание е предназначено да даде пояснения, свързани с Част-IS, като се вземат предвид основно AMC и GM, издадени от EASA.
Информационната сигурност влияе върху авиационната безопасност и обхватът на тези регулации е да адресира управлението на информационната сигурност от организации и доставчици на услуги по пропорционален начин с цел защита на авиационната безопасност.

5. НОРМАТИВНИ ИЗИСКВАНИЯ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2023/203 НА КОМИСИЯТА от 27 октомври 2022 година. Правила за прилагане на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета по отношение на изискванията за управление на рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност за организации, обхванати от обхванати от регламенти (ЕС) № 1321/2014, (ЕС) № 965/2012, (ЕС) № 1178/2011, (ЕС) 2015/340 на Комисията, регламенти за изпълнение (ЕС) 2017/373 и (ЕС) 2021/664 на Комисията, и за компетентните органи, обхванати от регламенти (ЕС) № 748/2012, (ЕС) № 1321/2014, (ЕС) № 965/2012, (ЕС) № 1178/2011, (ЕС) 2015/340 и (ЕС) № 139/2014 на Комисията, регламенти за изпълнение (ЕС) 2017/373 и (ЕС) 2021/664 на Комисията, и за изменение на регламенти (ЕС) № 1178/2011, (ЕС) № 748/2012, (ЕС) № 965/2012, (ЕС) № 139/2014, (ЕС) № 1321/2014, (ЕС) 2015/340 на Комисията и регламенти за изпълнение (ЕС) 2017/373 и (ЕС) 2021/664 на Комисията.

Съгласно Член 16 от РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2023/203:
Този Регламент влиза в сила на двадесетия ден след публикуването му в Официалното издание на Европейския съюз. Той ще се прилага от **22 февруари 2026 г**.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2022/1645 НА КОМИСИЯТА от 14 юли 2022 година за определяне на правила за прилагането на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета по отношение на изискванията за управление на рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност за организациите, обхванати от регламенти (ЕС) № 748/2012 и (ЕС) № 139/2014 на Комисията, и за изменение на регламенти (ЕС) № 748/2012 и (ЕС) № 139/2014 на Комисията

Съгласно Член 8 от ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) 2022/1645:
Този Регламент влиза в сила на двадесетия ден след публикуването му в Официалното издание на Европейския съюз. Той се прилага от **16 октомври 2025 г**.

Основни части на регламентите:

IS.I/D.OR.100 Обхват
IS.I/D.OR.200 Система за управление на информационната сигурност (ISMS)
IS.I/D.OR.205 Оценка на риска за информационната сигурност
IS.I/D.OR.210 Третиране на риска за информационната сигурност
IS.I/D.OR.215 Схема за вътрешно докладване във връзка с информационната сигурност
IS.I/D.OR.220 Инциденти, свързани с информационната сигурност — откриване, реагиране и възстановяване
IS.I/D.OR.225 Реагиране на констатациите, съобщени от компетентния орган
IS.I/D.OR.230 Схема за външно докладване във връзка с информационната сигурност
IS.I/D.OR.235 Възлагане на дейности по управление на информационната сигурност на подизпълнители
IS.I/D.OR.240 Изисквания към персонала
IS.I/D.OR.245 Водене на документация
IS.I/D.OR.250 Ръководство за управление на информационната сигурност (ISMM)
IS.I/D.OR.255 Промени в системата за управление на информационната сигурност
IS.I/D.OR.260 Постоянно подобряване.

Основни елементи на СУИС (ISMS)

СУИС (ISMS) е създадена по модела на СУБ (SMS) и това означава, че стълбовете на системата за безопасност могат да се използват в СУИС (ISMS). Принципно организацията трябва:

- Да има политика за сигурност и да дефинира обхвата и целите на информационната сигурност.
- Да назначи компетентен персонал за управление на информационната сигурност.

