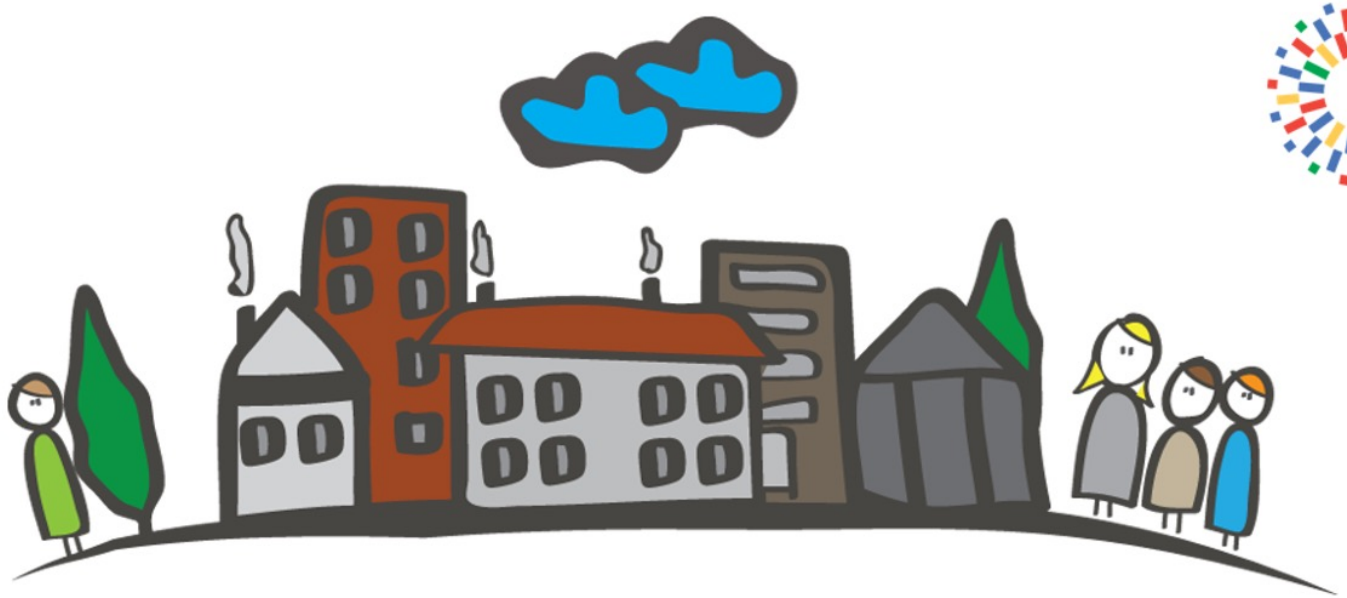
Etiske retningslinjer – Informasjonssikkerhet og beskyttelse av data



NORWEGIAN
SMART CARE
LAB

Tjenestepakken leveres av underleverandør
Egde i samarbeid med NSCL

Code of Conduct – Information Security and Data Protection

The norm for information security and privacy in the health and care service (the norm) is an agreed set of requirements for information security based on legislation.

A structured approach to implementation of the requirements will help both your organization and your device/service achieve the security level required for bringing your product to market.

This service package offers access to Information Security experts with extensive experience with the Code of Conduct for information Security in the Norwegian Healthcare Sector.

Egde

Practicalities

- Target group: members/partners/clients of NSCL
- Preliminary work facilitated by Egde, with inputs from company and subcontractor:
  - Identify the focus area of the workshops
  - Identify the companies needs
  - Set expectations, plan and prepare the three steps of digital workshops that will enable you to conform to national security requirements and recommendations, and properly securing your health and personal data.
- Governance: All participants must sign an NDA

Code of Conduct

The Code of Conduct for information security and data protection in the Norwegian healthcare industry is a holistic approach to an information security policy for organizations within the sector.

The Code of Conduct is rooted in the ISO/IEC 27000 family but offers a set of requirement directly targeted to organizations dealing with health data. The Code ensures a secure interoperability for all organizations that comply with the regulations set in the Code.

This service package will help to create a common understanding of the threats, requirements and offers an approach of how to deal with information security in businesses developing medical devices or services.

The service package will help the Company to implement the Codes requirements for the processing of health and personal data in medical equipment with associated system solutions and applications in a practical way.

Step 1 – Initiation Workshop

A workshop between the company and the subcontractor to define an initial overview of the scope of organizational requirements, data requirements and data flows for the Device or Service.

The company will be expected to share any relevant background information about their technology and organizational context. **Workload: 1-2 hours.**

During the workshop it is expected that the company will present their organizational structure, product, technology and objectives, as well as key milestones and delivery dates that need to be met. **Subcontractor** will facilitate a presentation of the main content of the Code of Conduct, and a discussion on the potential impact the implementation of the Code may have. **Workload: 3-4 hours.**

Outcome for this step will give the Company

- Visualised desired future state of the Company's Information Security Structure
- Overview of the guideline and security requirements of the Code of Conduct or other desired Information Security controls (ISO/IEC 27002)
- Overview of the requirements in the Code of Conduct not applicable for the Company

Step 2 – Mapping and Gap Analysis Workshop

This workshop is a collaboration between the Company and **subcontractor** to to determine what steps need to be taken in order to move from its current state to the desired, future state.

