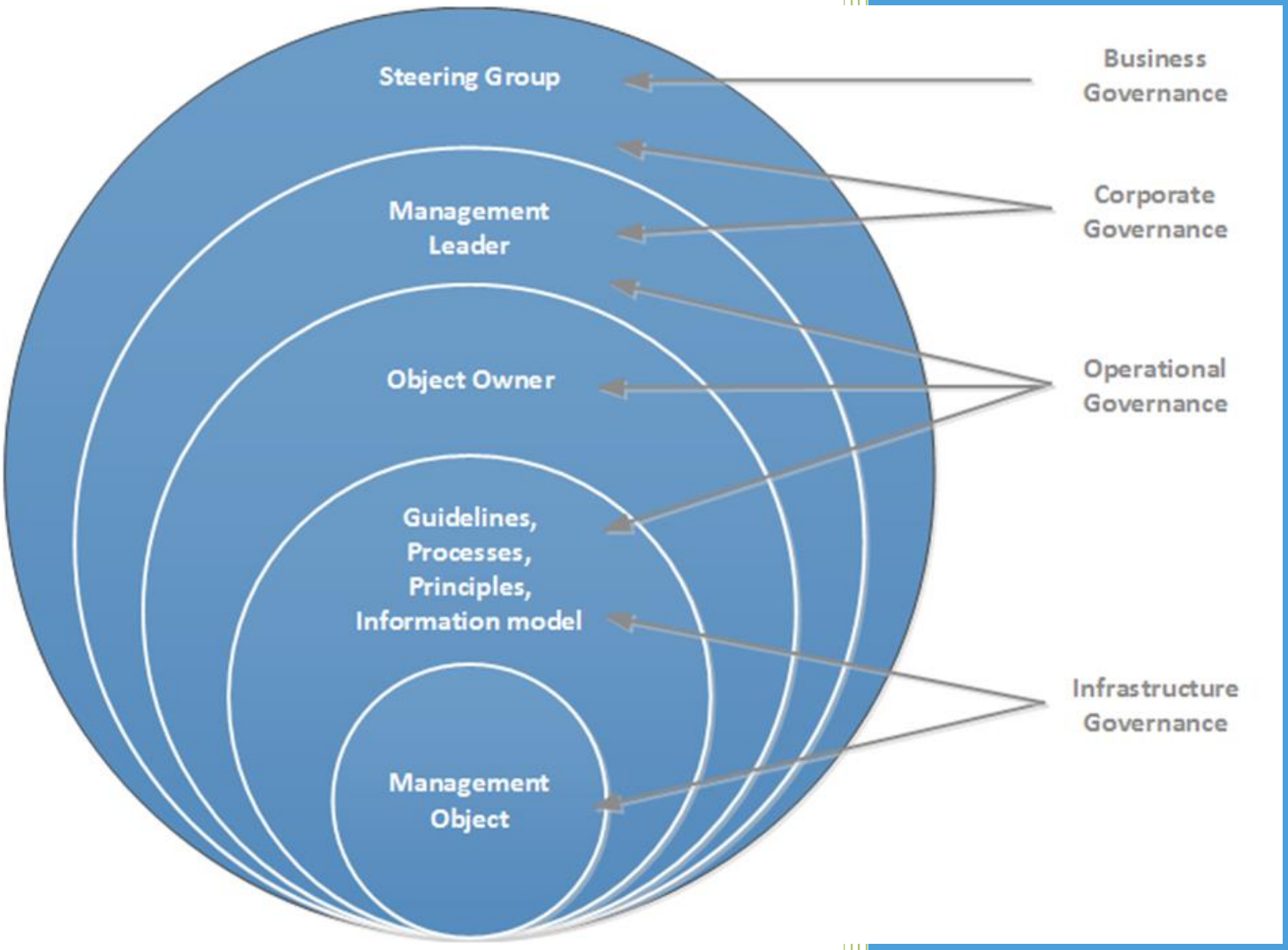
STM_ID_4.1.3
STM Governance
2019-02-01



Co-financed by the Connecting Europe Facility of the European Union

DOCUMENT STATUS

Authors

Name	Organisation
Päivi Morell Heinänen	Combitech AB
Nicklas Berndtsson	Combitech AB

Review

Name	Organisation

Approval

Name	Organisation	Signature	Date
Per Setterberg	SMA		

Document History

Version	Date	Status	Initials	Description

TEN-T PROJECT NO: 2014-EU-TM-0206-S

Table of contents

1 General Information

The Sea Traffic Management project has created technical interoperability between different actor's IT systems through standards at different levels, as well as a first set of services that could lead to fulfillment of the world's maritime stakeholders need for digitalization and online cooperation. A functional platform has been developed within the project but to maintain and develop a sustainable maritime digital infrastructure proper governance is needed.

Various models for governance have been briefly evaluated, where the pm3 model has been found suitable to manage developed solutions. However, since the preferred model is mainly developed to manage IT solutions, it needs to be supplemented with relevant parts to form a complete governance model.

The management objects which are absolutely critical to govern, for the developed solutions to live on, has been identified and the need for governance has been determined for each object. By this, the need for processes has been illustrated.

A study on governance is made to create an understanding of all parts needed to achieve good management and proper governance to maintain developed solutions within STM and maintain a sustainable maritime digital infrastructure.

The importance of identifying potential risks, associated with IT systems, is highlighted and some recommendations on how to achieve a satisfactory overall cyber security are made.

Finally, to establish an organization that can ensure proper government of STM, it is recommended that an Establishment Project is implemented and a brief model for such an establishment is provided in this report.

2 Introduction

The aim of Sea Traffic Management (STM) is to enable safe, sustainable, and efficient sea transports. STM is a response to the need to increase efficiency in operations within and between ports. STM has a holistic approach to services putting the berth-to-berth voyage in focus and uses that as a core element for process optimization, stakeholder interaction and information sharing.

An enhanced sharing of information ship-to-ship, ship-to-shore, and shore-to-shore is also an important enabler for increased situational awareness and safety during sea transports. STM has already shown that substantial savings of bunker costs could be earned and that high utilization of resources of the facilities in ports can be reached while the degree of safety is increased.

Sea Traffic Management is a concept that requires interaction between maritime actors, for instance, navigators and between a navigator and the operator of the Shore Center (SC). It requires the availability of functions, that enable the transfer of knowledge (information, data) from one actor to another, and the presentation of this information in a well-defined way, enabling each actor to act based on a common understanding of the situation at hand, and the intention of other actors.

STM is an information sharing framework that primarily deals with the benefits that different parties can get if they share their information (e.g. route) with others in real time. This is one of the fundamental pillars of STM: The organization who creates the information is always the information owner and shares the information they want with the parties they want. However, STM believe in the principle, you share, you win. The more players that share, the better the common awareness and the more each actor can optimize.

2.1 Purpose

Since the STM Validation Project is coming to an end it is vital to find a model for continued operation of the technical interoperability between different actors IT systems and maintain a sustainable maritime digital infrastructure that has been accomplished within all the STM projects.

