

National Genom Center Forskningsinfrastruktur

Troels Rasmussen , ISO projektleder

Jacob Gemmer Gasberg Hansen, Sektionsleder Compliance

DEIC konference 2022 26.10 kl 14.30

Dagsorden

- Om Nationalt Genom Center: Hvad er vores kerneopgave?
- Hvad er ISO? – hvordan implementerede vi det!
- Styring af risiko i et komplekst HPC miljø
- Q/A





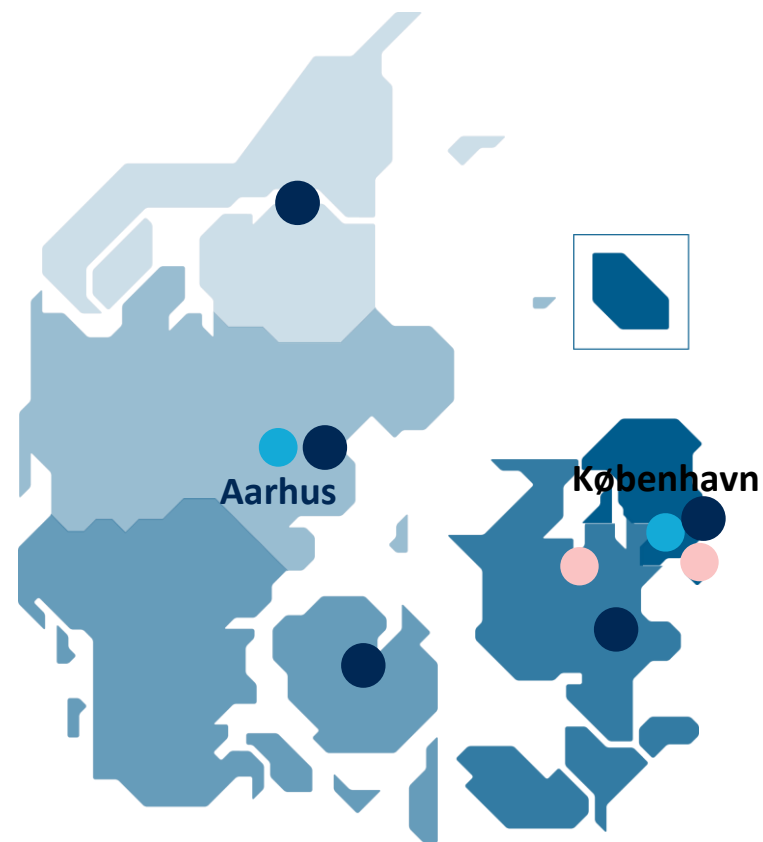
DANISH NATIONAL
GENOME CENTER

Om Nationalt Genom Center

- Hvad er vores kerneopgave ?

