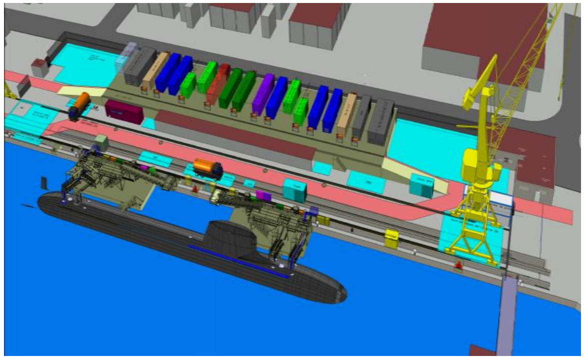
CYBERSECURITY FRAMEWORK

Introduction (1/5)

- **Le domaine maritime**
  - Transport maritime et passagers
  - Navire militaire
    - Partiellement isolé
    - Equipage réduit
    - Complexité technologique
    - Durée de vie variable >> 30 ans
  - Activités portuaires
  - Plateforme pétrolière
  - EMR, câblage SM, pêche, …



Introduction (2/5)

- **Le Cyber Security Framework (CSF) du NIST**
  - CSF = cadre général standardisé de la cybersécurité
  - Intérêts : orientation standardisée donc visible et lisible à l'international
  - Orientation Corporate mais aussi une ***déclinaison maritime*** :
    - BIMCO (Groupement international d'armateurs),
    - US Navy,
    - Et DCNS

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO

GUIDE DES BONNES PRATIQUES DE SÉCURITÉ INFORMATIQUE À BORD DES NAVIRES

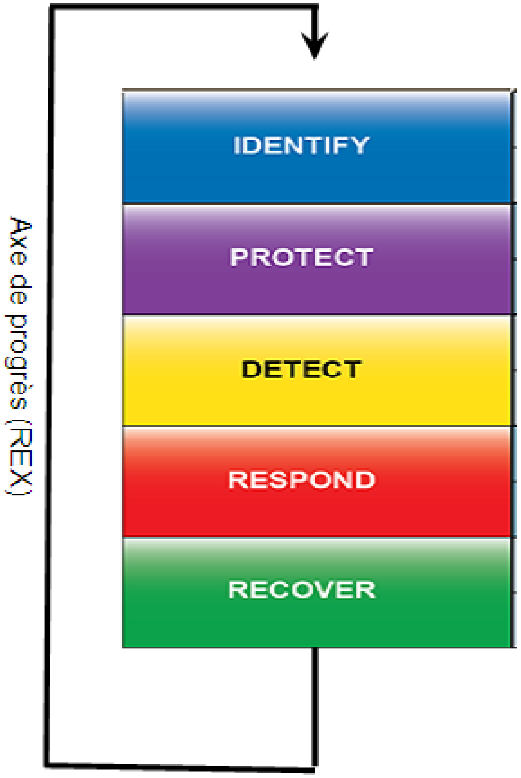
MINISTÈRE DE L'ENVIRONNEMENT, DE L'ÉNERGIE ET DE LA MER

« CYBER SECURITE »