With the above in mind, the purpose of this study has been to:

- identify administrative objects
- define the need for governance processes
- compare different management models (such as pm3, ITIL, COBIT and IT-CMF)
- describe a model for the establishment of a governing organization
- achieve a recommendation for post 2018

2.2 Limitations

The work, reported in this document, has been limited to the managements objects found within the STM projects. No efforts has been made to find new objects, identifying or describing objects or processes normally needed within an organization, such as support, economy and procurement. However, some effort has been made to identify business opportunities within the STM concept but this work needs further evalutation.

The work has been limited to governance of the infrastructure developed within STM.

2.3 Method

This study was made by reviewing existing material within the STM Projects.The study was made in five parts:

1. Different management models were compared
2. Management objects were identified and described
3. The need for a governance processes was defined
4. A model for establishment of a governing organization was described
5. A recommendation on how to maintain and manage solutions developed within the STM and administer a sustainable maritime digital infrastructure after 2018.

After every part of the study a status meeting has been held, with Swedish Martime Administration and RISE, to verify that the study is in line with the assignement. Continouous reconciliatons and interviews have been made with the Swedish Maritime Administration throughout the study. Further, interviews have been conducted with various experts.

2.4 Abbreviations

Acronym	Description
Authentication	Provision of assurance that a claimed characteristic of an entity is correct. SS-EN ISO/IEC 27000:2017 (E) Verification of a claim. For example, verification that a user is the one claims to be. This type of verification, performed by verifying part, is used e.g. upon login or communication between two systems or users. SIS-TR 50:2015
Authorization	Determining access permissions for a user (or system) to different system resources. SIS-TR 50:2015
COBIT	Control Objectives for Information and related Technology. A framework for IT governance, developed by IT Governance Institute, ITIG.
Governance	Governance is the way the rules, norms and actions are structured, sustained, regulated and held accountable.
Identification	Process where an identity specified by a user or resource is verified. SIS-TR 50:2015
Information Model	A representation of concepts and the relationships, constraints, rules, and operations to specify data semantics for a chosen domain of discourse. Typically it specifies relations between kinds of things, but may also include relations with individual things. It can provide sharable, stable, and organized structure of information requirements or knowledge for the domain context
ITIL	Information Technology Infrastructure Library

Management object	A managed object may represent a physical entity, a network service, or an abstraction of a resource that exists independently of its use in management
PM3	Maintenance Management Model
REST	Representational State Transfer (REST) is an architectural style that defines a set of constraints to be used for creating web services.
SeaSWIM	SeaSWIM enables information security and service lookup in a structured and governed manner.
Service	The provision of something (a non-physical object), by one, for the use of one or more others, regulated by formal definitions and mutual agreements. Services involve interactions between providers and consumers, which may be performed in a digital form (data exchanges) or through voice communication or written processes and procedures. Source E2 D3.4 Service Documentation Guidelines v01.01
Service Endpoint	A Service Endpoint is the URL where your service can be accessed by a client application. The same web service can have multiple endpoints, for example in order to make it available using different protocols.
Service Operation	Functions or procedure which enables programmatic communication with a service via a service interface.
Service Oriented Architecture (SOA)	Service-Oriented Architecture (SOA) means that a distributed IT system is organized as a structure of communication services. A service here is a serving function that is well defined, independent and independent of its surroundings. In a SOA-based system, resources are available to other systems within a network as independent services, and can be called and addressed in a standardized manner. SOA is often associated with web services based on XML, SOAP, WSDL and UDDI, but is, in principle, not limited to these technologies only.
Service Provider	A service provider provides instances of services according to a service specification and service instance description. All users within the maritime domain can be service providers, e.g., authorities, VTS stations, organizations (e.g., meteorological), commercial service providers, etc.
Service Specification	Describes one dedicated service at logical level. The Service Specification is technology-agnostic. The Service Specification includes (but is not limited to) a description of the Service

	Interfaces and Service Operations with their data payload. The data payload description may be formally defined by a Service Data Model.
Shore Center	Collection of services, activities and procedures of Shore Center. Formerly called Sea Traffic Coordination Center (STCC). Refers to entities offering services such as route check and/ or enhanced monitoring.
SOAP	SOAP stands for Simple Object Access Protocol and is an application communication protocol, is a format for sending and receiving messages, platform independent and is based on XML SOAP provides a way to communicate between applications running on different operating systems, with different technologies and programming languages The best way to communicate between applications is over HTTP, because HTTP is supported by all Internet browsers and servers. SOAP is created to accomplish this.
STM	Sea Traffic Management
UDDI	The Universal Description, Discovery, and Integration (UDDI) specification defines a SOAP-based Web service for locating Web services and programmable resources on a network. UDDI provides a foundation for developers and administrators to readily share information about internal services across the enterprise and public services on the Internet.
WSDL	WSDL stands for Web Services Description Language, is used to describe web services, it´s written in XML An WSDL document describes a web service. It specifies the location of the service, and the methods of the service, using these major elements: types, message, portType and binding <**types**> Defines the (XML Schema) data types used by the web service <**message**> Defines the data elements for each operation <**portType**> Describes the operations that can be performed and the messages involved. <**binding**> Defines the protocol and data format for each port type
XML	Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

3 Governance models in our analysis

The study aimed at compareing different management models (such as pm3, ITIL, COBIT and IT-CMF). Since the time to conduct the study was limited, it was decided to only evalute pm3, ITIL and COBIT. The comparison of the different governance models was made after various criteria such as:

- What is the purpose of the model
- Which are the models strengths
- Which are the models weaknesses
- How is management handled
- What is required for use of the model
- What size of the organization is the model most suitable for
- What kind of organization is the model most suitable for.

The comparison is compiled below.

Criteria	pm3	ITIL	COBIT
What is the purpose of the model?	pm3 is a control model with a foundation in the system management problem, but over time developed into a model used to control business development.	The essence of the methods is to make IT services explicit and strictly focused on client needs.	COBIT is an IT governance framework and toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. CobIT, Control Objectives for Information and Related Technology, is a general standard for IT management whose primary purpose is to define the organizational processes required for IT to meet the business's business goals. CobIT define the requirements that the business needs to put on the IT department. The standard recommends which elements should be included in IT processes, which key numbers should be used, how to measure the maturity of processes and identify risks.

