Kartverket

Cyber security – what are the risks and how do we handle them?

Stora Chefsmöte 2.-4. September 2019

Integrity
Availability

Background

Two serious events:

- Trojans in October in 2017
- Attempted crypto mining in January 2018

Audits and reviews:

- Office of the Auditor General
- Watchcom
- Internal audit
- Deloitte

Incident October 2017

- A core database in Kartverket was attacked
- The attack probably used a security hole in a component from a large international supplier used in several of our software solutions
- The security hole was exploited before the supplier was familiar with it
- The data in the base was not corrupted
- Everything indicates that the attack was carried out by an international player with huge strengths and ability

The big picture

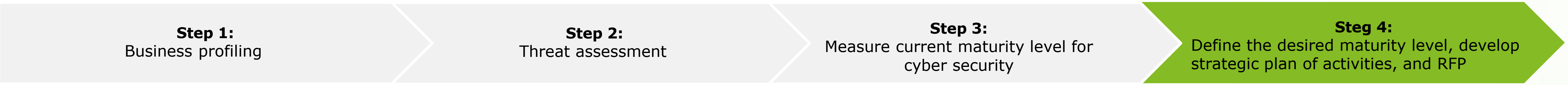
- Understanding the global situation
- Collaboration within the public sector
- Open data, a challenge?
- What are the impacts for NMCAs from the cyber risk
- How well are we prepared

Cyber security target

- ✓ Kartverket shall establish an IT cyber security level that will handle attacks by **state threat actors**

- ✓ To secure the information values against this type of threat actors, a **systematic, comprehensive and risk-based approach** to security work is necessary. It also involves establishing measures to **prevent** incidents, but also **to detect and respond** to incidents that occur.

Security evaluation of Kartverket

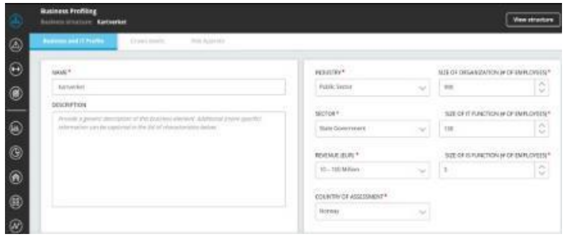


Step 1:
Business profiling

Step 2:
Threat assessment

Step 3:
Measure current maturity level for cyber security

Steg 4:
Define the desired maturity level, develop strategic plan of activities, and RFP



Business Profiling
Business structure: Kartverket
View structure

Business and IT Profile | Crown Jewels | Risk Appetite

NAME * Kartverket

DESCRIPTION
Provide a general description of the business element. Additional (more specific) information can be captured in the list of characteristics below.

INDUSTRY * Public Sector

SECTOR * State Government

REVENUE (EUR) * 10 – 100 Million

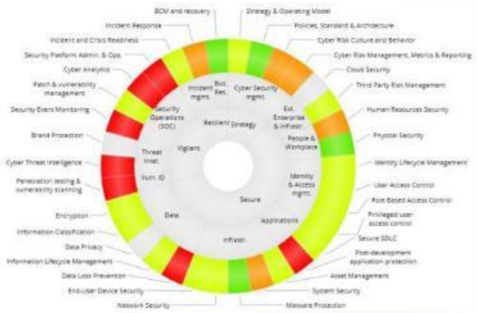
COUNTRY OF ASSESSMENT * Norway

SIZE OF ORGANIZATION (# OF EMPLOYEES) * 900

SIZE OF IT FUNCTION (# OF EMPLOYEES) * 150

SIZE OF IS FUNCTION (# OF EMPLOYEES) * 5

TOP THREAT SCENARIOS
TOP ATTACK VECTORS
TOP ADVERSARY GROUPS
Phishing
Ransomware
Social engineering
Spam
Insider



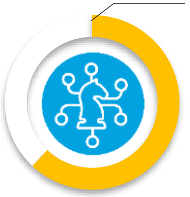
- ✓ Define the desired maturity level
- ❑ Develop strategic plan with activities to close gaps between preliminary and desirable maturity level
- ❑ Suggested safety organization
- ❑ List suggestions for RFP (Requirements for proposal)

Experience figures indicate that we must spend 10 - 15% of the annual IT budget over the next three years meet this security ambition

NIST – National Institute for Standards and Technology

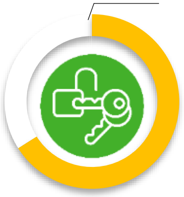
Overall results:

We see significant gaps across all analyzed areas in order to achieve the ambition level. The situation requires a substantial effort and a holistic approach.