- Да има дефинирани критерии за компетентност на персонала, отговорен за извършване на дейностите по Част-IS.
- Да има дефинирани критерии за установяване на самоличността и надеждността на персонала, който има достъп до информационните системи и данните, за които се прилагат изискванията по Част-IS.
- Да има въведени мерки за откриване, реагиране и възстановяване от инциденти и уязвимости, които показват потенциалното възникване на неприемливи рискове и които може да окажат потенциално въздействие върху авиационната безопасност.
- Да разполага с вътрешни и външни схеми за докладване.
- Да документира всички ключови процеси, процедури, роли и отговорности, необходими за спазване на точка IS.I/D.OR.200 и да установи процес за изменение на тази документация.
- Да идентифицира и управлява рисковете за информационната сигурност.
- Да идентифицира KPI по информационна сигурност.
- Да извършва измерване на KPI по информационната сигурност.
- Да извършва управление на промени, засягащи Част-IS.
- Да наблюдава съответствието на организацията с изискванията на Част-IS и предоставя обратна информация, относно констатации, на отговорния ръководител.
- Да извършва обучение и осведоменост на персонала.

  Организациите може да се позовават на Part-IS TF G-03 *„Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS“* за първоначален вътрешен преглед на съответствие на ISMS.

  Оценката на риска за сигурността трябва да започне от:

- Идентифициране на всички съответни активи (т.е. **хардуер, софтуер, мрежови и изчислителни ресурси**), използвани за създаване, обработка, предаване, съхранение или получаване на оперативните входове и изходи, съответни за **функциите**, **услугите** и **възможностите** на организациите.

- Идентифициране на оперативните среди (например офис, зона за обществен достъп, стая с контрол на достъпа и др.) и местоположения за всички съответни активи. Тъй като организациите вече имат система за управление, настоящата рамка и структура за управление на безопасността могат да се използват за интегриране на СУИС (ISMS) в системите за управление.

  Оценка на ефективността и зрелостта на ISMS може да бъде извършвана, след като се достигне „Оперативно“ ниво.

За всяка засегната организация се изисква:

СУИС (ISMS) да е на ниво „**НАЛИЧНА“** и „**ПОДХОДЯЩА“** към момента на влизане в сила и прилагане на Част-IS и до дата, в която започват да се прилагат изискванията, организацията да извърши дейност по преглед на съответствието.

СУИС (ISMS) да започне да се използва веднага след **датата на приложимост**.

Възлагане на дейности по управление на информационната сигурност на подизпълнители може да спомогне за осигуряване на достъп на организацията до опитен персонал и експертиза. По същия начин организациите може да искат да бъдат подпомогнати от доставчик на услуги при извършване на оценки на риска.

EASA е разработила матрица за оценка на СУИС (ISMS). ГД ГВА приема и представя този инструмент за оценка, като документ - **DG CAA PART-IS COMPLIANCE ASSESSMENT.** Този инструмент трябва да се използва, попълни и изпрати на ГД ГВА като част от пакета документи за внедряване на Част-IS.

6. ДЕРОГАЦИЯ

В случай, че дадена организация има намерения и необходимост от прилагане на дерогация е необходимо да се подаде заявление за дерогация, по образец - формуляр **DG CAA DEROGATION REQUEST** до ГД ГВА за разглеждане. Формулярът трябва да е подписан от Отговорния Ръководител на дадената организация.

Организациите трябва да следват указанията, предоставени в AMC1 IS.I/D.OR.205(a) и AMC1 IS.I/D.OR.205(b), и да извършат документирана оценка на риска за информационната сигурност.

Всяка организация трябва да докаже на ГД ГВА, че нейните дейности, съоръжения и ресурси, както и услугите, които предоставят, получават и поддържат, не представляват рискове за информационната сигурност с потенциално въздействие върху авиационната безопасност нито за себе си, нито за други организации.

