Introducing AstaaraCyber

#ResilienceandRecovery

KEY CONTACTS

Robert Dorey
Chief Executive
Officer

James Cooper
Group Managing
Director

William Egerton
Chief Cyber
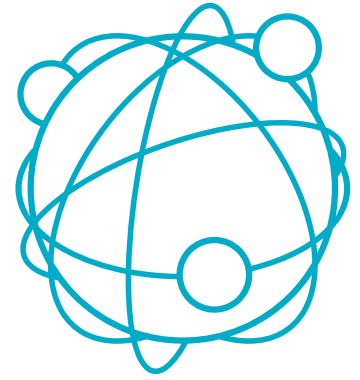Officer

Tom Graham
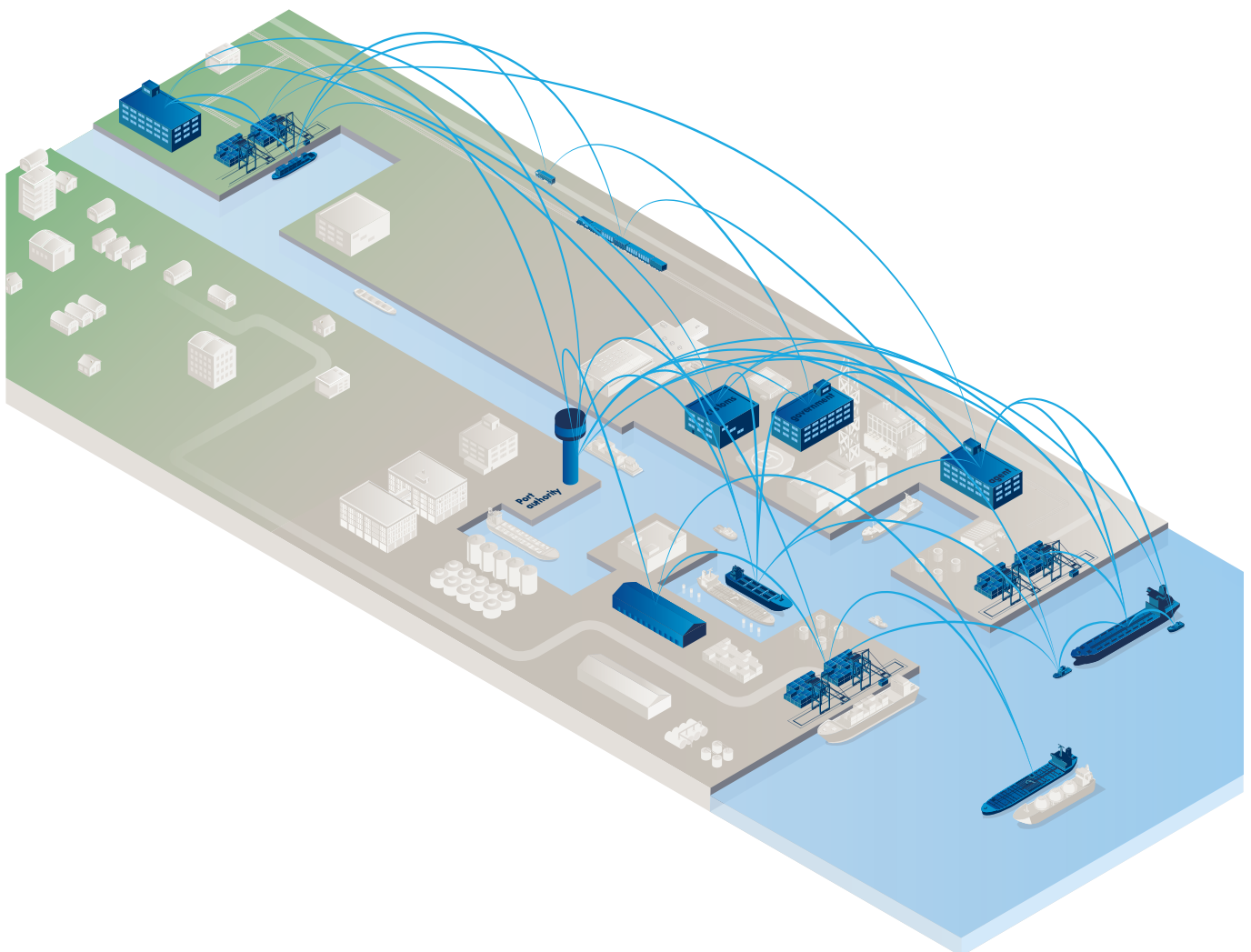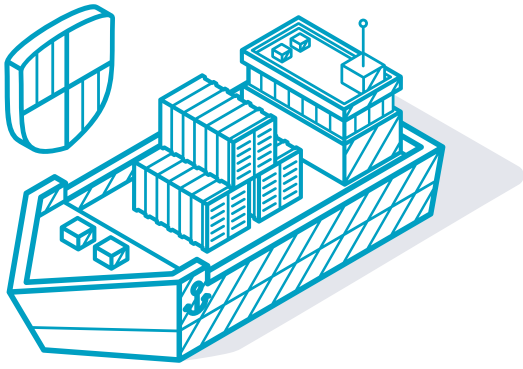Ports
Underwriter