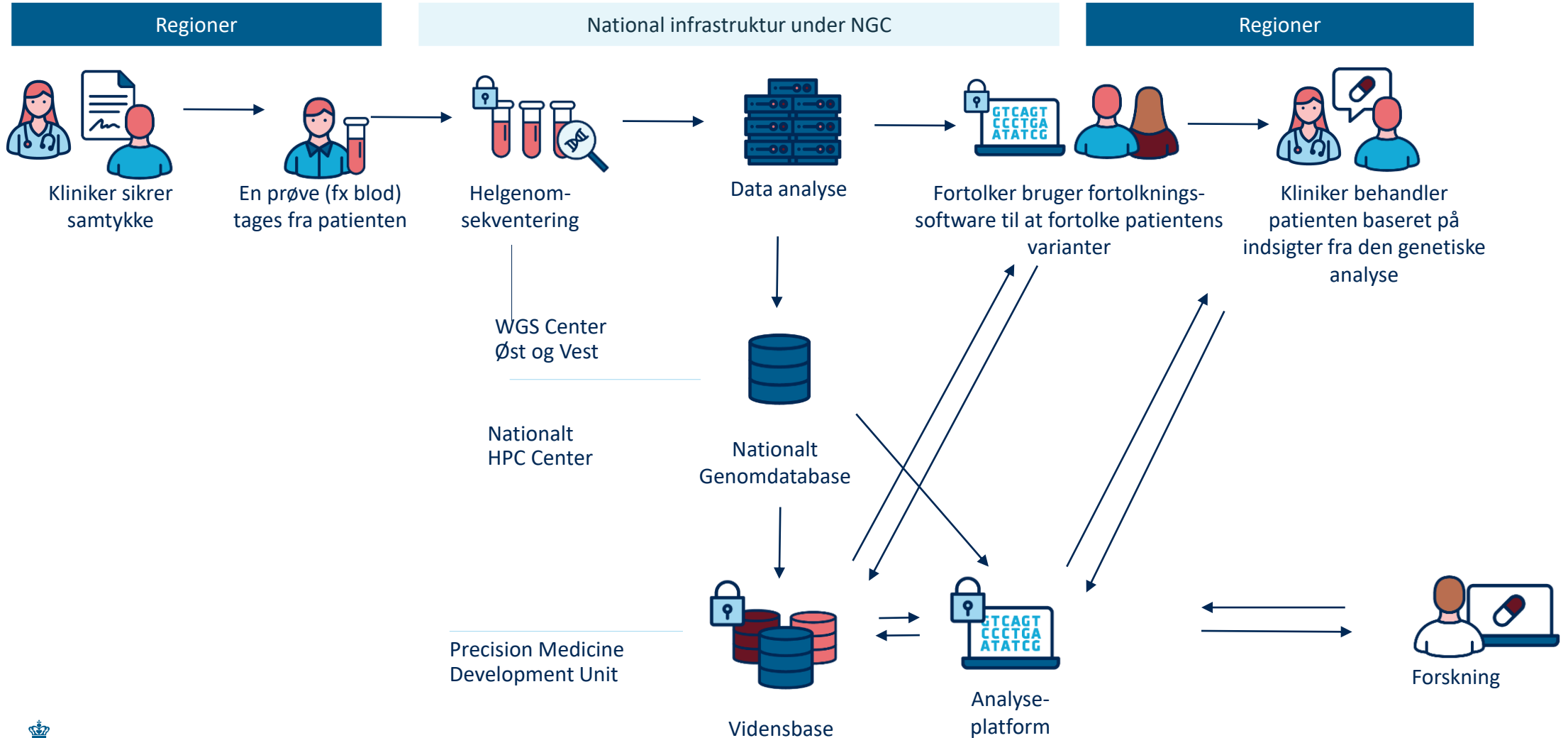
Nationalt Genom Centers kerneydelse

- NGC skal **understøtte læger, sundhedsfagligt personale og forskere** ved at udvikle og drive en **national infrastruktur** med følgende elementer:
 - A** Nationalt Center for Helgenomsekventering (faciliteter i Øst/Vest)
 - B** Nationalt High Performance Computing (HPC) Center til sikker opbevaring og analyse af genetiske oplysninger
 - C** Nationale vidensbaser og fortolkningsværktøjer til analyse af genetiske data
- Det primære fokus er at sikre **bedre og hurtigere diagnostik og behandling af patienter** – 60.000 helgenomsekventeringer af patienter forventes de næste 4,5 år



- Nationalt Genom Center og High Performance Computing Center
- Nationalt Center for helgenomsekventering i Øst- og Vestdanmark
- Universitetshospitaler

Forholdet mellem de forskellige elementer af infrastrukturen





NGC's supercomputer – netværk af 400 servers

Thin servers:

40 core 2.1GHz CPU, 192GB RAM, 1.9TB SSD, 10GB Ethernet, 100GB InfiniBand

Fat servers:

40 core 2.1GHz CPU, 1.536GB RAM, 3.8TB SSD, 10GB Ethernet, 100GB InfiniBand

GPU servers:

40 core 2.1GHz CPU, 192GB RAM, 1.9TB SSD, NVIDIA Tesla V100 16GB, 10GB Ethernet, 100GB InfiniBand



MANAGEMENT SYSTEM CERTIFICATE

Certificate no.: C553255

Initial certification date: 26 July 2022

This is to certify that the management system of **Nationalt Genom Center** Ørestads Boulevard 5, 2300 København S, Denmark and the sites as mentioned in the appendix accompanying this certificate

has been found to conform to the **ISO/IEC 27701:2019**

This certificate is valid for the following scope: **Privacy Information management related to data-, cloud- and High-Performance Computing services and the administrative processes, in accordance with 19.05.2022 Annex A**

This certificate depends on the following conditions:

Place and date: London, 26 July 2022



MANAGEMENT SYSTEM CERTIFICATE

Certificate no.: C534919

Initial certification date: 26 July 2022

This is to certify that the management system of **Nationalt Genom Center** Ørestads Boulevard 5, 2300 København S, Denmark and the sites as mentioned in the appendix accompanying this certificate

Valid: 26 July 2022 – 25 July 2025

has been found to conform to the Information Security Management System standard: **ISO/IEC 27001:2013**

This certificate is valid for the following scope: **Information security management system for data-, cloud- and technology processes for the development and operations of a High-Performance Computing infrastructure, the genome and variant databases, cloud services and the administrative processes, in accordance with statement of applicability 24.03.2022.**

