NIS2-direktivet
- innføring og forvaltning

Agenda

Hva er det
Hvor skorter det
Hva må vi gjøre




NIS2 – kort introduksjon

Innføring og forvaltning:

- Modenhet blant norske virksomheter
- Prioritering av tiltak
- Bruk av rammeverk, NSM GP, ISO2700x, CISv8

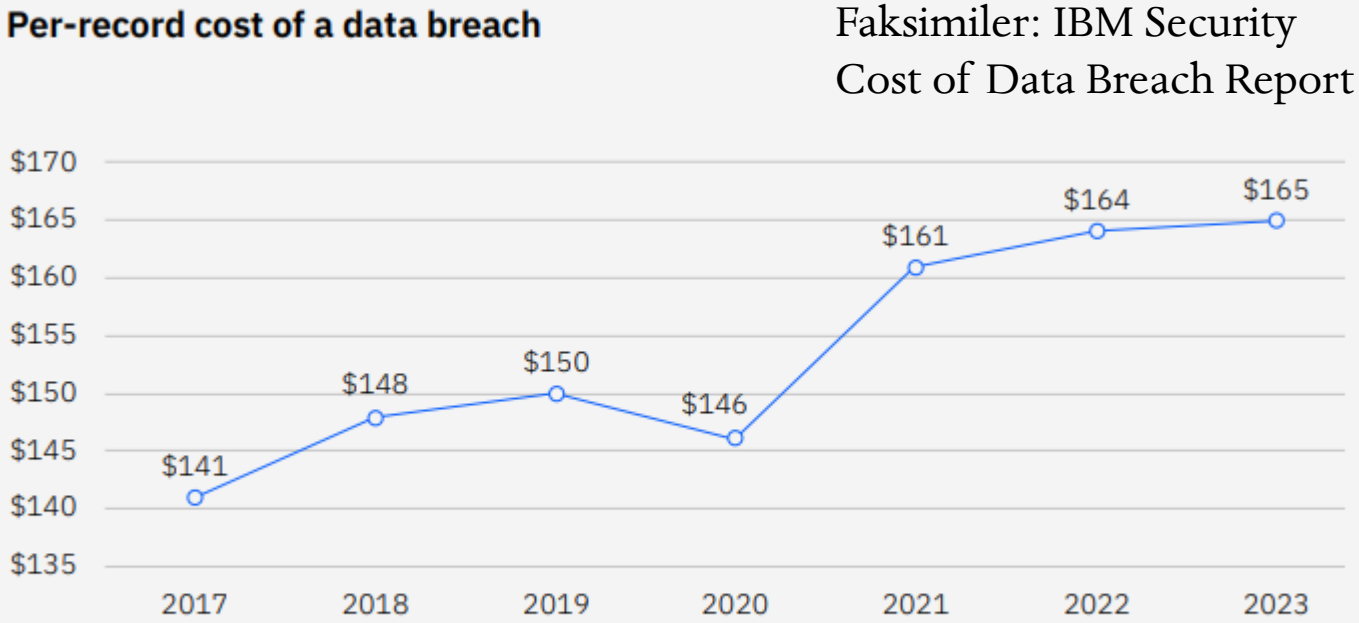
NSMs trusselrapport

- Bruk av **sammensatte trusler**: *summen av "tukling" med* olje og gass, droner, falske nyheter, etc.
- Angrep mot **Leverandørkjeder**
- Fordekte investeringer og oppkjøp truer nasjonal sikkerhet, innsidevirksomhet, spearphishing
- Utnyttelse av **cybersårbarheter** (persondata om 3,3M nordmenn er på avveie, bruk av nulldagssårbarheter, tjenestenektingsangrep)
- Bruk av ny teknologi (KI/AI, 5G, lavbanesatelitter)

Balanse er viktig,

«Så åpent som mulig, så sikkert som nødvendig»