RENFORCER LE NIVEAU DE PROTECTION DU NAVIRE

Edition septembre 2016

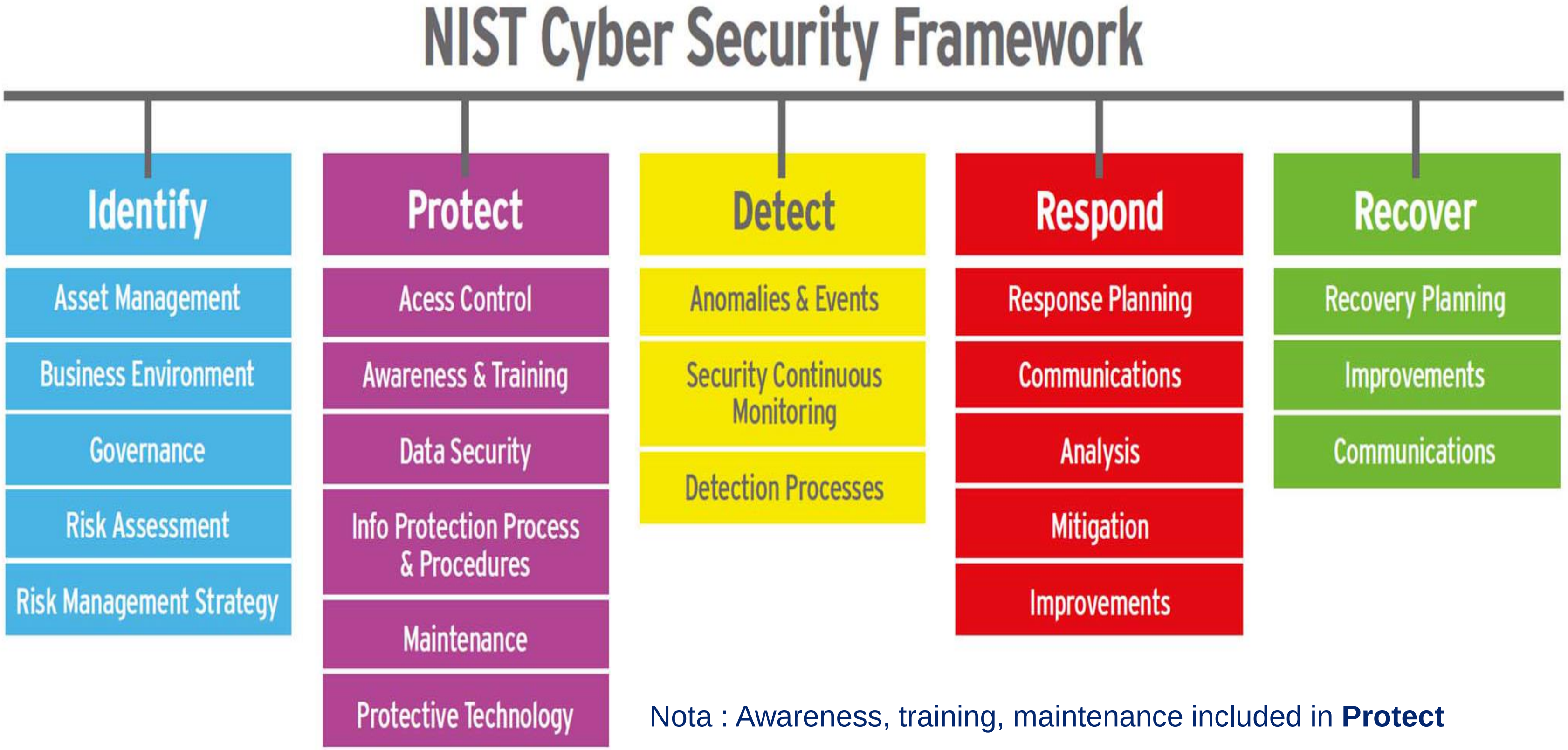
DGITM / Direction des Affaires Maritimes



Security Center (CERT+SOC)

Introduction (3/5)