Nick Welsh
Senior Cyber
Consultant

CONTENTS

1   THE INTERCONNECTED MARITIME WORLD

Taken from:
MOVE FORWARD: STEP BY STEP TOWARDS A DIGITAL PORT.
A White Paper issued by Port of Rotterdam and the British Ports Association

2 A SAMPLE OF SOME PUBLICLY KNOWN MARINE INDUSTRY CYBER ATTACKS

One common factor

- All have materially increased their response to the cyber threat
- Many other companies who have been hit have announced a response to the cyber threat
- It is not a case of if, but when
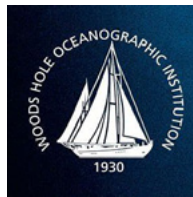
3 KEY RELATIONSHIPS NEED TO BE PROACTIVELY MANAGED IN THE EVENT OF A CYBER INCIDENT
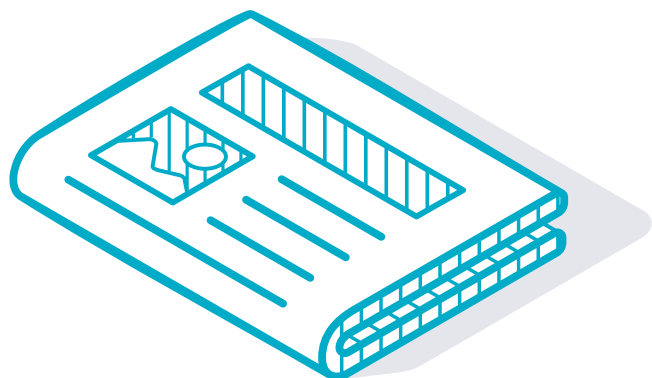
4   GLOSSARY OF TERMS USED

NISD

Network & Information Systems Directive – The EU Directive related to cyber security and marine. Establishes the idea of an Operator of Essential Services (OES)

