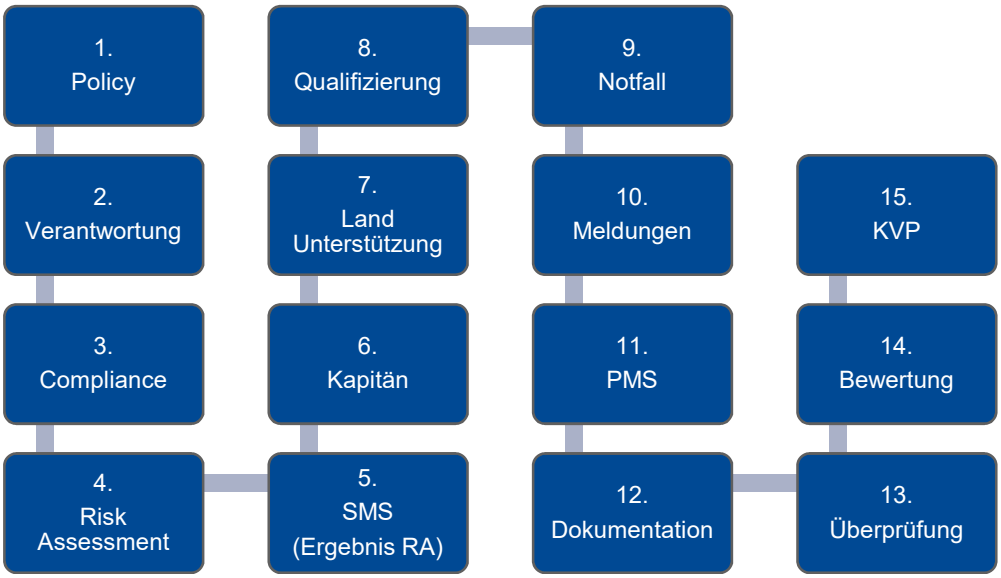
ISM
Cyber Security

DEUTSCHE FLAGGE

Berufsgenossenschaft Verkehrswirtschaft Post-Logistik
Telekommunikation
Dienststelle Schiffssicherheit

ISM Cyber Security Process



Der ISM Code regelt erforderliche Maßnahmen für die Organisation eines sicheren Schiffsbetriebs. Durch den modulartigen Aufbau des Codes können die durch Cyber Crime notwendig gewordenen Sicherheitsmaßnahmen in das bestehende Sicherheitsmanagementsystem (SMS) der Reederei integriert werden.

Dieses integrierte Managementsystem entspricht den Anforderungen der IMO Resolution MSC.428(98). Es wird der IMO *GUIDELINE ON MARITIME CYBER RISK MANAGEMENT* (MSC-FAL.1/Circ.3) gerecht und vermeidet den Aufbau eines eigenständigen, konkurrierenden Systems, welches zu einer weiteren administrativen und finanziellen Belastung auf See und in den Reedereien führen kann.

Die Integration erlaubt es dem Reeder, sein bestehendes System um die für ihn notwendigen, spezifischen Belange des Cyber Risk Managements zu erweitern und damit die Akzeptanz der Umsetzung hoch zu halten.

Cyber Risk Management

Zunehmende Interaktivität, der steigende Vernetzungsgrad und das zunehmende Verschwinden von Netzgrenzen an Bord trifft auf ein zunehmend höheres Potential krimineller Cyberaktivitäten und auf immer kürzer werdende Angriffszyklen. Schiffe können zu einem direkten und damit von außen gelenkten Angriffsziel werden. Gleichwohl können sie versehentlich durch ein Besatzungsmitglied geschädigt werden, wenn dieses eine nicht speziell für das Schiff vorhergesehene Schadsoftware über einen eMail Anhang oder USB Stick in ein vernetztes System einbringt. In einem ungeschützt vernetzten System könnten damit Angehörige theoretisch all das zum Ausfall bringen, was über eine Software gesteuert wird – vom Radar bis zum Maschinensensor. Darüber hinaus können in Krisengebieten die GNSS Signale (z.B. GPS) in einer Weise gestört werden, dass sie an Bord nicht mehr genutzt werden können – oder spontan die Position um Meilen versetzen. Bleibt das Schiff ungeschützt, kann die Gefahr exponentiell zunehmen. Diese und andere konkrete und weniger konkrete Gefahren machen es erforderlich, den sicheren Schiffsbetrieb mit einem individuellen Cyber Risk Management zu unterstützen.