- **Capacités techniques**

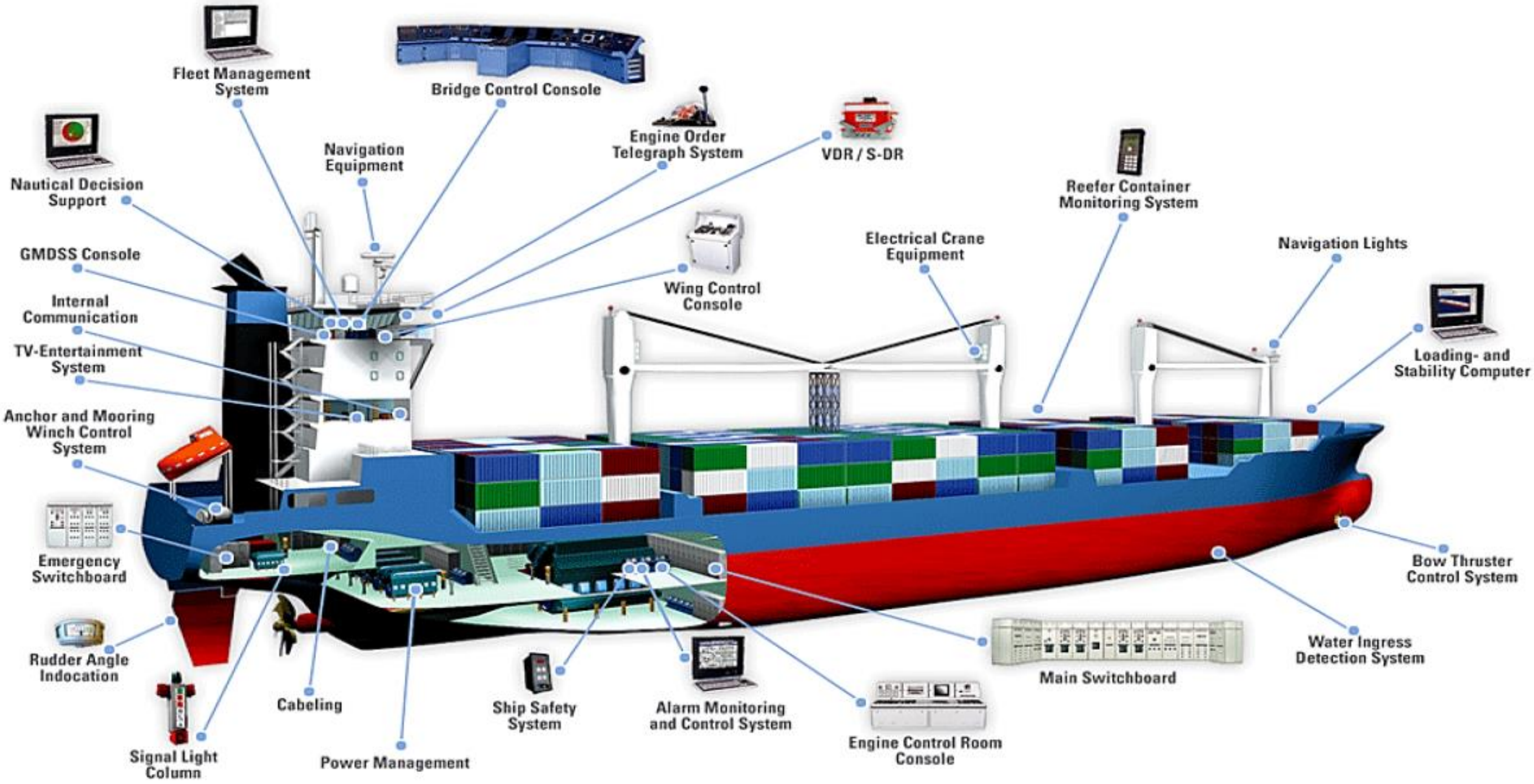


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Acess Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Process & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Nota : Awareness, training, maintenance included in **Protect**

Introduction (4/5)


Fleet Management System
Bridge Control Console
Engine Order Telegraph System
VDR / S-DR
Navigation Equipment
Nautical Decision Support
Reefer Container Monitoring System
GMDSS Console
Electrical Crane Equipment
Navigation Lights
Wing Control Console
Internal Communication
TV-Entertainment System
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Water Ingress Detection System
Rudder Angle Indocation
Main Switchboard
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

A IDENTIFY

VULNERABLE ASSETS

- Information and systems to be prioritised based upon classification, safety importance, criticality and business value
- Physical devices inventorised
- Software platforms and applications inventorised
- Organisational communication and data flows are mapped
- External information systems are catalogued

BUSINESS WORKING ENVIRONMENT

- Responsibilities are defined
- Role in the supply chain identified
- Place in critical infrastructure or sector identified
- Priorities for organisation's mission, objectives and activities established
- Resilience requirements to support delivery of critical services and the need for redundancy of shipboard OT systems are established

