ID	Business Objective	Risk Scenario	Consequences	Action Party	Business Impact	Likelihood	Severity Impact	Risk Level	Existing Controls	Residual Risk	Treatment Plan	Status of Mitigations Actions	Risk Re-evaluation date	Target Risk
1	IT Security	Data Breach	a) Loss of confidential information b) Reputational damage c) Regulatory fines	IT infrastructure & Services Dept	High	Low	Medium	Medium	a) Database containing sensitive information placed in internal network behind firewalls b) b) 24x7 Monitoring of CII Database logs by MSOC c) Deployed Privileged Identity Management (PIM) tools for CII system access system access d) Limited privileged accounts	Low	a) Deploy Database Activity Monitoring (DAM) solution	a) Implementing of DAM is in progress, target to complete by 3Q 2019	Jul-2020	Low

2	IT Security	Unauthorised changes	a) Unavailability of the CII system b) Sabotage c) Data theft	IT Infrastructure & Services Dept	Medium	Low	Medium	Low	a) PIM tools for CII system access b) Restricted physical access to datacenter room (guarded building, badge access, two factor authentication) c) Hardening systems in IT network d) Limited privileged accounts e) oy anti-virus solution for Linux based CII systems f) *** network security architecture is designed based on multi-layers	Low	a) Deploy Endpoint Detection & Response tools on operator desktops.	a) Implementing of EDR is in progress, target to complete by 3Q 2019	Jul-2020	Low

									defence-in-depth approach. g) It is a controlled environment where network access and endpoint equipment are locked down. h) Deployed application whitelisting on endpoint machines					
3	IT Security	Insider Threat	a) Loss of confidential information	Maritime Cybersecurity Dep	Medium	Low	Medium	Low	a) Small trusted team involved in CII operations b) 4 eyes principle for CII changes c) CCTV monitoring of critical areas	Low	a) Deploy user behavior analytics tools	a) Evaluation of user behavior analytic tools are in progress, target to implement by 1Q 2020	Jul-2020	Low

									d) Staff Training and awareness e) Restricted physical access to datacentre room (guarded building, badge access, two factor authentication)					
4	IT Security	Unauthorised Lateral movement	a) Unavailability of the CII system b) Sabotage c) Loss of confidential information	IT Infrastructure & Services Dept	Medium	Low	Medium	Low	a) Perimeter and internal firewalls with IPS modules deployed b) CII logs piped to SIEM solution for event co-relation and alerts c) 24*7 monitoring by SOC team d) Regular review of	Low	a) Evaluate network anomaly detection tool b) Deploy Endpoint Detection & Response (“EDR”) tools	a) Implementing of EDR is in progress, target to complete by 3Q 2019 b) **** is the midst of i nting network ano ** detection tool for ***	Jul-2020	Low

									CII system logs and firewall reviews					
5	Ensure 24*7 availability of the site	Malware propagation in the network	a) Unavailability of the CII system	IT Infrastructure & Services Dept Sectorial Sys Development Dept	High	Low	Medium	Medium	a) Hardened systems in the IT network. b) Intrusion prevention systems deployed. c) Vulnerability management program for timely discovery of vulnerabilities d) Anti-virus software deployed in environment e) Subscription to threat intelligence sources for malware alerts f) Deploy anti-virus	Low	a) Deploy Next Generation Firewall ("NGFW") b) Migrate **** to AIAS compliant architecture c) Deploy Endpoint Detection & Response (“EDR”) tools	a) NGFW has been completed in 3Q 2019 b) Migration of **** to AIAS compliant architecture is aligned with Infra Revamp project, target to deploy by Q1 2020 c) Implementing of EDR is in progress, target to complete by 3Q 2019	Jul-2020	Low

									solution for Linux based CII systems g) Regular firewall rules review h) It is a controlled environment where network access and endpoint equipment are locked down i) Internet Surfing Separation (ISS) j) Enforcement of authorized authorised USB k) Deployed application whitelisting on endpoint machines					

6	To ensure timely detection and effective handling of all cyber incidents	Cyber Incident Handling	a) Delayed or ineffective response to cyber incidents	a) Maritime Cybersecurity Dept b) Maritime Cybersecurity Dept (lead) Supported By: i. IT Infrastructure & Services Dept, i. Sectoral Sys Development Dept, i. Corporate Communications Dept v. Vessel Traffic Management Dept	Low	Low	Medium	Low	a) Incident response policy in place b) Established CIRT (Cyber Incident Response Team) team c) Crisis communication policy in place d) Developed incident response workflows for common cyber threats e) Annual table top exercise f) Backup and Restoration exercise	Low	a) Periodic checks on outsourced SOC team (creating events which SOC tea calates wit LA) b) Align *** SOC with *** 's internal playbooks	a) Conduct MSOC readiness assessment by 3Q 2020 b) igning of SOC and *** playbook, target to complete by 4Q 2019	Jul-2020	Low
7	Risk Management	Vulnerability & Risk Management	a) Operational inefficiency b) Vulnerability in CII	IT Infrastructure & Services Dept	Low	Low	Medium	Lo	a) IT security policies in place b) Vulnerability management	Low	a) Enhance asset inventory list as per CSA’s CII	a) Updating of asset inventory list as per CSA's CII asset dossier is	Jul-2020	Low

			environment						program in place c) Maintained asset inventory d) Annual risk assessment e) Review risk register f) Perform CII audit		asset dossier	expected to complete by 30 Jun 2019		