Place and date: London, 26 July 2022

International Organization for Standardization

ISO

27001



For the issuing office:
DNV - Business
4th Floor
Le

Hvad er ISO 27001 og hvad er målet

- ISO 27001 er en international standard for hvordan man administrerer informationssikkerhed
- ISO 27001 er sikkerhedsstandarden for statslige myndigheder i Danmark
- Certificering er ikke målet, men resultatet
- ISO certificering er ikke garanti for høj sikkerhed

Tager udgangspunkt i:

- Institutionens risikoprofil – og risikostyring
- Ledelsesansvar og –inddragelse
- Roller og ansvar
- Gennemførelse af kontroller
- Uddannelse og awareness
- Dokumentstyring – aktive dokumenter der beskriver alt det ovenfor

ISO projektet – Implementering af ISO 27001 standard

SCOPE – Hele NGC's forretning – det vil sige alle medarbejdere, alle relationer, alle processer, alle tekniske elementer – adgangskontrol, leverandører - alt!

Hovedudfordringer:

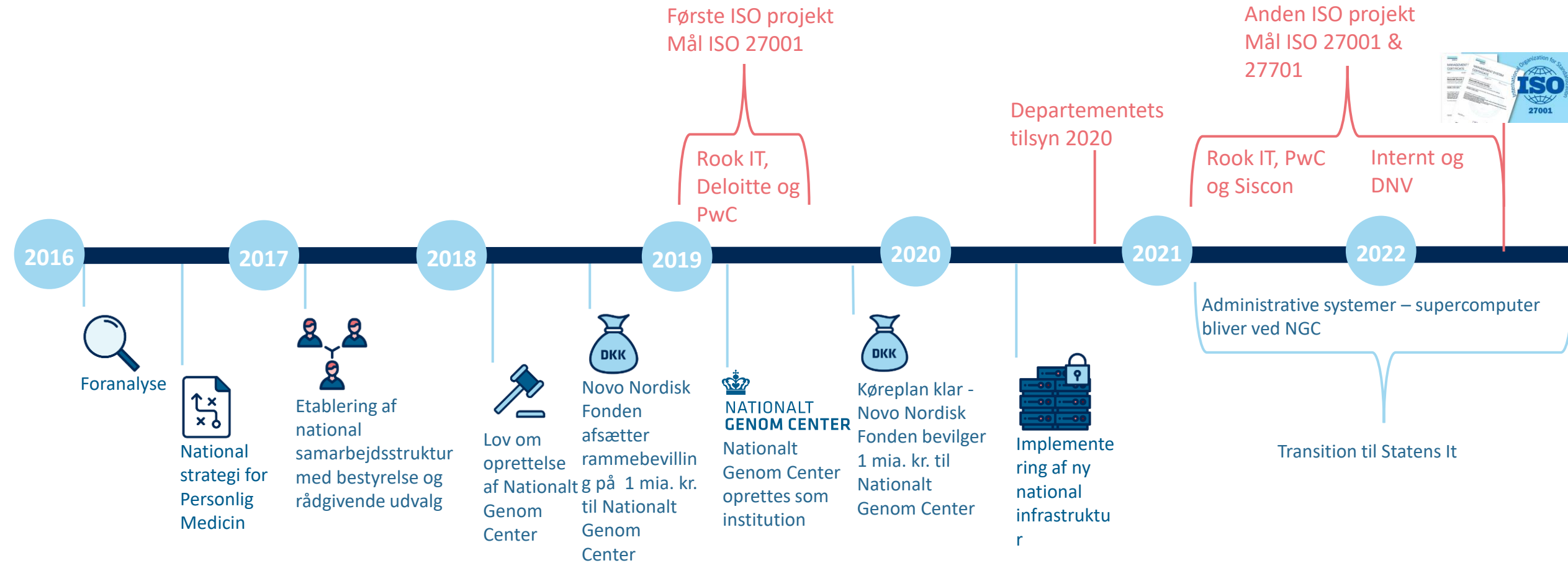
- NGC er en startup – etableret i juni 2019
- fra 3 medarbejdere i 2018 til 85 i 2022.
- Alt er nyt – begrænset struktur, ingen erfaring – alt skal udvikles og opbygges
- Rigtig mange udviklingsaktiviteter parallelt – Brugerstyring, workflows, software, integration med klinikker, infrastruktur
- Mange forskellige fagligheder – Dataspecialister, HPC managers, Jurister, Bioinformatikere, Klinikere, DJØF'ere
- Vi er en statslig styrelse – mellem Regioner og Departement

Styrker:

- Stærkt mandat fra Departementet og stor Novo bevilling
- Ren kanvas – kan bygge noget op fra bunden uden for meget legacy
- Nye medarbejdere – etablering af stærk sikkerhedskultur

Lille organisation – korte beslutningsgange

Tidslinje for NGC's ISO certificering



Lessons learned

- Målet er ikke at få et certifikat – det er at få et ledelsesystem i drift – det er vigtigt at kommunikere til medarbejdere og ledelse – Det rigtige arbejde starter når certifikatet er i hus.
- Forvent modstand – brug den konstruktivt – Langt de fleste er ikke imod! Men der skal sluges faglige kameler
- Prioritering – afhængig af medarbejdere der har andet at lave – Understøt, motivér og tving ledelsen til at træffe beslutninger
- Udbuddet af konsulenter (ikke mindst på SKI er ringe) – Mere proceskonsulenter end faglige sparringspartnere.
- Brug af konsulenter er bekvemme shortcuts – men ejerskabet er organisationens og konsulenter driver ikke ting fremad
- Omfanget af projektet steg inkrementelt i takt med at problemer blev identificeret
- Dokumentér fremdrift – Stærkt kommunikationsmiddel til ledelsen
- Balancegang – Fagpersoner – Har know how - skal drive implementeringen OG blive monitoreret/kontrolleret



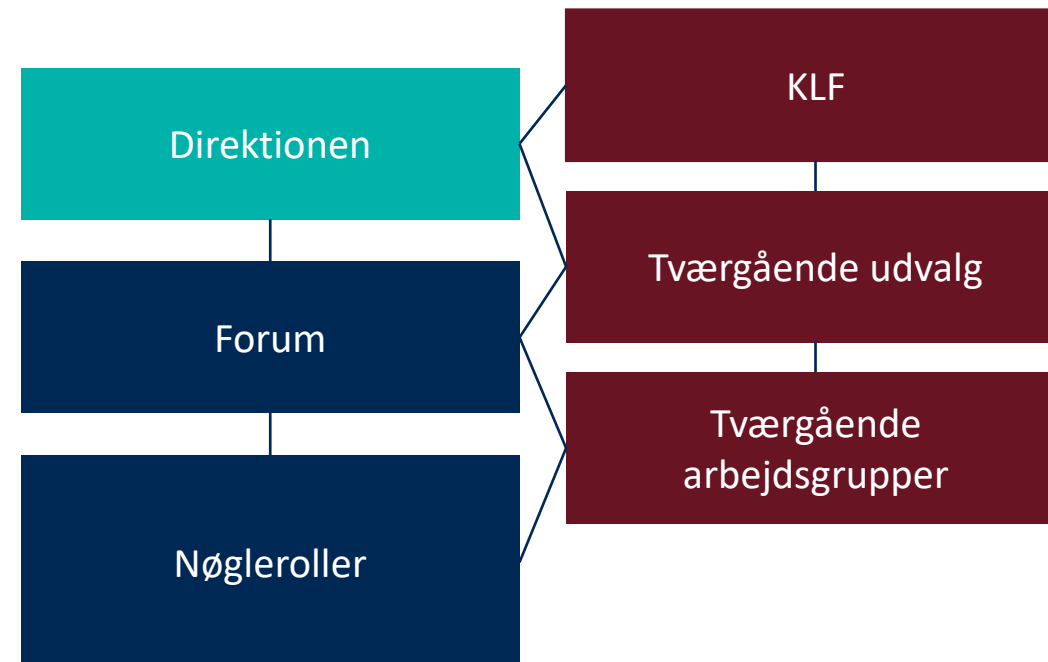
NATIONALT
GENOM CENTER

NGC's ledelsessystem for informationssikkerhed og persondatabeskyttelse



Organisation, roller og ansvar

- NGC er selv ansvarlig for NGC's eget ledelsessystem, men der kommer både krav, rammer og vejledninger fra koncernfælles fora
- Der er ikke fast rapportering til NGC's direktionen. Det er der til NGC's forum for informationssikkerhed og forummet vurderer hvad der skal videre til direktionen. Er der en høj risiko for NGC eller den registrerede rapporteres det til direktionen så hurtigt som muligt.
- På det operative niveau er der beskrevet 30 nøgleroller. Der er roller som har væsentlige opgaver i forhold til informationssikkerhed og persondatubeskyttelse
- Alle medarbejdere skal deltage i quiz's og bekræfte at de efterlever NGC's regler for acceptabel brug. Mens nøglerrollerne gennemgår en særlig træning og opfølgning.