Which are the models strengths?	Has the management object as a starting point Clarifies the management activities and the joint business that it represents for business partners and IT parties. Creates the conditions for secure business benefits, structure for collaboration and cost control	Ensure that an organization's IT needs are met (support, maintenance, development etc.) Strictly focused on client needs Clearly defined responsibilities for the service provision within the IT organization Effectively designed IT processes. IT organization concentrates on the services required by the business, rather than being focused on technologies.	Better strategic focus based on business focus (customer focus) A common approach, which management understands, about what IT actually performs. Clear ownership and responsibility roles based on process orientation A generally accepted framework Common understanding between all stakeholders based on a common language Compliance with the COSO Requirements for Control of the IT Environment
Which are the models weaknesses?	Focused on IT governance needs to be supplemented with tools for overall governance (business, corporate and operational).	Focused on IT governance needs to be supplemented with tools for overall governance (business, corporate and operational).	Focused on IT governance needs to be supplemented with tools for overall governance (business, corporate and operational).
How is management handled?	Interaction between different line organizational parties. Split into four model components: • business-oriented object sharing • controllable assignments • governance structure for collaborative tasks • integrated control processes	Managing services from their creation to retirement (the Service Lifecycle). Each of the five stages is focused on a specific phase of a service's lifecycle: • Service Strategy determines which types of services should be offered to which customers or markets • Service Design identifies service requirements and	Differentiate between governance and management. **Governance** ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritization and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives (EDM).

		devises new service offerings as well as changes and improvements to existing ones • Service Transition builds and deploys new or modified services • Service Operation carries out operational tasks • Continual Service Improvement learns from past successes and failures and continually improves the effectiveness and efficiency of services and processes.	**Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM). Starts from 5 principles. (Meeting stakeholders need, covering the enterprise end to end, applying a single integrated framework, enabling a holistic approach, separating governance from management) and 7 enablers: 1.principles, policy and framework, 2. processes, 3.Organizational structures, 4. culture, ethics and behavior, 5. information, 6.services, infrastructure, and applications, 7. people, skills and competence
What is required for use of the model?	Membership (license) and training to access the toolbox.	Documentation available for purchase. Certification available.	Membership and training to access the toolbox. Certification available.
What size of the organization is the model most suitable for?	Can be used regardless of the size of the organization	Can be used regardless of the size of the organization	Can be used regardless of the size of the organization
What kind of organization is the model most suitable for?	Public administration	Public administration	Used more in commercial companies

3.1 Conclusions

ITIL is primarily developed to control IT operations and provides the opportunity for well-structured work, by including detailed processes, functions and routines for the daily work. IT operations are controlled with action control and contract control. This ensures good routines which gives a high delivery capacity from the IT-organization.

Pm3 clarifies management activities and the joint deal, as this is for all parts of business, and IT operations. Management objects, used by object business, gives the opportunity to oversee the whole operation instead of downpipes.

COBIT, whose primary purpose is to define the organizational processes required for IT operations to meet the business's business goals, is a framework and toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. The standard recommends which elements should be included in IT processes, which key numbers should be used, how to measure the maturity of processes and identify risks.

All of the models could to some extent, supplemented with relevant parts, work to govern the Digital Maritime Infrastructure. For instance, there are advantages to using the combination of pm3 and ITIL to manage the infrastructure, as this has added value in getting a common structure for governance and follow-up of an organization's entire management portfolio.
Since the pm3 model requires less start up time it is recomended compaired to the other models which are more complex and require more time. However none of the models are complete, they all need to be supplemented in some way.

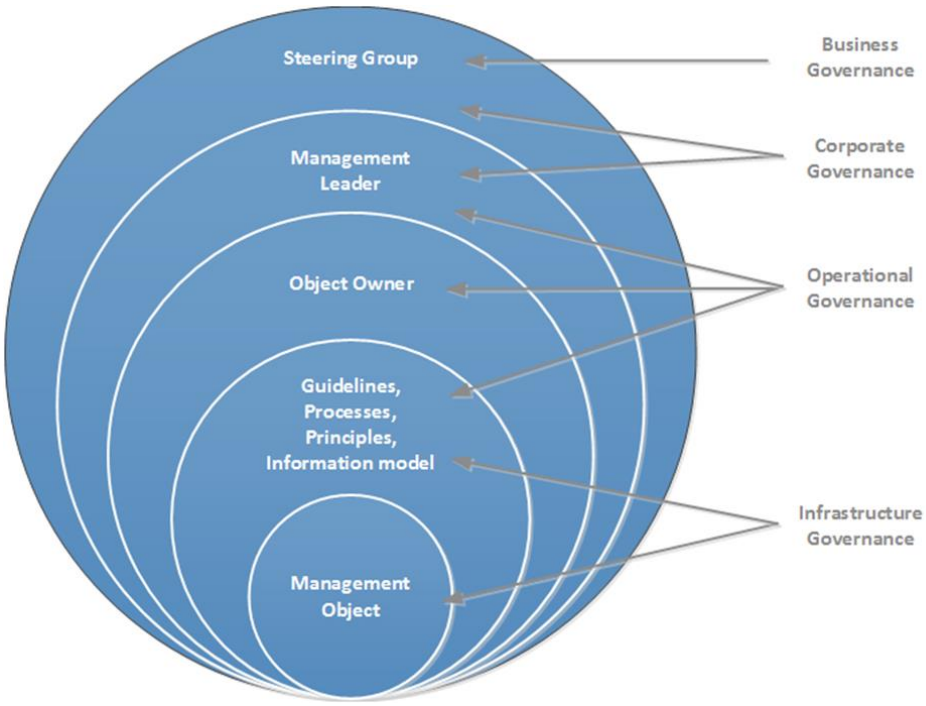
Where ITIL and COBIT are more internationally established, pm3 is mainly known in Sweden. However, pm3 is available in English and doesn't require much effort to get going.

4 Governance

The main function of a governance is to organize operational, financial, risk-management and reporting processes so that the board receives the information it needs to put good governance into practice and business units can conduct their work in compliance with regulations and strategic goals. The governance also extends the organization's governance framework down to the level of roles, responsibilities and reporting in order to bridge the gap between the governance framework and operational realities.

Management structures and principles identify the distribution of rights and responsibilities among various players in the STM (such as the board, managers, shareholders, creditors, accountants, supervisors and other stakeholders) and contain rules and procedures for decisions in corporate affairs. It also includes management for business and economics (Business and Economical Governance) and Operational management for further development and maintenance of STM.

Governance should be implemented at the following levels throughout the STM; infrastructure governance, operational governance, business governance and corporate governance as where the identified management object is a part of the infrastructure governance.



4.1 Infrastructure governance

The infrastructure governance is the ground level or the core of which STM is built on. The governance of the management objects aim to keep the objects in operation and ensure that they always will be able to provide the various services in STM.

Information shall be shared with dedicated stakeholders in a secure way including business constraints and tight economic constraints for sharing that ensure fair and efficient competition amongst stakeholders. STM connects and updates the maritime

world in real time, with efficient information exchange among selected parties such as ships, ports, service providers, shipping companies and authorities.

Aiming for interoperability means to ensure technical and operational interoperability. Interoperability includes a common information model (agreed data formats and data content), service specification standards, protocols (authentication of users, registration of services, service discoverability) but additionally interoperability on application service level and on operational level where users and existing non-STM systems are involved.

A clear definition of interoperability goes along with a set of standards and rules that have to be followed in order to ensure interoperability. That means for example to check if application services comply with these standards and rules. This means that safety aspects are important and need to be considered.

Information security or cyber security means that the technical specifications, API:s, payloads and xml-codes, the configuration and functionalities of the whole STM ship system including communication with the online access point is, anticipated to be accurate. Also administrative procedures, processes and guidelines need to be in place to achieve the right level of security throughout the STM.

4.2 Operational Governance

To govern the management objects we need tools and platforms. To organize the business associated with the infrastructure we also need descriptions, processes, other various information together with resources like object owners and management leaders.

