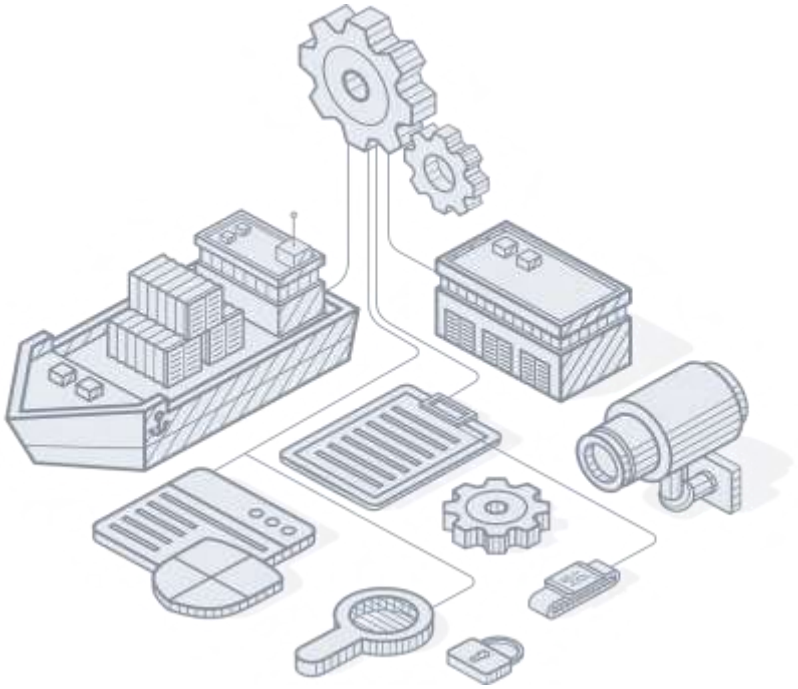
ASTAARA
RISK MANAGEMENT

Astaara Risk Management



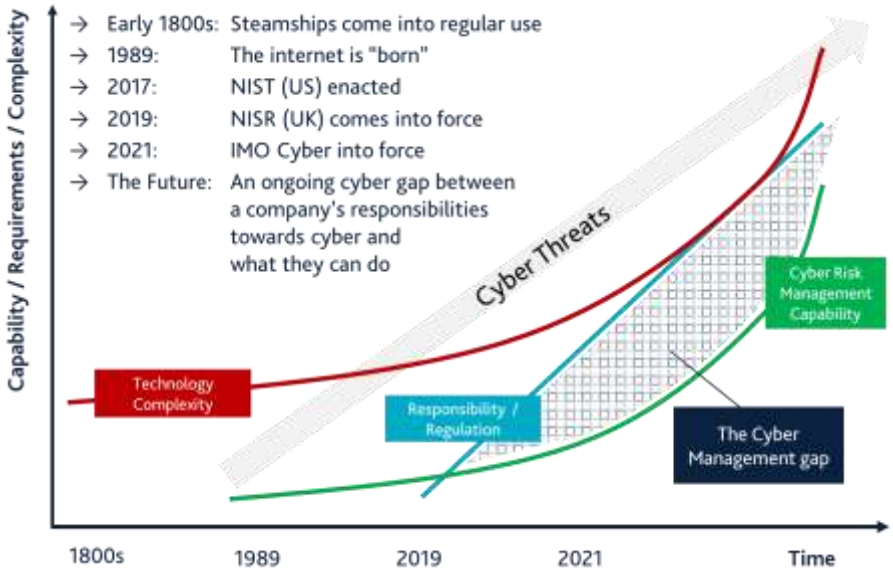
Services and Capabilities: an introductory guide

1 An introduction

Welcome to the introductory guide to Astaara Risk Management (ARM) and its services and capabilities.

Astaara Company Limited (Astaara) was founded with the aim of supporting the maritime industry in minimising the operational and financial disruption caused by cyber-attacks on your business. We know that it is a case of when, not if, your business will suffer a cyber-attack.

Unfortunately, it does not matter how high and how thick you build your defensive walls there will always be a way through. We also know that the cyber threat landscape is constantly evolving and the regulatory requirements you are subject to are increasing. Standing still is not an option. We would like to be your partner in navigating these choppy waters and close the cyber management gap to fit within your corporate risk appetite.



