Cybersecurity og risikohåndtering

Kartverket

Nokios 31. oktober 2019

Olav Petter Aarrestad

Fakta om Kartverket

365 mill oppslag i Matrikkelen pr. år

1,5 mill tinglysinger pr. år

1200 servere, 12 PB lagrings-kapasitet

80 000 km2 flyfotograferes hvert år

Nasjonal geoportal for alle off. etater og kommuner

Navigasjons-kartene til sjøs inngår i kritisk infrastruktur

Kartverket

Trusselbildet er reellt

- En alvorlig sikkerhetstruende hendelse oppdaget oktober 2017
- Antatt angrepsvektor via hull i standard programvare
- Godt samarbeid med NorCERT
- Foretok strakstiltak
- PST og andre deler av NSM ble også involvert i tiltakene
- En «nødvendig» vekker
  - besluttet å sette i gang et dedikert sikkerhetsprosjekt

Integritet
Tilgjengelighet

Tillit

Sikkerhetsmål

- Kartverket skal etablere et IT sikkerhetsnivå som vil håndtere angrep fra **statlige trussel aktører**

- For å sikre informasjonsverdiene mot denne typen trussel aktører er det nødvendig med en ***systematisk, helhetlig og risikobasert tilnærming*** til sikkerhetsarbeidet. Det innebærer videre å etablere tiltak for å kunne ***forhindre*** hendelser, men også ***oppdage*** **og** ***respondere*** på hendelser som inntreffer.

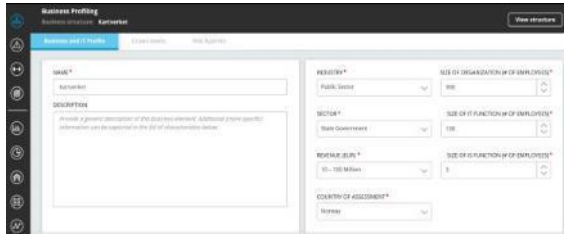
Sikkerhetsevaluering av Kartverket 2018

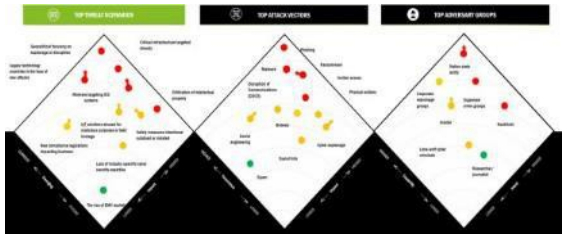
Steg 1:
Forretningsprofilering

Steg 2:
Trusselvurdering

Steg 3:
Måle nåværende modenhetsnivå for cyber sikkerhet

Steg 4:
Definere ønsket modenhetsnivå, utvikle strategisk plan med aktiviteter, og RFP





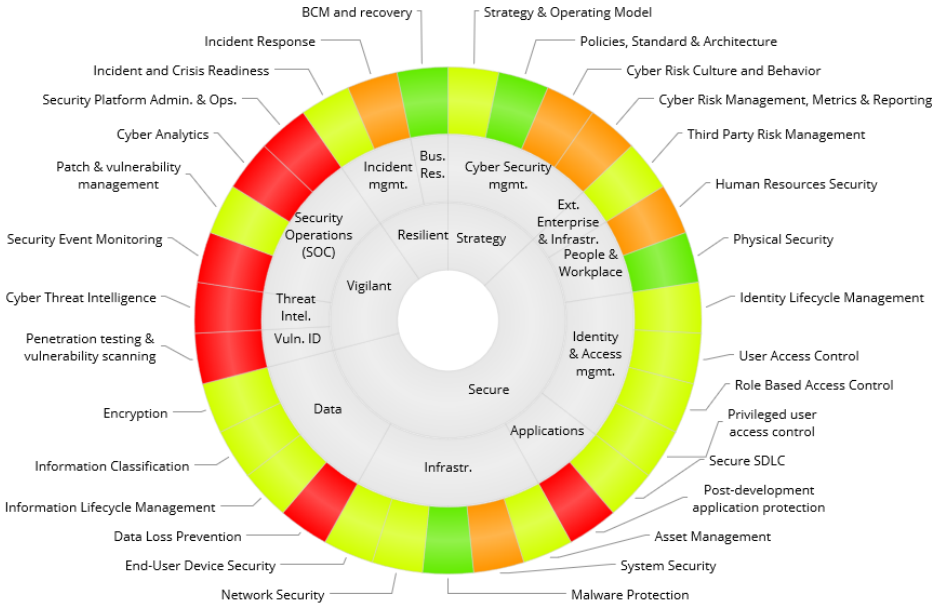
- ✓ Definere ønsket modenhetsnivå
- ❑ Utvikle strategisk plan med aktiviteter for å lukke gap mellom foreløpig og ønskelig modenhetsnivå
- ❑ Forslag til sikkerhetsorganisasjon
- ❑ Liste opp forslag til RFP (Requirements for proposal)