▼ Resources, competencies and capabilities

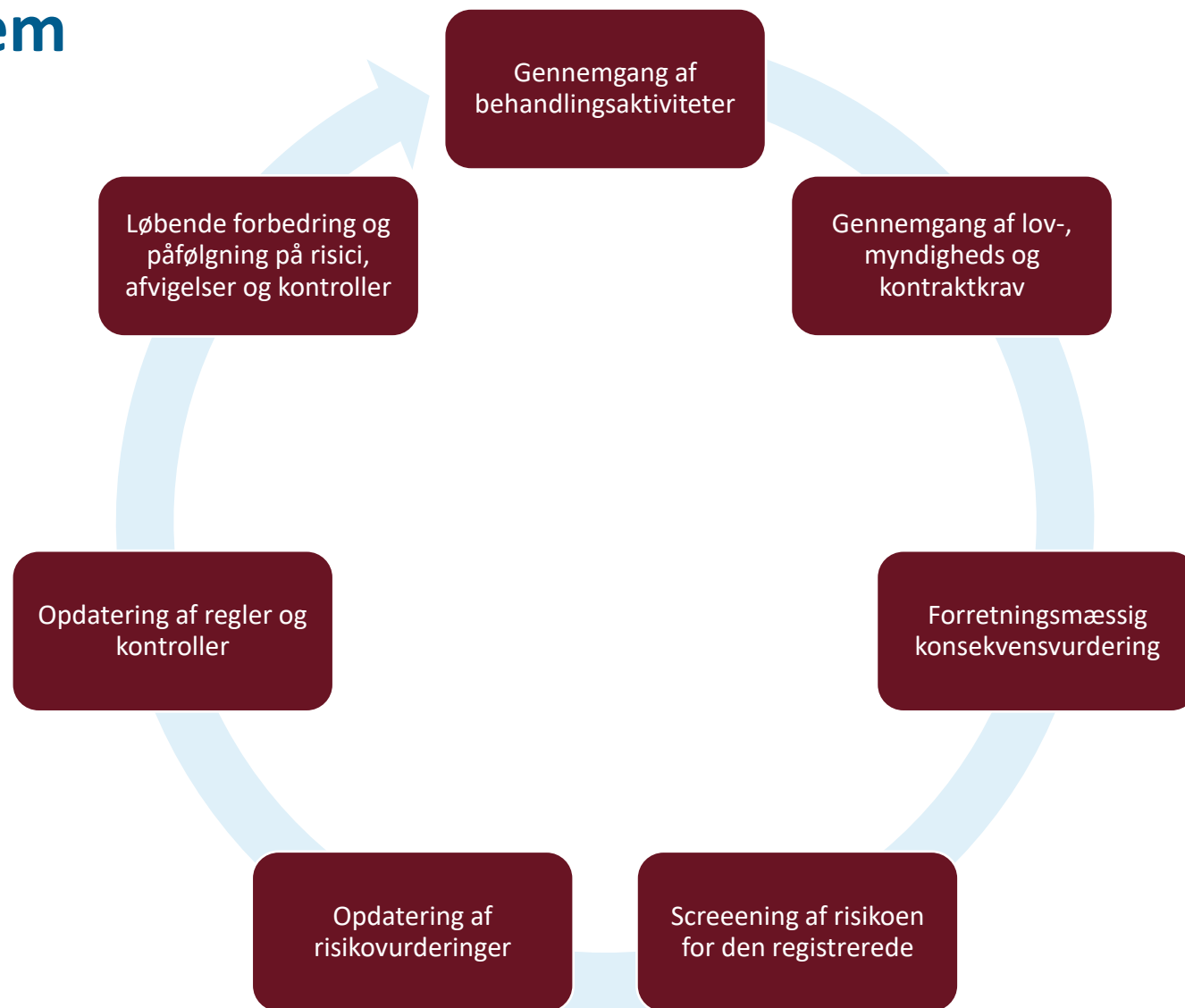
- Chief of Information Security and Personal Data Protection
- Information Security Officer (CISO)
- › Data Protection Agent (DPA)
- Business Continuity Officer
- Awareness Officer
- HPC Platform Manager
- Incident Manager
- Change Manager
- Identity and Access Officer
- Log and Security Event Officer
- Monitoring and Detection Officer
- Network Security Architect
- System Security Architect
- HR security officer
- Asset Manager
- Data Manager