Забележка: Има определени разпоредби, които остават в сила и трябва да се спазват, независимо от одобрението на дерогация. Те са:

- Спазване на изискванията за докладване, посочени в точка IS.I/D.OR.230; изискванията на точка IS.I/D.OR.200(a)(13);
- Свързаните изисквания, посочени в точки IS.I/D.OR.205 до IS.I/D.OR.260;
- Свързаното изискване, посочено в точка IS.I/D.OR.240(a)(3), относно основното разбиране на отговорния ръководител за изискванията на Регламент (ЕС) 2023/203 или 2022/1645.

За допълнителни насоки за изискванията за дерогация може да се ползва документ Part-IS TF G-02.

7. ВЪВЕЖДАНЕ НА СУИС (ISMS)

При извършване на оценка на риска съгласно IS.I/D.OR.205(c) трябва да се вземат предвид взаимодействията между рисковете за информационна сигурност и авиационната безопасност.

8. РЪКОВОДСТВО ЗА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ (ISMM)

Ръководството за управление на информационната сигурност (ISMM) може да бъде представено като отделен документ или да бъде интегрирано в описанието на организацията, като същото следва да притежава всички елементи, изброени в IS.I/D.OR.250(a). Когато документите са интегрирани, изброените елементи в IS.I/D.OR.250 (a) трябва да бъдат ясно посочени.

Съдържанието на ISMM е следното:

1) Декларация, подписана от отговорния ръководител, потвърждаваща, че организацията винаги ще работи в съответствие с това приложение и с ISMM. Ако отговорният ръководител не е главен изпълнителен директор (CEO) на организацията, тогава и изпълнителният директор трябва да подпише декларацията;
2) Име, длъжност, задължения, отговорности и правомощия на лицето или лицата, определени в точка IS. I/D.OR.240(b) и (c);
3) Име, длъжност, задължения, отговорности и правомощия на лицето или лицата, определени в точка IS. I/D.OR.240(d).
4) Политика за информационна сигурност на организацията, както е посочено в точка IS. I/D.OR.200(a)(1);
5) Общо описание на броя и категориите персонал, на разположение за извършване на дейностите, според изискванията на точка IS. I/D.OR.240;
6) Име, длъжност, задължения, отговорности и правомощия на ключовите лица, отговорни за изпълнението на точка IS. I/D.OR.200, включително лицето или лицата, отговорни за функцията за наблюдение на съответствието, посочена в точка IS. I/D.OR.200(a)(12);
7) Организационна структурна схема, показваща връзките на докладване и комуникация на ръководния персонал посочен в точки (2) и (6);
8) Описание на вътрешната схема за докладване, посочена в точка IS. I/D.OR.215;
9) Процедурите, които определят как организацията гарантира спазването на Част-IS, и по-специално:

- Документирането на всички ключови процеси, процедури, роли и отговорности в съответствие с точка IS.I/D.OR.200(c);
- Процедурите, които определят как организацията контролира всякакви договорени дейности, посочени в точка IS. I/D.OR.200(a)(9);
- Процедурата за изменение на ISMM;
- Подробности за приложимите одобрени алтернативни начини на съответствие.

IS.I/D.OR AMC/GM включва инструкции за съдържанието на ISMM и допълнителни указания. Указания се съдържат също в документ Part-IS TF G-03.

9. ПЕРСОНАЛ

Отговорният ръководител **назначава** лице или група лица (**appoint** a person or group of persons) с отговорността да гарантира(т) спазването на Част-IS.
Отговорния ръководител може също да делегира отговорността си по отношение регулациите на Част-IS на **общо отговорно лице (Common Responsible Person)**. Това трябва да се прецени и съобрази, в случай, че дадената организация притежава повече от едно одобрение, има обширни договори и / или отношения с мултинационални организации. В такива случаи е важно да се установят методи за координация между отговорния ръководител на организацията и общото отговорно лице, за да се осигури адекватна интеграция на управлението на информационната сигурност в организацията.

Назначеният персонал трябва да притежава необходимата компетентност и да бъде надежден, като в тази връзка Част-IS AMC/GM, включва указания за оценка на компетентността и надеждността на персонала, които следва да бъдат ясно дефинирани и документирани в ISMM.