1. Policy

Die Geschäftsführung der Reederei erkennt die grundsätzlichen Risiken für den sicheren Schiffsbetrieb durch Cyber Crime und die Notwendigkeit zur Regelung und damit Erweiterung der Managementziele. Die bestehende Policy wird um Cyber Security und der Beschreibung der dafür grundlegenden Maßnahmen erweitert. Cyber Security ist ein unmittelbares Anliegen der Geschäftsführung.

2. Verantwortung

Die ultimative Verantwortung im Bereich Cyber Security bleibt bei der Unternehmensleitung. Soweit die Organisation und ihre Größe es zulässt, wird eine geeignete Person – üblicherweise der Leiter der Unternehmens-IT – benannt als zuständige oder verantwortliche Person zum Schutz vor Cyber Security und zur Unterstützung von Kapitän, Besatzung und DPA. Darüber hinaus werden im SMS alle Personen erfasst, denen Aufgaben und Verantwortlichkeiten im Bereich Cyber Security zugewiesen werden.

3. Compliance

Regelwerke und Empfehlungen der IMO, des Flaggenstaates, Klasse und der entsprechenden Industrie werden identifiziert und die grundlegenden Anforderungen abgeleitet. Sie bilden eine Basis für die Erstellung und Fortschreibung des Risk Assessments (RA) und SMS. Rechtskataster werden entsprechend erweitert oder neu erstellt und listen die Vorgaben und Empfehlungen auf.

4. Risk Assessment

Über das ISM RA werden die Risiken und die erforderlichen Gegenmaßnahmen festgestellt. Sofern kein gleichwertiges System besteht, kann der folgende Ansatz für eine systematische Beurteilung dienen:

1. Vorbereitung:	1. HAZID	Hazard Identification
	2. RESID	Ressource Identification
	3. TOP	Mögliche Sicherheits-maßnahmen.
2. Durchführung:	Anhand der Vorbereitung: Risiken bewerten, Sicherheitsmaßnahmen und Verantwortlichkeiten festlegen.	

5. SMS (Ergebnis RA)

Die Ergebnisse des Risk Assessments - und damit die notwendigen Sicherheitsmaßnahmen - finden ihren Ausdruck im SMS der Reederei. Sie werden als Prozess, Reedereianweisung oder in anderer geeigneter Art aufgenommen. Grundsätzlich sollen damit die erforderlichen Maßnahmen der Besatzung bekannt gemacht werden. Wird über das RA festgestellt, dass bestimmte Maßnahmen nicht frei zugänglich gemacht werden sollen, können diese im SSP aufgeführt werden.

ISM Ziel

Das oberste Ziel aller zu treffenden Maßnahmen ist die Gewährleistung eines sicheren Schiffsbetriebs und des Meeresumweltschutzes in allen situationsbedingten Lagen.

Management & Stellenwert

Rückfragen beim P&I und Kasko-versicherer können Einfluss auf die Betrachtung des Stellenwerts und damit den Umfang der Maßnahmen nehmen, insbesondere bei der Betrachtung finanzieller Risiken.

Cyber Risk Management

Die Maßnahmen müssen der Organisationsgröße gerecht werden. Der Anspruch der kontinuierlichen Verbesserung sollte immer höher wiegen als der Versuch der einmaligen und oft nicht alles abdeckenden Regelung.

Compliance

IMO Resolution MSC.428(98)
IMO Guidelines MSC-FAL/Circ.3
ISM Circular 04/2017
The Guidelines on Cyber Security on-board Ships (BIMCO, ICS Guide)

Weitere nützliche Informationen zum Thema Cyber-Sicherheit sind unter www.bsi.bund.de zu finden.

IPDRR Check

Decken die ISM Maßnahmen die folgenden Maßnahmen ab?

Identify	Identifizieren von Gefahren / Anlagen.
Protect	Schutz vor einem Angriff.
Detect	Identifizieren eines Angriffs.
Respond	Reagieren auf einen Angriff.
Restore	Wiederherstellen nach einem Angriff

HAZID

Hazard Identification

Liste ohne Wertung & Risiko erstellen mit allen potentiellen Gefährdungen und potentiell gefährdeten Anlagen - ÜBERSICHT GEWINNEN

IT	IF	OT	ACP
Informations-technologien und Netzwerke	**Interface - Schnittstellen zwischen IT & OT**	**Systemanlagen Operational-PC´s**	**Access Points**
Office-PC´s		GNSS	USB
EMAIL & Internet		AIS	LAN
IP Telefon		RADAR & ECDIS	WLAN
SAT-Telefon		Maschinensteuerung	BT
Wetter PC		System- und Ventilsteuerung	DVD/CD ROM
PMS Server		Sensoren	Andere mobile Speicher & Geräte
WLAN / LAN (Ladungs-PC)		Ruderanlage	…
…		Alarm & Überwachung	Konkrete Darstellung: an welchen Anlage?