To perform the operational governance we can divide the need into at least four different areas:

- Organizational (committees)
- Operations
- Service functions
- Technical aids (for IT-management)

4.2.1 Organizational (committees)

To be able to handle needs and demands in a non-profit organization with several stakeholders you have to consider the impartial view, that each stakeholder contributes and get the fair benefit of the work. One way is to work with committees for different areas. If each committee represent an area of the infrastructure they can meet regularly and work with the needs and demands. They will get the needs and demands from some kind of system or organization that will take a first decision if any committee will handle it. It’s up to the upcoming organization to handle what kind of funnel is to be used in order to take care of the demands. The organization also has to decide the organization of the committees.

To operate the organization, beyond the committees, the upcoming organization has to define and find appropriate roles and persons with suitable skills.

4.2.2 Operations

Some of the management objects has to be available from the Internet and therefore must be hosted in an environment, either in a cloud service or at a server that is

exposed to Internet. The MCP-portal is a web based portal to handle a web based self-service where to register ones company and/or services that can be used within STM. The portal has to exist in a web server that are stored and exposed to the Internet where the users can access it. There has to be somewhere where information can be stored, maybe in a simple server with a simple storage interface like Windows Explorer or a more advanced repository that handles check in/check out and version of documents and code. All these operational tools have to be handled and hence also associated with a cost.

Example of operations tools in governance:

- Cloud service (ID-register, Service Register)
- IT-operations (mail, IT-programs, internal network)
- Portal operations (MCP-portal, home page, possible upcoming extranet)
- Server operations (to store documents, code repositories)
- Vetting process (handle the authorizations)
- IT-Development (develop API:s, portal etc.)

4.2.3 Service functions

When an organization has to handle or govern different kinds of task there are usually people involved. There can either be employees, consultants or volunteers and they are bound by some kind of contract or job description. When there are services offered to either members or external stakeholders someone has to perform them. To work with the people, services and members it arises a cost for it as well. Example of service functions that may appear in the upcoming STM organization are:

- system to handle or store information about employees and contracts
- handling the organizations economy
- system for member management
- project support (depending on what is decided by the upcoming organization) and IT-management.

4.2.4 Technical aids

When the governance is about complex infrastructure and digital applications there are some technical aids that are used to describe the different objects and the context of the STM-system. Those management objects that are used today are likely to be used even in the future because the projects had the need to describe, help or bring order in a complex part of STM. In this section there are more or less well developed tools or directions in different parts. To govern the different management objects there are guidelines written, processes described and principles to consider that are produced and has to be developed as the needs and demands are required.

To describe the complex environment and infrastructure where we find and use STM the projects has used a tool called Information model that are continuously changing because of the earlier mentioned needs and demands. The information model is important to govern and store to let the participants and stakeholders understand the role of the different management objects in STM and how they are connected.

Last but not least is the need of working together as well as to identify what kind of problems and shortcomings there might be in the STM-environment that consists of

data sets, API:s, applications, portals and so on. In the recent project, STM Validation, a user group forum has been created where participants can exchange experienced problems, solutions and experiences in general. If the future STM organization can maintain such a forum in a similar way that would be very useful in governing the STM infrastructure.

4.3 Business Governance

To govern a business or an organization, requires financial resources. However, since STM is creating benefit for several stakeholders in the shipping industry there will also be some business opportunities for the coming organization that can lower their monetary contributions such as member fees. To be sure that the coming organization will work with the opportunities there has to be a process and a description of how to take care of the opportunities.

Below are some examples of typical business opportunities.

One of the most obvious areas that is both central and important is handling the authentication. When a company will register in the Service Registry they have to prove that they are who they claim to be. This is either a manual process or an automatic process connected to other registers. Regardless of which, this is one of the most basic things for creating and maintaing the trust in STM. After successful authentication, a certificate is issued as a proof for it. This process is causing some cost but also a possible income.

Other business opportunities are:

- Quality certification with actions like monitoring certifications, keep a register of certificates, accredit installations and functionality.
- Development tools and knowledge for international projects where there is need for project managers and so on, coordination of development, developer forum, repository forum, development support, development of concept.
- Develop better functions for MCP which can be used to Pay-by-service us, like SAAS (System as a service within IT)

4.4 Corporate Governance

Corporate governance is the mechanisms, processes and relationships through which companies are controlled. Tasks that are suitable for the upcoming organization to work with, in the context to keep developing the area of e-navigation and establish STM as the leading concept. The STM organization will govern the following areas:

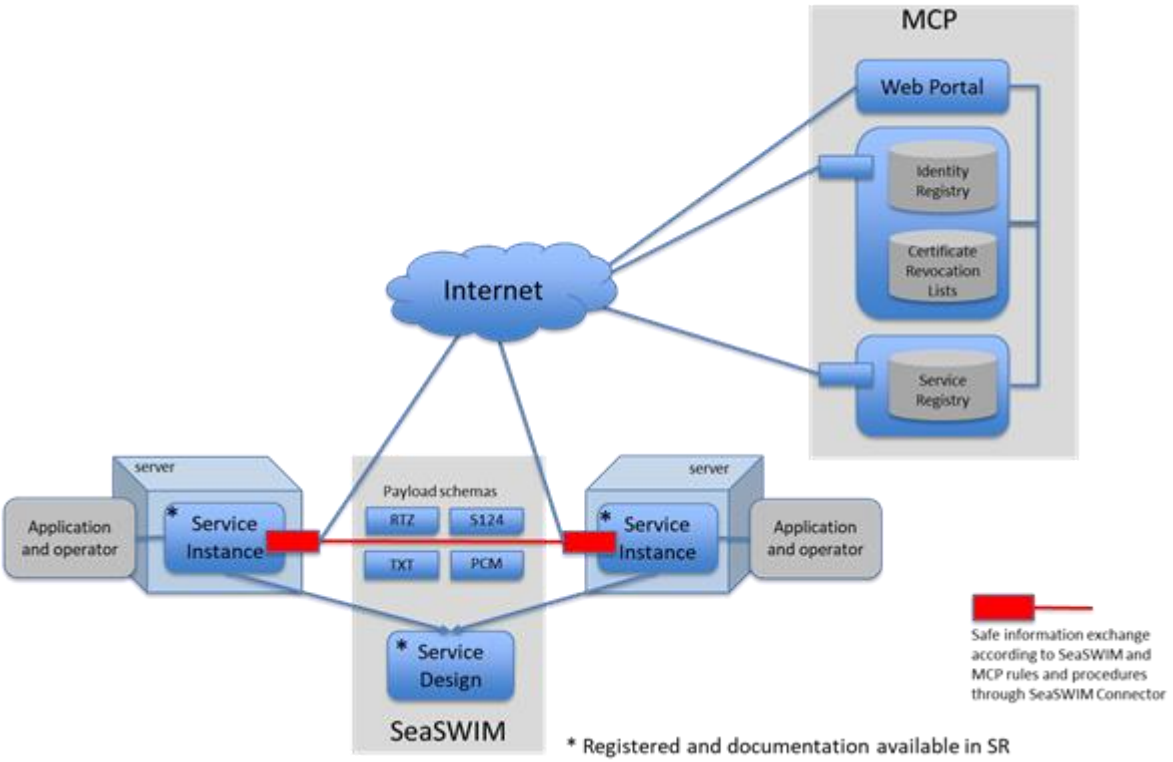
- Organization cooperation
- Research
- Communication (about STM and e-navigation)
- Market Intelligence (find out needs and demands)
- Cooperation with other maritime bodies
- Projects (provide knowledge and maintain STM as leading concept)
- Management of Standardisation (work together with other organization and develop standards that are used within STM)

5 Identified management objects within the maritime digital infrastructure (STM)

The Identified management object is the items that need to be managed and are important for the services provided by the Sea traffic Management system (maritime digital infrastructure). The identified management objects are:

- MCP portal
- MCP
- ID-register
- Service-register
- API (REST and SOAP)
- Standard messages (Payload-schemas)

The management objects are described separately to clarify the characteristics of each management object that needs to be managed to fully function in the STM concept.