GOVERNANCE POLICY

- Organisational information security policy is established
- Safety and security roles and responsibilities are coordinated and aligned with onboard roles and external partners
- Legal and regulatory requirements regarding cyber security are understood and managed

RISK MANAGEMENT STRATEGIES

- Governance and risk management processes address cyber safety and security risks
- Risk management processes are established, managed, and agreed by organisational stakeholders
- Organisational risk tolerance is determined and clearly expressed
- The organisation's determination of risk tolerance is informed by the ship, trade and cargo based on sector-specific risk analysis

RISK ASSESSMENT PROCESSES

- Asset vulnerabilities are identified and documented
- Threat and vulnerability information is received from information-sharing forums and sources
- Threats, both internal and external, are identified and documented
- Potential business impacts and likelihoods are identified
- Threats, vulnerabilities, likelihoods and impacts are used to determine risk
- Risk responses are identified and prioritised

B PROTECT

ACCESS CONTROL PROCESSES

- Identities and credentials are managed for authorised devices and users
- Physical access to assets is managed and protected
- Remote access is managed
- Access permissions are managed, incorporating the principles of privileges and separation of duties
- Network integrity is protected, incorporating network segregation where appropriate

AWARENESS AND TRAINING

- All users are informed and trained
- Privileged users understand roles and responsibilities
- Third-party stakeholders understand roles and responsibilities (eg, suppliers, authorities, port personnel, customers, partners)
- Senior executives and senior officers understand roles and responsibilities
- Physical and information security personnel understand roles and responsibilities

DATA SECURITY

- Data-at-rest is protected
- Data-in-transit is protected
- Assets are formally managed throughout removal, transfers and disposition
- Adequate capacity to ensure availability is maintained
- Protection against data leaks is implemented
- Integrity-checking mechanisms are used to verify software, firmware and information integrity
- Development and testing environments are separate from the production environment
- A baseline configuration of IT and OT systems on board is created and maintained

INFO PROTECTION PROCESSES AND PROCEDURES

- A system development life cycle to manage systems is implemented
- Configuration of management processes are in place
- Backups of information are conducted, maintained and tested periodically
- Policy and regulations regarding the physical operating environment for organisational assets are met
- Data is destroyed according to policy
- Protection processes are continuously improved
- Effectiveness of protection technologies is shared with appropriate parties
- Response plans (Cyber Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
- Response and recovery plans are tested
- Cyber safety and security is included in human resources practices (de-provisioning, personnel screening)

MAINTENANCE POLICY AND PROCEDURES

- A vulnerability management plan is developed and implemented
- Maintenance and repair of organisational assets are performed and logged in a timely manner, with approved and controlled tools
- Remote maintenance of organisational assets is approved, logged and performed in a manner that prevents unauthorised access
- Assessment/log records are determined, documented, implemented and reviewed in accordance with policy

PROTECTIVE TECHNOLOGY APPLIED

- Removable media is protected and its use restricted according to policy
- Access to systems and assets is controlled, incorporating the principle of "least functionality"
- Communications and control networks are protected

C DETECT

ANOMALIES AND INCIDENTS

- A baseline of network operations and expected data flows for users and systems is established and managed
- Detected incidents are analysed to understand targets and methods
- Incident data is aggregated and correlated from multiple sources and sensors
- Impact of incidents is determined
- Cyber incident alert thresholds are established

SECURITY MONITORING

- The network is monitored to detect potential cyber security incidents
- The physical environment is monitored to detect potential cyber incidents
- Activity is monitored to detect potential cyber incidents
- Malicious code is detected
- Unauthorised code is detected
- External service provider activity is monitored to detect potential cyber incidents
- Monitoring for unauthorised personnel, connections, devices and software is performed

DETECTION PROCESSES

- Vulnerability scans are performed
- Roles and responsibilities for detection are well defined to ensure accountability
- Detection activities comply with all applicable requirements
- Detection processes are tested
- Incident detection information is communicated to appropriate parties
- Detection processes are continuously improved