HAZID

Auflistung aller potentiellen Gefahren und potentiell gefährdeten Anlagen als nicht abschließende und weiter fortzuschreibende Liste. Sie dient als Grundlage für das Risk Assessment.

Wird sie im Team diverser Beteiligter (Kapitäne, Ltd. Ing., DPA, QM, Inspektoren, CSO, IT Personal / Experten, Management u.a.) erstellt und im Vorwege in die vier Bereiche IT, IF, OT und ACP unterteilt, kann sie ein umfassendes Gefahrenbild darstellen.

RESID

Ressource Identification

Kompetenzliste erstellen und bewerten: potentiell eigene oder externe Ressourcen ?

IT	IF	OT	ACP
Kompetenzen: Eigene? Dienstleister?	Kompetenzen: Eigene? Dienstleister?	Kompetenzen: Eigene? Dienstleister?	Kompetenzen: Eigene? Dienstleister?
Auflistung: Hersteller und möglichen Servicepartner.		Auflistung: Hersteller und möglichen Servicepartner.	

EXTERNE

Hersteller und Dienstleister müssen einbezogen werden, wenn eigene Ressourcen nicht ausreichen – dies kann insbesondere bei OT und IF Schutz notwendig werden. Wo welche Ressource notwendig wird, kann anhand der RESID Liste erkannt werden.

T Technische Maßnahmen

Beispiel möglicher Maßnahmen

Firewall	Remote access control: Authentisierung von Zugänge (RAS,VPN)	Crew Internet email: Stand alone Lösungen statt Kammernetzwerk (physische Trennung vom Netzwerk)
Virenschutzprogramme	Verplombung Zugänge Geräte (USB,LAN), (Sealmanagement)	Logfiles für IT Experten (Nachverfolgung, Aufarbeitung)
Spam-Filter	BUS Management	Meidung einfacher Cloud-Dienste (Reederei), sonst eigene Dienste
Firewall & Virenschutz & Spam-Filter auf allen relevanten PCs	Netzwerke: mehrfache Segmentierung (Operation/Master/Crew/…), insbesondere WLAN Netze (nach neuestem Standard gesichert)	Aktivierung automatischer Updates / Patches: - Software allgemein - MS Office - OT Systems - IT System - Antivirenprogramme
USB Sperre (Massenspeichermedien)	Stand alone Lösungen statt Netzwerk (z.B. Ladungs-PC)	Unnötige Software Funktionen & Plug-ins entfernt / gesperrt
Backup Storage (externe Lösung)	Quarantäne PC (für Virenüberprüfung)	Serverstandort: restricted area
Sperrung bestimmter EMAIL Anhänge (z.B. Crew: nur jpg,txt,pdf) .exe, .cpl, .bat, .com, .scr, .vbs, .vba	Software: Zugangsdifferenzierung – unterschiedliche Level. Nur der bekommt Rechte, der sie braucht (Software, Laufwerke)	
Limitierung von EMAIL Anhängen (Account abhängig)		
Konfigurationsmanagement		
Trennung von internen und externen Systemen		
VPN		

TOP Maßnahmen:

Auflistung aller potentiellen Sicherheitsmaßnahmen als nicht abschließende und weiter fortzuschreibende Liste. Sie dient als Grundlage für das Risk Assessment. Eine Möglichkeit der Erstellung: "Brain Storming" mit IT, DPA, QM / QHSE, Nautische & Technische Abteilung, Geschäftsführung.

Datenschutz

Cyber Security schließt Maßnahmen des Daten-schutzes ein.