5.1 Maritime Connectivity Platform portal - MCP –portal

Maritime Connectivity Platform portal is a communication framework enabling efficient, secure, reliable and seamless electronic information exchange between all authorized and authenticated maritime stakeholders across available communication systems. The MCP Portal is just a collective interface for Identity and Service Registry as well as documentation about MCP.

MCP Portal provides quick access to a wide variety of digital and navigational tools for the maritime world.

MCP-portal manages login to MCP (Maritime Connectivity Platform). Login to MCP Portal is done with an Open ID account and authenticated with Identity Register via :

- Username and password (open source),
- Federation via Baltic and International Maritime Council (BIMCO), Danish Maritime Administration (DMA), International Association of Marine Aids to Navigation and Lighthouses Authorities (IALA) members, for authentication, or
- Certificates produced by MCP.

Each organization must "Join to MCP" and in this approval process, an admin account for the organization is created. This person can then create additional users, ships, devices and services. Depending on the rights, you can also create, modify and remove service specifications, technical designs and instances. Service instance can also be linked to a Vessel ID. Through the portal, you also generate, and get the Client Certificates. Through the portal you can also report bugs.

5.1.1 Need for governance processes

If the MCP-Portal shall be operated in a cloud solution or hosted by a external part, a service level agreement (SLA) needs to be obtained. The purpose of SLA is to specify the quality level of delivery. An SLA regulates the availability of a system, how long it should be before error recovery is started, how fast the error is fixed and how many times an error may occur during a given period of time.

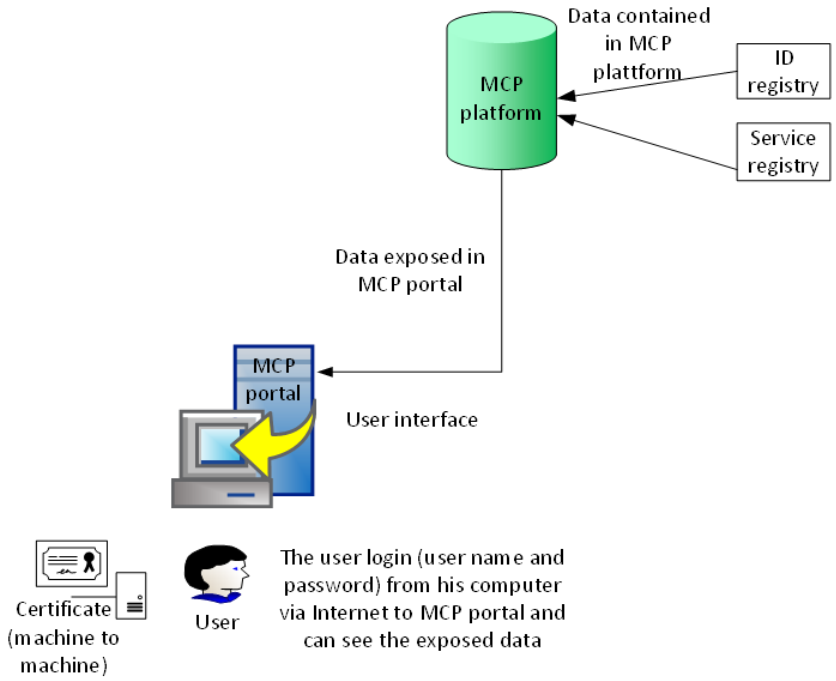
User interface, functions and documents about MCP and processes needs to be managed and kept up to date.

5.2 Maritime Connectivity Platform - MCP

Maritime Connectivity Platform is a communication framework enabling efficient, secure, reliable and seamless electronic information exchange between all authorized maritime stakeholders across available communication systems.

MCP consist of core components as Identity Registry and Service Registry. The Identity Registry provides a single login to all services, using identity information provided by trusted stakeholders.

The Service Registry contains information about the services and is the main source of service information for both developers, providers and consumers of services. The aim is to allow for convenient and attributable register, discover and use of all relevant maritime services. Thus, the Service Registry provides functionality to publish and find services, their functionality and endpoints. All the core components are Open Source. The picture below shows the connection between MCP-portal, MCP, Identity Registry and Service Registry.



MCP has the following capabilities:

- Capability to handle identities in MRN format
- Capability to handle X.509 Certificates
- Capability to handle service registrations on several levels
- Capability to search for identities and services
- Capability for delegating access to other registred organizations to act (i.e. register services) on behalf of your own organization (useful for Agents acting on behalf of shipping companies)

MCP for ship owner/maritime stakeholders:

Before the services will be available to ship owner/maritime stakeholders, the ship owner/ maritime stakeholders need to be validated in the ID-registry/ MCP portal

MCP for service provider:

The MCP offers easy distribution of service providers services to several platforms and onboard equipment. Before the services will be available, the service provider need to be validated in the ID-registry/ MCP portal.

5.2.1 Need for governance processes

MCP needs to be managed with the following items, however, this is not comprehensive:

- MCP needs to be managed by an internal or external party ie, the server is always available to authorized users
- Maritime Messaging Service - An information broker that intelligently exchanges information between communication systems connected to the cloud, taking into account the current geographical position and communication links available to the recipient. Maritime Messaing Service is only used in Korea.

- User Administration – that information about the users always are up to date and current
- Service administration - that information about the services always are up to date and current
- Process for Certificate management which include creation and revocation
- Processes and procedures to set the right requirements.
- Source code (production, staging, test)
- Process for the Domain Name Management
- Process for maintaining compliance (standards, regulations, legal requirements and security)
- The ownership of MCP needs to be clarified and a shared ownership is prefered

5.3 ID-registry

The main purpose of the Identity Registry is to provide secure and reliable identity information. It provides a single login mechanism to all services, using identity information provided by trusted stakeholders. The Identity Registry contains relevant information to authenticate stakeholders and enable confidentiality in information transfer processes. The aim is that all services depend on unique identifiers that, for example, define specific users, services and transferred data objects to avoid conflicts.

The Identity Registry enables identity management and authentication mechanisms, while the Service Registry provides functionality to publish and find services, their functionality and endpoints.

After the initial registration and filtering process of the central services (Identity Registry and Service Registry) the communication is primarily between the provider and the consumer.

For ship owner to get the opportunity to access all of the services on the MCP, the ship owner/ organization need to be a validated ship owner/organization.