Overview of roles essential for the ISMPS:

| Role | Primary | Secondary |
|--|-------------------------|--|
| Chief of Information Security and Personal Data Protection | Christian Dubois | Camilla Borchorst |
| Information Security Officer (CISO) | Jacob Hansen | Elisabeth Odélgård Helm Lars Emde Poulsen |
| Data Protection Agent (DPA) | Lars Emde Poulsen | Jacob Hansen |
| Business Continuity Officer | Elisabeth Odélgård Helm | Jacob Hansen (Crisis and compliance) Ali Syed (Recovery, restore and Back-up) |
| Awareness Officer | Elisabeth Odélgård Helm | Jacob Hansen |
| HPC Platform Manager | Ali Syed | Rafal Wolanin/ Damon Kasajak / Carsten Stiborg |
| Incident Manager | Martin Anqvist | Lars Poulsen / Sayan Roy |
| Change Manager | Tue Bendtsen | Sayan Roy |
| Identity and Access Officer | Damon Kasajak | Sayan Roy |
| Log and Event Officer | Torben Jakobsen | Sayan Roy |

Årshjulet for NGC ledelsessystem

- Helt overordnet består NGC ledelsessystem af et årshjul med de syv faser der fremgår af figuren til højre
- Ledelsessystemet systemunderstøttes af fire systemer Confluence, ControlManager, WorkZone and Intranettet.
- Confluence anvendes til dokumentation
- ControlManager understøtter compliance, kontrol og tilsyn
- WorkZone anvendes til dokumentation, der ikke effektivt kan være i Confluence
- Intranettet anvendes til at udstille dokumenter til alle medarbejdere



NGC's 14 behandlingsaktiviteter

- Alt arbejdet med informationssikkerhed og persondatabeskyttelse tager udgangspunkt i behandlingsaktiviteterne
- Vi anvender Confluence til at dokumentere behandlingsaktiviteterne
- Vi laver en screening af risikoen for den registrerede og en forretningsmæssig konsekvensvurdering. Ud fra de vurderinger, vurderes det om der skal laves en DPIA og processen får en kritikalitet

- ▾ Data Protection Impact Assessment
- ▾ HPC processing activities
 - NGC Controller - Indsamling og opbevaring af genetiske data
 - ▾ NGC Controller - Udstilling af genetiske data
 - Screening af risikoen for den registrerede - Udstillinger af genetiske data
 - Business Impact Assessment - Udstillinger af genetiske data
 - ▾ Systematisk beskrivelse - Udstillinger af genetiske data
 - Artikel 30 oplysninger - Udstillinger af genetiske data
 - Risikostyring - Udstillinger af genetiske data
 - Hearing of the data subject other stakeholders - Udstillinger af ge...
- ▾ NGC Processor - Cloud services
- NGC Controller - Drift og sikkerhed
- ▾ OLD NGC Processor - NGC managed clouds (cloud services)
- ▾ OLD NGC Processor - Self managed clouds (cloud services)
- ▾ OLD NGC Processor - Strategiske samarbejdspartnere (cloud services)
- ▾ NGC Administration processing activities

Systematisk beskrivelse - Udstillinger

Oprettet af Lars Emde Poulsen, senest ændret d. okt. 03, 2022

Formålet med den systematiske beskrivelse, er, at give dataansvarlig, projekt grundlæggende beskrivelse af processen med at skabe et overblik over akt hvilke risici der er forbundet med en aktivitet eller et aktiv, er det en fordel, hvilke midler der anvendes, og beskriver den kontekst som aktiviteten skal Den systematiske beskrivelse af behandlingsaktiviteten opfylder også kravene bl.a. fremgår, at (august 2020, side 6 (dataansvarlig)):

- "I visse tilfælde vil du dog kunne samle flere behandlingsaktiviteter i ét formuleres under ét samlet, logisk og sammenhængende formål. Det v...

Identification of Data Processing Activities

The purpose of this document is to identify the Processing Activities in the context of the processing operations. To this end, the processing activities are identified and described in a structured way. The identification of processing activities is a key step in the DPIA process.

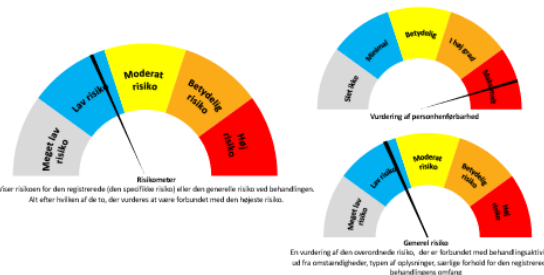
| No | Data Processing | Local or Shared Process | Impact level (see Impact scale) | IT Dependencies | Internal Dependencies | External Dependencies |
|----|---------------------------|-------------------------|---------------------------------|-----------------|-----------------------|-----------------------|
| 1 | Indsamling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 2 | Behandling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 3 | Udstilling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 4 | Udstilling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 5 | Udstilling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 6 | Udstilling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 7 | Udstilling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |
| 8 | Udstilling af DNA/protein | Local | 5. Catastrophic | IT Support | None | None |