Erfaringstall tilsier at vi må bruke 10 – 15 % av årlig IT-budsjett de neste tre årene for å møte denne sikkerhetsambisjonen

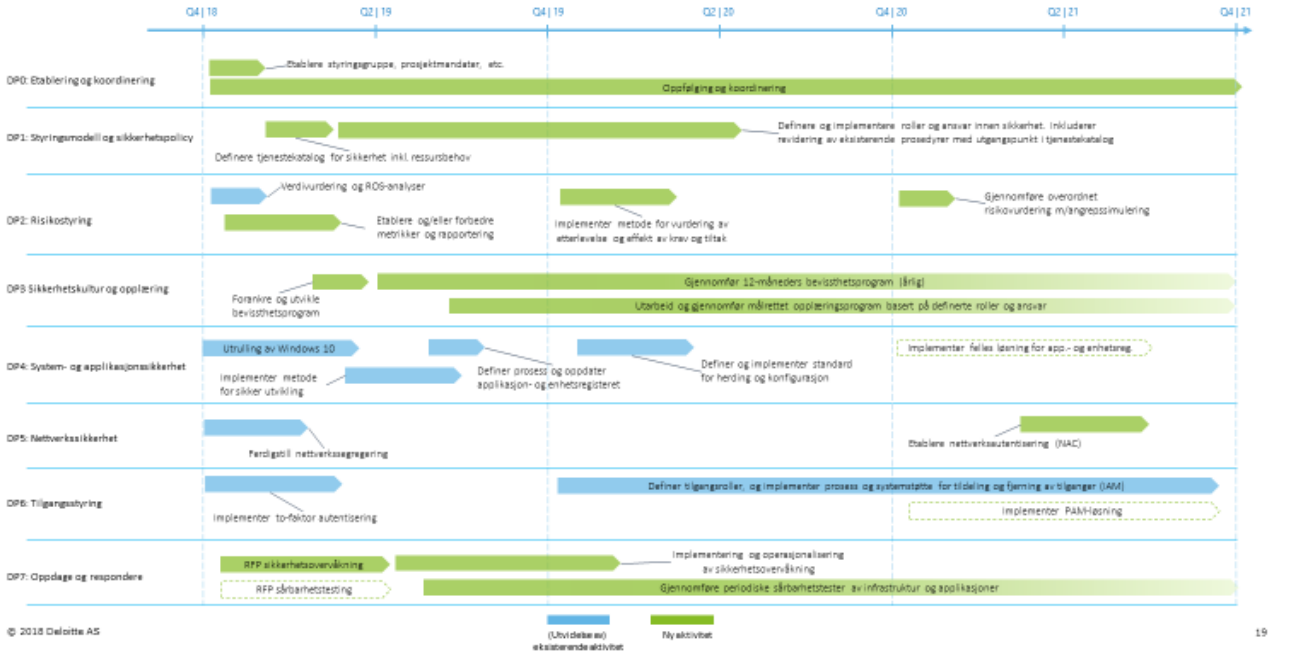
NIST – National Institute for Standards and Technology