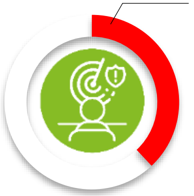
62%
achievement of objectives

Leadership and control



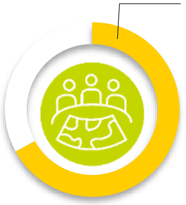
66%
achievement of objectives

Basic security



38%
achievement of objectives

Prevent and detect



67%
achievement of objectives

Respond and handle incidents

Leadership and control

Involves having the necessary structures and policies in place to maintain and improve the organization's security capabilities, thus providing a systematic, comprehensive, and risk-based approach to security work.

Basic security

Involves working proactively to protect systems and infrastructure from cyber attacks, by identifying, implementing, and improving the measures that protect the organization's values.

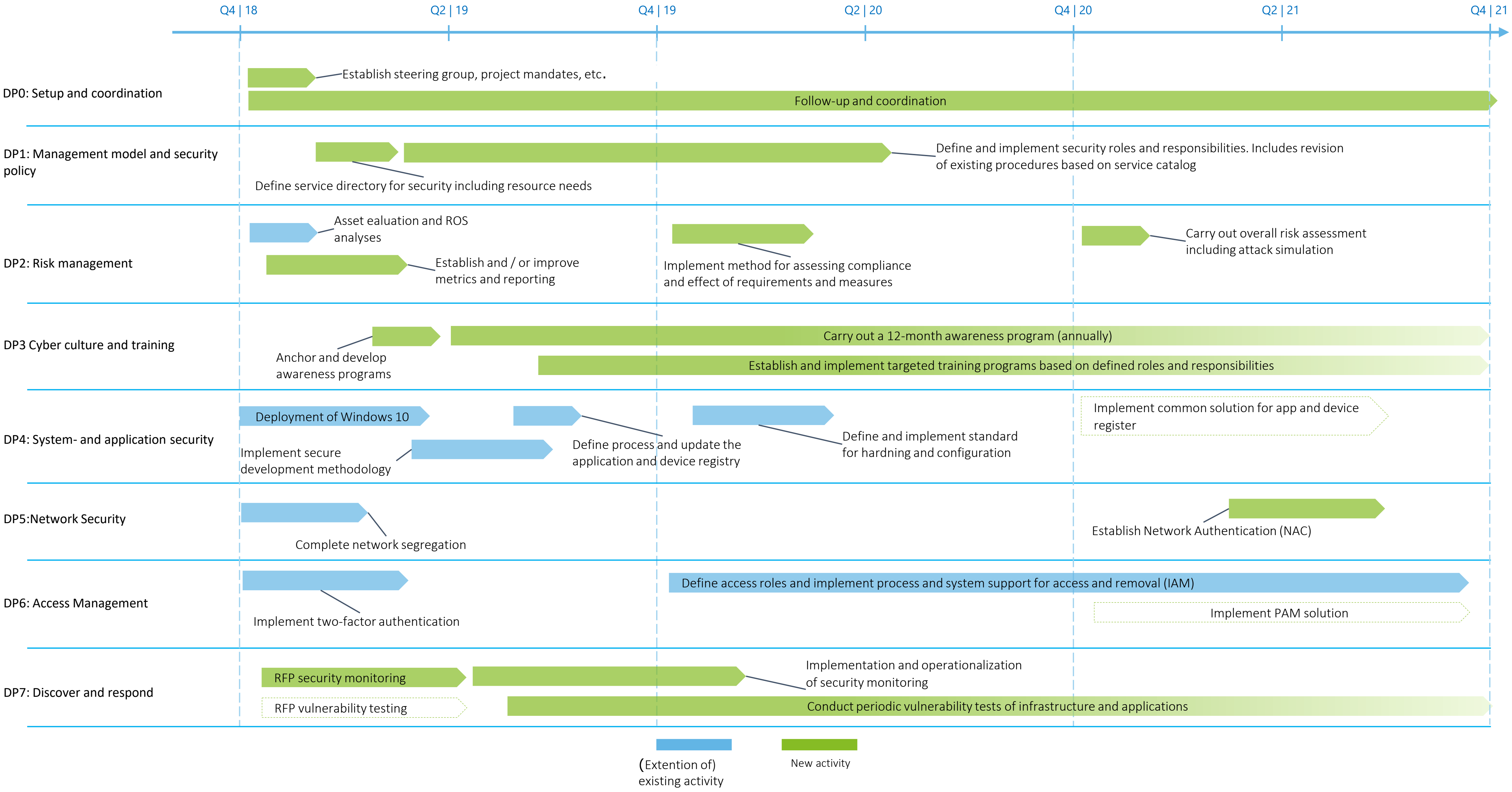
Prevent and detect

Involves the ability to detect internal and external threats by relying on intelligence and log sources, and work proactively to prevent incidents or minimize the consequences of such events.