Udvalgte aktiviteter - konsekvensanalyse (DPIA) af

Udvalgte aktiviteter - konsekvensanalyse (DPIA) af...
 Vurderingen er kun vejledende. Projektteamet eller den dataansvarlige er ansvarlige for at foretage en rettslig vurdering og høring af DPA og DPO.

| | Lav | Moderat | Høj |
|--------------------------------------|-----|---------|-----|
| Omtæthed af oplysninger | | | |
| Typen af oplysninger | | | |
| Særlige forhold for den registrerede | | | |
| Behandlings omfang | | | |

| Individuelle konsekvenser | 1. Liv | 2. Helse | 3. Medicin | 4. Arbejd | 5. Andet |
|--------------------------------------|--------|----------|------------|-----------|----------|
| Liv, psyk og helbred | | | | | |
| Mønstre eller materiel | | | | | |
| Ære og omdømme | | | | | |
| Forskerbeholdning og sikkerhed | | | | | |
| Identitetstyper eller identitetssvig | | | | | |
| Sociale forhold | | | | | |
| Registreredes rettigheder | | | | | |
| Fysiske personers frihedsrettigheder | | | | | |
| Technologisk risiko | | | | | |



Specifikke risiko

| | 1. Liv | 2. Helse | 3. Medicin | 4. Arbejd | 5. Andet |
|--------------|--------|----------|------------|-----------|----------|
| 1. Identitet | 0 | 0 | 0 | 0 | 0 |
| 2. Helse | 0 | 0 | 0 | 0 | 0 |
| 3. Medicin | 0 | 0 | 0 | 0 | 0 |
| 4. Arbejd | 0 | 0 | 0 | 0 | 4 |
| 5. Andet | 0 | 0 | 0 | 0 | 2 |

Er arket udfyldt korrekt?

| | |
|--------------------------------------|----|
| Omtæthed af oplysninger | OK |
| Typen af oplysninger | OK |
| Særlige forhold for den registrerede | OK |
| Behandlings omfang | OK |
| Mulige konsekvenser | OK |
| Personhenførelse | OK |

operations
 recovering data and processes

Management review

- Alle risici, herunder uoverensstemmelser, skal rapporteres til forummet
- Hændelser skal rapporteres til forummet månedligt
Høje risici for den registrerede og NGC skal løbende rapporteres til bestyrelsen
- Uvildig vurdering af eksterne (én gang om året) og interne gennemgang (én gang om året) rapporteres til forum og direktion
- Sårbarhedsscanninger og pentest udført af NGC eller eksterne, skal rapporteres til forummet og direktionen, hvis der er høje risici
- Bestyrelsen skal gennemgå og godkende de årlige risikovurderinger af behandlingsaktiviteterne
- Driftsmodellen for ISPMS skal gennemgås en gang årligt af forummet og derefter bestyrelsen



Compliance

- Lov-, myndigheds- og kontraktkrav er lagt ind i NGC's GRC system og relateret til NGC regler for informationssikkerhed og persondataskyttelse.
- Risikovurderinger er også lagt ind som krav.

| Status | Titel |
|--------|--|
| ✓ | ISO/IEC 27001 Informationssikkerhed (2) |
| | ISO 27001:2017 – ISMS |
| ● | SoA – Statement of applicability ISO 27001 (ISPMs) |
| | ISO 27001:2017 Anneks A |
| ● | SoA – Statement of applicability ISO 27001 – Appendix A |
| > | ISO/IEC 27701 privatlivsbeskyttelse (3) |
| > | ISO27XXX, øvrige standarder for informationssikkerhed, IT-sikkerhed, cybersikkerhed og persondataskyttelse (1) |
| > | Databehandlerkrav (9) |
| > | Myndighedskrav (3) |
| > | Behandlingsaktiviteter i HPC (7) |
| > | Organisatoriske og tekniskekrav fra fortegnelserne i administrationen (10) |

Krav

- ● 9. Adgangsstyring
- ● 9.1. Forretningsmæssige krav til adgangsstyring
- 9.1.1. Politik for adgangsstyring (1. Tilstrækkelige)

En politik for adgangsstyring skal fastlægges, dokumenteres og opretholdes som et krav til informationssikkerhedskrav.

Direkte:

ISO 27001 (Anneks A) – Regler for informationssikkerhed og databeskyttelse i NGC

9.1.1. NGC generelle politikker/regler for bruger- og adgangsstyring

CISO er ansvarlig for at udarbejde og vedligeholder NGC's regler for bruger og adgangsstyring. Reglerne skal sikre at NGC håndterer bruger og adgangstyring i henhold til krav fra risikovurderingerne vedrørende behandlingsaktiviteter og sikre at NGC efterleve alle lov-, myndigheds-, og kontraktkrav vedrørende bruger- og adgangsstyring.