This introductory guide focuses on services and capabilities of ARM which are designed to reduce the impact of a cyber-attack on your business and to speed up your operational recovery after a cyber-attack – and as a result materially reducing the financial impact to your business.

1.1 What is ARM?

We define ARM as a supra-consulting business who works with you, our clients, to provide a bespoke approach to improving your cyber security posture. We seek to understand your business before we start delivering our services to make sure the approach is appropriate for your business.

We do this by offering a range of services and capabilities that provide maritime companies with the ability to improve their cyber security posture and an insurance solution, AstaaraCyber, that allows risk transfer to take place.

What differentiates Astaara from other cyber consultancies is:

- We understand what the costs to a business are following a cyber-attack as we underwrite these risks and therefore know the disruption and associated costs to the business of an attack

What differentiates Astaara from other cyber insurers is:

- We seek to prevent and minimise losses before they happen by providing pre-breach consultancy and advice and maintaining regular contact with you during the policy period

1.2 How does ARM work with you?

ARM can enhance your cyber security posture and keep you evolving as the cyber threat changes.

We recognise that you will most likely have already taken considerable steps in this area and probably already have services provided to support you. Managing the cyber threat is a whole enterprise matter, and in the world of digitisation affects shoreside and shipping operations.

Our services and capabilities wrap around and fill in where there are gaps to provide comfort to your stakeholders and take you to the benchmark standard:

Stakeholders >>>	Expectations >>>	First Base >>>	Benchmark
Shareholders	Statute / Regulation	Understanding & Managing cyber exposure	Security of Systems & Facilities
Board of Directors	Ability to operate	Identifying Cyber Incidents	Incident Handling Capability
Investors / Financiers	Accreditations	Defence & Response	Business Continuity Management
Customers	Value maintenance	Business Continuity & Reporting	Monitoring Auditing & Testing
Employees	Minimise threats / Maximise opportunity		Compliance With International Standards
Regulators	Robust plans (designed & tested)		
Government	Response to vulnerabilities		

ARM will help you become a smaller target by minimising risk aggravators and enhancing risk mitigators.

Cyber Risk Management is about Resilience and Recovery and always needs to be worked on:

- **Understand your relationships:** know your vulnerabilities and dependencies
- **Resilience:** be a small and difficult target
- **Recovery:** minimise disruption and get back up and running

In summary ARM provides you with a holistic approach to managing the cyber risk you face.

2 Overview of offering

ARM provides a broad offering of cyber security services that are designed to improve your cyber security posture. As the cyber landscape is constantly evolving, we would like the opportunity to work with you on an ongoing basis. This approach will allow you to benefit from:

- a consistency of advice
- the development of trust between you and us
- accessing market leading intelligence on how best to tackle the cyber security risk you face

2.1 The Astaara Cyber Maturity Model

An integral part of the Astaara offering is the Astaara Cyber Maturity Model. This allows us to assess your business against the key cyber security regimes:

- The US NIST Cybersecurity Framework (NIST)
- The EU Network Information Systems Directive (NISD) and local interpretations
- The UK Network Information Systems Regulations (NISR)
- The UK Cyber Assessment Framework (CAF)
- The UK Cyber Essential Plus certification scheme
- IMO/ISPS cyber guidelines

Our proprietary model provides you with external assurance of where you are with regards to the various cyber regulations and regimes that are in-force where you operate.

Our model not only says whether you pass, or not, the specific requirement: It tells you how well you have performed. This gives you a much more informed position of where you are, and importantly identifies where improvements are most required.

2.2 The Initial Review

We recognise that each business is different: different operational demands; different approaches to tackling similar problems.

Therefore, before we provide a service to you, we undertake an Initial Review. This allows us to understand your business and your current approach to cyber security – importantly the review enables us to tailor the offering to your business and how we can most effectively work with you.

The Initial Review involves the completion of our Scoping Questionnaire. We will also undertake interviews with key personnel involved in your cyber security to assist with the completion of the Scoping Questionnaire.

2.3 The Capability Grid

Each of these services is available on a standalone basis or as part of a wider package. The design and delivery of many of the services is bespoke to you: to represent your particular requirements and the different levels of complexity and scale different businesses are and the budgets that are available.