NISR

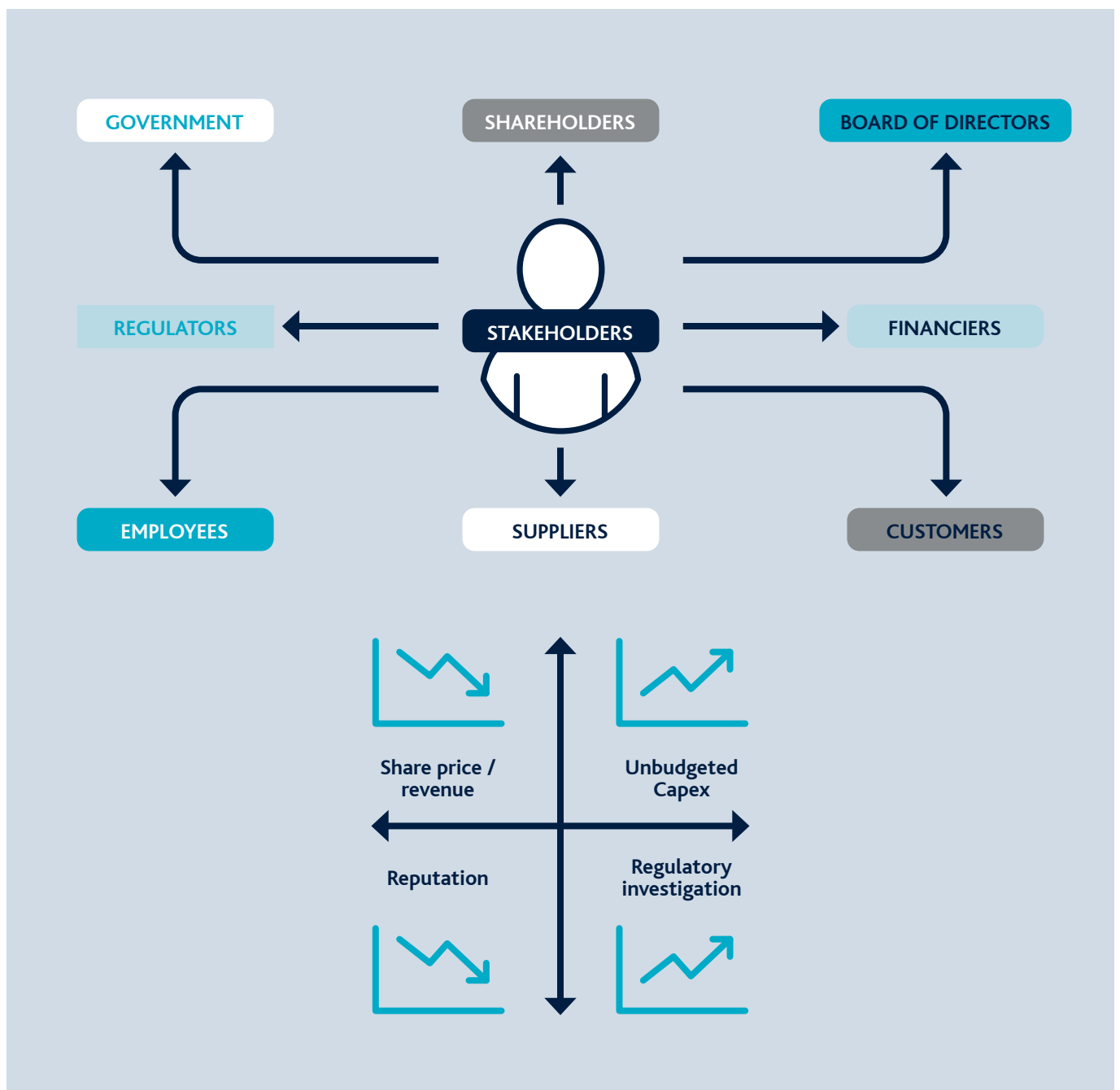Network & Information Systems Regulations 2018– The UK implementation of NISD

CAF

Cyber Assessment Framework – The UK Department for Transport model for assessing an OES against NISR

NIST

National Institute of Standards and Technology Cyber Security Framework – The US regulatory approach to cyber security

DPA 2018/GDPR

General Data Protection Requirements – the EU data protection legislation

5   WHAT IS CYBER?

Definition
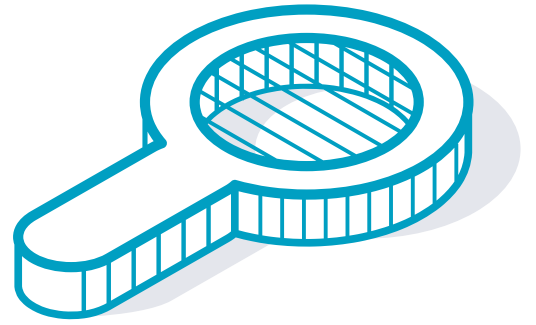
Unauthorised acts or activities occurring to/on your data, systems and networks

Who does it affect?

