ISM
Cyber Security

DEUTSCHE FLAGGE

Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation
Dienststelle Schiffssicherheit

BSH - Bundesamt für Seeschifffahrt und Hydrographie

Mitherausgeber:

Bundesamt
für Sicherheit in der
Informationstechnik

Hamburg, August 2020

Impressum

Herausgeber:
Deutsche Flagge

Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation
Dienststelle Schiffssicherheit
Brandstwiete 1
20457 Hamburg
Internet: https://www.deutsche-flagge.de

Bundesamt für Seeschifffahrt und Hydrographie
Postfach 30 12 20
20359 Hamburg
Internet: https://www.deutsche-flagge.de

Mitherausgeber:
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Inhaltsangabe

Hamburg, August 2020

Einleitung

Zunehmende Digitalisierung, verstärkte Interaktivität, steigender Vernetzungsgrad und zunehmendes Verschwinden von Netzgrenzen an Bord von Schiffen bieten vermehrt Möglichkeiten für Bedrohungen durch interne und externe Cyber-Risiken.

In ein vernetztes und ungeschütztes IT/OT-System können Dritte, aber auch Besatzungsmitglieder, bewusst oder unbewusst Schadsoftware einbringen. Technische Ausfälle und eine damit einhergehende Gefährdung des Schiffsbetriebs wären eine mögliche Folge.

In Krisengebieten können GNSS Signale (z.B. GPS) in einer Weise gestört werden, dass sie unbrauchbar werden.

Bleibt das Schiff ungeschützt, kann die Gefahr exponentiell zunehmen.

Es ist notwendig, den Schiffsbetrieb mit individuellen Maßnahmen und einem Cyberrisikomanagement (CRM) zu unterstützen.

Die im vorliegenden Dokument aufgeführten Informationen bauen auf dem Rundschreiben 04/2018 (ISM) auf, haben einen empfehlenden Charakter und beschreiben Ansätze zur Erstellung eines Cyberrisikomanagements zur Integration in das bestehende SMS der Reederei.

Das Dokument zeigt weiterhin die Schnittstellen auf zum

- IT-Grundschutz des BSI
- ISPS-Code

und soll so eine Hilfestellung für ein ganzheitliches maritimes Cyberrisikomanagement geben.

Dieses Rundschreiben erhebt keinen Anspruch auf Vollständigkeit und ist keine Interpretation von internationalen oder nationalen Regeln.

Cyberrisikomanagement

Nach der IMO Resolution MSC.428(98) sind Cyber-Risiken spätestens ab der ersten jährlichen Überprüfung des **ISM DOC** nach dem **1. Januar 2021** im Sicherheitsmanagementsystem (**SMS**) angemessen zu adressieren. Dabei sind die IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/Circ.3) zu berücksichtigen.

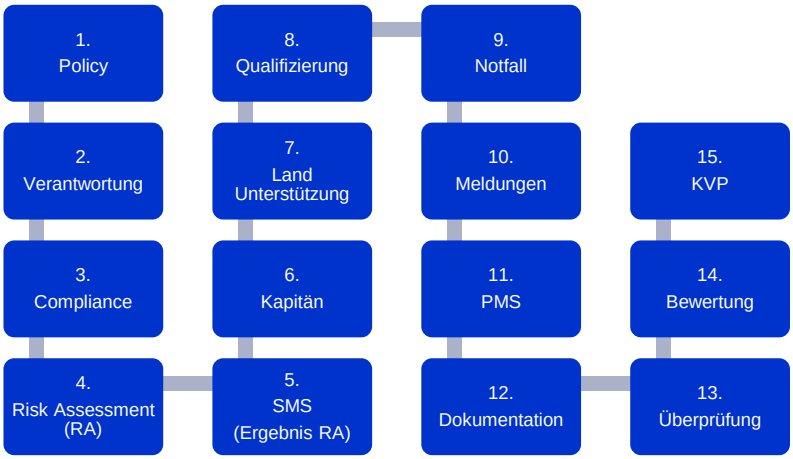
ISM-Code

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

Der ISM-Code regelt erforderliche Maßnahmen für die Organisation eines sicheren Schiffsbetriebs. Durch den modulartigen Aufbau des Codes können die durch Cyber-Bedrohungen notwendig gewordenen Sicherheitsmaßnahmen in das bestehende ISM Sicherheitsmanagementsystem (SMS) der Reederei integriert oder in einem eigenen Informations-Sicherheitsmanagementsystem (ISMS) mit Überleitung zum ISM SMS beschrieben werden. In allen Fällen sind die Anforderung der IMO zu berücksichtigen.

Prozess

In Anlehnung an die Elemente des ISM-Codes sind die Inhalte der nachfolgenden Bausteine bei der Erstellung eines Managementsystems angemessen zu berücksichtigen.



Anwendungshinweise

Auf den folgenden Seiten werden die ISM Bausteine tabellarisch beschrieben (die Informationen sind unverbindlich):

Beschreibung	Mögliche Maßnahmen	Referenzierung
Die Anforderung	▪ [Maßnahme 1] ▪ [Maßnahme 2]	ISM ISPS BSI

ISM — Verweis auf die Elemente des ISM-Codes

ISPS — Verweis auf die Kapitel des ISPS-Codes oder ISPS relevante Hinweise

BSI — Verweis auf IT-Grundschutz des BSI bzw. die IT-Grundschutz-Profile für Reedereien

BSI IT-Grundschutz

Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eine seit mehr als 25 Jahren bewährte Methodik, um das Niveau der Informationssicherheit in Institutionen jeder Größenordnung zu erhöhen. Durch seine Kompatibilität in der Standard-Absicherung zur ISO 27001 ist er international angesehen. Die modulare und strukturierte Herangehensweise ermöglicht einen passgenauen Einstieg in den Sicherheitsprozess:

- **BSI-Standards:** Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für die Informationssicherheit (ISMS). Mit Hilfe des BSI-Standards 200-2 zur IT-Grundschutz-Methodik kann dieses solide aufgebaut werden. Der BSI-Standard 200-3 zum Risikomanagement beinhaltet alle risikobezogenen Arbeitsschritte für die Umsetzung des IT-Grundschutzes.

- **IT-Grundschutz-Kompendium:** Die IT-Grundschutz-Bausteine bieten konkrete Anforderungen für ca. 100 Top-Themen der Informationssicherheit. Sie beinhalten bereits Risikoanalysen zu fast 50 potenziellen Gefährdungen. Die Basis-Anforderungen bilden gemeinsam mit den Standard-Anforderungen den Stand der Technik ab und werden vom BSI kontinuierlich weiterentwickelt.

Die Bausteine im IT-Grundschutz-Kompendium sind in Prozess- und System-Bausteine aufgeteilt und diese jeweils in insgesamt zehn Schichten untergliedert. In dem vorliegenden Dokument erfolgt eine Referenzierung insbesondere auf Bausteine aus den folgenden Schichten:

- ISMS (Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess)
- ORP (Organisatorische und personelle Sicherheitsaspekte)
- CON (Konzepte und Vorgehensweisen)
- DER (Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen)

Zudem wird die Nutzung der zwei „IT-Grundschutz-Profile für Reedereien“, Landbetrieb (2018) sowie Schiffsbetrieb (Anfang 2020) empfohlen. Sie entstanden im Rahmen der Kooperation des Vereins Hanseatischer Transportversicherer (VHT) mit dem BSI. Experten aus der Schifffahrtsbranche identifizierten im Rahmen einer Strukturanalyse, welche Prozesse aus ihrer Sicht besonders schutzbedürftig sind. Anhand dieser Prozesse wurden die relevanten Bausteine aus dem IT-Grundschutz-Kompendium ermittelt. Daraus ergibt sich ein Muster-Sicherheitskonzept für Reedereien, welches helfen kann, die Anforderungen der IMO zu erfüllen.

ISPS-Code

Dieses Dokument nimmt Bezug auf Vorschriften des ISPS-Codes. Der Grund dafür ist, dass das Kapitel XI-2 SOLAS und der ISPS-Code Anforderungen zum Umgang mit „sicherheitsrelevanten Ereignissen“ (SOLAS XI-2/1.1.13) enthalten. Nach den einschlägigen IMO-Vorgaben zum Cyberrisikomanagement (MSC-FAL.1/Circ.3, Resolution MSC.428(98)) sind darunter auch solche Ereignisse zu verstehen, die einen digitalen Ursprung haben.

Eine nach Abschnitt 8 ISPS/A erforderliche Risikobewertung für das Schiff sollte auch Funk- und Telekommunikationssysteme einschließlich Computersysteme und Netzwerke erfassen (Abschnitt 8.3.5 ISPS/B). Diese Anforderung ist gemäß Abschnitt 8.3.5 ISPS/B i.V.m. Art. 3 Abs. 5 Verordnung (EG) Nr. 725/2004 verbindlich für die Mitgliedstaaten der EU. Die Flaggenstaatsverwaltungen der EU Mitgliedstaaten haben für die Umsetzung dieser Vorgabe Sorge zu tragen. Das bedeutet, dass eine Risikobewertung, die die Grundlage für den Gefahrenabwehrplan an Bord des Schiffes (Ship Security Plan, SSP) bildet, auch Cyber-Risiken erfassen muss.

Um diese Vorgabe sinnvoll umzusetzen bestehen folgende Möglichkeiten:

1. Cyber-Risiken sind in der Risikobewertung für den SSP nach Abschnitt 8 ISPS/A zu betrachten

oder

2. die im Rahmen des Safety Management Systems (SMS) zu erstellende Risikobewertung bzw. die darin relevanten Aspekte zu den Cyber-Risiken sind dem BSH als zuständiger „ISPS-Behörde“ zusammen mit dem zu genehmigenden SSP vorzulegen. Dies setzt voraus, dass die Inhalte des Abschnitts 8 ISPS/A bei der Risikobewertung abgedeckt werden.

Grundlage für den SSP ist die Bewertung der Cyber-Risiken nach dem ISPS-Code. In dem SSP sind die aus der Risikobewertung folgenden Maßnahmen zu adressieren. Je nach Maßnahme kann dies durch direkte Verankerung im SSP oder auch durch Verweis auf das SMS erfolgen. Das Symbol (ISPS) im Abschnitt „Module“ hilft zu identifizieren, an welchen Stellen die Vorschriften des ISPS-Codes im Hinblick auf Cyber-Risiken zu beachten sind.

Module

1. Policy

Das Cyberrisikomanagement (CRM) ist ein unmittelbares Anliegen der Unternehmensleitung. Sie erkennt die grundsätzlichen Risiken für den Schiffsbetrieb durch Cyber-Bedrohungen an und erweitert die Managementziele um das Thema Informationssicherheit (IT & OT).

- Policy um Cyber-Risiko Aspekte erweitern

2.1
ISMS.1

2. Verantwortung

Die Unternehmensleitung trägt die grundlegende Verantwortung für das CRM an Bord ihrer Schiffe. Sie kann - je nach Organisation und Größe der Reederei - Verantwortung und Aufgaben übertragen.
Im SMS werden alle Personen mit zugewiesenen CRM Aufgaben erfasst.

- Pflichtenübertragung vom Unternehmer an die verantwortliche Person
- Verantwortliche(n) benennen
- Aufgabenbeschreibungen und Kommunikationswege im SMS erweitern (z.B. Job Description und Organigramm)

3.2
ISMS.1

3. Compliance

Rechtskataster listen anzuwendende Regeln und Empfehlungen auf, z. B. von der IMO, Flaggenstaatsverwaltung, BSI, Klassifikationsgesellschaften, Industrieverbänden. Aus diesen werden die relevanten Anforderungen abgeleitet, sie bilden eine Basis für die Erstellung und Fortschreibung des Managementsystems / SMS und des Risk Assessment (RA).

- Vorhandene Rechtskataster um Dokumente der Informationssicherheit erweitern:
  - Vorschriften, die zu beachten sind
  - Guidelines, die zu berücksichtigen sind

1.2
ORP.5
CON.2
CON.7

4. Risk Assessment

Über das Risk Assessment werden Gefährdungen ermittelt, deren Risiken beurteilt und erforderliche Schutzmaßnahmen festgestellt. Dazu kann das bestehende ISM RA genutzt werden. Der Umfang richtet sich nach Faktoren wie Unternehmensstruktur, Schiffstyp, Automatisierungsgrad an Bord und Zugang zu IT/OT. Zur Ermittlung von Gefährdungen (HAZID) und Beurteilung von Risiken (RA) eignen sich auch umfängliche Schwachstellenanalysen (z.B. Penetration-Tests).

- Risiken beurteilen.
- Hinweis ISM:
  Die Risiken für den Schiffsbetrieb sind zu berücksichtigen, d.h. über ein RA sind die Auswirkungen und Folgen eines Cybervorfalls ebenso zu berücksichtigen wie das Risiko eines Cybervorfalls selbst.
- Hinweis IT-Grundschutz-Profil:
  Die Basis- und Standard-Anforderungen der IT-Grundschutz-Bausteine basieren auf einer Betrachtung der potenziellen Gefährdungen und den daraus resultierenden Risiken, so dass dazu passende Maßnahmen für den normalen Schutzbedarf und für typische Anwendungsszenarien einen ausreichenden Schutz bieten. Für abweichende Szenarien finden sich in den Profilen Hinweise zur „Durchführung einer Risikoanalyse auf Basis von IT-Grundschutz“.
- Hinweis ISPS-Risikobewertung
  Zur ISPS-Risikobewertung wird auf den Abschnitt „ISPS-Code“ auf Seite 2 verwiesen.
- Maßnahmen zur Risikominimierung festlegen
- regelmäßige Wirksamkeitskontrolle durchführen

1.2
Hinweis
Hinweis
IT-Grundschutz-Profil
Hinweis

5. SMS (Ergebnis RA)

Ein Ergebnis des RA sind technische, organisatorische und personenbezogene Schutzmaßnahmen. Sie werden als Prozess oder Verfahrensanweisung im SMS beschrieben und stehen damit der Besatzung zur Verfügung.

- Verfahren und Anweisungen im SMS erstellen, ggf. ändern oder anpassen
- Anregungen aus dem IT Grundschutz-Profil nutzen, z.B. durch Referenzierung auf einzelne Bausteine
- Ggf. Referenz zum SSP, z.B. für vertrauliche Informationen und Maßnahmen, die nicht frei zugänglich gemacht werden sollen

1.4
9.4
IT-Grundschutz-Profil

6. Kapitän

Das SMS beschreibt die CRM Verantwortung und Aufgaben des Kapitäns sowie dessen Entscheidungs- und Weisungsbefugnis. Dazu zählen neben der Umsetzung und Überwachung der Maßnahmen auch das Erkennen und Melden von Mängeln und Schwachstellen an die Reederei sowie die Motivation der Besatzung zur Mitwirkung. Qualifizierungsmaßnahmen für CRM können erforderlich sein und sind im SMS darzustellen.

- Aufgabenbeschreibung des Kapitäns erweitern (z.B. Job Description)
- Qualifizierungsanforderung festlegen
- Qualifizierungsmaßnahmen festlegen
- Overriding authority sicherstellen
- Motivation: Unterstützung durch geeignete Tools und konkrete Vorgaben

5
6.1
6.2
6.1
ORP

7. Landunterstützung

Durch geeignete Organisation steht dem Kapitän qualifizierte landseitige Unterstützung durch die Reederei zur Verfügung zum
- Reagieren auf einen Cyber-Vorfall,
- Reagieren auf die Folgen eines solchen Vorfalls,
- Wiederherstellen von Systemen (Backup & Restore).

- Verantwortliche(n) benennen
- Aufgaben "Landorganisation" festlegen
- Aufgabenbeschreibung erweitern
- Notfallteam bilden (siehe auch Pkt.9)
- Prävention
- IT Grundschutz-Profil für Reedereien - Landbetrieb berücksichtigen

3.2
3.3
4
6.5
6.2
9.4.12
IT-Grundschutz-Profil

8. Qualifizierung

Das SMS beschreibt die CRM Verantwortung und Aufgaben der betroffenen Personen auf See und an Land. Diese werden bei Dienstantritt, Veränderungen und regelmäßig wiederkehrend unterwiesen. Dazu enthält das SMS einen Trainings- und Qualifizierungsplan sowie Maßnahmen zum Feststellen von Trainingsbedarf (Land / See).

- Aufgabenbeschreibung im SMS erweitern (z.B. Job Description)
- Qualifikationsplan erweitern (Matrix)
- Trainingsplan erweitern (Matrix)
- Vorgaben für Unterweisung für See- und Landbereich
- Sensibilisierungsmaßnahmen nach BSI ORP
- Aufgaben des Schiffspersonals

6.4
6.5
8.2
9.4.7
9.4.9
ORP

9. Notfall

Die bestehenden ISM Notfallpläne werden um Aspekte des CRM ergänzt (See & Land) und regelmäßig durch Übung, Simulation und Schulung eingeübt (Ziel: reflektierendes Handeln).
Die Pläne schließen ein:
- Reagieren auf Cyber-Vorfälle und deren Folgen
- Wiederherstellen (Backup & Restore)
- Notfallrufnummern und Meldeketten
- Notfallteam "Land" (inkl. Zusammensetzung)

- Notfallplan See
- Notfallplan Land
- Notfallteam & Organisation Land
- ISM Drill Plan ergänzen
- Notfallkontaktdaten
- Notfall-Meldekette

8.1
8.2
8.3
9.4.4
9.4.6
DER

10. Meldungen

Vorfälle, Unfälle, Beinahe-Unfälle und sonstige relevante Vorkommnisse werden über das ISM Meldewesen an die zuständigen internen Stellen gemeldet, dort untersucht und analysiert. In deren Folge werden korrigierende und präventive Maßnahmen eingeleitet. Ziel: kontinuierliche Verbesserung. Meldeketten und externe Meldepflichten werden beschrieben.

- Vorgabe für die Meldung
- Kontaktdaten
- Meldeketten

9.1
9.2
9.4.12
DER.2.1

11. PMS

Die Sicherstellung der Instandhaltung von Schiff und Ausrüstung ist bereits durch ein Verfahren im SMS beschrieben und wird um CRM Maßnahmen erweitert. Aus dem Risk Assessment abgeleitete Schutzmaßnahmen, die regelmäßig wiederkehrend zu überprüfen oder durchzuführen sind, werden im PMS verwaltet (Planned Maintenance System / Planung, Durchführung, Dokumentation). Dazu können Software-Updates zählen. Der Bereich Critical Equipment wird fortgeschrieben.

- Überprüfungs- und Wartungsaufgaben definieren
- Aufgaben im PMS verwalten
- Liste "Critical Equipment" überprüfen und ggf. erweitern

10.1
10.2
10.3
10.4
9.4.16
ISMS.1

12. Dokumentation

Anforderungen an die Dokumentation und der Zugriff auf diese sind bereits Bestandteil des SMS; sie werden um CRM Belange erweitert.

- Bestehendes Verfahren erweitern
- ISM-Dokumentation erweitern

ISM 11
10.4
ISMS.1

13. Überprüfung

Durch interne und externe Audits wird das Managementsystem, der Grad der Umsetzung und die Wirksamkeit nach festgelegten Kriterien fortlaufend überprüft. Interne Audits an Bord und an Land werden um das Thema CRM erweitert und in Intervallen von nicht mehr als 12 Monaten durchgeführt.

- Interne Auditverfahren erweitern
- Interne Prüflisten & Prüfkriterien erweitern
- Auditoren qualifizieren

ISM 12.1
9.4.8
DER.3.1

14. Bewertung

Regelmäßig jährlich wird das Sicherheitsmanagement bewertet zur Prüfung, ob die Organisation auf See und an Land entsprechend den SMS Vorgaben arbeitet, die Maßnahmen effektiv sind, das Personal und interne Auditoren ausreichend qualifiziert sind und Auditergebnisse - soweit vertretbar - bekannt gemacht sind und notwendige korrigierende und präventive Maßnahmen zeitnah eingeleitet wurden.

- Topic einbinden im Management Review
- Ergebnisse zusammenfassen aus Audits, Vorfällen und Beinahe-Vorfällen, Beratung, Analysen, Korrektur-/Präventivmaßnahmen, Folgemaßnahmen vorheriger oder anderer Bewertungen, Einhaltung der Politik, vorhandene Ressourcen

12
8.5
9.4.11
DER.3.1

15. KVP

Kontinuierlicher Verbesserungsprozess – die Reederei muss den ständigen Veränderungen und den im eigenen System erkannten Schwachstellen Rechnung tragen und eine Fortschreibung des SMS und RA Systems sicherstellen und damit den kontinuierlichen Verbesserungsprozess einleiten.

- Maßnahmen für KVP und Fortschreibung im SMS festlegen

SMS
14
DER.3.1
ISMS.1

Anhang I - Bedienungshinweise zu den IT-Grundschutz-Profilen für Reedereien

Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept, das als Schablone für Institutionen mit ähnlichen Rahmenbedingungen dient, beispielsweise in einer bestimmten Branche. In einem IT-Grundschutz-Profil werden die einzelnen Schritte eines Sicherheitsprozesses für einen definierten Anwendungsbereich gebündelt und dokumentiert. Dazu gehören: Festlegung des Anwendungsbereichs, Durchführung einer verallgemeinerten Strukturanalyse, Schutzbedarfsfeststellung und Modellierung für diesen Bereich, Auswahl und Anpassung von umzusetzenden IT-Grundschutz-Bausteinen sowie Beschreibung spezifischer Sicherheitsanforderungen und -maßnahmen.

Anwenderinnen und Anwender können die Sicherheitsbetrachtungen auf die individuellen Rahmenbedingungen ihres Unternehmens übertragen und das Sicherheitsniveau im Betrieb modular erhöhen. Das spart ihnen viel Zeit und Arbeit. Ein IT-Grundschutz-Profil ist somit eine praktikable Lösung, um mit überschaubarem personellen und finanziellen Aufwand die ersten Schritte in Richtung Informationssicherheit zu gehen.

Mit den hier empfohlenen IT-Grundschutz-Profilen für Reedereien stehen praktische Muster-Sicherheitskonzepte zur Verfügung. In dem IT-Grundschutz-Profil für Reedereien - Seebetrieb sind bereits die Prozesse „Technischer Betrieb“, „Nautischer Betrieb“, „Landungsbetrieb“ und „Kommunikation“ identifiziert und bieten sogenannte Landkarten zur Umsetzung der notwendigen Anforderungen für die Gewährleistung der Informationssicherheit an Bord. Das IT-Grundschutz-Profil für Reedereien - Landbetrieb fokussiert die Prozesse „Accounting“ und „Technisches Management“ und dient als Umsetzungshilfe für die unter Punkt 7 aufgeführten Themen rund um die Landunterstützung.

Hinweise zur Nutzung der IT-Grundschutz-Profile

Die beiden IT-Grundschutz-Profile beschreiben jeweils, wie das Muster-Sicherheitskonzept als Grundlage für den Informationssicherheitsprozess in der Reederei dient und ist an die realen Gegebenheiten im Betrieb anzupassen. An dieser Stelle sind zusätzlich hilfreiche Tipps für den Umgang mit den einzelnen IT-Grundschutz-Bausteinen zusammengefasst.

Wie arbeite ich zeitsparend und zielgerichtet mit dem Original IT-Grundschutz-Baustein?

Der eigentliche IT-Grundschutz-Baustein ist auf der Website des BSI verortet und dort erreichbar. Die Struktur ist immer gleich, die einzelnen Kapitel sind per „Sprungmarken“ gezielt anzusteuern. Das spart viel Zeit, denn so gelangen Sie auf direktem Wege zu den für Sie relevanten Textpassagen.

Kapitel (Inhalt)	Lese-Empfehlung
1. Beschreibung (Einleitung, Zielsetzung, Abgrenzung zu anderen Bausteinen)	KANN – Bietet allgemeine Hintergrundinformationen und dient der Einordnung
2. Gefährdungslage	KANN – Überblick zu Risiken, die auftreten können, wenn die Anforderungen nicht umgesetzt werden
3. Anforderungen	
3.1 Basis-Anforderungen	MUSS – die Basis-Anforderungen sind die notwendigen Anforderungen für die Steigerung der Informationssicherheit in Ihrem Betrieb.
3.2 Standard-Anforderungen	MUSS – wenn Standard-Absicherung angestrebt wird.
3.3 Anforderungen bei erhöhtem Schutzbedarf	KANN – z. B. relevant, wenn dieser Baustein sich auf ein für Sie besonders schützenswertes Zielobjekt ihres Betriebs bezieht.
4. Weiterführende Informationen (Literatur)	KANN – zur Vertiefung des Themas
5. Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen	KANN – hier ist zu sehen, welche Risiken Sie mit der Umsetzung des Bausteins minimieren konnten.

[!] WICHTIG: Basis-Anforderungen sind ein MUSS, Standard-Anforderungen ein SOLLTE

Jede Anforderung mit der Nummerierung A.1 bis A.n beinhaltet MUSS- bzw. SOLLTE-Sätze. Betrachten Sie den Textabschnitt wie eine Checkliste: Jeder Satz ist eine eigenständige Anforderung, die zu betrachten ist. Ist sie bereits in Ihrem Betrieb erfüllt – Haken dran. Ist sie NICHT erfüllt, dann gibt es noch etwas zu tun.

Wie kann ich die Umsetzungshinweise zum IT-Grundschutz-Baustein nutzen?

Für viele IT-Grundschutz-Bausteine hat das BSI praktische Umsetzungshinweise herausgegeben. Die gute Nachricht: Sie müssen die umfassenden Ausführungen nicht in Gänze lesen, sondern nur das, was Sie in dem Moment wirklich interessiert. Der Trick: Aus A wird einfach M. Denn zu jeder Anforderung mit dem Kürzel A.[Nummer] im Baustein gibt es eine passende Maßnahme mit dem entsprechenden Kürzel M.[Nummer] in den Umsetzungshinweisen (sofern diese vorhanden). In der Online-Version erleichtern auch hier Sprungmarken den direkten Einstieg zu den „Basis-Maßnahmen".

Beispiel: Die Basis-Anforderung „OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen" im Baustein „OPS.1.1.4 – Schutz vor Schadprogrammen" korrespondiert mit der Maßnahme „OPS.1.1.4.M1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen" in den dazu passenden Umsetzungshinweisen.

Anhang II - Glossar

ACP-Liste: Acess point list - Auflistung aller elektronischer Zugänge zur Schiffs-IT und Schiffs-OT als Grundlage für das Risk Assessment und Ermittlung potentieller Schwachstellen.

APP: Applikation – Anwendungssoftware im Allgemeinen und nicht reduziert auf Smartphone oder Tablet Anwendungen.

Audit: Systematischer, unabhängiger interner oder externer Prozess für die Überprüfung eines Managementsystems und zur Erlangung von Nachweisen sowie deren Auswertung zur Ermittlung, ob definierte Auditkriterien erfüllt und die Anforderungen des Managementsystems umgesetzt werden.

Awareness: Bewusstsein und Aufmerksamkeit - fehlende oder nicht fortlaufende Unterweisung / Fortbildung für See- und Landpersonal erhöhen die Wahrscheinlichkeit von Fehlverhalten beim Verhindern, Erkennen und Reagieren auf Gefahren und Bedrohungen.

BDSG: Das BDSG ergänzt die unmittelbar geltende Verordnung (EU) 2016/679 (Datenschutz Grundverordnung) um die Bereiche, in denen die EU-Verordnung den Mitgliedstaaten Gestaltungsspielräume belässt. Durch den erforderlichen Schutz von Daten ist das BDSG ein im Managementsystem zu berücksichtigendes Element.

Cyber Risk Management (CRM): Dies sind Unternehmensgrundsätze, Verfahrensweisen und Ressourcen, die ein Unternehmen umgesetzt hat und weiterentwickelt, um potentielle Risiken, resultierend aus der Benutzung von IT und OT, zu erkennen, zu reduzieren und abzuwehren.

Gefährdung: Quelle, Situation oder Handlung, die zu einem Schaden führen kann.

IT-Grundschutz: Das IT-Grundschutz-Profil sind Empfehlungen zur Umsetzung der Informationssicherheit und bestehen aus System- und Prozessbausteinen mit konkreten Handlungsempfehlungen.

HAZID: Hazard Identification - Auflistung potentieller Gefahren und gefährdeter Anlagen und Einrichtungen als eine nicht abschließende und weiter fortzuschreibende Liste. Diese Gefahrenidentifizierung dient als Grundlage für das Risk Assessment.

Industrial: Guideline: "Guidelines on Cyber Security Onboard Ships" - dies sind anerkannte Informationen der Fachverbände und können bei der Erstellung und Fortschreibung des Management Systems unterstützen. Details können bei der BIMCO oder den weiteren Verfassern eingeholt werden.

Integriert: Cyber Risk Management kann durch Einzelmaßnahmen und -verfahren in das bestehende SMS der Reederei integriert werden oder aber als eigenständiges Managementsystem mit einer Schnittstelle zum ISM SMS geführt werden.

IPDRR: Das Managementsystem soll die von der IMO empfohlenen IPDRR Grundsätze und Maßnahmen berücksichtigen:

IDENTIFY	Identifizieren von Gefahren
PROTECT	Schutz vor "Gefahren"
DETECT	Identifizieren eines "Vorfalls"
RESPOND	Reagieren auf einen "Vorfall"
RESTORE	Wiederherstellen

ISM-Code: Internationaler Code für Maßnahmen zur Organisation eines sicheren Schiffsbetriebes und Verhütung der Meeresverschmutzung. Dies ist eine international gültige Norm für Maßnahmen zur sicheren Betriebsführung von Schiffen und zur Verhütung der Meeresverschmutzung. Der Code regelt erforderliche Maßnahmen für die Organisation eines sicheren Schiffsbetriebs. Durch den modulartigen Aufbau des Codes können die durch Cyber Bedrohungen notwendig gewordenen Sicherheitsmaßnahmen in das bestehende Sicherheitsmanagementsystem (SMS) der Reederei integriert werden.

ISMS: Informationssicherheitsmanagement (ISMS) - ein Managementsystem auf dem IT Sektor, es steht in keiner Verbindung zur IMO und dem ISM-Code. Dadurch besteht Verwechslungsgefahr.

ISPS-Code: Internationaler Code für die Gefahrenabwehr auf Schiffen und in Hafenanlagen, gültig für Schiffe unter deutscher Flagge seit 2004.

IT / OT: IT: Informationstechnologie und Netzwerke, z.B. Kommunikationseinrichtungen Email / Telefon sowie Internet, Office-PC, PMS Server, W/LAN.

OT: Systemanlagen / Operational-PC´s (z.B. GNSS, Radar, ECDIS, Maschinensteuerung, Sensoren, Alarm, Überwachung).

RA und SMS dürfen sich nicht auf IT reduzieren, Maßnahmen müssen OT und Schnittstellen zwischen IT und OT berücksichtigen.

Korrektur: Korrekturmaßnahmen zur Beseitigung einer erkannten Abweichung oder Schwachstelle (englisch: CA corrective action).

KVP: Kontinuierlicher Verbesserungsprozess - ein Grundprinzip zur Fortschreibung und Weiterentwicklung des Managementsystems durch stetige Anpassung und Verbesserung, insbesondere in der Folge von Bewertungen.

Ladung: Die Richtigkeit von Ladungsangaben (Gewicht, Gefahrgut, Stauposition z.B. bei Containerladung) ist primär die Aufgabe vom Terminal und Charterer. Der sichere Datenaustausch Land-Schiff und damit die sichere Stauung müssen gewährt bleiben.

Anhang II - Glossar Fortsetzung

Navigation: Mögliche Gefährdungen können sein:
- Ausfall oder Manipulation GPS / DGPS.
  GPS-Spoofing: falsche Positionsdaten.
  GPS Jamming: Störsender, Signalstörung oder Signalverhinderung.
- Ausfall oder Manipulation der AIS Daten.
- Fehlerhafte Geschwindigkeitseingabe führt zur fehlerhaften ARPA Auswertung.
- Fehlerhafte ECDIS Angaben.
- Ausfall (Absturz) und Reboot-Fehler der Radaranlagen / integrierter Anlagen.
- Manipulation oder Ausfall von DP-Systemen.
- Ausfall Echolot und anderer softwarebasierter und/oder integrierter Navigationssysteme.
- Beeinflussung der Steuerung und Überwachung von Maschinenanlagen / Aggregaten.
- Fehlerhafte Reiseplanung.

RA: Risk Assessment / Risikobeurteilung – der Prozess der von einer Gefährdung ausgehenden Bewertung des Risikos. Über das RA werden die Risiken und erforderlichen Gegen- bzw. Schutzmaßnahmen festgestellt.

RA Methode: Es gibt unterschiedliche Modelle und Ansätze. Die Auswahl und das konkrete Vorgehen obliegen dem Unternehmen.
Beispiel über die HAZID und RESID Modelle:
Zunächst werden die Gefahren identifiziert (HAZID Liste) und die zur Verfügung stehenden Ressourcen (RESID Liste). Darüber hinaus alle Möglichkeiten, über die ein Zugang zur Schiffs-IT oder Schiffs-OT möglich ist (ACP Liste). Wird über die ACP Liste festgestellt, dass es keine Zugänge gibt, ist der Umfang der erforderlichen Maßnahmen gering. Auf Basis dieser Listen werden die Risiken der identifizierten Gefährdungen bewertet und bei Bedarf Schutzmaßnahmen nach der TOP Maßnahmenhierarchie festgestellt (technische Maßnahmen haben Vorrang vor personen- u. verhaltensbezogenen Maßnahmen).

Risiko: Verbindung aus Eintrittswahrscheinlichkeit und der Schadensschwere einer Gefahr bzw. eines gefährlichen Ereignisses.

Risko =
Eintrittswahrscheinlichkeit x Schadensschwere

Ein Risiko zu reduzieren bedeutet, mit einer Schutzmaßnahme die Eintrittswahrscheinlichkeit und/oder die Schadensschwere positiv zu beeinflussen. Bei einem akzeptierbaren Risiko können Maßnahmen entfallen. Akzeptierbar ist ein Risiko, wenn es soweit reduziert wurde, dass es unter Berücksichtigung der rechtlichen und vertraglichen Verpflichtungen und der eigenen Politik toleriert werden kann.

Risikoanalyse: s.h. RA.

Risikomatrix: Darstellung der unterschiedlichen Risiken, von geringem Risiko über mittlerem noch tolerierbaren Risiko (ALARP) bis hin zum sehr hohen Risiko zur Durchführung der Risikobeurteilung. Beispiel: Risikomatrix nach Nohl.

RESID: Ressource Identification - Auflistung der Ressourcen und Kompetenzen als Grundlage zur Bewertung, ob eigene Möglichkeiten ausreichend sind oder Hersteller, externe Dienstleister oder Experten hinzugezogen werden müssen. Sie ist eine Grundlage für das Risk Assessement (s.h. auch HAZID) und listet potentielle Hersteller und Servicepartner auf.

TOP: Maßnahmenhierarchie - ein bestehendes Risiko mit Schutzmaßnahmen nach der TOP Hierarchie reduzieren:

(T) Technisch

(O) Organisatorisch

(P) Personenbezogen

(T) Maßnahmen haben Vorrang vor (O) und (P), eine technische Maßnahme ist sicherer als eine Verhaltensanweisung (P).
Beispiel Email-Verkehr:
(P): Anweisung an die Besatzung "keine Anhänge mit .exe & .mpg öffnen".
(T): ein Filter ermöglicht nur .pdf & .jpg Anhänge. Diese (T) Maßnahme ist sicherer als die Verhaltensanweisung (P).

Umfang: Abhängig von den erkannten Gefährdungen muss der Umfang der Maßnahmen den festgestellten Gefährdungen und der Organisationsgröße gerecht werden. Der Anspruch der kontinuierlichen Verbesserung sollte möglichst höher wiegen als der Versuch der einmalig alles abdeckenden und abschließenden Regelung.

Verfahren: Festlegung der Art und Weise, wie eine Tätigkeit oder ein Prozess auszuführen ist.

Vorgaben: Es gibt keine konkrete Vorgabe über Inhalte und formales Vorgehen oder Aufbau eines Managementsystems. Gesetzliche Anforderung: die Pflicht für ein Cyber Risk Management ergibt sich primär aus den IMO Anforderungen zum ISM-Code, der EU DSGVO und dem BDSG.

Zertifizierung: Eine Zertifizierung zusätzlich zum ISM ist auf der Basis der Anforderungen der IMO nicht erforderlich, solche Anforderungen können privatwirtschaftlich notwendig werden oder sich aus den ermittelten Gefährdungen und Risiken, der Betriebsorganisation oder der Betriebsgröße ergeben.

Zertifiz. ISM: Das Sicherheitsmanagementsystem der Reederei wird erstmalig und jährlich wiederkehrend durch interne und externe Audits überprüft. Die Überprüfung der Umsetzung dieses Systems an Bord der Schiffe erfolgt ebenfalls regelmäßig durch interne und externe Audits. Im Anschluss erfolgt die Zertifizierung.

Verweis auf weitere Glossare des BSI:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyberglossar/cyberglossar_node.html

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/glossar_node.html

Anhang III - Regeln & Guidelines

Verweis auf weiterführende Informationen, Regeln und Guidelines.

IMO Resolution MSC.428(98)	*IMO* *www.imo.org*
IMO Guidelines MSC-FAL.1/Circ.3	*IMO* *www.imo.org*
ISM Circular 04/2017	*BG-Verkehr* *www.deutsche-flagge.de*
ISM Circular 04/2018	*BG-Verkehr* *www.deutsche-flagge.de*
IT-Grundschutz-Profil für Reedereien – Landbetrieb	*BSI* *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Reedereien_Land.html*
IT-Grundschutz-Profil für Reedereien - Schiffbetrieb	*BSI* *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Reedereien_Schiff.html*
The Guidelines on Cyber Security on-board Ships (Industrial Guidelines)	*BIMCO, CLIA, ICS, INTERCARGOL, INTERMANAGER, INTERTANKO, IUMI, OCIMF, WORLD SHIPPING COUNCIL* *www.bimco.org*

Anhang IV - Kapitänsreeder

Die nachfolgende Auflistung sind mögliche Beispiele technischer, organisatorischer und persönlicher Maßnahmen und dienen der Orientierung für sogenannte Einschiffs-Kapitänsreeder oder Reedereien mit vergleichbaren Schiffsbetrieb.

