



नौवहन महानिदेशालय, मुंबई
DIRECTORATE GENERAL OF SHIPPING, MUMBAI

**Information Security Steering Committee Charter
for
Directorate General of Shipping
administratively controlled by the Ministry of Ports,
Shipping and Waterways, Govt. of India.**

DIRECTORATE GENERAL OF SHIPPING, MUMBAI

Postal Address: 9th Floor Beta Building, I-Think Techno Campus, Kanjurmarg (East), Mumbai -
400 042 (India)

E-Mail: dgship-dgs[at]nic[dot]in
Tel. No.: 91-22-25752040/41/42/43/45
(From 9:30 A.M. to 6:00 P.M.)

Table of Contents

1.0	Directorate General of Shipping Information Security Committee Charter.....	3
1.	Committee Purpose.....	3
2.0	Organization and Membership.....	3
3.0	Committee Hierarchy.....	5
4.0	Responsibilities and Duties.....	5
1.	Strategic Oversight.....	5
2.	Policy Governance.....	5
3.	Risk Governance.....	6
4.	Information Security Practices for Protected Systems.....	6
5.	Monitoring and Reporting.....	7
5.0	Application wise Accountability.....	8
6.0	Committee Procedures and Agendas.....	9
1.	ISSC Procedures.....	9
2.	Meeting Agenda & Frequency.....	9
3.	SIPOC Models.....	10
4.	Risk Champions.....	11

1.0 Directorate General of Shipping Information Security Committee Charter

1. Committee Purpose

The purpose of the Information Security Steering Committee (the "Committee") is to act on the behalf of, and assist, the Executive Management of Directorate General of Shipping in fulfilling its oversight responsibilities with respect to the organization's information security programs and risks, including:

- Overseeing and reviewing the organization's internal controls (e.g. Conformity to NIST Cyber Security Framework/ DPDP Act etc) to protect and ensure the confidentiality, integrity & availability of information assets.
- Governing the practices, procedures, and controls management used to identify, assess, and manage key information security programs and risks.
- Ensuring the effectiveness of the organization's risk governance structure, policies, and risk tolerances in enabling the achievement of business objectives.
- Providing strategic direction and prioritization of cybersecurity investments, including technology upgrades, audits, training, and compliance initiatives.
- Facilitating cross-departmental coordination, especially between IT, legal, operations, and compliance, to ensure a unified cybersecurity posture.
- Monitoring compliance with national regulatory requirements, including CERT-In advisories, GIGW guidelines, and Certifications like - STQC mandates (as applicable) for all the applications. (Refer Annexure 1.)

The Committee fulfills these responsibilities by carrying out the activities enumerated under the heading *Responsibilities and Duties* in this Charter. In carrying out its responsibilities, the Committee has the authority to

- (i) wholly investigate any matter brought to its attention that may impact the organization's ability to ensure adequately the protection of the organization's information assets, and
- (ii) to involve current members of the Committee, Board, other steering committees, government agencies, and law enforcement, as determined appropriate by the circumstances.

2.0 Organization and Membership

The Committee shall appoint Committee members, fill vacancies occurring on the Committee, and designate the Chair of the Committee.

The Committee shall consist of 8 members from the security leadership team, with broad representation from organizational personnel with backgrounds representing the organizational interests and with the capacity to address decision-making matters within the scope of the Committee's authorities. Additionally, the Committee may invite to its meetings any relevant parties it deems appropriate to sufficiently carry out its responsibilities. The Committee may form and delegate authority to subcommittees when appropriate and met with consensus from Committee membership.

In its current form, Committee membership shall be comprised of the following individual members:

Job Role	Department/Wing/Branch	Individual
Chief Information Security Officer*	IT & e-Governance	Shri Deepender Singh Bisen
Additional Director General of Shipping	Administration Wing	Shri. Sushil Mansing Khopde
Chief Surveyor -cum- Additional Director General (Engineering)	Engineering Wing	Shri Ajithkumar Sukumaran
Nautical Advisor –cum- Additional Director General (Nautical)	Nautical Wing	Capt. S.I. Abul Kalam Azad
Chief Ship Surveyor	Naval Architecture Wing	Shri. Pradeep Sudhakar K.
Deputy Director General of Shipping	Merchant Shipping Law Branch	Shri. Ash Mohomad
Nautical Surveyor-cum-DDG (Tech.)	Crew Branch	Capt. P.C. Meena
Assistant Director General of Shipping	IT & e-Governance Branch	Shri. Jitendra Jadhav
Assistant Director General of Shipping	Training Branch	Major Anutosh Singh
Executive Officer	Personnel Branch	Shri P.L. Muthu
Deputy Director General of Shipping	Administration Branch	Dr. Sudhir Kohakade

