MEGATUGS
SALVAGE & TOWAGE

How Megatugs prepared in accordance with IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3)

As technology continues developing, Information Technology (IT) and Operational Technology (OT) are being networked together and more frequently connected to the Internet, the need for every organization to protect its information assets and related services is undoubtedly inevitable.

We implemented an **Information Security Strategy and Program** to improve Company's information security posture, aligned with business goals and objectives, manage Cyber Risk and consequently to comply with the IMO 2021 Guidelines.

The need to comply with Guidelines motivated Companies to assess maturity level and improve their Information Security posture

"Goals help set objectives that drive strategy"

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Set a Cyber Information Security Officer (CISO)

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Identified and inventory Assets and related Services

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Asset Classification (Asset value)
- Asset Categorization (IACS UR E22)

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Asset Classification (Asset value)
- Asset Categorization (IACS UR E22)

Hardware Asset Inventory

Last update:		15/12/2020						
No	**Asset Type**	**Location / Dept**	**Asset Owner**	**Model**	**OS/Firmware Updated**	**Network Connection**	**Criticality (CAT I, II. III)**	**C**
1	Router/Firewall	Headquarters	IT	DrayTek 2925	YES	Yes	CAT II	
2	Automatic Identification System (AIS)	All Vessels	Captain of each Vessel		YES	No	CAT I	
3	Global Maritime Distress and Safety Systems (GMDSS)	All Vessels	Captain of each Vessel		YES	No	CAT I	
4	Power management	All Vessels	Captain of each Vessel		N/A	No	CAT II	
5	Integrated control system	All Vessels	Captain of each Vessel		YES	No	CAT II	

System categories based on their effects on system functionality, as defined in IACS UR E22:

CATEGORY I: Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
CATEGORY II: Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
CATEGORY III: Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- GAP and Risk Analysis

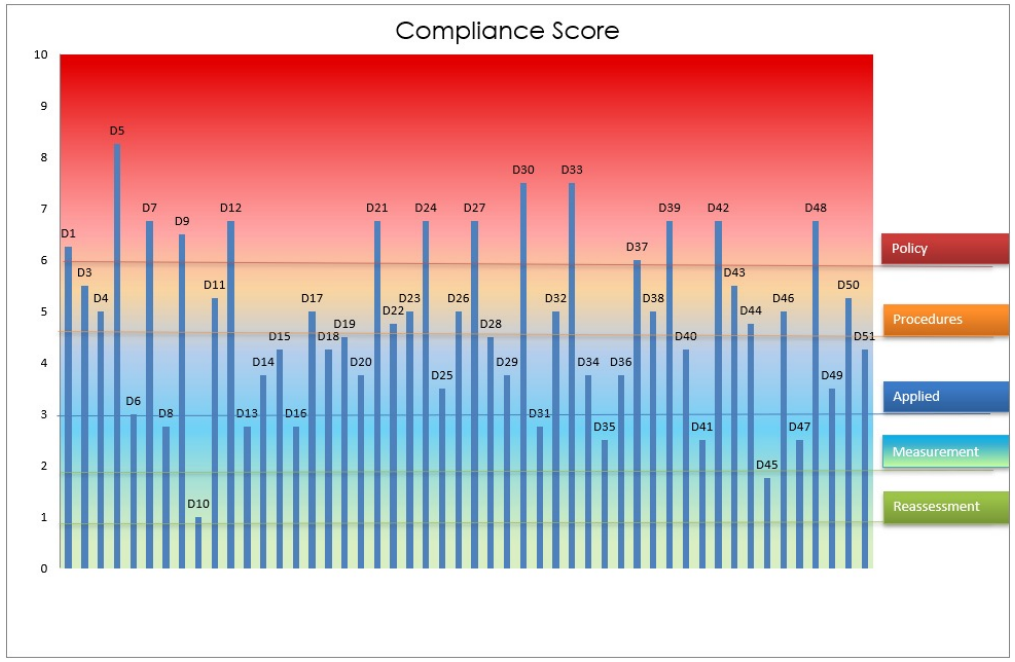
Steps followed both onboard and ashore to implement the Cyber Security Strategy