Fra innsikt til handling

Kartverket gjør mye bra, men ambisjonsnivået gir et betydelig gap som må adresseres

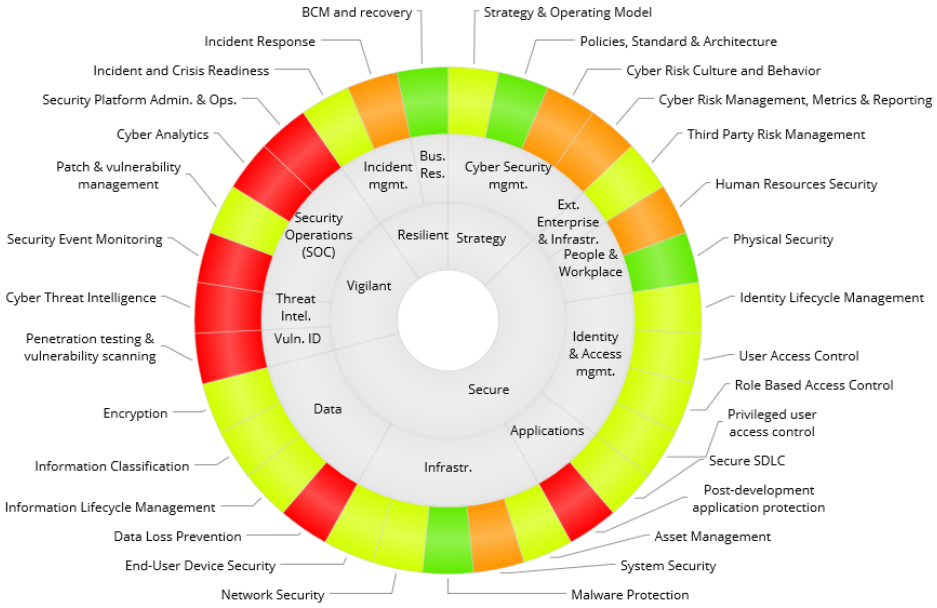


Tidslinjen for handlingsplan



Kartverket

Kartverket gjør mye bra, men ambisjonsnivået gir et betydelig gap som må adresseres



Tidslinjen for handlingsplan

Del-prosjekter

DP0: Etablering og koordinering

DP1: Styringsmodell og sikkerhetspolicy

DP2: Risikostyring

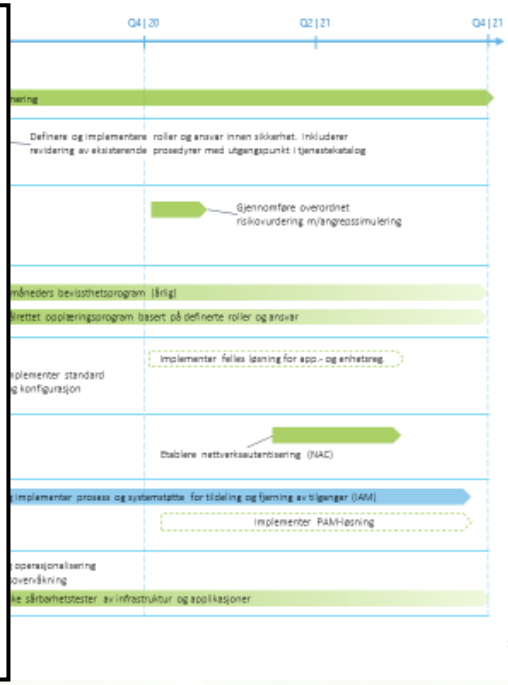
DP3: Sikkerhetskultur og opplæring

DP4: System- og applikasjonssikkerhet

DP5: Nettverkssikkerhet

DP6: Tilgangsstyring

DP7: Oppdage og respondere



Kartverket

Hvordan gå fra innsikt til handling?