O Organisatorische Maßnahmen

Beispiel möglicher Maßnahmen

Policy der Unternehmensleitung (Ultimative Verantwortung)

Passwort-Policy

Passwortmanagement

Dynamische (regelmäßige) Passwortänderung

Vergabe der Zugriffsrechte (unterschiedliche Level)

Eindeutige Verantwortlichkeit Land

Benennung IT Experte

Verantwortlichkeit See

Zuständigkeiten Land/See

Zuständigkeit Dritter

Service an Bord (Autorisierung, Work Permit)

Backup Organisation (regelmäßig)

Audit

IT Überprüfungen (durch interne oder externe Sicherheitsfirmen)

PMS – regular IT checks

PMS – Software Update

Administratoren bekommen nur die Rechte, die sie brauchen

Manuelle Updates (PMS), bei zeit-/systemkritischen Patches:

- für Stand-alone Einheiten
- IT/OT ohne auto-update
- Antivirus Software
- …

Bildschirmsperre (automatisch nach x Minuten / manuell bei Verlassen des Arbeitsplatzes)

Office support:

- Notfallplan Office
- Hotline / Kontakt

Notfall Wiederherstellungsplan

PMS Backup (Erhalt der Historie)

OT Zugangsberechtigung, Systembeschränkung, Work Permit für Service

Expertenrat, wenn die eigene Organisation/IT überfordert ist (Notfallkontakt)

Überwachungsmaßnahmen (Monitoring / Erkennen)

Kontrolle: terrestrische Navigation (Kontrolle GNSS, ECDIS)

Navigation: Redundanz, Backup Astronomische Navigation

Backup Seekarten für bestimmte / sensible Bereiche

ARPA und Auswertung, Datenfehler Geschwindigkeit (ARPA: RADAR Daten statt AIS. Speed: LOG statt GPS)

Fortlaufende Schwachstellenanalyse und Auswertung des Meldewesens

Sicherstellen: alle PC´s einer Reederei sind betroffen und müssen geschützt sein und überprüft werden, insbesondere Notebooks

Meidung Inselwissen (Administrator, externer Dienstleister, bei Wechsel kann Wissen verloren gehen).

Administrator Dokumentation vorhalten (knowledge base)

Informieren (Schiff, Beschäftigte)

P Persönliche Maßnahmen

Beispiel möglicher Maßnahmen

Erstunterweisung

Wiederkehrende Unterweisung

Anlassbezogene Unterweisung

Schulung an Land

Schulungsschwerpunkt Navigation: Erkennen von Manipulation GNSS, AIS

Awareness Programme

Unterlassungserklärung zur Manipulation / Einwahl in Netzwerke (Crewhacking, Vertrag, Vertragsergänzung)

Disziplinarische Maßnahmen bei bewusster/unbewusster Missachtung der Vorgaben

Zeitnahe Informationsweitergabe an Mitarbeiter (aktives Kommunizieren)

Training nach Bedarf (Administrator, Beschäftigte)

Trainingsinhalte: Verhalten, Monitoring, Erkennen, Sofortmaßnahmen, Passwortmanagement

Poster & Informationsmaterial

RA

Risk Assessment

Risiko = Eintrittswahrscheinlichkeit x Schadensschwere

Risk Assessment

Durchführung des RA zum Erkennen und Bewerten von Risiken. Risikoeinschätzung: *Eintrittswahrscheinlichkeit x Schadensschwere.*

Wird ein Risiko erkennbar, werden geeignete Sicherheitsmaßnahmen mit einer bestimmten Hierarchie eingeleitet. Diese richtet sich ähnlich dem Arbeitsschutz nach dem TOP-Prinzip:

(T) Technisch,
(O) Organisatorisch,
(P) Personenbezogen.

Damit abgedeckt: Technik, Prozesse, Mensch.

Technische Maßnahmen haben Priorität.

Beispiel EMAIL Verkehr:

Verhaltensbezogene persönliche Maßnahme (P): Anweisung an Crew "keine email Anhänge mit .exe oder .mpg öffnen".

Technische Maßnahme (T): Es werden keine .exe Anhänge zugelassen, ein Filter ermöglicht nur das Empfangen von .JPG, .PDF.

Die verhaltensbezogene Maßnahme ist die schneller umzusetzende und zudem die günstigere. Sie kann aber nicht gesichert werden. Dies ist nur über die technische Maßnahme möglich.

Das RA muss aufgrund der schnellen Entwicklung neuer Risiken ständig überprüft und fortgeschrieben werden.

6. Kapitän

Im ISM werden Qualifizierungsmaßnahmen für den Kapitän aufgeführt, damit dieser die an ihn gestellten SMS Anforderungen erfüllen kann. Die Organisation durch den Reeder berücksichtigt, dass neue Cyber Security Aufgaben nicht ausschließlich in die Verantwortung des Kapitäns gelegt werden.