5.3.1 Need for governance processes

The ID-Registry needs to be managed with the following items, however, this is not comprehensive:

- Process and routines to always have the ID-registry current and up to date with authorized user (user name, password, certification etc.)
- Process for validation of organizations, ships owner, service provider etc.
- Process and routines of certification management, always have current certification and trusted third party certificate
- Process to always have a valid root certification, certification authority (CA)
- Process to have a list of valid certification
- Process and routines to have current revocation list (not valid certification)
- Process to have a list of current Identity provider
- The structure of current identities in the ID Registry which are possible to use today needs to follow the development of STM and be valid and current:
    - Organization
    - User

- Vessel
- Device
- Service

- Process to be compliant with General Data Protection Regulation (GDPR)

5.4 Service Registry

The aim is to easily register, discover and use all relevant maritime services. The Service Registry provides functionality to publish and find services, their functionality and endpoints. The Service Registry improves the visibility and accessibility of available maritime information and services. This enables service providers, consumers, and regulatory authorities to share a common view on service standards and provisioned services. The Service Registry does not provide actual maritime information, but a specification of various services, the information they carry, and the technical means to obtain it.

The service register contains all available services. Before services will be available the service provider needs to upload following:

- the service specification, which is a description of what the service does,
- the technical design, which is the technological description of how user can access the services
- the service instance, which is a description of where the service can be accessed

5.4.1 Need for governance processes.

In order for different services and service providers to be found in the Service Registry, the following should be in place:

- Process, standard and routines how a service must be documented and implemented in order to be part of the SeaSWIM environment
- Process of Management service
- Process for managing service updates or changes in services
- Process, routines of status management
- Development of Technical Compliance Checker and process to validate the technical compliance checker. The technical compliant checker used to control if a service is in accordance with IALA template and XML schemas)
- Process for approval
- Development of checklist for release on three levels:
  - Test
  - Staging
  - Production
- Process for compliance and audit
- Current List of service providers
- Current List of service providers services

5.5 Technical design API

An Application Programming Interface (API) is a set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service. Simply put, API allows two applications, which are not initially meant to interact, to talk to each other.

In STM:s maritime digital infrastructure, a number of API:s are used to communicate. These are:

- SeaSWIM Connector.
- VIS
- PortCDM (SPIS)
- ID Registry API
- Service Registry API

SeaSWIM Connector

The main purpose of the SeaSWIM Connector is to aid in authentication of services requests and provide a simplified API to the ID and service registry. SeaSWIM Connector (SSC) is designed in order to support inbound and outbound communications. Inbound receive information from other services offering an out of the box, while outbound communications send information to core services (ID Registry and Service Registry) and application services. More information regarding the SSC can be fount in document "SeaSWIM Connector Service Specification"[1].

Voyage information service (VIS)

The main purpose with Voyage Information Service is to support sharing of voyage plans to authorized actors. Sharing of voyage plan is primarily initiated by the ship by authorizing the voyage plan to concerned actors and by direct accessing e.g. route optimization or route check, but sharing can also be on request by other service providers such as enhanced monitoring.

The Voyage Information Service can be used both to support exchange of voyage plans from ship as well as other service providers and consumers such as shore centers and route optimization providers.

The Voyage Information Service is specified in such way that by using VIS in front of consuming or providing application services that intend to share/exchange voyage plans, interoperability can be reached. That enables new services to be exposed in Service Registry based on VIS Design for voyage plan exchange to be used without new implementation on consumer side.

Each Voyage Plan shall refer to a UVID (Unique Voyage Identity) generated by the service provider and contain status on the voyage/route.

Requirements briefly:

- VIS has a storage (for storing sent and received messages, XML schemas, logs)
- VIS is an information service registered in SeaSWIM central Service Registry

[1] https://s3-eu-west-1.amazonaws.com/stm-stmvalidation/uploads/20171005130802/SeaSWIM_Connector_Technical_Design_v1.0.docx

- VIS has service endpoints for exposing methods
- VIS has a function to validate message payload according to the following predefined schemas (rtz, text, area)

All communication between VIS and SeaSWIM Central services or and other information services is achieved using SeaSWIM connector.

Port CDM

The main objective of PortCDM is to enhance coordination among port call actors. By sharing their time stamp data related to port calls, information will be available for actors to utilize in real time. This will facilitate just-in-time arrivals, increase predictability, berth productivity, punctuality, reduce waiting and anchoring times and boost resource utilization. Moreover, the number of phone calls will be significantly reduced, resulting in reduced administrative burden.

ID Registry API

Service Registry and Identity Registry provide their own API:s (REST and SOAP) and data formats to communicate with any kind of MCP services or with a ship-side Maritime Connectivity Platform component.

Service Registry API

The Service Registry contains service specifications according to a Service Specification Standard and provisioned service instances implemented according to these service specifications. This enables service providers, consumers, and regulatory authorities to share a common view on service standards and provisioned services. The SR does not provide actual maritime information, but a specification of various services, the information they carry, and the technical means to obtain it. The Service Registry also provides the mechanisms to manage the lifecycle of service specifications and service instances.

The Service Registry is intended to facilitate or implement the Maritime Service Portfolio (MSP) concept by providing a repository for the specification of operational and technical services and provisioned service instances. It is intended to potentially support all maritime services, not only digital services, thereby making it a single reference point for provisioning and discovery.

5.5.1 Different techniques to use

Representational State Transfer (REST) is an architectural style that defines a set of constraints to be used for creating web services. Web services that conform to the REST architectural style, or RESTful web services, provide interoperability between computer systems on the Internet. REST-compliant web services allow the requesting systems to access and manipulate textual representations of web resources by using a uniform and predefined set of stateless operations. Other kinds of web services, such as SOAP web services, expose their own arbitrary sets of operations

Simple Object Access Protocol (SOAP) is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to induce extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. Web Services Security (WS-Security, WSS) is an extension to SOAP to apply security to Web services. It is a member of the Web service specifications and was published by OASIS.

The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as Security Assertion Markup Language (SAML), Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. WS-Security describes three main mechanisms:

- How to sign SOAP messages to assure integrity. Signed messages also provide non-repudiation.
- How to encrypt SOAP messages to assure confidentiality.
- How to attach security tokens to ascertain the sender's identity.

The specification allows a variety of signature formats, encryption algorithms and multiple trust domains, and is open to various security token models, such as:

- X.509 certificates,
- Kerberos tickets,
- User ID/Password credentials,
- SAML Assertions, and
- custom-defined tokens.

WS-Security incorporates security features in the header of a SOAP message, working in the application layer.

JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is based on a subset of the JavaScript Programming Language, is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

JSON is built on two structures:

- A collection of name/value pairs. In various languages, this is realized as an object, record, structure, dictionary, hash table, keyed list, or associative array.
- An ordered list of values. In most languages, this is realized as an array, vector, list, or sequence.

These are universal data structures. Virtually all modern programming languages support them in one form or another. It makes sense that a data format that is interchangeable with programming languages also be based on these structures.

These mechanisms by themselves do not provide a complete security solution for Web services. Instead, this specification is a building block that can be used in conjunction with other Web service extensions and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies. In general, WSS by itself does not provide any guarantee of security. When implementing and using the framework and syntax, it is up to the implementer to ensure that the result is not vulnerable.