All data and all systems across the whole business

it is the Head Office and your remote offices, including ships

Why does it happen?

Drivers are varied — money, political advantage, kudos

Future Developments

Attacks continue to increase in scale, complexity and sophistication. Cyber regulation increases

Estimated Cost

2019 global cost of cyber crime est. $2tn pa, however the global cyber security budget est. $150bn pa
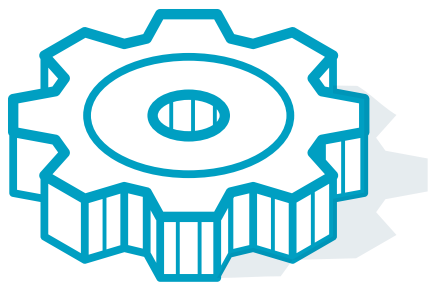
6 THIS CYBER RISK CAN BE MANAGED...

TECHNOLOGY

PROCESS

PEOPLE

RISK AGGRAVATORS

RISK MITIGATORS

| Understanding | Next Steps | Activities | Evidence & Monitoring | Improvement |
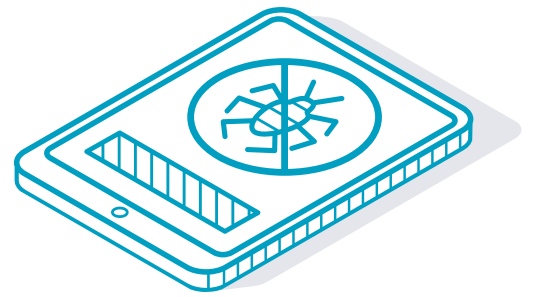
7 THE REGULATORY PICTURE
= WHY YOU CANNOT IGNORE RESPONDING TO CYBER

The current situation
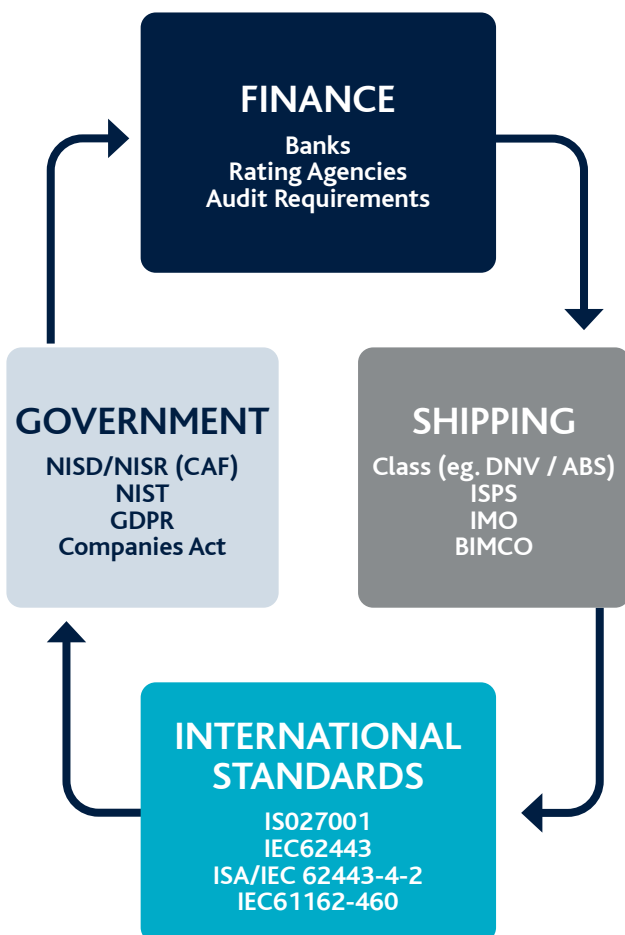
The Future: There will be more...