The following Capability Grid provides details of what we offer, our aim and specific aspects.

Capabilities	Our aim	Specific aspects
Vulnerability review / Penetration test ("Pen Test")	To enable you to understand how effective your cyber defences are working	• Identify weakness to allow remedial action to be taken to improve • Improved protection against cyber-attacks
Policy & procedure documentation assessment	We aim provide assurance to you that you have the appropriate policies and procedures to enable your business to manage the cyber risk	• Identify the required policies and procedures to enable an effective cyber security design posture • Identify improvements to enhance your policies & procedures
Training (design & delivery)	People are any organisations greatest asset and potentially their greatest vulnerability. We aim to provide tailored cyber training advice from Board level downwards.	• Reduction in risk to the business • Significant improvement in the understanding of cyber in the entire workforce and therefore increase in their productivity and efficiency.
Managed service proposition (e.g. Security Operations Centre / Network Monitoring)	To enable you to effectively outsource cyber services where appropriate.	• Analysis of your service needs and advice on whether to meet within your own resources or outsource. • Provide you with a solution that provides value for money and meets your specific business needs.
Business Continuity Plans (BCP) / Disaster Recovery Plans (DRP)	In the event of a serious cyber incident you need to be able to maintain your vital business processes.	• BCP and Disaster Recovery planning. • Significant reduction in business disruption.
Cyber Enterprise Risk Management (C-ERM) / Cyber Risk Appetite	To enable you to effectively identify and manage cyber risk.	• Help you identify cyber risk and implement a dynamic risk management process. • Ensure you are deploying resources in the most effective and cost-efficient manner.
Leadership / Governance & Culture	To ensure you have effective cyber policies in place that promote a company-wide cyber security culture.	• Help you to establish a culture that recognises cyber security as a core function that is relevant to all aspects of the business. • Ensure you preserve the best of your existing culture.
Cyber Strategy	To enable you to develop, articulate and implement your cyber security strategy.	• Help you to design an effective cyber security strategy that is tailored to your company's specific needs. • Advise on how best to implement your selected strategy
Cybermetrics: Performance and Analysis	To provide you with the metrics you require to enable you dynamically measure and analyse your cyber risk profile.	• Enable you to continuously assess and improve your cyber security posture. • Ensure that resources are being applied in the most cost-efficient manner.
Dependency Management	To provide you with the confidence that your exposure to risk related to a cyber-attack on your key suppliers is minimised.	• Minimise the disruption to your business in the event of a failure in your key suppliers. • Ensure that you have processes in place for alternative means of supply and you are compensated for downtime.

In addition, we normally include within our offering the following where you would like to take advantage of an ongoing relationship with ARM.

Capabilities	Our aim
Quarterly reviews	To provide you with a regular catch-up on the development of your cyber security posture to enable it to remain focused
Affirmative cyber insurance benchmark review	To provide you with assurance that you are buying the right insurance cover appropriate for your business against AstaaraCyber – an affirmative cyber insurance policy designed for the maritime industry

Each of these offerings is available on a standalone basis or as a combination or all. We review the offerings

3 Specific products

In addition, ARM has developed the following products that bring together different elements of the ARM offering. Currently, these products are:

- **CyberStaart** – an introductory review which incorporates an Initial Review, a Vulnerability Review and a high-level review of your policies and procedures
- **Regulatory Reviews** – an external review provided by ARM of how your company's cyber security performs against the regulatory environment you operate within
    - **IMO** (International Maritime Organisation) Cyber Guidelines for SMS audits
    - **ISPS** (International Ship and Port Facility Security Code) Cyber Guidelines for ports & terminals
    - **NISD/NISR/NIST** for companies that are Operators of Essential Services or Critical State Infrastructure
    - **DORA** (Digital Operational Resilience Act) the (proposed) EU cyber requirements for financial services domiciled in the EU

  NB: All our regulatory reviews are tailored to the local jurisdiction and where your company operates
- **Astaara Dynamic Risk Management** – the co-ordinated delivery of a range of services that will improve your cyber security posture and provide improved assurance to your stakeholders

These products benefit from different elements of the services we provide from the Capability Grid.