Respond and handle incidents

Involves the ability to respond to security incidents that minimize the business impact.

Project plan



Q4 | 18
Q2 | 19
Q4 | 19
Q2 | 20
Q4 | 20
Q2 | 21
Q4 | 21

DP0: Setup and coordination

Establish steering group, project mandates, etc.

Follow-up and coordination

DP1: Management model and security policy

Define service directory for security including resource needs

Define and implement security roles and responsibilities. Includes revision of existing procedures based on service catalog

DP2: Risk management

Asset ealuation and ROS analyses

Establish and / or improve metrics and reporting

Implement method for assessing compliance and effect of requirements and measures

Carry out overall risk assessment including attack simulation

DP3 Cyber culture and training

Anchor and develop awareness programs

Carry out a 12-month awareness program (annually)

Establish and implement targeted training programs based on defined roles and responsibilities

DP4: System- and application security

Deployment of Windows 10

Implement secure development methodology

Define process and update the application and device registry

Define and implement standard for hardning and configuration

Implement common solution for app and device register

DP5:Network Security

Complete network segregation

Establish Network Authentication (NAC)

DP6: Access Management

Implement two-factor authentication

Define access roles and implement process and system support for access and removal (IAM)

Implement PAM solution

DP7: Discover and respond

RFP security monitoring

RFP vulnerability testing

Implementation and operationalization of security monitoring

Conduct periodic vulnerability tests of infrastructure and applications

🟦 (Extention of) existing activity

🟩 New activity

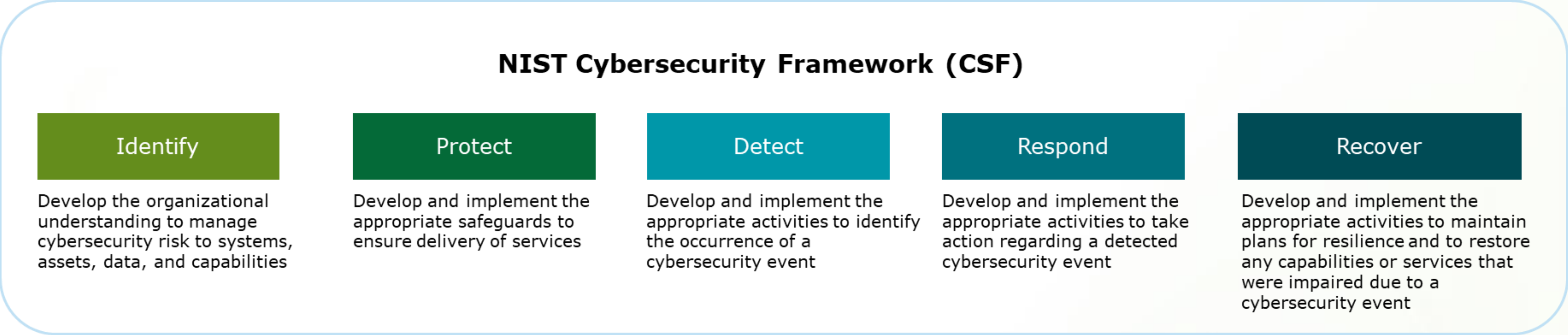
The road ahead – a three year program

- The program sets Kartverket in the driver's seat regarding cyber security

- Established a three-year comprehensive program to achieve level four according to the NIST standard

- Ensure that other parallel activities are also well coordinated with this program

Approach



NIST Cybersecurity Framework (CSF)

Identify	Protect	Detect	Respond	Recover
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Develop and implement the appropriate safeguards to ensure delivery of services	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

- NIST Security service catalog
  - Controls

- Agee current security level
- Establish delta to NIST Level 4
- Implement new controls, awareness programs etc

Discussion / reflexions

- Reflect on this presentation and how you are prepared
- Is this kind of incidents a threat to your reputation?
- Is there a value in being open about this kind of incidents?