10. КОМПЕТЕНТНОСТ НА ПЕРСОНАЛА

За разработване на **списъка с компетенции**, организацията може да използва насоките в IS.I/D.OR AMC/GM, Appendix VI.
В IS.I/D.OR AMC/GM, Appendix II основните роли по Част-IS са изброени и съпоставени с компетенциите, произтичащи от NIST CSF. Това съпоставяне може да се използва като база за идентифициране на пропуските в компетенциите. Въпреки това, трябва да се отбележи, че съществуващите рамки за компетентност в областта на киберсигурността/информационната сигурност обикновено се фокусират основно върху защитата на стандартните информационни технологии, поради което предложеният списък с компетенции може да се наложи да бъде адаптиран към технологиите или интегриран с процесите, използвани в организацията.

11. ВЪЗЛАГАНЕ НА ДЕЙНОСТИ ПО УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА ПОДИЗПЪЛНИТЕЛИ.

Според IS.I/D.OR.235 дейности по управление на информационната сигурност могат да бъдат възложени на подизпълнители. В такъв случай организацията трябва да формализира това чрез писмено подписано споразумение с подизпълнителя.

GM3 IS.I/D.OR.235 дава примери за дейности по управление на информационната сигурност, които могат да бъдат възложени.

При възлагане на дейности по управление на информационната сигурност организацията трябва предварително да оцени подизпълнителя (компетентност, способности, персонал и др.), да управлява свързаните рискове за сигурността и да включи подизпълнителя в плана за преглед на съответствието на организацията.

12. ПОДАВАНЕ НА ДОКУМЕНТИ

Документите за въвеждане на изискванията на Part-IS трябва да бъдат подадени в ГД ГВА преди **22 февруари 2026 г. за всички организации, засегнати от Регламент за изпълнение (ЕС) 2023/203.**

Организациите трябва да предоставят следното:

1) Първата версия на Ръководство за управление на информационната сигурност (ISMM), което може да бъде интегрирано с други ръководства или описания, вече установени и прилагани от организацията.
2) Процедурата, описана в Част-IS, точки IS.I/D.OR.255 „Промени в системата за управление на информационната сигурност“. Тази процедура може да бъде част от ISMM или интегрирана в съществуваща процедура за промяна (напр. съгласно ORO.GEN.130 или подобни изисквания в други домейни).
3) Първоначална оценка на риска, идентифицираща:

   а) Дейностите, съоръженията и ресурсите на организацията, както и услугите, които организацията управлява, предоставя, получава или поддържа.

   б) Оборудването, системите, данните и информацията, които допринасят за функционирането на елементите, изброени в точка (а) по-горе.

   в) Интерфейсите, които тя има с други организации и които биха могли да доведат до взаимно излагане на рискове за информационната сигурност.

   г) Основните рискове и свързаните с тях сценарии на заплахи, както вътрешни, така и на интерфейсите с други организации.
4) Доказателства, че са извършени вътрешни дейности по наблюдение на съответствието, описващи нивото на съответствие с всички критерии, посочени в колона „Elements to be assessed for “Present” and “Suitable” levels (including readiness to start operating the ISMS)“

от документ **DG CAA PART-IS COMPLIANCE ASSESSMENT**, като се идентифицират всички елементи. Където нивото „Налично“ и „Подходящо“ не е достигнато, се представя и план за коригиращи действия.

*Към момента на влизане в сила на Регламент (ЕС) 2023/203 съществува вероятност организациите да не могат да представят пълна / всеобхватна оценка на риска за сигурността на своята СУИС (ISMS), но се очаква като минимум **основните** рискове за сигурност да бъдат идентифицирани и да се извърши първоначална оценка на риска.
За допълнителни указания може да се ползва документ Part-IS TF G-03.

Приложения:

1. DG CAA PART-IS COMPLIANCE ASSESSMENT
2. DG CAA DEROGATION REQUEST

Източници:
https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables