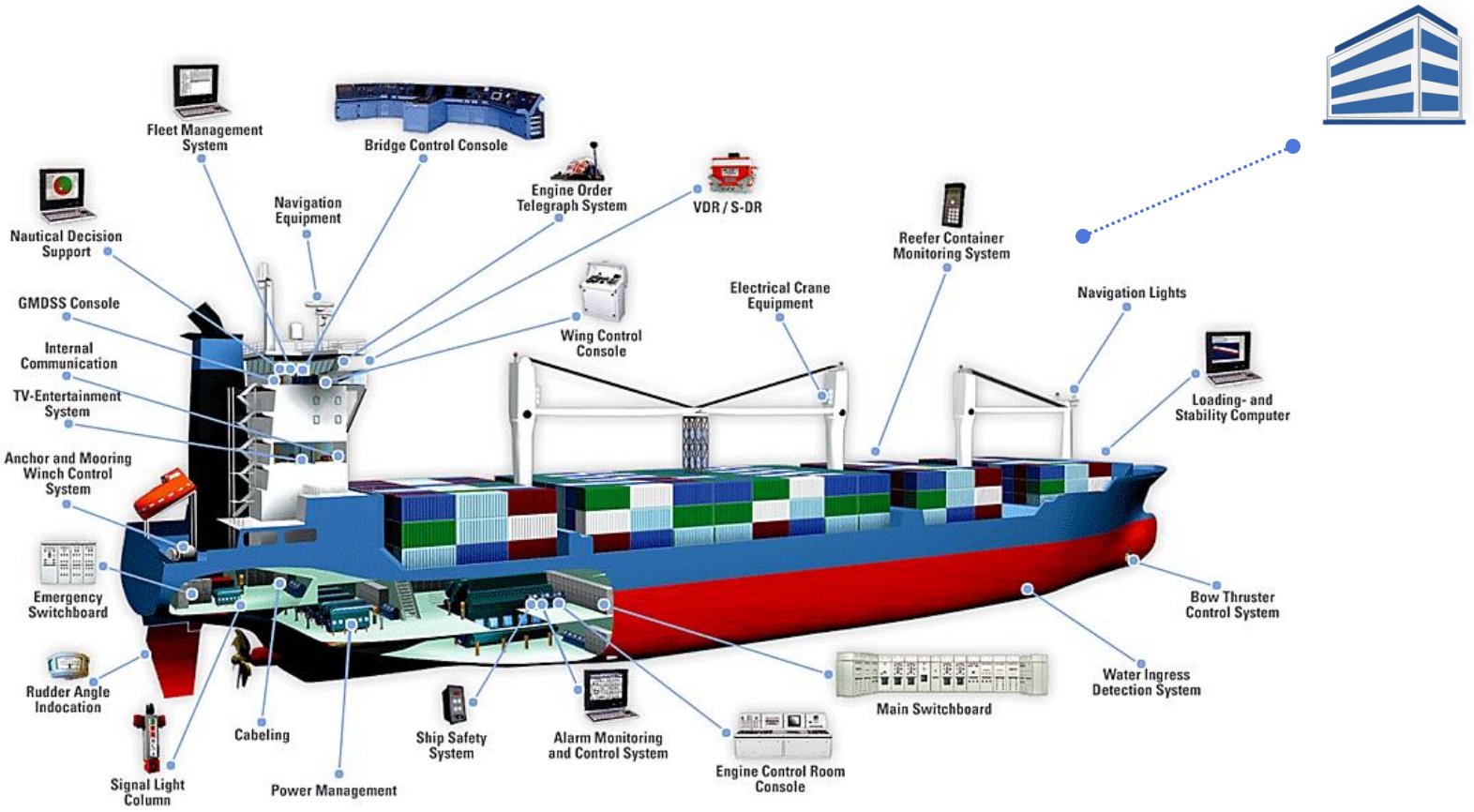
Wie kann man Cyber-Security im maritimen Kontext sicherstellen?

Svante Einarsson, DNV GL Maritime Advisory

Die Cyberwelt ist längst in der Schifffahrt angekommen



Welche Systeme sind Cyber-Gefahren ausgesetzt?

Information Technology (IT)

- IT Netzwerke
- E-Mail
- Administration, Accounts, Crew Daten, …
- Geplante Instandhaltung
- Ersatzteilmanagement
- Elektronische Handbücher
- Elektronische Zertifikate
- Arbeitsfreigabe
- Frachtbrief, Mietvertrag, …

Auswirkungen: Finanzen und Ruf

Operational Technology (OT)

- PLCs (Programmable Logic Controller)
- SCADA (Supervisory Control and Data Acquisition)
- On-board Messungen- und Kontrollsysteme
- ECDIS
- GPS
- Sensoren für Motoren
- Data loggers
- Maschinen- und Ladungskontrollsysteme
- DP System, …

Auswirkungen: Leben, Eigentum und Umwelt

Trends

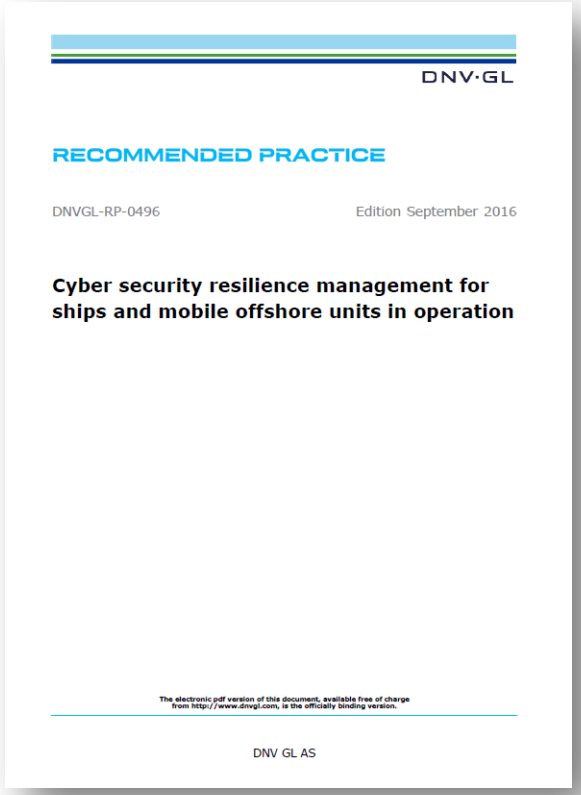
- **Cyber-Gefahren häufen sich** und werden zum Alltag

- **Richtlinien sind in der Entwicklung:**
  IMO-MSC 1/CIRC 1526 1.Juni 2016 →
  … Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping…

- Die **Cyber-Attack-Exclusion-Klausel** in Versicherungen (Klausel 380) muss **neu überdacht werden:**
  - Eigentümer erwarten kompletten Versicherungsschutz
  - Versicherer müssen die Risiken richtig kalkulieren

DNV GLs Branchenlösung

Die Reaktionen der Industrie auf Cyber-Security-Gefahren


DNV·GL

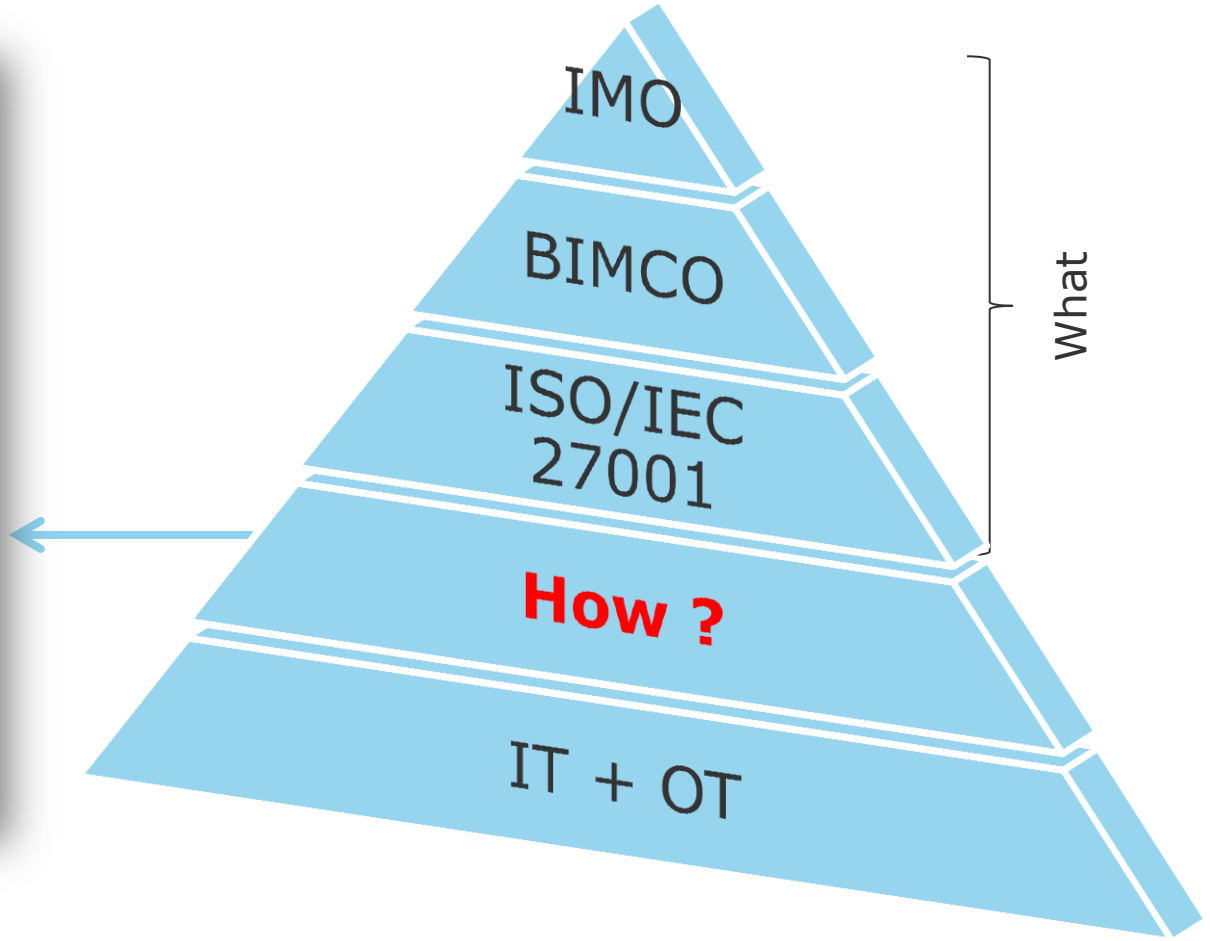
RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

Cyber security resilience management for ships and mobile offshore units in operation

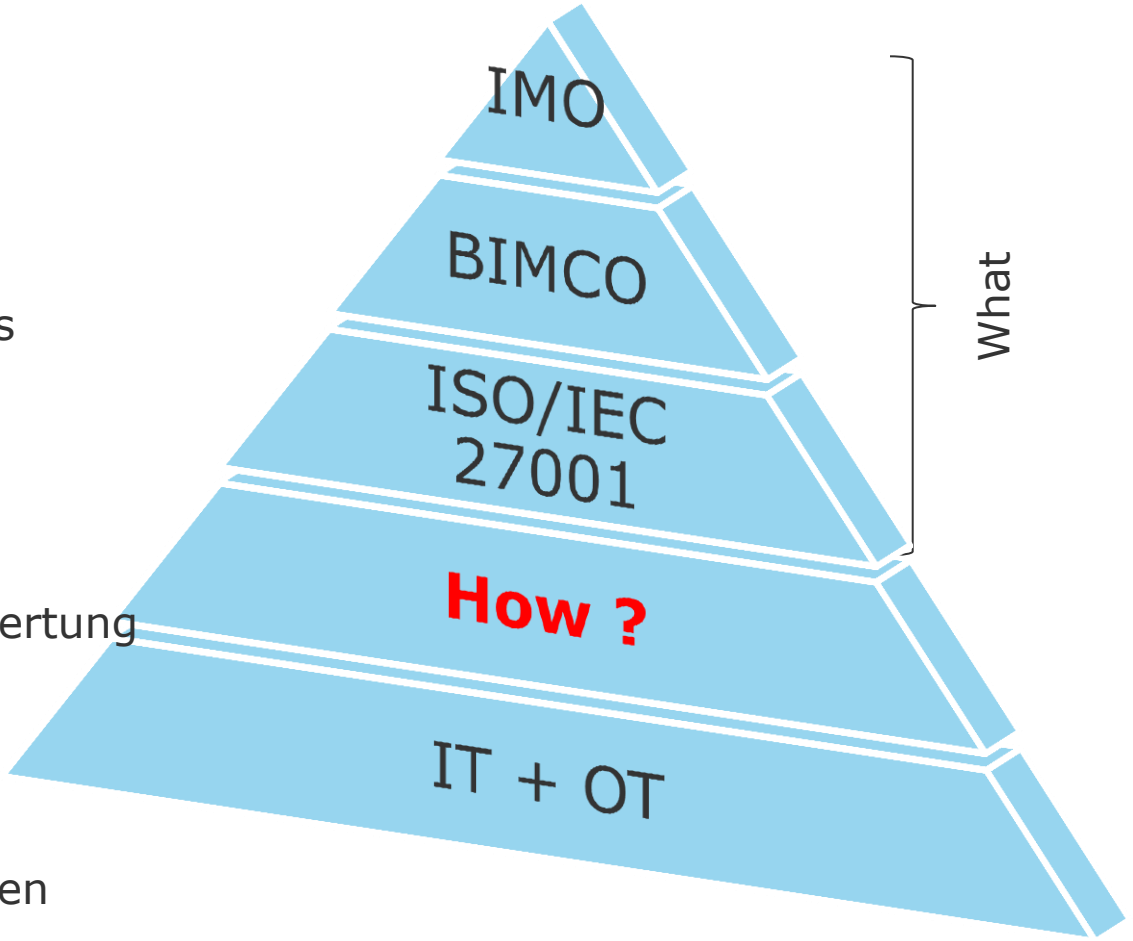
The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS



DNV GLs Lösung: Cyber Security Recommended Practice

- Erklärt das „Wie” und nicht nur das „Was”
  → füllt die Lücken unter den verfügbaren Richtlinien
- Leicht anwendbar für IT und OT Systeme
- Basiert auf etablierten Standards
  - ISO/IEC-27001
  - ISO/IEC 62443 (OT)
  - BSI Grundschutz (IT)
- Erweitert die typische Risikobewertung um den Bow-Tie-Ansatz
- Bietet praktische Beispiele und Richtlinien
- Beruht auf Erfahrungen aus realen Projekten



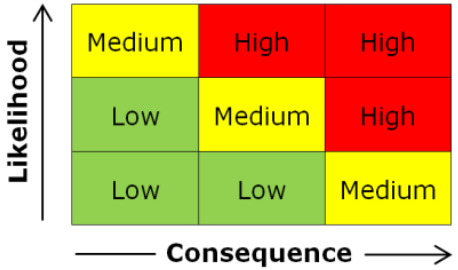
DNVGL-RP-0496 Ansatz

Start of cyber security assessment program

High level Assessment [2.1]

Focused Assessment [2.2]

Comprehensive, In Depth Assessment [2.3]



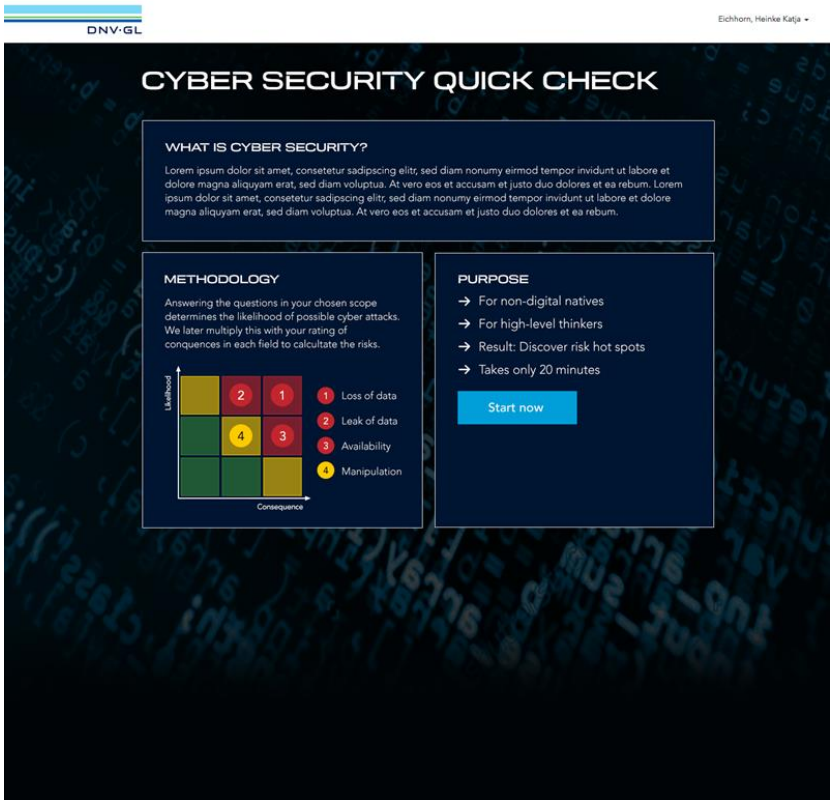
Improvement [3]

Verification & Validation [4]

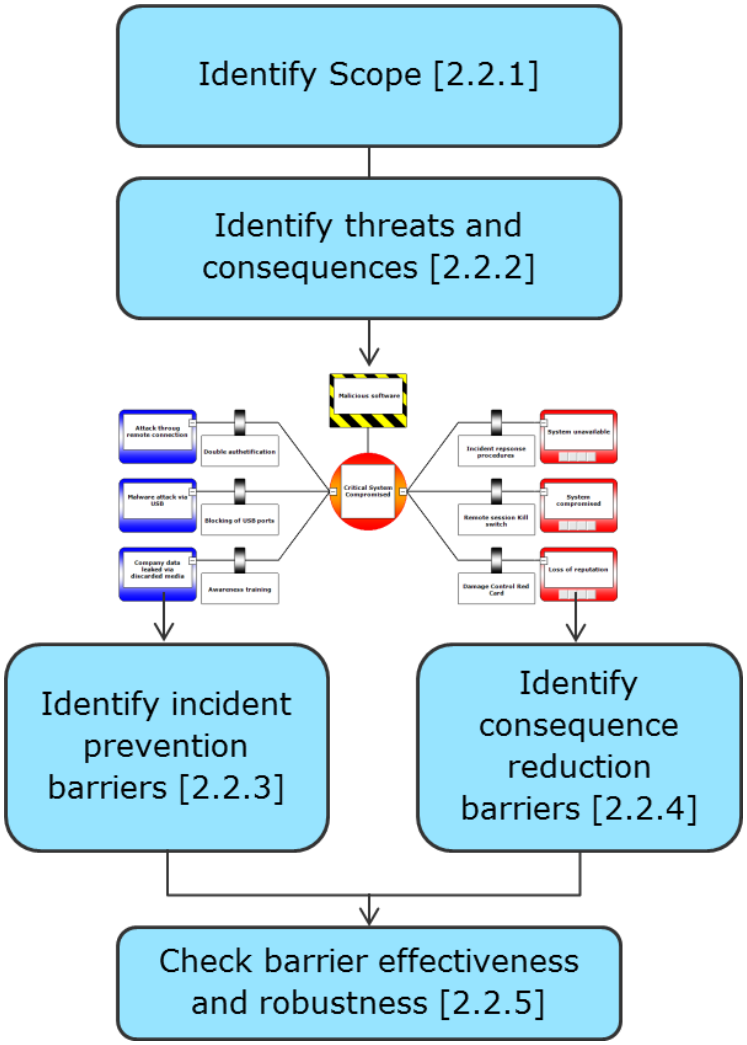
Wie funktioniert die RP?

“Cyber Security Self-Assessment” App

- Was ist es?
  Fragebogen zur Selbsteinschätzung
- Für wen?
  Mittleres bis oberes Management
- Nutzen:
  - Erste Indikation des Sicherheitsstatus
  - Bewusstsein für mögliche Lücken und Angriffspunkte
- Wie funktioniert es:
  - Erreichbar über MyDNVGL (my.dnvgl.com)
  - 3 Ebenen: Management, Awareness, Technical
  - Multiple Choice Fragen
- Kostenlos

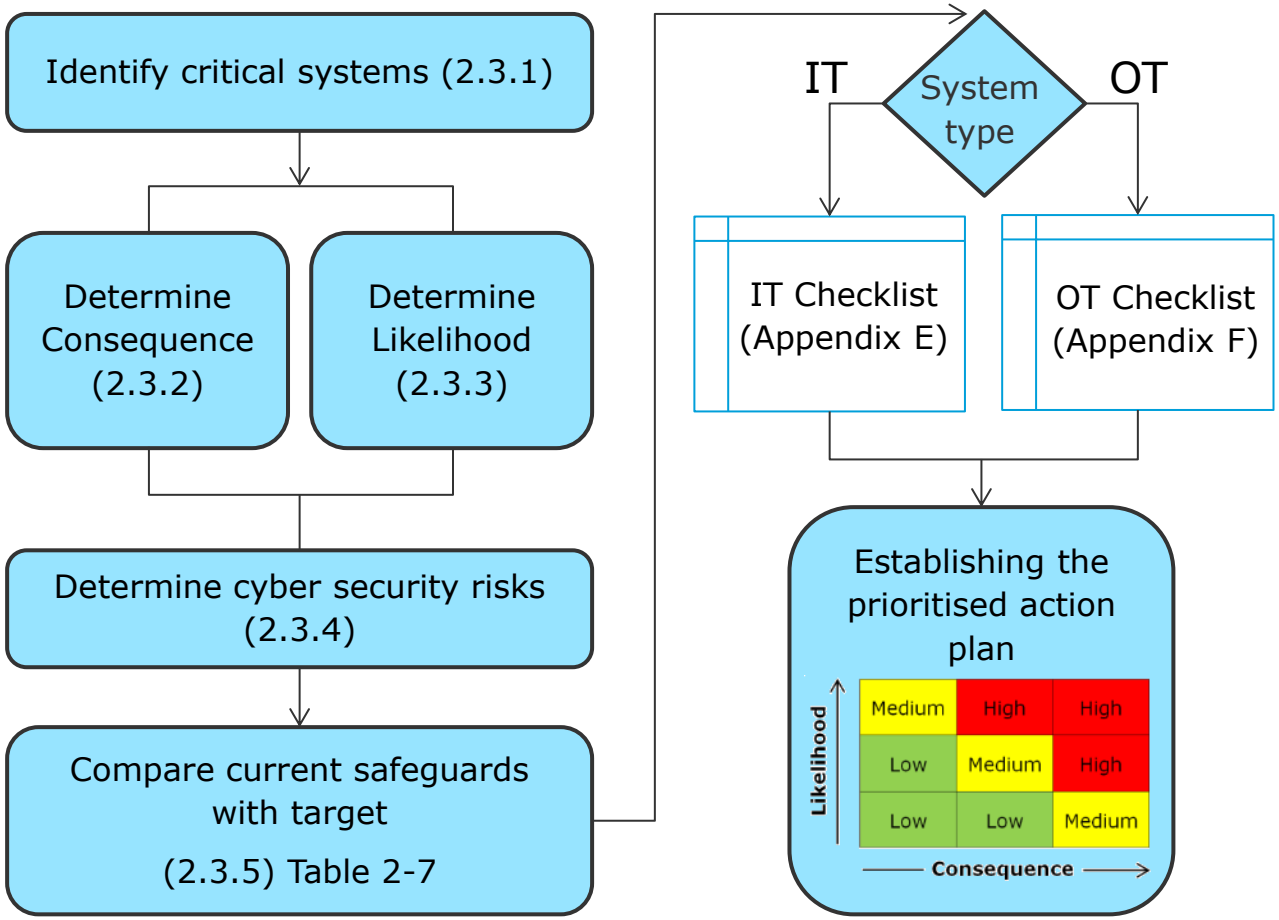


DNVGL-RP-0496: Detaillierter Ansatz

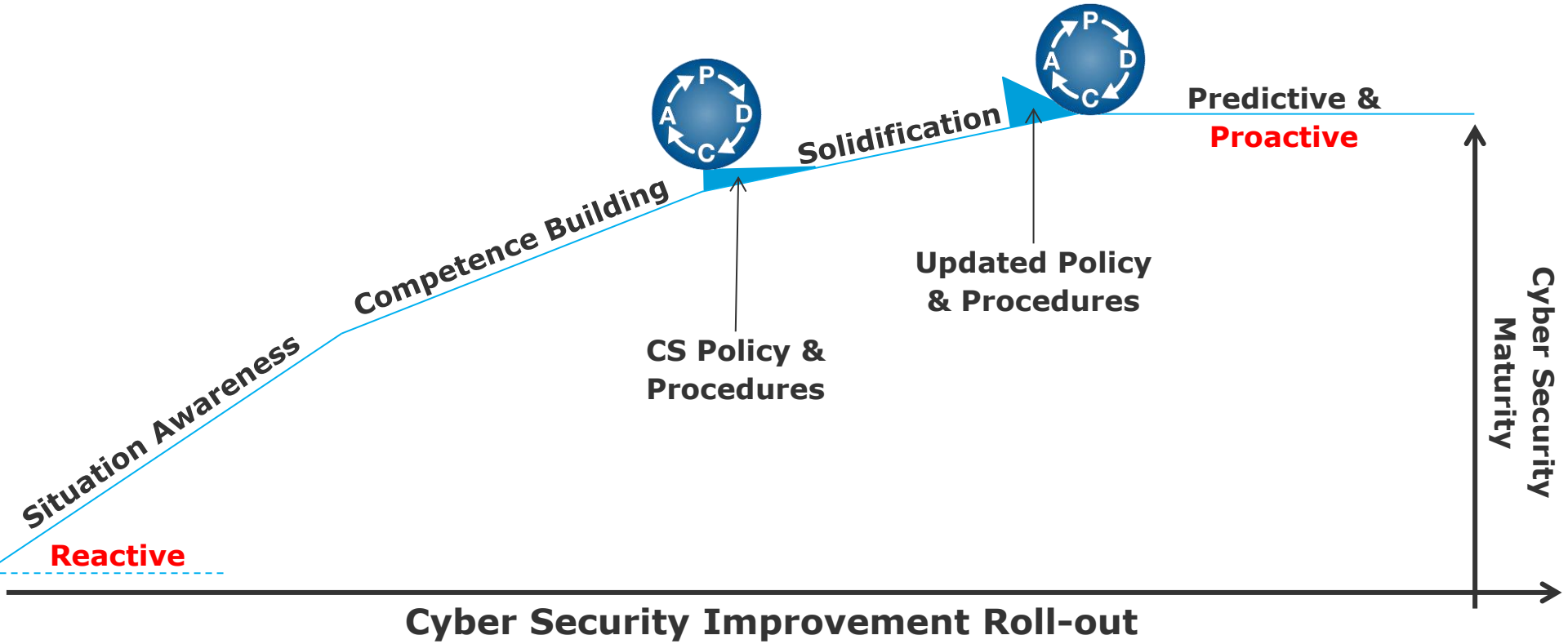


DNVGL-RP-0496: Focused approach

DNVGL-RP-0496: Focused approach

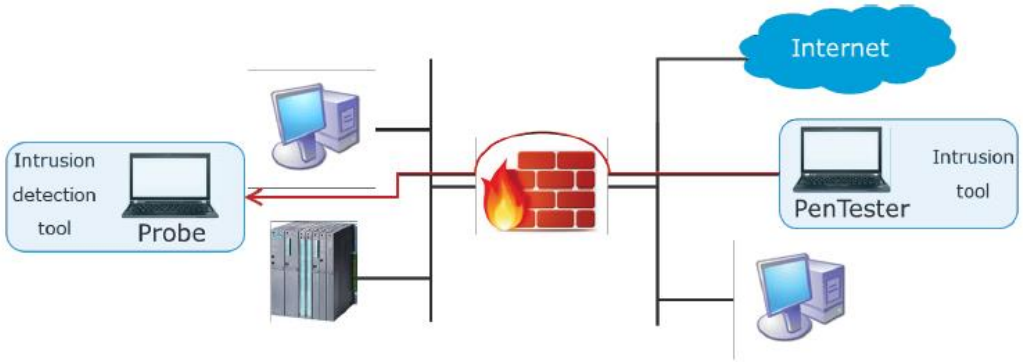


DNVGL-RP-0496: Verbesserungen



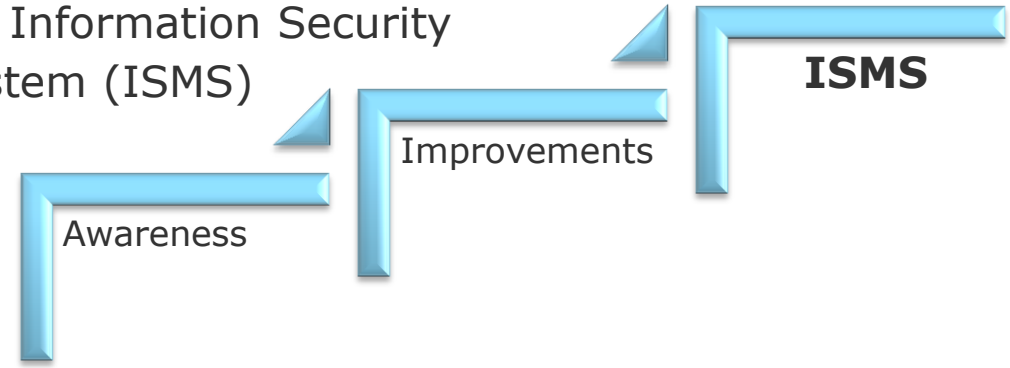
DNVGL-RP-0496: Prüfung

- Prüfung der Effektivität der technischen Barrieren



  - (Simulierte Angriffe): erzwungener Zugang, Suche nach Anomalien, fehlende Patches und veraltete Firmware, Schwächen in der Authentifizierung, gefälschte E-Mails (Phishing), Denial-of-Service-Attacken…

- Überprüfung des Information Security Management System (ISMS)



Ausrichtung unserer Dienstleistungen nach DNVGL-RP-0496

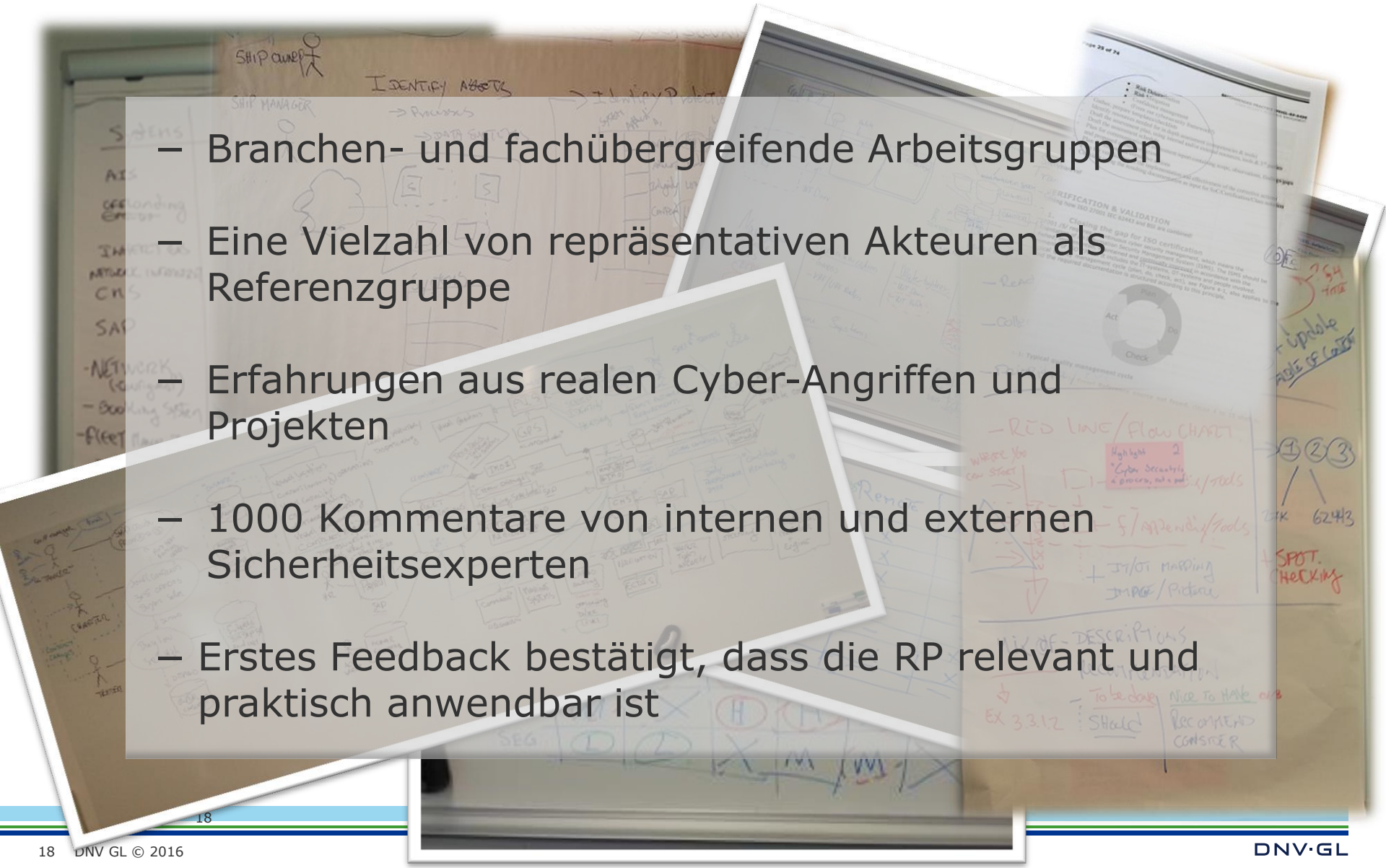
BEWERTUNG	VERBESSERUNG	ÜBERPRÜFUNG
▪ **High-Level Assessment** Identifikation von Hauptrisiken ▪ **Focused Assessment** Methoden des Barrier-Managements für Hochrisikosysteme ▪ **In-depth Assessment** Umfassende Risikobewertung, Vergleich aktueller Schutzmaßnahmen	▪ **Competence & Awareness Building** ▪ **Technical measures** z.B., Zugangskontrolle, Konfigurationsmanagement und Barrier-Management ▪ **Information Security Management System (ISMS)** Dokumentation und Umsetzung	▪ **Monitoring and testing** der technische Barrieren ▪ **Verification of ISMS -** gegen ISO/IEC 27001

DNV GL Services

▪ **Self-Assessment App** ▪ **Focused assessment** ▪ **In-depth assessment**	▪ **E-Learning & Courses** ▪ **Cyber Security Enhancement** ▪ **ISO 27001 Preparedness**	▪ **Security testing** ▪ **ISO 27001 certification**

Wie wurde die RP entwickelt?

Rasche Entwicklung (14 Iterationen in 16 Wochen)



- Branchen- und fachübergreifende Arbeitsgruppen
- Eine Vielzahl von repräsentativen Akteuren als Referenzgruppe
- Erfahrungen aus realen Cyber-Angriffen und Projekten
- 1000 Kommentare von internen und externen Sicherheitsexperten
- Erstes Feedback bestätigt, dass die RP relevant und praktisch anwendbar ist

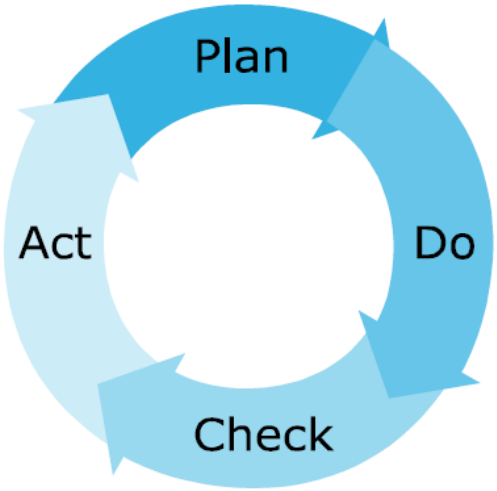
Einen besonderer Dank an...

- ...unseren Kunden und Partnern, die uns mit vielen Informationen versorgt haben:
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Color Line
  - Consolidated Marine Management Inc. (CMM)
  - Farstad Shipping ASA
  - Fred. Olsen Energy
  - Lufthansa Industry Solutions
  - Rickmers Group
  - Royal Caribbean Cruises Ltd. (RCCL)
  - The United States Coast Guard (USCG)
  - Wilhelm Wilhelmsen ASA
  - …..and more

Abschließender Kommentar

Cyber-Security benötigt eine kontinuierliche Anpassung an die sich stets wandelnden Bedrohungen

- ✓ Bewusstsein schaffen
- ✓ Identifikation von zu schützenden Systemen
- ✓ Bewertung der Risiken
- ✓ Entwicklung einer eigenen Sicherheitsstrategie
- ✓ Vergleich der Ist- und Sollzustände
- ✓ Umsetzung sinnvoller Verbesserungen (technisch und organisatorisch)
- ✓ Überprüfung



➢ **Ein lebendes Cyber/Information Security Management System (ISMS) ist unerlässlich, um die Sicherheit heute und in Zukunft sicherzustellen**

Vielen Dank für die Aufmerksamkeit!

Laden Sie die RP kostenlos herunter:
www.dnvgl.com/rpcs

Svante Einarsson
svante.einarsson@dnvgl.com