D RESPOND

RESPONSE PLANNING

- Prepare and implement a response plan
- Response plan is executed during or after cyber incident
- Personnel know their roles and what to do when a response is needed

COMMUNICATIONS

- Incidents are reported consistent with established criteria
- Information is shared consistent with the response plan
- Coordination with stakeholders consistent with response plans
- Voluntary information sharing occurs with external stakeholders to achieve broader cyber safety and security situational awareness

ANALYSIS

- Notifications from detection systems are investigated
- The impact of the cyber incident is understood
- IT forensics are performed

MITIGATION

- Cyber incidents are categorised consistent with response plans
- Cyber incidents are contained and mitigated

IMPROVEMENTS

- Newly identified vulnerabilities are mitigated or documented as accepted risks
- Response plans incorporate lessons learned
- Response strategies are updated

E RECOVER

RECOVERY PLANNING

- Recovery plan is executed during or after a cyber incident

IMPROVEMENT MODIFICATIONS

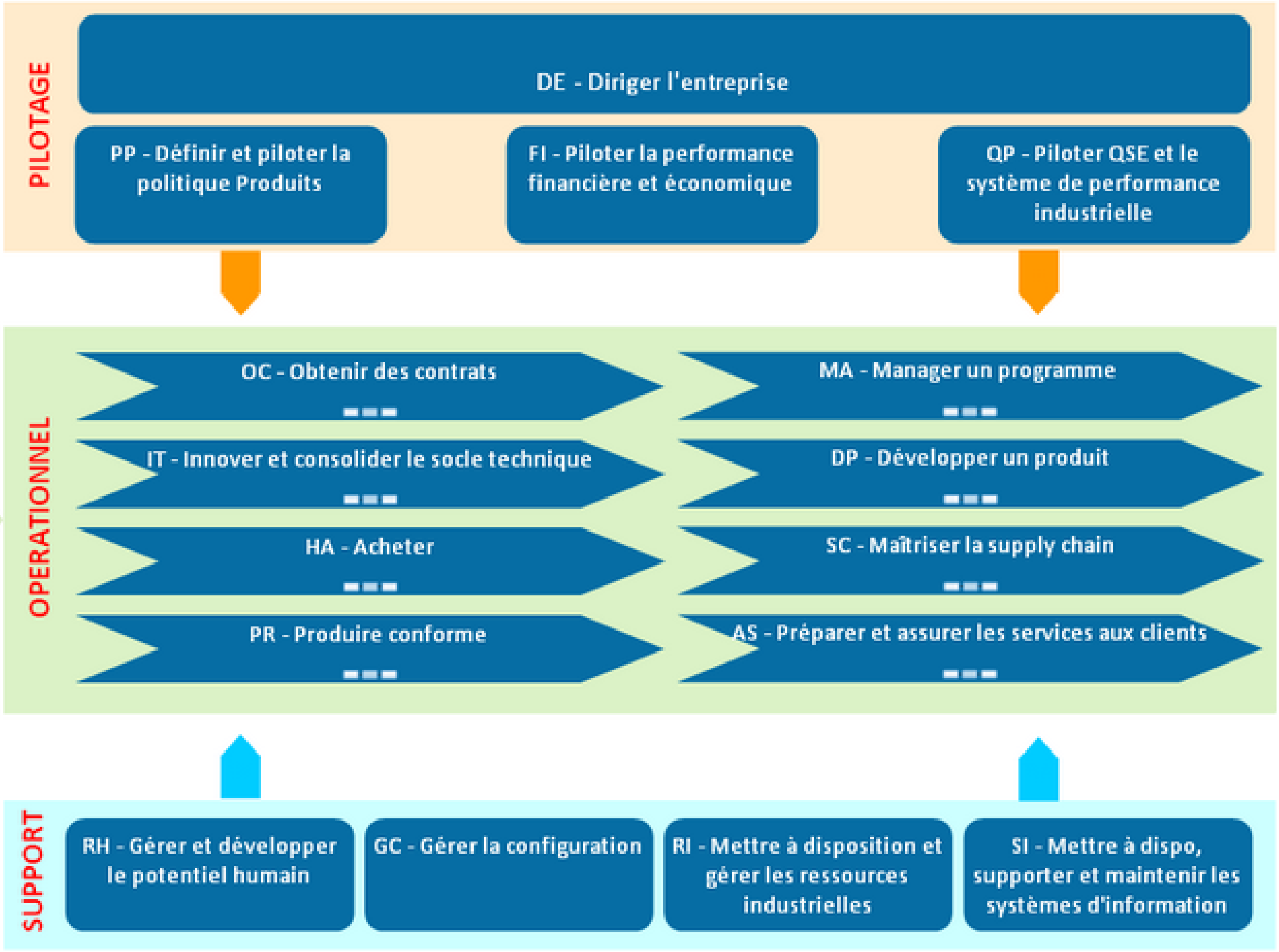
- Recovery plans incorporate lessons learned
- Recovery strategies are updated