FINANCE
Banks
Rating Agencies
Audit Requirements

GOVERNMENT
NISD/NISR (CAF)
NIST
GDPR
Companies Act

SHIPPING
Class (eg. DNV / ABS)
ISPS
IMO
BIMCO

INTERNATIONAL STANDARDS
IS027001
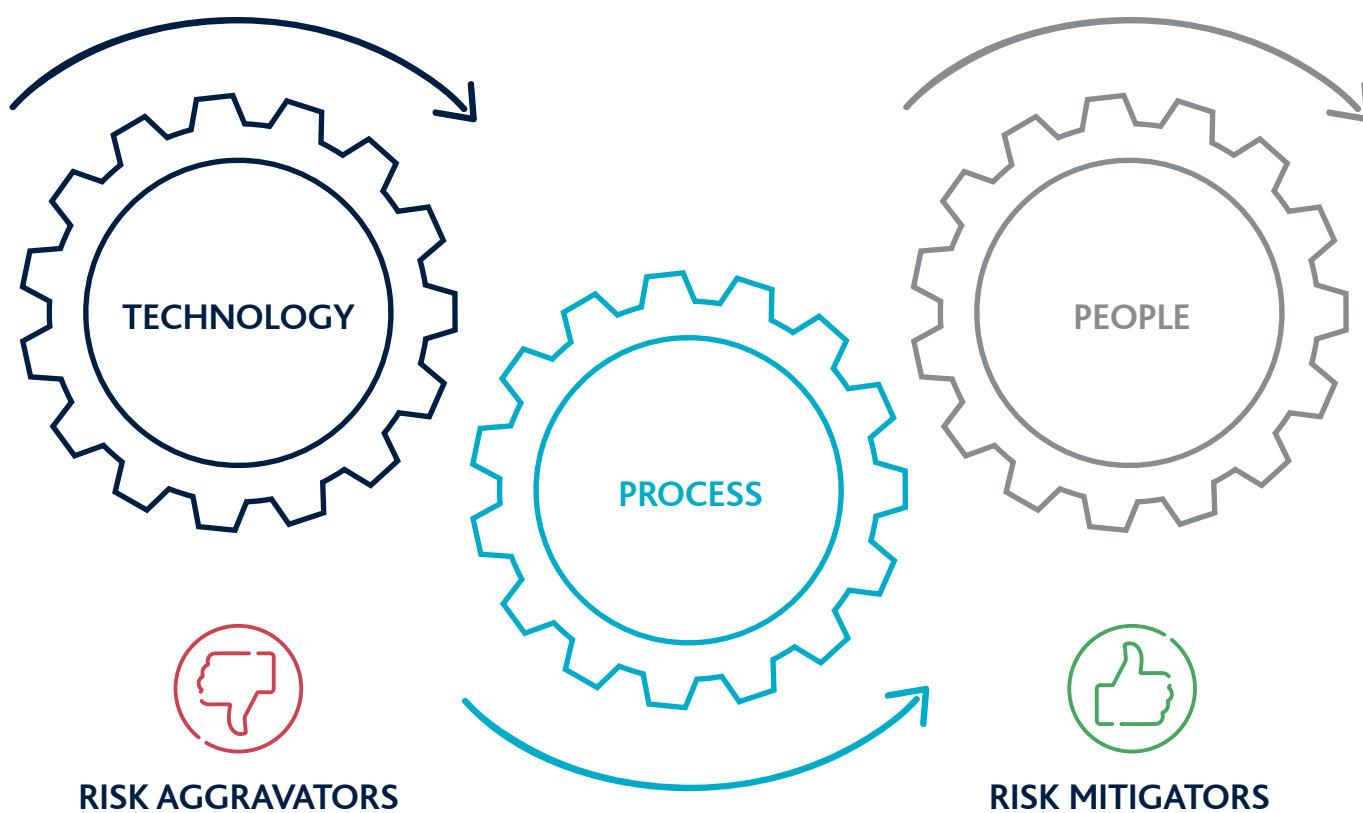IEC62443
ISA/IEC 62443-4-2
IEC61162-460

REGULATION & ENFORCEMENT

CYBER SECURITY LEGISLATION

TOUGHER STANDARDS

EVIDENCE OF CYBER SECURITY (COMPULSORY?)