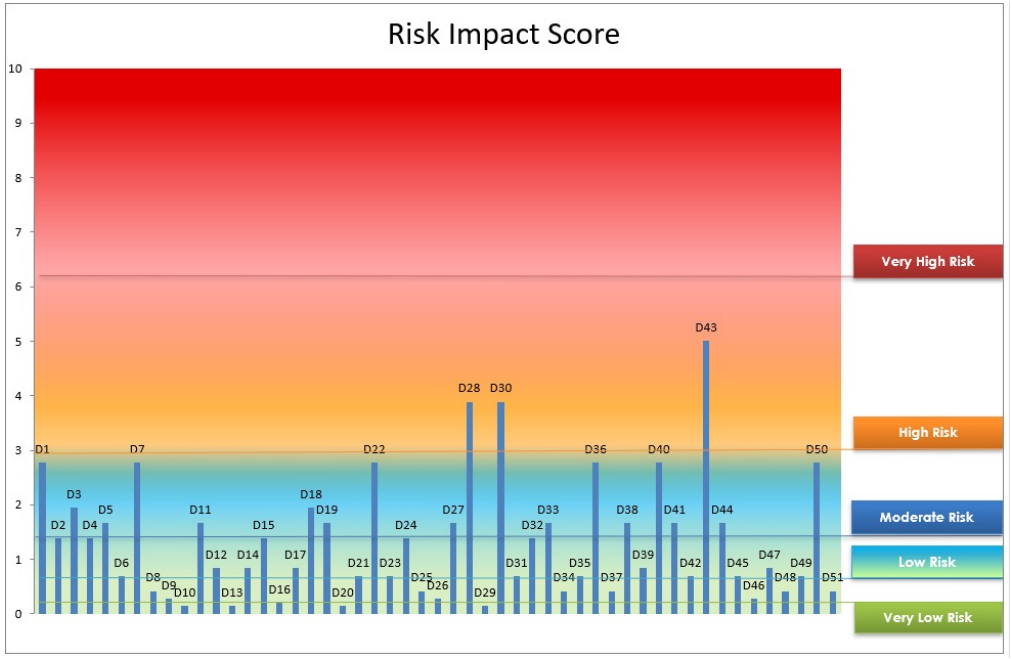
- GAP and Risk Analysis (NIST 800-53 and ISO 27001)

Annex	Code	Control	Ranking						Risk Decisions			
			L.1	L.2	L.3	L.4	L.5					
			Policy	Procedures	Applied	Effectiveness Measurement	Reassessment	Compliance Score	Description of identified risk	Likelihood	Impact	Risk Impact Assessment Score
A.6.1 Organization of Information Security	D3	Establish a management framework that initiates and controls the implementation and operation of information security (It contains 7 controls).	PARTIAL	PARTIAL	PARTIAL	NO	NO	5,5	No formal framework is documented and any undocumented Policies and Procedures are partially applied.	HIGH	MODERATE	1,9
A.6.1.1 Information Security Roles & Responsibilities	D4	All information security responsibilities must be defined and allocated. Information security responsibilities can be general (e.g. protecting information) and/or specific (e.g. the responsibility for granting a particular permission).	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	5	No clear responsibilities are defined	MODERATE	MODERATE	1,4
A.6.2.1 Mobile device policy	D5	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices	NO	PARTIAL	NO	PARTIAL	PARTIAL	8,25	There are few rules concerning mobile devices, although there are not formally documented and has not been communicated to employees. In case of stolen device stolen a security and personal data breach is possible.	LOW	HIGH	1,7
A.6.2.2 Teleworking	D6	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	NO	PARTIAL	YES	PARTIAL	PARTIAL	6,75	No formal Policy exists, a Procedure exists but is not documented and formally communicated to people.	MODERATE	LOW	0,7

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- GAP and Risk Analysis (NIST 800-53 and ISO 27001)





Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Risk and Impact Analysis

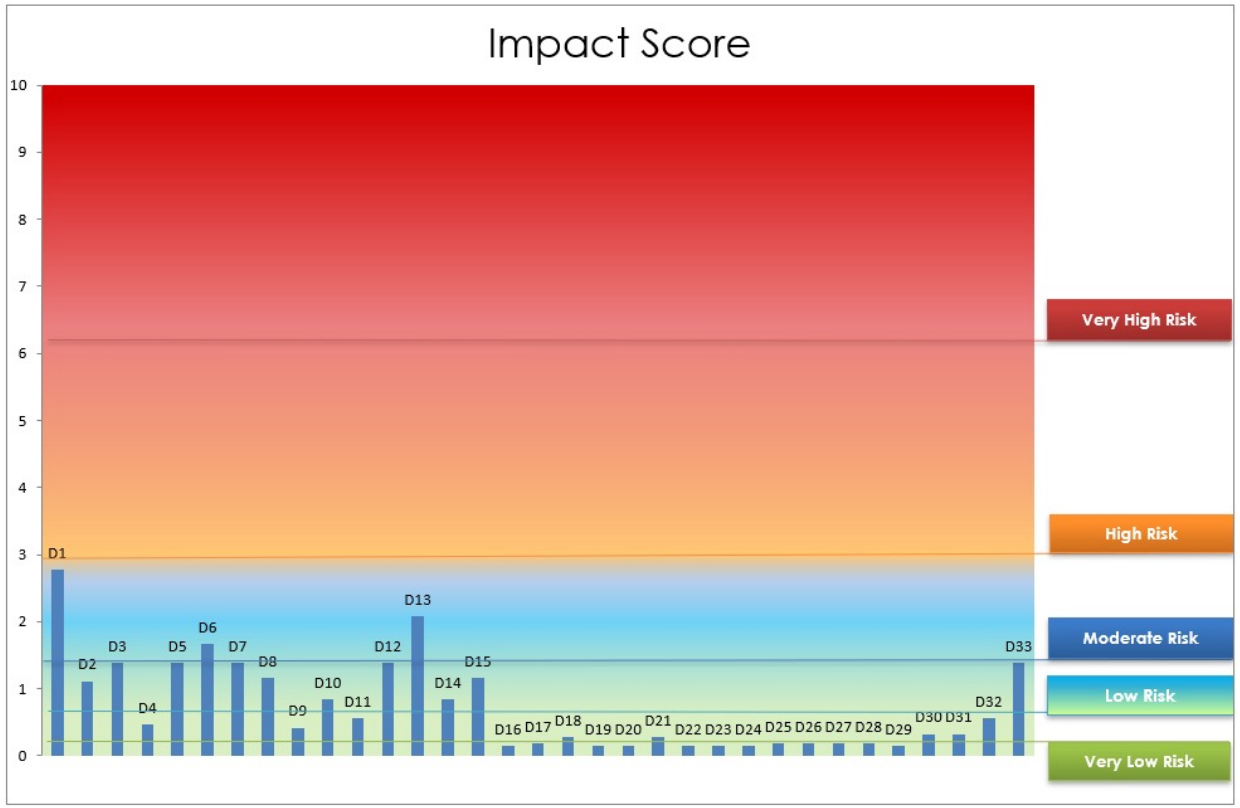
				Vulnerability Impact											
Code	Item	Target / Location	Impact description	Impact probability		Confidentiality		Integrity		Availability		Impact Score	Action(s) performed	Risk Response Strategy	Probability of Recurrence	Residual Risk
D1	Router / Firewall	HQs' Internal Network	Anauthorized access to company's private network. Malicious actors can harm Company's resources (S/W, H/W, data files) and connections.	MODERATE	0.5	HIGH	8	HIGH	8	HIGH	8	2.8	Use of complex password and frequently change and update firmware.	MITIGATE	MODERATE	MODERATE
D2	VPN to Headquarters	Remote users	Track user's online activity and compromise privacy, increase network latency and can directly impact application performance.	LOW	0.3	HIGH	8	MODERATE	4	MODERATE	4	1.1	Use of complex password and frequently change and update firmware. Use of SSH	MITIGATE	VERY LOW	LOW
D3	Switces	HQs' Internal Network	Anauthorized access to company's private network. Malicious actors can harm Company's resources (S/W, H/W, data files) and connections.	MODERATE	0.5	MODERATE	4	MODERATE	4	MODERATE	4	1.4	Use of complex password and frequently change and update firmware.	MITIGATE	VERY LOW	LOW
D4	Wireless Network (WiFi) MT-WiFi	Any WiFi user is located on the corporate network at Headquarters	Data leak or intentionally damage to company's systems.	VERY LOW	0.1	HIGH	8	HIGH	8	MODERATE	4	0.5	Use of complex password and frequently change and update firmware.	MITIGATE	LOW	VERY LOW

CIA Triad

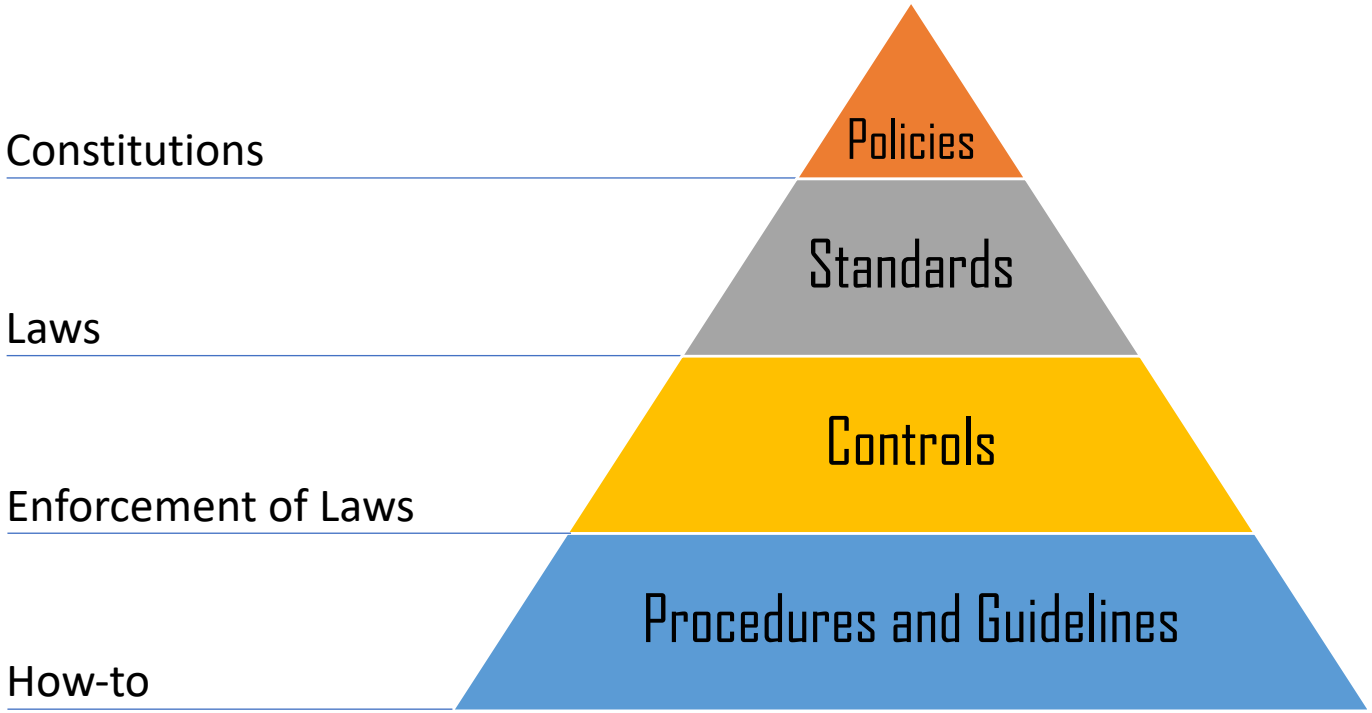
Confidentiality, Integrity and Availability

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Risk and Impact Analysis



Steps followed both onboard and ashore to implement the Cyber Security Strategy



Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Incorporated automated security tool

Steps followed both onboard and ashore to implement the Cyber Security Strategy

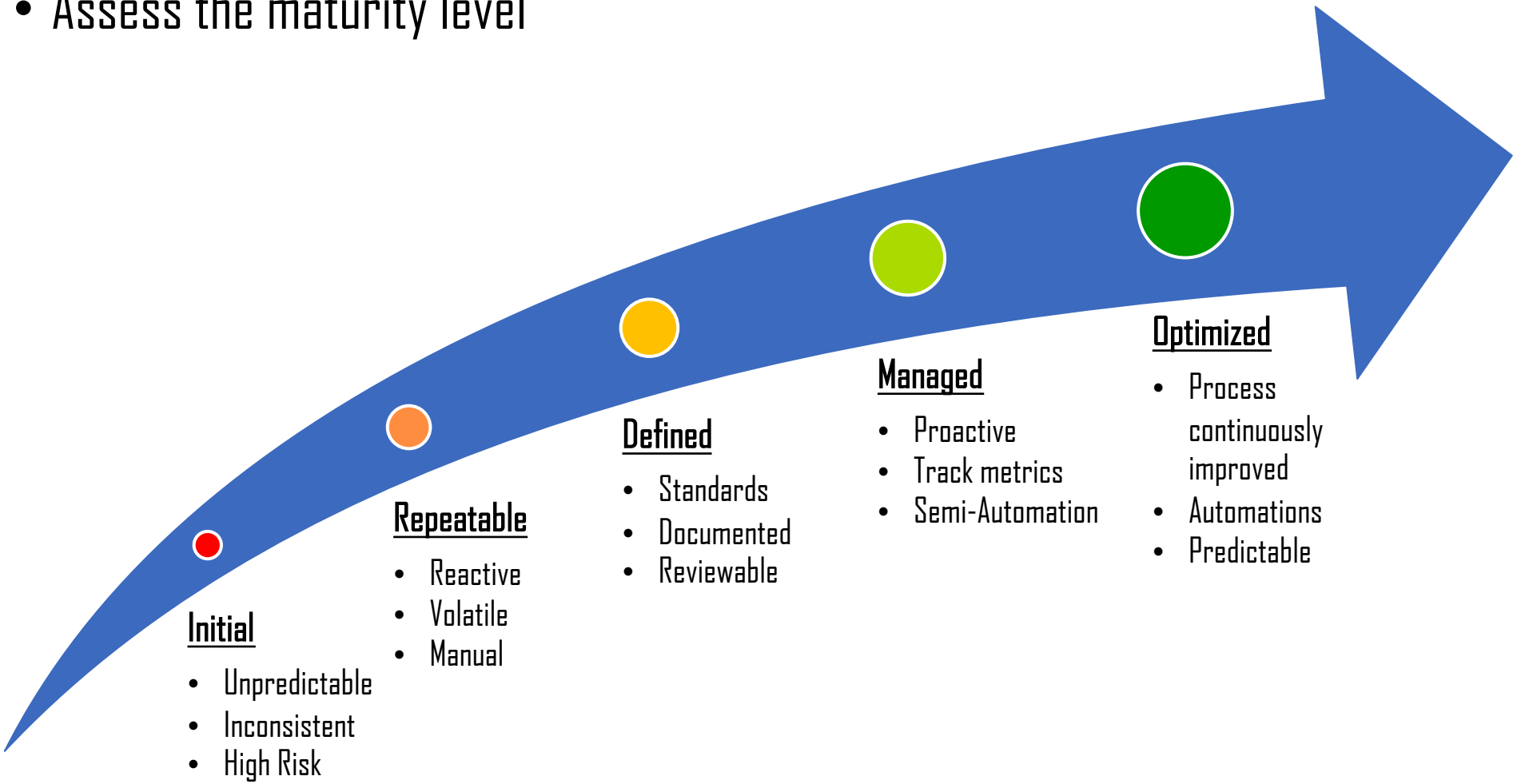
- Established Business Continuity Plan (backups, disaster recovery site, etc)

Steps followed both onboard and ashore to implement the Cyber Security Strategy

- Training and Awareness

Future Plans

- Assess the maturity level



Pitfalls in Strategy Development

- Overconfidence / Optimism
- Anchoring
- Status quo bias
- Mental accounting
- Herding instinct
- False consensus

Recommendations and Tips

1. Align the Strategy with Business Objectives
2. Talk to your people in a way that builds trust and gains buy-in
3. Identify and document all the potential risks
4. Assess the maturity level
5. Training and Awareness (Educate +Train)

Recommendations and Tips

6. Managing Cyber Risk is an ongoing endeavor
7. Perform Third-party risk assessment
8. Subscribe to Cybersecurity updates
9. Key Relationships
10. Event/Incident Management
11. Test as frequently as it is possible the BCP

Thank You!