COMMUNICATION

- Public relations are managed
- Reputation after cyber incident is repaired
- Recovery activities are communicated to internal stakeholders and executive and management teams

Déclinaison DCNS

- Le Business Management System (BMS)



PILOTAGE

DE - Diriger l'entreprise

PP - Définir et piloter la politique Produits

FI - Piloter la performance financière et économique

QP - Piloter QSE et le système de performance industrielle

OPERATIONNEL

OC - Obtenir des contrats

MA - Manager un programme

IT - Innover et consolider le socle technique

DP - Développer un produit

HA - Acheter

SC - Maîtriser la supply chain

PR - Produire conforme

AS - Préparer et assurer les services aux clients

SUPPORT

RH - Gérer et développer le potentiel humain

GC - Gérer la configuration

RI - Mettre à disposition et gérer les ressources industrielles

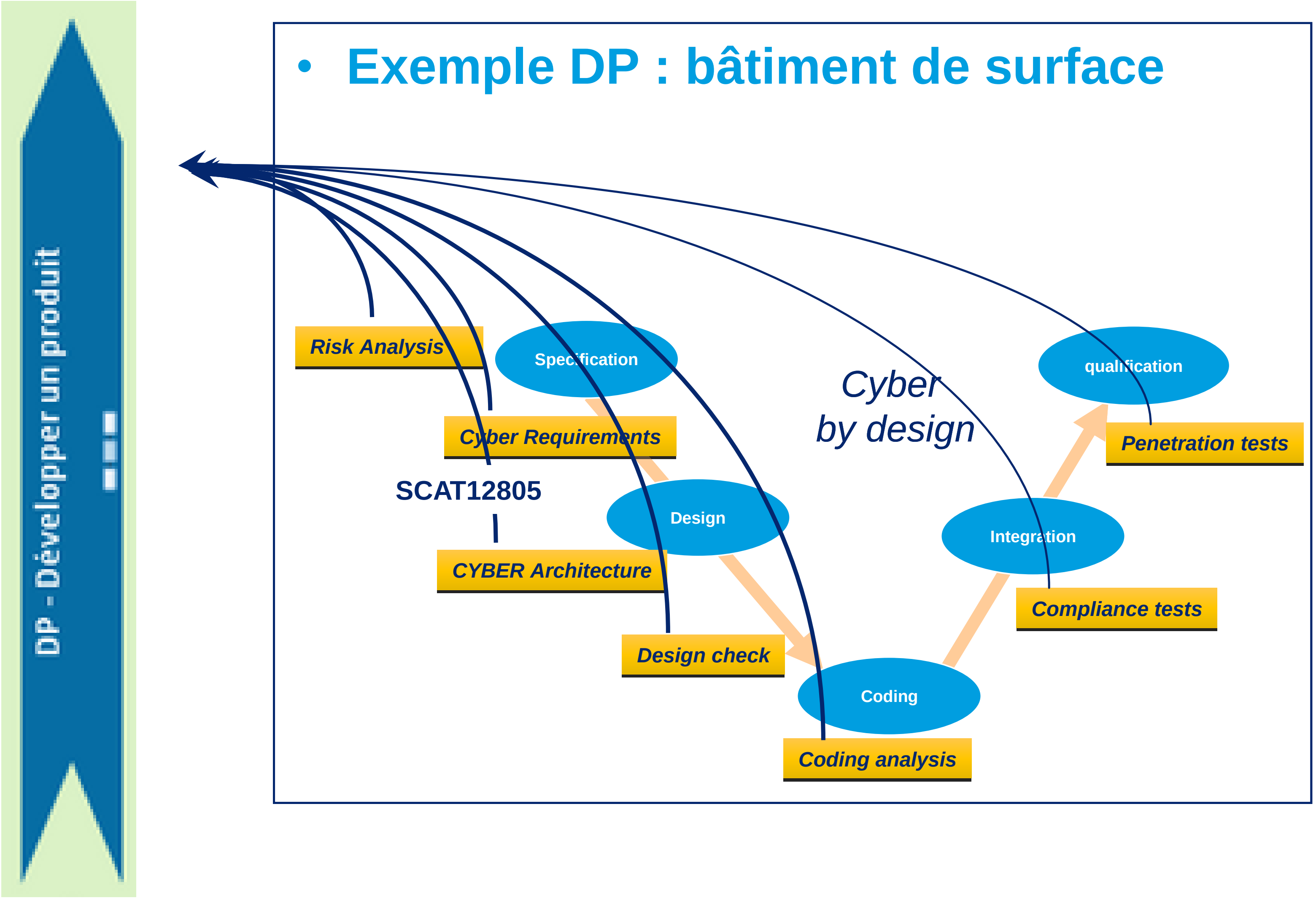
SI - Mettre à dispo, supporter et maintenir les systèmes d'information