7. Land Unterstützung

Durch geeignete Organisation steht dem Kapitän qualifizierte landseitige Unterstützung zur Erfüllung seiner SMS Aufgaben zur Verfügung. Diese schließt ein
- Reagieren auf einen Cyber Angriff.
- Reagieren auf die Folgen eines Angriffs.
- Wiederherstellen (Backup Restore).

8. Qualifizierung

Schiffsbesatzungen und landseitiges Officepersonal werden bei Dienstantritt in die SMS Cyber Security Maßnahmen des Unternehmens unterwiesen. Dieses erfolgt zusätzlich bei einer Veränderung der Tätigkeitfelder bzw. bei einer Beförderung.

Die Unterweisung wird notwendig für alle Personen mit Aufgaben im Bereich Cyber Security und für alle Personen, die im Kontakt mit einem Schiff stehen.

Unterweisungs- und weitere Trainingsmaßnahmen sind regelmäßig wiederkehrend und bei Bedarf zu wiederholen. Das SMS enthält einen Trainings- und Qualifizierungsplan und beschreibt Maßnahmen, um Trainingsbedarf festzustellen. Dieses schließt Land und See ein. Der Umfang richtet sich nach der Position an Bord / im Unternehmen – nicht Jeder muss alles wissen.

9. Notfall

Das SMS enthält einen Notfallplan "Cyber Security" für den Bereich See und Land. Der Notfallplan "Cyber Security" wird regelmäßig durch Übungen, Simulationen und Schulungen eingeübt. Ziel: reflektierendes Handeln. Die Landorganisation hält Notfallpläne zur Unterstützung des Kapitäns vor.
Diese schließen ein
- Reagieren auf: Cyber Angriff und Folgen.
- Wiederherstellen (Backup Restore).

Erforderlich (falls vorhanden) im Notfallteam der Reederei: IT Fachleute.

10. Meldungen

Vorfälle, Unfälle, Beinaheunfälle und sonstige relevante Vorkommnisse werden über das ISM Meldewesen an die zuständigen Bereiche gemeldet, dort untersucht und analysiert. Als Folge werden korrigierende und präventive Maßnahmen festgelegt und kommuniziert. Ziel: kontinuierliche Verbesserung.

Risiko

Navigation

Kapitäne und nautische Offiziere müssen geschult werden um Gefahren zu kennen, zu erkennen und um auf diese reagieren zu können. Neben allgemeinen Navigationsanweisungen und Qualifizierungsmaßnahmen sind die vorhandenen ISM Notfallpläne bei Bedarf zu ergänzen.

Gefährdungen können sich z.B. ergeben durch:
- Ausfall oder Manipulation der GPS und DGPS Daten (Störsender).
- Ausfall oder Manipulation der AIS Daten.
- Fehlerhafte Geschwindigkeitseingabe führt zur fehlerhaften ARPA Auswertung.
- Fehlerhafte ECDIS Angaben.
- Ausfall (Absturz) und Reboot-Fehler der Radaranlagen.
- Ausfall Echolot und andere softwarebasierte und oder integrierte Navigationssysteme.
- Beeinflussung der Steuerung und Überwachung der Maschinenanlage inkl. Energieerzeugung.

Mensch

Mangelndes Bewusstsein, fehlende oder nicht fortlaufende Unterweisung und Fortbildung für See- und Landpersonal erhöhen die Wahrscheinlichkeit von Fehlverhalten.

IT Reduzierung

Das RA und das SMS dürfen sich nicht auf IT reduzieren. OT, Schnittstellen und Zugänge zu IT/OT müssen einbezogen werden.

Nachhaltigkeit

RA und SMS müssen fortlaufend überprüft und angepasst werden, um auf die sich ständig ändernden Cyber Gefahren zu reagieren. Einmaliges Integrieren in das SMS ist unzureichend.

Risiko Ship-Shore-Connections

Verbindungen nach "draußen" können ungeschützt zum Einfallstor werden.

Risiko Containerladung

Richtigkeit von Containerangaben (Gewicht, Gefahrgut, Staupositionen) ist primär die Aufgabe vom Terminal und Charterer und sind ein wichtiger Baustein bei der sicheren Beförderung von Ladung. RA und SMS sollen daher auch Bezug nehmen auf den elektronischen Datenaustausch zwischen Land und Schiff hinsichtlich der Stauplanung.

11. PMS

PMS (Planned Maintenance System): die über das Risk Assessment festgestellten erforderlichen Sicherheitsmaßnahmen, die regelmäßig wiederkehrend eingesetzt werden, z.B. Software updates, werden in das PMS aufgenommen. Damit erfolgt die Überwachung und Dokumentation der Maßnahmen.