DIGITISED / AUTONOMOUS SHIPPING
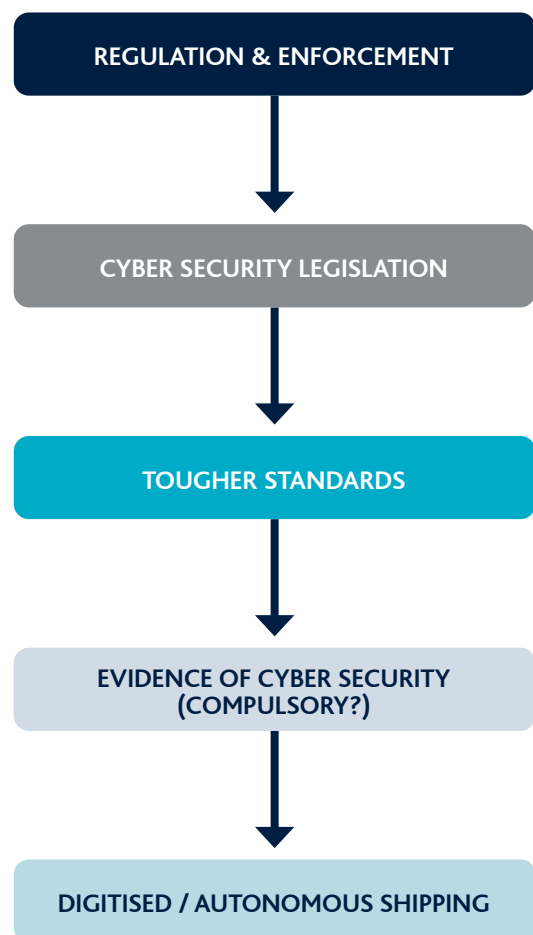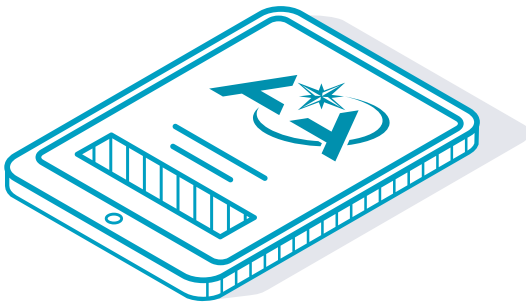
8 AN INTRODUCTION TO ASTAARA

The problem

- Cyber risk advisory response is not focused on marine
- No current comprehensive insurance response

The offering

```
                    ASTAARA
         ┌─────────────┼─────────────┐
         ▼             ▼             ▼
CYBER RISK MANAGEMENT  UNDERWRITING  ANALYTICS
```
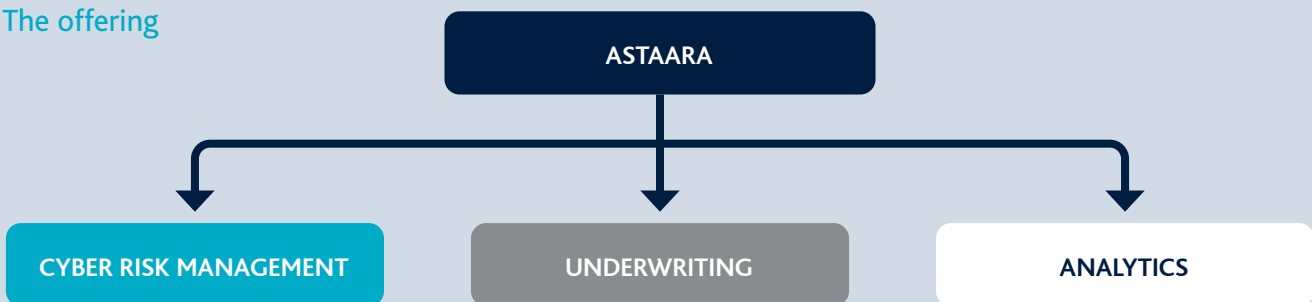
AstaaraCyber makes your business stronger