Table 1

*Designates Current Chair of the Committee

3.0 Committee Hierarchy

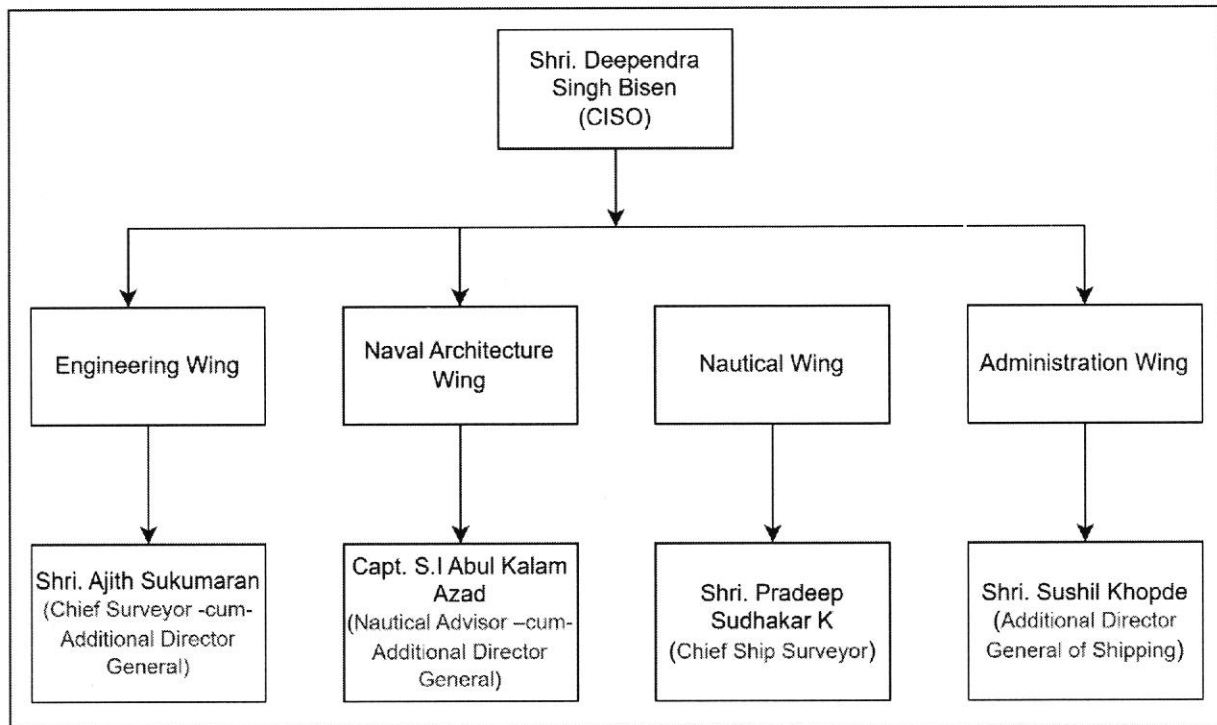


Figure 1

4.0 Responsibilities and Duties

The Committee shall be responsible for the following:

1. Strategic Oversight

- Provide oversight and ensure alignment between information security strategy and organizational objectives.
- Assess the adequacy of resources and funding to sustain and advance successful security programs and practices for identifying, assessing, and mitigating cybersecurity risks across all business functions.
- Review control audit reports and resulting remediation plans to ensure business alignment
- Review the organization's cyber insurance policies to ensure appropriate coverage.
- Provide recommendations, based on security best practices, for significant technology investments.

2. Policy Governance

- Review policy-exception requests to determine if potential security risks can be accepted or if a workaround exists.
- Assess the ramifications of updates to policies and standards.

- c. Establish standards and procedures for escalating significant security incidents to the board, other steering committees, government agencies, and law enforcement, as appropriate.

3. Risk Governance

- a. Review and approve the company's information risk governance structure.
- b. Assess the company's high-risk information assets and coordinate planning to address information privacy and security needs.
- c. Provide input to executive management regarding the enterprise's information security risk tolerance.
- d. Review the company's cyber-response preparedness, incident response plans, and disaster recovery capabilities as applicable to the organization's information security strategy.
- e. Promote an open discussion regarding information risk and integrate information risk management into the enterprise's objectives.