- Benytter NIST CyberSecurity Framework som overordnet rammeverk for arbeidet

- **Vi tar utgangspunkt i tre kontrollrammeverk:**
  - CIS Critical Security Controls
  - NIST 800-53
  - ISO 27001

Kategoriene i NIST CSF knyttes til de ulike del-prosjektene

- **Arbeidsgruppene vurdere tilhørende kontroller**
  - Er kontrollen relevant?
  - Tilpasse kontrollen til Kartverket
  - Sørger for operasjonalisering (inkl. hand-over til linjen)

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

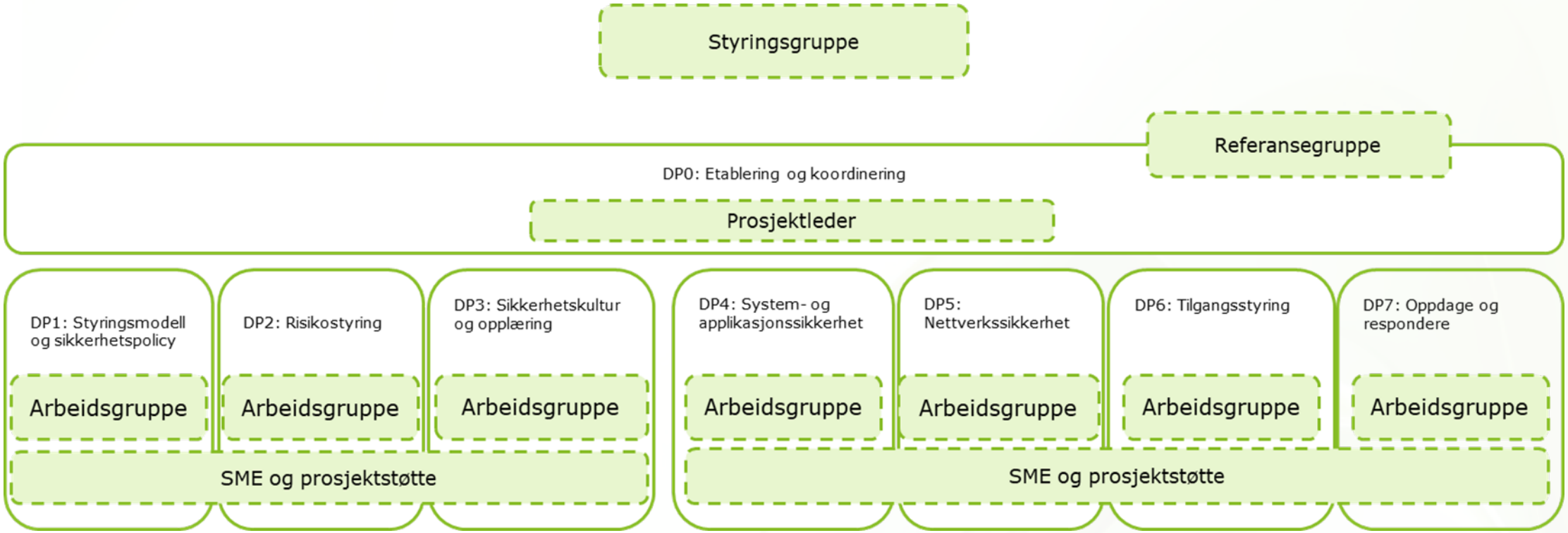
Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

http://www.nist.gov/cyberframework/online-learning/components-framework

Kartverket

Forankring, involvering og kommunikasjon

- Kartverkssjefen i linje
- Divisjonsdirektørene i styringsgruppen
- Arbeidsgruppene består av medarbeidere på tvers av divisjonene



Kartverket