RESILIENCE **+** RECOVERY **=** STRONGER

The solution

ASTAARA COMPANY LIMITED

9 ASTAARA OFFERS MARITIME COMPANIES AN INTEGRATED APPROACH TO TACKLING THE CYBER THREAT

UNDERSTANDING
THE CYBER RISK

MANAGING
THE CYBER RISK

LEARN &
IMPROVE

INSURANCE

CYBER CONSULTING

ANALYTICS

RISK MANAGEMENT

UNDERWRITING

CLAIMS SERVICE
AND BCP

STATEMENT
OF KNOWN RISK
(PEOPLE, PROCESS, TECHNOLOGY)

INSURANCE
POLICY

10 HOW DO WE DELIVER STRATEGIC OUTCOMES TO SHIPOWNERS

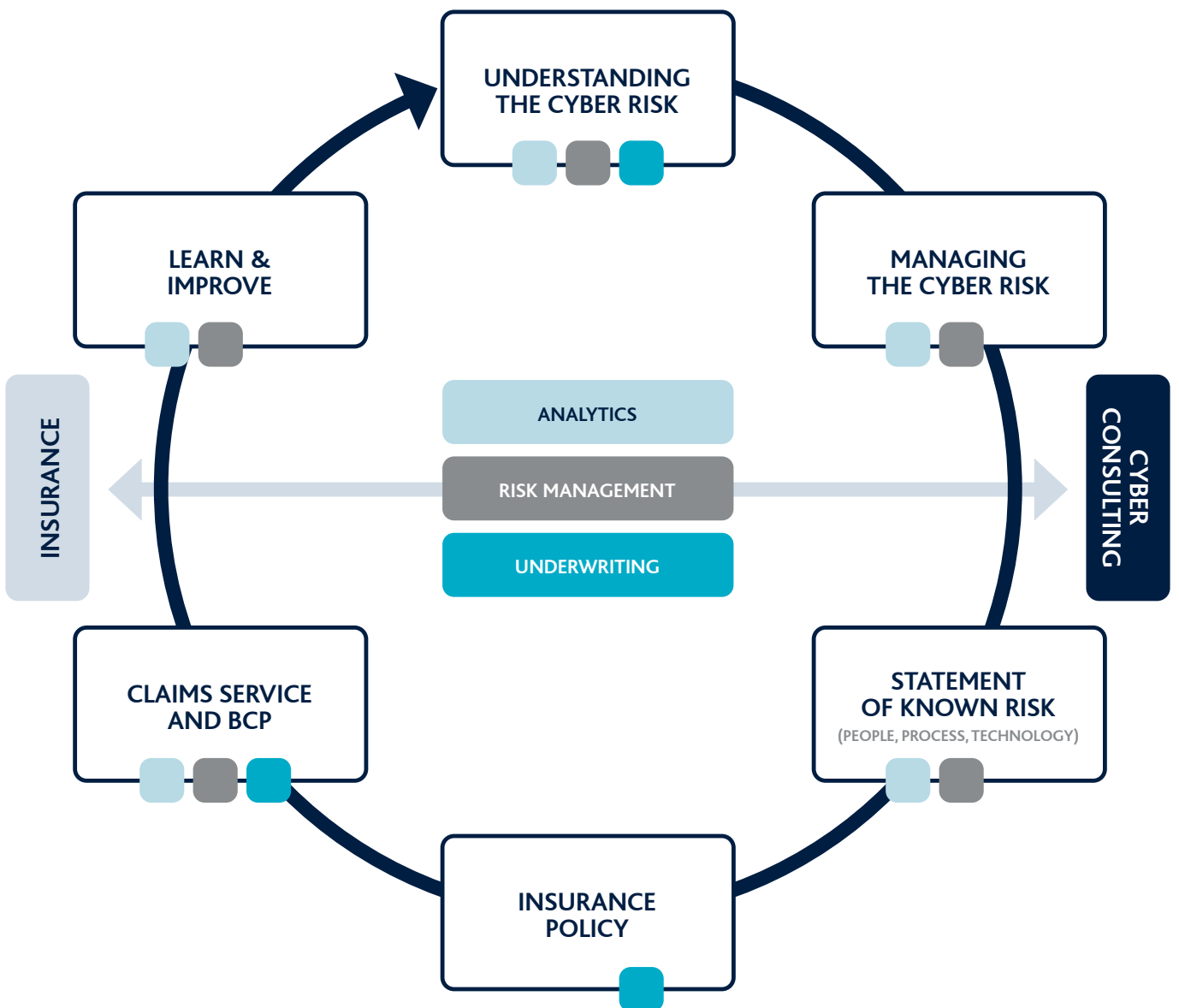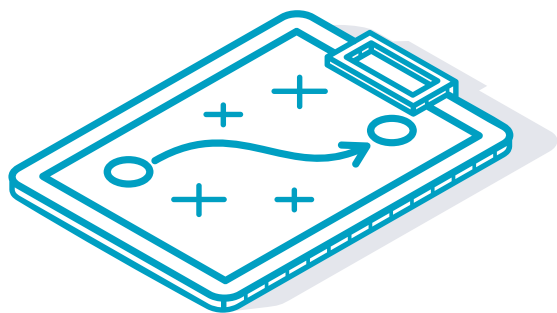| Understanding | Next Steps | Activities | Evidence & Monitoring | Improvement |