5.5.2 Need for governance processes.

The API:s used in STM need to be managed and configured so that the correct level of security is installed. These are:

- SeaSWIM connector.
- VIS
- PortCDM (SPIS)
- ID Registry API
- Service Registry API

Poor planning and insufficient implementation of a security protocol and misunderstanding regarding the differences between Authorization, Authentication, Federation, and Delegation can cause a potential revenue loss. Having an API that allows for full access to the entirety of STM:s systems and resources is an absolute nightmare. When establishing a security system for STM:s API:s, understanding Authentication, Authorization, Federation, and Delegation is vitally important. Deciding the access and specific circumstances behind sharing the STM:s resources will help establish a security shield to protect internal assets and solve many security issues before they arise.

Each API used in STM requires analysing who will be granted access and how to access the resource to avoid compromising security. That is, to balance access and permissions.

Authentication:	Authentication is a base security layer that deals specifically with the identity of the requesting party. Authentication as an agreement based on trust. For instance, a user could log in using an authentication service that only requires a username and password. For greater levels of assurance, may be to provide a single-use token generated on a smart card or mobile device.
Authorization:	Authentication verifies that the requester is who they say they are, authorization determines the access level they should be granted.
Federation and Delegation	Federation the user is granted the ability to use the same set of credentials across multiple services. By having the authentication take place in one single domain, other security realms that trust this primary domain can reuse the authentication and trust the authenticity of the identity established. This results in what is called a federation. While this works fine in some cases, if the authentication and authorization protocols were to be broken or violated, then the barrier between the resources and the user would also be broken. This could allow an attacker to take complete control of the domain.

Delegation	Delegation is another process by which access and rights can be given to authorized users while maintaining a relatively limited amount of access. Whereas federation works by giving the user a token to use on multiple domains, delegation works by authorizing a user to function partially as if they were another user**.**

Opening only what's needed to be opened, and making sure those openings don't tie into vital systems that could be damaged. Functionally, this means assigning elements of authority to API consumers based on the minimal amount of access they need to do the functions they are required to do. By assigning different roles and levels of responsibilities to clients, STM can create an environment that keeps the data safe.

5.6 Payload schemas

A payload schema is an outline, diagram or model. In computing schemas are often used to describe the structure of different types of data. In STM a various range of payload schemas are used today. They are technical descriptions and standards how to describe different services. The payload schemas can be changed in the future

The defined standards include, among other things, how a service must be documented and implemented in order to be part of the STM environment. As these STM-standards are new, potential service providers need support with the development and/or provision of their services. The services are evolving over time and need to be adapted, for instance, if a small change is made such as the optimization of the algorithm to calculate a more efficient route.

The payload schemas which is used today are:

- RTZ
- S124
- TXT
- PCM

RTZ

The RTZ, the Route Exchange Format which make it possible to exchange routes, irrespective of system provider.The RTZ format considers a route as a collection of waypoint elements. Single waypoint element contains both inherent waypoint data (i.e. coordinates, name etc.) as well as data related to the route leg directed to this waypoint (i.e. speed on the leg, cross-track deviation limits etc.). The RTZ format is based on XML. The XML route exchange file uses the extension .rtz.

The route plan exchange format is based on standardizing a route plan. A route plan consists of waypoints where each waypoint contains information related to the leg from the previous waypoint. The route exchange format is a file - RTZ - containing an XML coded version of the route plan.

The route plan exchange format is intended be used for many purposes. For example it can be used onboard for route plan exchange between main and backup ECDIS, ECDIS and radar, ECDIS and optimization systems, etc. Another example use is

between ship and shore where it can be used to inform the shore about the plan of the vessel, the shore can recommend a route, the shore can optimize a route, etc.

S124

S124 format by itself is developed for transmission of Navigational warnings from shore centers to the ships. The current format corresponds to the next aims:

1) to transmit urgent marine safety information on the vessels;

2) to provide full life cycle transmitted warning beginning from it's creation to cancellation of this warning

TXT

The text message is a lightweight message intended to be used in communication between Voyage Information Services implemented in STM. Normally a text message is submitted as a complement in sending voyage plans between different parties in STM.

PCM

Within STM, a Port Call Message (PCM) Format has been developed to enable the coordination of stakeholder activities associated with port calls by providing a standard format to share the necessary information, particular time stamps, for example on Estimated Time of Arrival (ETA) and Estimated Time of Departure (ETD).

5.6.1 Need for governance processes

Improvment in the development, which is more critical, should be considered. This may involve changes in the business logic of services or in the interface itself. It should be investigetaed ifthe service is still providing the expected result and performing the task initially defined. Other relevant aspects to consider is, does the service description document follow the right template in a correct way and are all relevant description documents for service available?

In order to always have the payload schemas, correct, current and compliant with the standards, the following should be considered:

- Processes must exist to always comply with current standards within IALA, IMO, IHO etc that affect STM
- In developing services that affect standards, there should be a process for revising the standards
- Roles and managers in STM must be appointed as responsible for compliance with the standards
- Process for service approval needs to be established

6 Overall cyber security

The maritime digital infrastructure (STM) is designed according to Service-Oriented Architecture (SOA) which means that a distributed IT system is organized as a structure of communication services. A service is a serving function that is well defined, independent and independent of its surroundings. In a SOA-based system, resources are available to other systems within a network as independent services, and can be called and addressed in a standardized manner. SOA is often associated with web services based on XML, SOAP, WSDL and UDDI, but is, in principle, not limited to these technologies only.

The services offered within STM are information-based and depending on that the information is always available, correct and current, and available to authorized users.

Ignoring administrative security, focusing only on IT security and the technical aspects may cause fail in security. To ensure complete security, STM needs security from a holistic perspective with both administrative security and technical security (information security).

Information security or these days cyber security is a set of strategies to prevent, detect threats and risk, counteract threats to digital and non-digital information, strategies for managing processes, policies, guidelines and tools. Information security/cyber security responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage. These objectives ensure that sensitive information is only disclosed to authorized parties (confidentiality), prevent unauthorized modification of data (integrity) and guarantee that the data can be accessed by authorized parties when requested (availability).

To identify potential threats and risks to which STM will be encountered a risk analysis (probability x impact) should be conducted on the entire STM concept including the infrastructure to find appropriate organizational and technical security measures.

To reduce the consequences of any loss of data or infrastructure a contingency plan is designed. This enables organization personnel to restore critical IT functions and connectivity rapidly, effectively, and safely. The contingency plan defines the procedures, resources, tasking, and information required for performing recovery actions in response to a broad range of events. A well-executed and tested contingency plan also gives confidence that critical resources will be available when needed and facilitates an organization’s continuity of operations in an emergency situation. The plan is a living document that must be updated regularly to reflect changes to the system’s configuration and operations.

An IT security incident is an adverse event in a computer system or network caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms. To provide the ability to react quickly and efficiently to disruptions in normal processing and achieve incident-handling capability an incident handling plan can be produced. The incident management processes, provided by the plan, should have the following phases:

- Prepare
- Respond

- Follow up

The incident management process should be consistent and compatible with any forensic services that the organization may require to ensure that critical evidence is handled properly.