4. Information Security Practices for Protected Systems

- a. All the Information Security Policies of the "Protected System" shall be approved by Information Security Steering Committee.
- b. Significant changes in network configuration impacting "Protected System" shall be approved by the Information Security Steering Committee.
- c. Each significant change in application(s) of the "Protected System" shall be approved by Information Security Steering Committee.
- d. A mechanism shall be established for timely communication of cyber incident(s) related to "Protected System" to Information Security Steering Committee.
- e. A mechanism shall be established to share the results of all information security audits and compliance of "Protected System" to Information Security Steering Committee.
- f. Assessment for validation of "Protected System" after every two years.
- g. Plan, establish, implement, operate, monitor, review, maintain and continually improve Information Security Management System (ISMS) of the "Protected System" as per latest "Guidelines for Protection of Critical Information Infrastructure" released by the National Critical Information Infrastructure Protection Centre or an industry accepted standard duly approved by the said National Critical Information Infrastructure Protection Centre.
- h. Ensure that the network architecture of "Protected System" shall be documented. Further, the organisation shall ensure that the "Protected System" is stable, resilient and scalable as per latest National Critical Information Infrastructure Protection Centre "Guidelines for Protection of Critical Information Infrastructure". Any changes to network architecture shall be documented.
- i. Plan, develop, maintain the documentation of authorized personnel having access to "Protected System" and the same shall be reviewed at least once a year, or whenever required, or according to the Information Security Management System (ISMS).
- j. Plan, develop, maintain and review the documents of inventory of hardware and software related to "Protected System"

- k. Ensure that Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of "Protected System" shall be carried out at least once a year. Further, Vulnerability/Threat/Risk (V/T/R) Analysis shall be initiated whenever there is significant change or upgrade in the system, under intimation to Information Security Steering Committee
- l. Plan, establish, implement, operate, monitor, review, and continually improve Cyber Crisis Management Plan (CCMP) in close coordination with National Critical Information Infrastructure Protection Centre; ensure conduct of internal and external Information Security audits periodically according to Information Security Management System (ISMS) as suggested in clause (b). The Standard Operating Procedure (SOP) released by National Critical Information Infrastructure Protection Centre (NCIIPC) for "Auditing of CIIs/Protected Systems by Private/Government Organization" shall be strictly followed
- m. Plan, develop, maintain and review documented process for IT Security Service Level Agreements (SLAs). The same shall be strictly followed while designing the Service Level Agreements with service providers
- n. Establish a Cyber Security Operation Center (C-SOC) using tools and technologies to implement preventive, detective and corrective controls to secure against advanced and emerging cyber threats. In addition, Cyber Security Operation Center is to be utilized for identifying unauthorized access to "Protected System", and unusual and malicious activities on the "Protected System", by analyzing the logs on regular basis. The records of unauthorized access, unusual and malicious activity, if any, shall be documented
- o. Establish a Network Operation Center (NOC) using tools and techniques to manage control and monitor the network(s) of "Protected System" for ensuring continuous network availability and performance
- p. Plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting "Protected System" and the logs shall be handled as per the Information Security Management System (ISMS).

5. Monitoring and Reporting

- a. Receive Monthly Cybersecurity Compliance reports from Risk Champions and coordinate with committee on the metrics used to measure, monitor, and manage cyber risks posed to the company and to review the monthly reports on selected security risk topics as the committee deems appropriate.
- b. Monitor and evaluate the quality and effectiveness of the company's technology security, capabilities for disaster recovery, data protection, cyber threat detection, and cyber incident response, and management of technology-related compliance risks.
- c. Reporting the Conformity status of the existing and newly-onboarded vendors to Data Standards, NIST Cyber Security Framework, DPDP Act, ISO 27001, ENISA, NCIIPC, MeiTY Guidelines etc wherever applicable

5.0 Application wise Accountability

Name of Department/Branch	Name of Application	Designation Accountable	Module Name
Engineering Wing	Exit Exam	Chief Surveyor	Training & Exam Reform Initiative
	MEO Class 4 COC examination		
Nautical Wing	Long Range Identification & Tracking	Chief Ship Surveyor	LRIT
Crew Branch	BSID	Nautical Surveyor	Shipping Master Office
	Sea Fearer's Welfare Fund Society		Autonomous Bodies
	Seamen's Provident Fund Organization		
Engineering Wing	Swacchh Sagar Module - Port Reception Facility	Chief Surveyor	Swacchh Sagar
	Swacchh Sagar Module - Ballast Water Management		
	Swacchh Sagar Module - Bunker Supplier Information System		
	Swacchh Sagar Module - Single Use Plastic		
	RO Audit		Survey & Certification
	PRF Audit		
	Flag State Inspection		
IT & E-Governance	e-Governance	Assistant Director General of Shipping	e-Governance Application
	E-office		Office Purpose Applications
	NIC Mail egov		
Naval Architecture	SBFA	Nautical Advisor	
Training Branch	ADU Learning	Assistant Director General of Shipping	Training Module
	BES Ratings Exam		
	Centralized Automated Attendance System		
Personnel Branch	NIC Sparrow	Executive Officer	HR Applications
	e-HRMS		
Admin Branch	Visitor Attendance Management System	Deputy Director General	Office Purpose Application

