

Sjöfartstillsyn - ISPS (2026)

SKYDDSÖVNING (*drill*) OCH OMFATTANDE ÖVNINGSHELHET (*exercise*)

Medlemsstaten/flaggstaten ska säkerställa (övervaka/kontrollera) att skyddsövningar (*drills*) och mer omfattande övningshelheter (*exercises*) genomförs ombord på fartyg, eftersom förordning (EG) nr 725/2004 gör ISPS-kodens krav obligatoriska för fartyg som omfattas av tillämpningsområdet, och medlemsstaterna övervakar efterlevnaden både som flaggstat och som hamnstat.

Dessutom bör medlemsstaterna/flaggstaterna säkerställa (vid övervakning/inspektion eller dokumentgranskning) att skillnaden mellan skyddsövningar och övningshelheter samt deras syften förstås och genomförs korrekt.

Skyddsövningar och övningshelheter är obligatoriska krav som gäller fartyg i enlighet med ISPS-koden (sådan den blir tillämplig genom förordning (EG) 725/2004).

Fartyg ska genomföra:

Skyddsövningar (*drills*) minst var tredje månad (samt dessutom en extra övning inom en vecka, om mer än 25 % av besättningen byts ut och bytet omfattar personer som inte har deltagit i en övning under de senaste tre månaderna).

En övningshelhet (*exercise*) minst en gång per kalenderår, så att intervallet mellan övningshelheterna är högst 18 månader.

Skyddsövning / Operativ övning (*Drill*)

Syfte: säkerställa att fartygets personal behärskar sina egna skyddsuppgifter och att fartygsskyddsplanens (SSP) förfaranden fungerar i praktiken.

Karaktär: operativ, praktisk prestation - ett enskilt förfarande, en uppgift eller en rutin övas och testas (inte hela systemet).

Form: en mindre, för besättningen avsedd och praktiskt inriktad övning där ett visst förfarande, en viss uppgift eller en viss rutin testas och övas (t.ex. kontrollåtgärder, bagagekontroll, användning av skyddsutrustning). Dessutom ska en skyddsövning testa enskilda delar/element i fartygsskyddsplanen (t.ex. vissa hotscenarier).

Mer omfattande övningshelhet / systemövning (*Exercise*)

Syfte: att testa en större helhet av skyddssystemet/-arrangemangen: kommunikation, samordning, tillgång till resurser och respons.

Karaktär: mer omfattande än en skyddsövning; ofta deltar även andra aktörer (t.ex. rederiets skyddschef (CSO), rederiets informationssäkerhetschef (CISO), skyddschefen för hamnanläggningen (PFSO), myndigheter, ibland även andra fartyg/organisationer).

Form: kan vara en praktisk (fullskalig) övning, en skrivbordsövning (seminarie-/simuleringsövning) eller kombinerad med andra övningar (t.ex. SAR- eller olika beredskapsövningar, inklusive cyber-/hybriddimensioner såsom organiserad brottslighet).

MINIMIINNEHÅLL I EN ISPS-ÖVNINGSRAPPORT ENLIGT EU-KRAVEN

Använd dessa som minimikrav vid dokumentation av varje ISPS-övning som genomförs ombord:

Fartygets identifikationsuppgifter

- fartygets namn
- IMO-nummer

Övningens identifikationsuppgifter

- datum
- start- och sluttid
- fartygets position / hamn / terminal
- skyddsnivå
- typ av övning eller scenario

Grund / utgångspunkt för övningen

- planerlig kvartalsvis övning, omfattande övningshelhet (årlig) eller
- övning efter besättningsbyte (>25 %), eller
- övning med anknytning till ett visst förhöjt skyddshot (inkl. cyber-/hybriddimensioner såsom organiserad brottslighet).

Mål

- vilket delområde i fartygsskyddsplanen (SSP) testades (*drill*)
- vilka skyddssystem/-arrangemangen: kommunikation, samordning, resurser och responser testades (*exercise*).

Exempel: tillträdeskontroll, skydd av begränsade områden, sökförfaranden, reaktion på misstänkt paket, obehörig ombordstigning, kommunikation, åtgärder av fartygets skyddschef (SSO). Alternativt en beredskapsövning, inklusive cyber-/hybriddimensioner såsom organiserad brottslighet.

Sammanfattning av scenariot

- kort beskrivning av övningen / den simulerade händelsen

Deltagare

- befälhavaren, fartygets skyddschef (SSO), vakthavande personal / övrig personal och sökgrupp
- eventuellt deltagande från landsidan (rederiets skyddschef (CSO), rederiets informationssäkerhetschef (CISO), skyddschefen för hamnanläggningen/terminalen (PFSO), myndigheter (inkl. cybersäkerhetscentret) om de har deltagit.

Vidtagna åtgärder

- besättningens/deltagarnas åtgärder, fas för fas
- genomförd kommunikation (intern/extern)
- tillträdeskontroll (inkl. digitalt intrång) eller sökåtgärder
- eventuella testade larm- / anmälnings- / rapporteringsskeden.

Testad utrustning / testade system

- radioapparater / telefoner / intern kommunikation (PA)
- datorsystem
- tillträdeskontrollarrangemang
- belysning / CCTV / lås / säkerhetsbarriärer, i tillämpliga fall
- annan skyddsutrustning som användes i övningen

Resultat / utvärdering

- uppnåddes övningens mål
- observerade brister
- feedback från dem som deltagit i övningen
- feedback från myndigheten(-r), om den har deltagit i övningen
- förseningar, missförstånd, utrustningsfel eller brister i fartygsskyddsplanen (SSP).

Korrigerande åtgärder

- vad som ska korrigeras
- vem som ansvarar
- måldatum / datum för slutförande

Anteckning om debriefing

- tidpunkt för debriefingen
- deltagande personer
- viktigaste lärdomarna

Godkännande / underskrift

- skyddschefens (SSO) underskrift
- befälhavarens godkännande, om rederiets förfarande förutsätter det
- distributions- / arkiveringsplats (skyddsmapp och/eller elektroniskt system)
- anteckning i skeppsdagboken.

MYNDIGHETENS DOKUMENTGRANSKNING

Transport- och kommunikationsverket Traficom kan genom att granska fartygens årliga planer för ISPS-övningar samt rapporter om skyddsövningar och övningshelheter säkerställa att ISPS-övningarna och rapporteringen (dokumentationen) uppfyller kraven i Europaparlamentets och rådets förordning (EG) nr 725/2004 (inkl. Bilagor).