Der Bereich Critical Equipment wird erweitert. Notwendigkeit und Details werden über das RA festgestellt.

12. Dokumentation

Das SMS beschreibt die Anforderungen an die Dokumentation, diese werden für den Bereich Cyber Security übernommen.

Befinden sich dokumentierte Maßnahmen und Anforderungen in einem Sensibilitätsbereich, der eine öffentliche Dokumentation im SMS nicht zulässt, sind spezifische Maßnahmen umzusetzen, die nur einem beschränkten Personenkreis an Bord und an Land zugänglich sind. Beispiele: Darstellung der Administratorrechte an Bord, detailliertes Passwortmanagement, Backup- und Wiederherstellungsmanagement.

13. Überprüfung

Interne Audits an Bord und an Land werden um die festgestellten Cyber Security Maßnahmen erweitert und in Intervallen von nicht mehr als 12 Monaten durchgeführt.
Durch die internen und externen Audits wird die Integration und Fortschreibug des Cyber Security Managements in das ISM System überwacht.

14. Bewertung

Regelmäßig wiederkehrend findet die Bewertung des Sicherheitsmanagements statt mit den Fragestellungen:
Arbeitet die Organisation (See & Land) entsprechend den SMS Vorgaben?
Sind die Maßnahmen des SMS effektiv?
Interne Auditoren sind ausreichend qualifiziert im Bereich Cyber Security?
Auditergebnisse sind – soweit vertretbar- bekannt gemacht?
Notwendige korrigierende und präventive Maßnahmen sind zeitnah eingeleitet / umgesetzt?

15. KVP

Cyber Security ist starken Veränderungen unterworfen. Daher ist ein einmaliges Einführen von Sicherheitsmaßnahmen unzureichend. Die Reederei muss den ständigen Veränderungen und den im eigenen System erkannten Schwachstellen Rechnung tragen und eine Fortschreibung des Risk Assessments Systems und SMS sicherstellen und damit den kontinuierlichen Verbesserungsprozess einleiten.

ISM Check

Risk Assessment **ISM 1.2**
Gefahren sind identifiziert (HAZID Liste)?
Risiko beurteilt?
Maßnahmen zur Risikoreduzierung?

Compliance **ISM 1.2**
Internationale und nationale Regeln und Richtlinien vorhanden und berücksichtigt?

Policy **ISM 2.1**
Beschreibung der grundlegenden Maßnahmen zur Zielerreichung vorhanden?

Verantwortung **ISM 3.2**
Verantwortliche Personen identifiziert und Aufgaben zugewiesen?

Kapitän **ISM 6.1, 6.2**
Qualifizierungsmaßnahmen für den Kapitän?
Qualifizierte landseitige Unterstützung?

Unterweisung **ISM 6.3**
Bei Dienstantritt und regelmäßig wiederkehrend?
Für See- und Landpersonal?
Fortlaufende Qualifizierungsmaßnahmen?

Qualifizierungsplan **ISM 6.5**
Bedarfsanforderung & Trainingsinhalte?

SMS Anweisungen **ISM 6.5**
RA Ergebnis? Qualifizierte Anweisungen?

Notfall **ISM 8.1, 8.2**
Notfallplan für See und Land?
Regelmäßige Übung anhand des Plans?
Landseitige Unterstützung? (Notfallteam)

Meldewesen **ISM 9.1, 9.2, 9.3**
Meldung: Vorfälle, Unfälle, Beinaheunfälle?
Meldungen werden untersucht und analysiert?
Korrigierende und präventive Maßnahmen?

Maintenance **ISM 10.1, 10.2, 10.3**
Maßnahmen im PMS integriert & dokumentiert?
Critical Equipment – überprüft?

Dokumentation **ISM 11**
Anforderungen beschrieben für allgemeine und für sensible Dokumentation mit limitiertem Zugang?

Überprüfung **ISM 12.1**
Interne Audits um Aspekt Cyber Security erweitert?

Bewertung **ISM 12.2 – 12.7**
Arbeitet die Organisation gemäß SMS?
SMS Maßnahmen effektiv?
Auditoren qualifiziert? Auditergebnisse bekannt?
Korrigierend und präventive Maßnahmen?

Check sensibler Bereiche

Administratorrechte an Bord?
Passwortmanagement?
Backup und Wiederherstellungsmanagement?