| STAGE 1 | STAGE 2 | STAGE 3 | STAGE 4 | STAGE 5 |

THE BASELINE REVIEW

BCP REVIEW

INITIAL REVIEW → DETAILED REVIEW → STATEMENT OF KNOWN RISK

DEPENDENCY REVIEW

GAP ANALYSIS & WORK PLAN

CO-ORDINATED ACTIVITIES & RESPONSE

QUARTERLY VISITS

DEPENDENCY REVIEW UPDATE

ANALYSIS

GAP ANALYSIS UPDATE

UPDATED STATEMENT OF KNOWN RISK

LEADERSHIP IMPROVEMENT PLAN

BCP IMPROVEMENT

CULTURE IMPROVEMENT

CYBER STRATEGY IMPROVEMENT

ERM IMPROVEMENT

RISK APPETITE IMPROVEMENT

MI IMPROVEMENT

TRAINING IMPROVEMENT

INSURANCE ENGAGEMENT STARTS HERE → **INSURANCE**

11 NEXT STEPS… FROM UNDERSTANDING YOU AS A CLIENT TO IMPROVING YOUR CYBER SECURITY POSTURE

SCOPING

- Engage with ACL and allows proper resourcing for project

BASELINE REVIEW

- Detailed sharing on information necessary to produce an Statement of Known Risk

- The Statement of Known Risk (SKR) provides management with an independent reference point of their cyber security posture.

- This is carried out by Astaara Risk Management

STATEMENT OF KNOWN RISK

- An assessment of you Cyber Security posture

- Enables Underwriting process

ONWARDS INTERACTIVE CONSULTANCY

- Next steps to improve

- Co-ordinated activities and Evidence & Monitoring

- Astaara Underwriting will only offer terms after the SKR

- The SKR outcomes need to be sufficient before being acceptable for underwriting

IMPROVEMENT

An improved cyber security posture

#ResilienceandRecovery

ASTAARA
COMPANY LIMITED