Table 2

6.0 Committee Procedures and Agendas

1. ISSC Procedures

1. The Information Security Steering Committee meetings will be held on the last Thursday of each quarter.
2. The CISO will serve as the chair of the Information Security Steering Committee.
3. Documentation for the meeting will be submitted Tuesday at 5pm (**one week prior to the meeting**) to the IT & E-Governance Branch Team and will be sent on the file.
4. The agenda and documentation will be sent out by the CISO **one week prior to the meeting**.
5. Participants will be expected to have **read and reviewed all documentation prior to the meeting** and should be prepared with questions to be asked during the meeting.
6. Decisions within the meeting will be made through **consensus**.
7. Minutes will be captured by IT & E-Governance Branch Team during the meeting and shall be sent on the file.
8. Attendance will be taken at the meeting and, if the participant is unable to attend, regrets must be sent prior to the meeting and an alternate from the department must be identified. Absent participants will be expected to read the meeting minutes and are bound by decisions made in the meeting, notwithstanding extenuating circumstances.
9. The committee may establish **task forces or subcommittees** to focus on a particular business process, technology, or emerging issues as deemed necessary.

2. Meeting Agenda & Frequency

Agenda Item	Frequency	Time Allotment	Accountable Party
Security Strategy Presentation	Quarterly	30 minutes	CISO
Review Security Performance Metrics & Improvement Recommendations <ul style="list-style-type: none">• Security Risk Metrics Report• Monthly Cybersecurity Compliance Reports• Security Project Metrics Report• Security Service Metrics Report• Security Policy Metrics Support• Information Lifecycle Metrics Report	Quarterly	30 minutes	CISO

Portfolio Review <ul style="list-style-type: none"> Review capital planning and adequacy of resourcing Monitor and report on project status and outcomes Approve prioritized list of projects Evaluate and select projects to endorse for funding Approve standards and policies for resource allocation 	Quarterly	50 minutes	CISO + Risk Champions
Policy Management <ul style="list-style-type: none"> Review privacy and information security policies and standards and review the ramifications of updates to policies and standards 	Quarterly	20 minutes (as needed)	CISO
Risk Management <ul style="list-style-type: none"> Review prioritized list of risks and mitigation strategies Approve plans for new or changed security service requirements 	Quarterly	10 minutes (as needed)	Risk Champion
Information Lifecycle <ul style="list-style-type: none"> Review information lifecycle process ownership 	Quarterly	10 minutes	Wing Head
New Business	Quarterly	20 minutes	Wing Head

3. SIPOC Models

Supplier	Input	Process (Governance Responsibility)	Output	Customer
CISO	<ul style="list-style-type: none"> Security Strategy and Roadmap 	Provide oversight and ensure alignment between information security strategy and organizational objectives.	<ul style="list-style-type: none"> Approval of strategic direction and roadmap for FY25-26 Rejection of strategic direction and roadmap for FY24-25 Request for additional information 	Wing/Branch/Division Heads

CISO	<ul style="list-style-type: none"> Security Budget Plan 	Assess the adequacy of resources and funding to sustain and advance successful security programs and practices for identifying, assessing, and mitigating cybersecurity risks across all business functions.	<ul style="list-style-type: none"> Signed endorsement of the security budget Request for additional information Recommendation for changes to the security budget 	Wing/Branch/Division Heads
CISO	<ul style="list-style-type: none"> Security Controls Documentation ISMS Documentation Improvement Recommendations 	Review controls to prevent, detect, and respond to cyberattacks or information or data breaches involving electronic information, intellectual property, data, or connected devices.	<ul style="list-style-type: none"> Approval of security control objectives and documentation Launch corrective task force Accept recommendations 	Wing/Branch/Division Heads

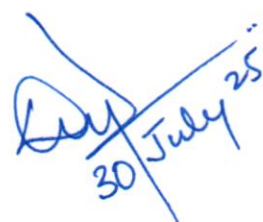
4. Risk Champions

The risk champions for each Project/Module/Initiative will be designated by the Branch/Wing/Department Head.

They will be performing the below responsibilities:

1. Monthly reporting of the Cyber Security Compliance Report

This issues with the approval of the Director General of Shipping, Mumbai.



(Deependra Singh Bisen)

Dy. Director General of Shipping (IT & e-Gov)
Directorate General of Shipping, Mumbai.