In the workshop, all applicable requirements will be reviewed, and it will be determined if the Company complies to the measure, or if additional organizational or technical measures need to be implemented.

With the output from this workshop the Company and **subcontractor** will have:

- An overall picture of the challenge areas.
- A list of high-level measures prepared with priorities and a timetable for when to solve the challenges.

Company input/ workload: technical and product input to a workshop of 6 hours plus follow-up questions.

Step 3 - Implementation

This step consists of collaboration between the company and **subcontractor** to define the course of action of when and how to close all gaps and associated risks.

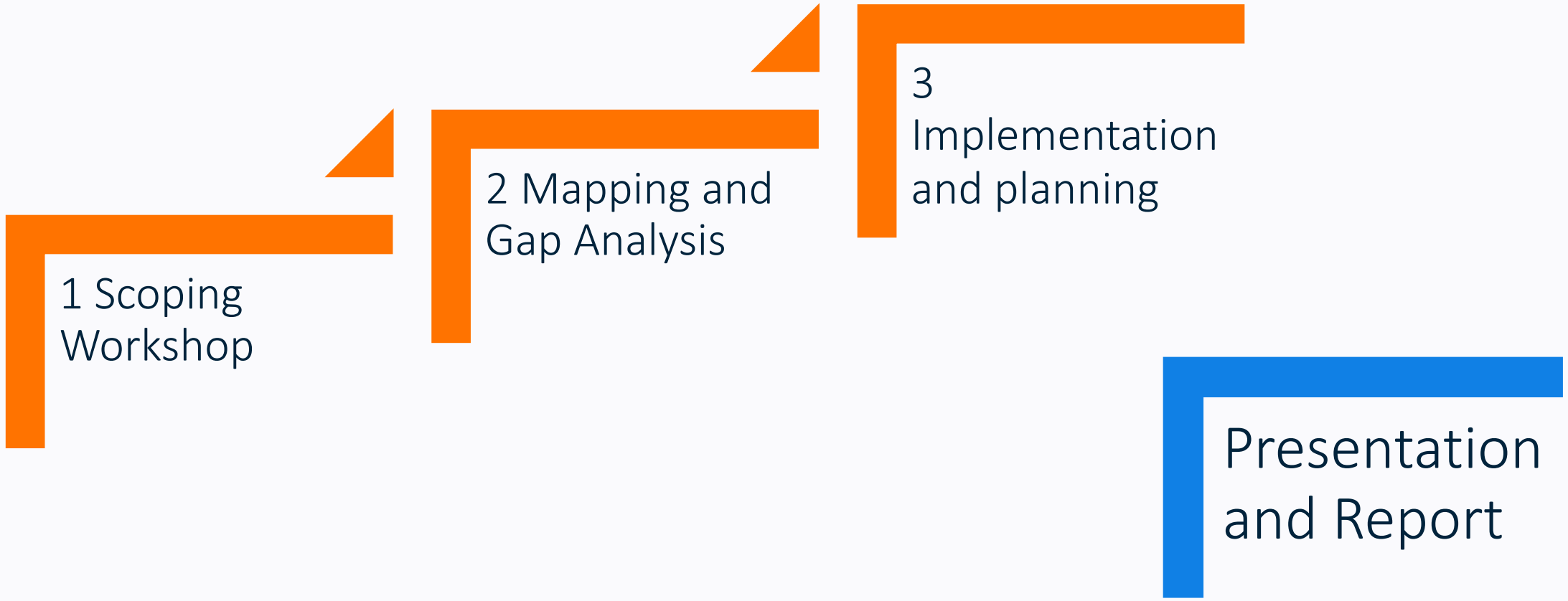
With the output of this step the Company will have a Risk Management file, containing:

- A documented Security Review/Gap analysis;
- Gaps are reported as information security risks (direct input to risk assessment);
- Risk Register for tracking mitigating all associated risks;
- A System Security Plan, including detailed measure to be implemented to comply with the Code of Conduct;
- A Organizational Security plan to comply with the Code of Conduct or other applicable Information Security Standard

***Company input**:* answer questions via email and online meetings as required. **Workload: 2-4 hours.**

***Outcome**:* will be presented to the company in a c.1 hour meeting and as a PowerPoint presentation.

Preparation & Execution Summary



Egde

Ta kontakt dersom du ønsker mer informasjon om hva pakken inneholder og hva laben kan tilby din bedrift.

Marit Hagland
Leder
Norwegian Smart Care Lab
+47 452 61 799
Marit.h@valide.no

Karoline Blikra Mokleiv
Forretningsutvikler
Norwegian Smart Care Lab
+47 92 414 043
karoline@valide.no