NGC har et sæt overordnede regler beskrevet under denne regel som alle de øvrige skal efterleve:

1. Ingen brugere skal ændre standardkontoindstillinger til NGC-specifikke indstillinger (f.eks. længde, kompleksitet, historik og konfigurationer) eller understøtte NGC i disse ændringer. Adgangsreglens kompleksitet skal kunne konfigureres af administratorer i forhold til minimal adgangskodelængde;
 1. minimal adgangskodelængde
 1. Klienter
 1. Ved to-faktor 8 tegn
 2. Uden to-faktor 12 tegn
 2. Mobiltelefon
 1. Mindst 6 tegn
 2. Biometrisk
 2. maksimal adgangskodelængde
 1. systemer skal understøtte mindst op til 128 tegn
 3. mindste antal specifikke tegn eller tegngrupper
 1. Adgangskoder skal indeholde små og store bogstaver, mindst et tal, mindst et specialtegn (inkl. mellemrum)
 4. minimum og maksimum brugsperiode;

Selvevaluering

NGC's regel

Kontroller

- NGC har 1xx kontroller, hvor vi kontrollerer overholdelse og effektivitet af regler og sikkerhedsforanstaltninger.
- Nedenfor er et eksempel på en kontrol. Til højre ses en oversigt over fremskridtene.

| Status | Titel |
|--------|--|
| ● | K. 7.1.2b - Ansættelsesvilkår og -betingelser til vikarer, ulønnede medarbejdere & konsulenter |
| ● | K. 7.2.1.(a.b.c.d.e) - Ledelsesansvar |
| ● | K. 7.2.2a, K. 6.2.1a, ISPMS 7.3.1 - Bevidsthed om informationssikkerhed |
| ● | K. 7.3.1(a.c.d) - Sikringstiltag ved ansættelses ophør |
| ● | K. 8.2.3.b - Bevidsthed om, og anvendelse af, procedure for håndtering af aktiver |
| ☰ | K. 9. 2. 3 - Styring af privilegerede adgangsrettigheder |
| ☰ | K. 9.1.1a - Begrænset adgang baseret på funktion |
| ● | K. 9.1.2a - Adgang til netværk og netværkstjenester |
| ● | k. 9.1.2b - To-faktor autentifikation |
| ● | K. 9.2.1a - Brugeregistrering og -afmelding i brugere i HPC |
| ● | K. 9.2.1a - Gennemgang af AD-brugere for HPC-miljøet |

K. 9.2.1a - Brugeregistrering og -afmelding i brugere i HPC

Start Nuværende kontrol Review

Kvalitet

Status

Godkendelse

%-udførelse

Overskridelse

Beskrivelse

Kontrollens formål
Formålet med denne kontrol er at sikre at brugere kun bliver oprettet/afmeldt i HPC miljøet efter korrekt anmodning.

Kontrollfrekvens
Denne kontrol udføres halvårligt.

Sådan udføres kontrollen
Gennemgå de 5 seneste oprettede og afmeldte brugere i HPC miljøet og verificer at oprettelsesproceduren er fulgt.

Dokumentation
Dokumentation kan enten være i dokumentform og vedhæftet, eller illustreret med screenshots.

Konklusion - kriterier og handlinger
Konklusionen *Ingen fejl fundet* anvendes når alle nyoprettede brugere har fulgt proceduren.
Konklusionen *Ikke-kritiske fejl fundet* anvendes når oprettelsen af nye brugere minimalt afviger fra proceduren.
Hvis konklusionen på kontrollen må angives som Kritiske fejl fundet (Kontrollen er fejlet) og der dermed er ide, en kontrolmæssig svaghed gennemføres følgende handling(er):

- Konsekvenser for organisationen som følge af den fejlede kontrol vurderes
- Det vurderes, om der skal iværksættes yderligere undersøgelse af konsekvenserne for at fastslå, om den fejlede kontrol har haft reelle konsekvenser i relation til informationssikkerheden
- Årsagen til den fejlede kontrol identificeres
- Der iværksættes aktiviteter til at udbedre den kontrolmæssige svaghed.
- Mulige handlinger til at rette fejlen beskrives i logbogen og drøftes eventuelt med IT chef

Alle ovenstående vurderinger og aktiviteter bør oprettes og beskrives som en hændelse med relation til denne kontrol.



NATIONALT
GENOM CENTER

Spørsmål