If STM processes personal data, STM must comply with General Data Protection Regulation (GDPR). If STM is not compliant, there is a risk of a penalty of up to 4% of total sales.

When processing Personal data the treatment shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; not be considered to be incompatible with the initial purposes (‘purpose limitation’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (‘storage limitation’);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

Note that! The controller is responsible for, and shall be able to demonstrate compliance with the principles above (‘accountability’).

Some important concepts.

Personal data	means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

7 Establishment model

The establishment of an organization that will ensure a truly sustainable maritime digital infrastructure (i.e. maintain and develop solutions developed within STM) requires a holistic view to be maintained.

Such an establishment would require an extensive work in many areas, requireing many different skills and many decisions. Extensive work like this is advantageously implemented in project form, an establishment project.

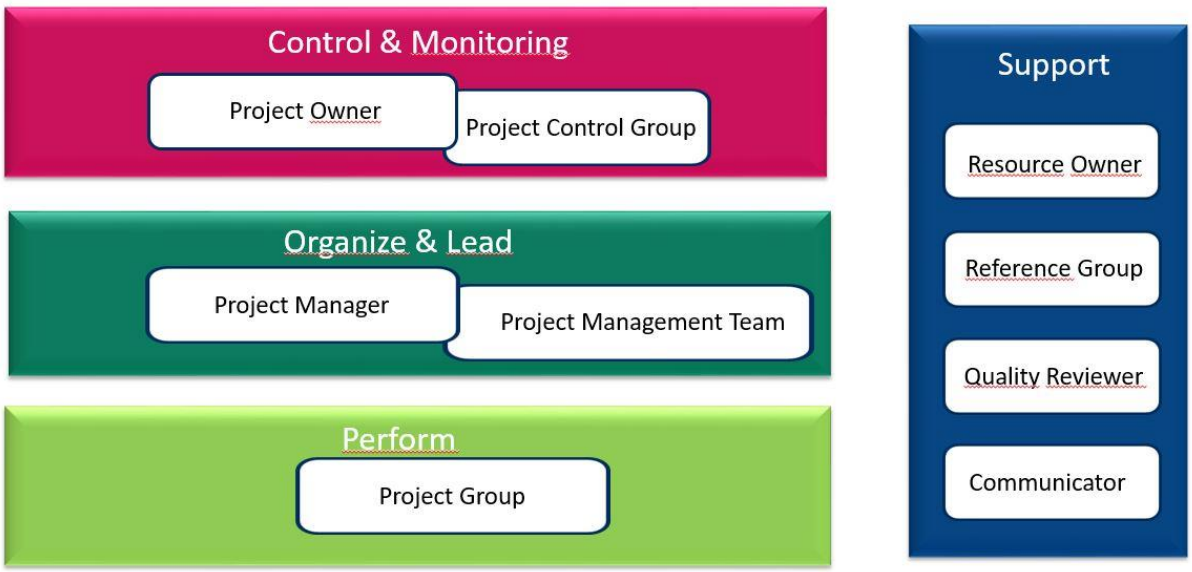
Before commencing the project the owners need to decide what they want to govern and why. The purpose of the project must be agreed and relevant project activities must be decided. Since it is unclear which resources will be available, this report only gives an overall review of what can be considered important in a project of this character.

7.1 Establishment project

For a successful outcome of the project a well-structured project organization must be established and maintained. The project organization should provide arrangements and decisions about the realization and the process of the project.

7.1.1 Roles

If the project is to succeed it is vital to have clear and defined roles and responsibilities. The image below provides a structure with defined roles and areas of responsibility which gives a preferable project management.



The project owner is the entity who has ordered the project, has overall responsibility for the project and must ensure that there is a clear mission and sufficient resources.

7.1.2 Project documents

A project of this magnitude need to have a certain level of control documents, at least the following:

- Project manager job description

- Project directive
- Project management plan
- Decision log
- Status report
- Final report

7.1.3 Activities

Activities that need to be fulfilled during the project should be decided when the project management plan is procuded. However, some activities seem more necessary for a sucessful outcome of the project, for instance:

- Review and decide on which management objects the project should establish government for.
- Analysis of the management objects, containing at least:
    - Risk analysis (for each of the management objectes as well as the overall perspective)
    - Needs analysis
- Benefit analysis
- Establishment of a management plan for each management object containing at least:
    - Annual schedule
    - System description
    - Roles and responsibilities
    - Budget
    - Processes and routines
- Establishment of an operating plan containing at least:
    - Forms for support and case management
    - Forms for service level agreement
- Overall cyber security
    - General Data Protection Regulation (GDPR)
- Establishment of the governance organization
    - Seat of the organization
    - Organizational structure
    - Staffing
    - Legal issues
- Hand over to the governance organization
- Decomissioning of the project organization

8 Recommendation

8.1 Establishment

Based on the work done within this project it is recommended that an establishment project is implemented to establich an organization that will maintain and develop a sustainable maritime digital infrastructure. Hence, developing an organization to manage the identified management objects.

It is strongly recommended that the project has a holistic and including approach to its task. To maintain and a develop a sustainable maritime digital infrastructure all stakeholders need to be a part of the project and the organization which will be the result of the project.

Proper funding, both to finance the establishment project and the organization which is intended to be established, needs to be secured.

8.2 Governance model

It is also recommended that pm3 model is used as a base for the governance model and that it's supplemented with relevant parts, needed for the development of an entire organization.

8.3 Overall cyber security

To achieve a satisfactory overall cyber security, i.e. identify potential risks to which STM will be encountered, it is recommended to perform the following:

- Risk analysis on the entire STM concept including the infrastructure and the proposed organization
- Identify if STM processes personal data and identify who is the controller and processor, may be several.
- Obtain a contingency plan
- Obtain an incident management process

38 partners from 13 countries - Creating a safer more efficient and environmentally friendly maritime sector

Demonstrating the function and business value of the Sea Traffic Management concept and its services.

SAFETY - ENVIRONMENT - EFFICIENCY

Swedish Maritime Administration ◦ SSPA ◦ RISE Viktoria ◦ Transas/ Wärtsilä Voyage ◦ Chalmers University of Technology ◦ The Swedish Meteorological and Hydrological Institute ◦ Danish Maritime Authority ◦ Navicon ◦ Novia University of Applied Sciences ◦ Fraunhofer ◦ Carnival Corp. ◦ Italian Ministry of Transport ◦ SASEMAR ◦ Valencia Port Authority ◦ Valencia Port Foundation ◦ CIMNE ◦ University of Catalonia ◦ Norwegian Coastal Administration ◦ GS1 ◦ Cyprus University of Technology ◦ Port of Barcelona ◦ Costa Crociere ◦ Svitzer ◦ OFFIS ◦ Finnish Transport Agency ◦ Southampton Solent University ◦ Frequentis ◦ Wärtsilä SAM Electronics ◦ University of Flensburg ◦ Airbus ◦ Maritiem Instituut Willem Barentsz ◦ SAAB TransponderTech AB ◦ University of Oldenburg ◦ Magellan ◦ Furuno Finland ◦ Rörvik ◦ University of Southampton ◦ HiQ

www.stmvalidation.eu

Co-financed by the Connecting Europe Facility of the European Union