Im Vier-Stufen-Modell gilt:

- PRÜFEN
- BEWERTEN
- UMSETZEN
- ANALYSIEREN.

Die hier dargestellten Maßnahmen sind stark vereinfacht und erreichen nicht das in diesem Dokument vorgeschlagene Niveau für Informationssicherheit.

Die **Dienststelle Schiffssicherheit** schlägt diese Maßnahmen zur Orientierung für den Fall vor, dass andere in diesem Dokument beschriebenen Maßnahmen aufgrund der Betriebsgröße von Kapitänsreedern nicht umgesetzt werden können.

Vier-Stufen-Modell

1. Prüfe!
Welche Cyber-Risiken bringt mein Schiffsbetrieb mit sich?

2. Bewerte!
Sind meine derzeitigen Maßnahmen ausreichend oder sind weitere Maßnahmen notwendig?

3. Setze um!
Geeignete weitere technische / organisatorische / persönliche Maßnahmen sind festzulegen und umzusetzen.

4. Analysiere!
Maßnahmen zur Vermeidung bzw. Reduzierung von Cyber-Risiken sind einer regelmäßigen Wirksamkeitskontrolle zu unterziehen.

T Technische Maßnahmen

Verschluss / Verplombung von Zugängen (USB/LAN)
keine Möglichkeit zum Anschluss von Massenspeichermedien durch Dritte

Physische Entfernung
von CD/DVD, Floppy- und anderen Laufwerken

Stand-alone-Lösung
Einzel-PC statt Netzwerk (z.B. Ladungs-PC)

Quarantäne PC
Netzwerkunabhängiger PC für Virenüberprüfung

Zutrittsbeschränkung:
physischer Schutz, Abschrankung. Serverstandort: restricted area

Backup Storage
Datensicherung auf externe Medien

Schutz & Filter
- Firewall
- Virenschutzprogramm
- Spam-Filter

Software / APPS
- nur notwendige Anwendungen installieren
- unnötige Funktionen & Plugins deaktivieren

Berechtigungskonzept
Unterschiedliche Zugriff-Level, nur der bekommt Rechte, der sie braucht

Updates / Patches:
APPS, MS Office, IT, OT. Anwendungen aktuell halten, Sicherheitslücken schließen

Cloud
Meidung einfacher Cloud-Dienste

Physische Trennung
Trennung von internen und externen Systemen

VPN – Verschlüsselung
Virtual Private Network, Verschlüsselung der Kommunikation

Remote access control:
Authentisierung von Zugängen (RAS, VPN)

Netzwerke:
mehrfache Segmentierung (Operation/Master/Crew/…).

WLAN Schutz
- nach neuestem Standard gesichert
- unterschiedliche Netze für Crew und Schiffsbetrieb

Email
Crew Internet Email: Standalone-Lösung statt Netzwerk (physische Trennung)

Sperrung bestimmter Email Anhänge wie ".exe, .cpl, .bat, .com, .scr, .vbs, .vba" (z.B. für Crew nur zulassen: .jpg, .txt, .pdf)

Limitierung von Email Anhängen, Account abhängig

Zugangskontrolle
IT Nutzung nur nach Login / Authentifizierung

O Organisatorische Maßnahmen

Rechte
Administratorenrechte und Zugriffsrechte einschränken

Verantwortlichkeiten und Zuständigkeiten
regeln: See / Land / Dritte

Service / Dritte an Bord
Autorisierung, Work Permit, Zugangsbeschränkungen, Warnhinweise, OT Zugangsberechtigung

PMS System
Erweitern für Planung, Durchführung & Dokumentation
- regelm. IT Überprüfung
- Updates / Patches
- Backup

IT Überprüfungen
- durch interne oder externe Sicherheitsfirmen
- Beratung durch Fachfirma

Bildschirmsperre
automatisch nach x Minuten / manuell bei Verlassen des Arbeitsplatzes

Unterstützung d. Reederei:
- Hotline / Kontakt / Beratung
- Notfallplan Office
- Wiederherstellungsplan

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

Überwachungsmaßnahmen
Monitoring / Erkennen

Datenumgang
Regelungen zur Datensparsamkeit

P Persönliche Maßnahmen

Unterweisung
- erstmalige
- wiederkehrende
- anlassbezogene

Qualifizierung
Schulung, Training & Info-Programme (Sensibilisieren)
- an Land
- auf See

Mögliche Inhalte
- Navigation: Manipulation des GNSS, AIS, Bahnführung erkennen
- Monitoring & Erkennen
- Reagieren & Melden
- Wiederherstellen
- Aufmerksamkeit / awareness
- Gefahren
- Schutzmaßnahmen
- Verhaltensmaßnahmen

Informieren
Poster, elektr. Medien & Informationsmaterial

Verhaltenshinweise
Aushänge, Textanweisung über den Bildschirmschoner

Verhaltensanweisung (a):
Klare Anweisungen für sensible Bereiche

Verhaltensanweisung (b):
Unterlassungserklärung zur Manipulation / Einwahl in Netzwerke (Crew-hacking, Vertrag, Vertragsergänzung)

Disziplinarische Maßnahmen
bei bewusster Missachtung der Vorgaben

Qualifizierungs-Maßnahmen
bei unbewusster Missachtung der Vorgaben