Volet Corporate

Volet Produits

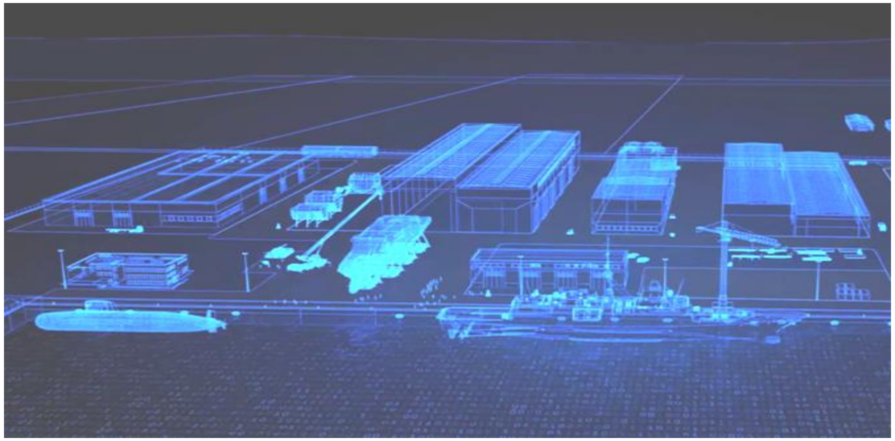
Le CyberSecurity Framework touche tous les processus de l’entreprise

Exemple du processus Développer un Produit



Conclusion

- ***DCNS se dote d'un véritable référentiel de Cyber sécurité :***
  - *Qui est une instance du CSF du NIST dans son environnement centré sur le navire*



  - Qui concrétise nos ambitions et qui dérisque au sens cyber nos produits/services
  - Qui structure notre approche de la cyber dans un contexte standardisé
  - Qui permet d'être lisible, visible et crédible à l'international
  - Qui permet d'offrir à nos clients un cycle Cyber complet (de l'identification à la remédiation de la menace) et modulable

Le référentiel Cyber de DCNS sera mis en place et déployé progressivement dès 2017 au fur et à mesure de sa montée en puissance.

DCNS

sea THE FUTURE®