Faksimiler: IBM Security
Cost of Data Breach Report 2023



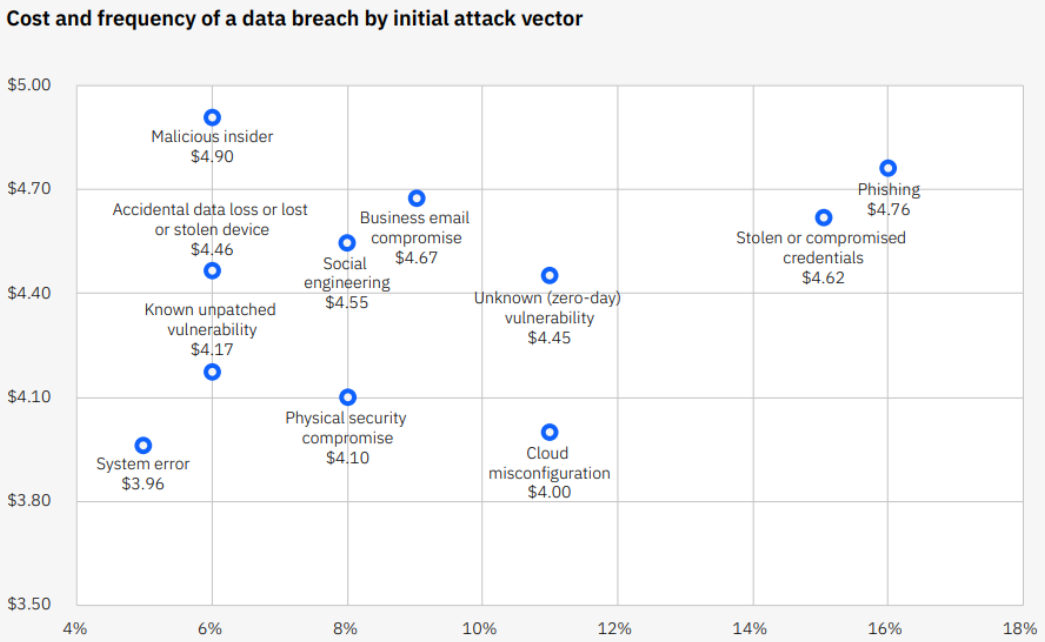


Figure 10. Measured in USD millions

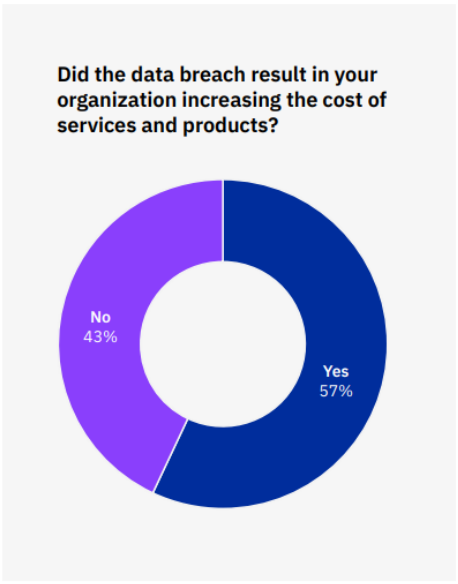


Figure 8. Share of total sample of breached organizations

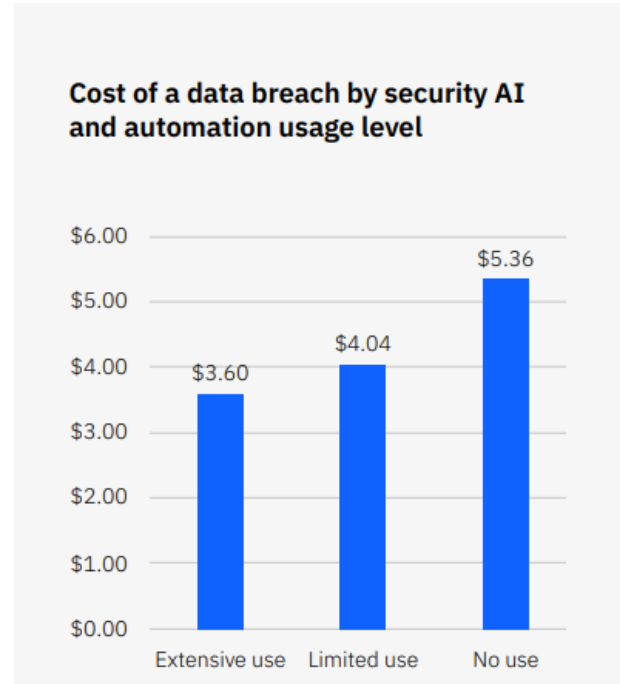


Figure 41. Measured in USD millions

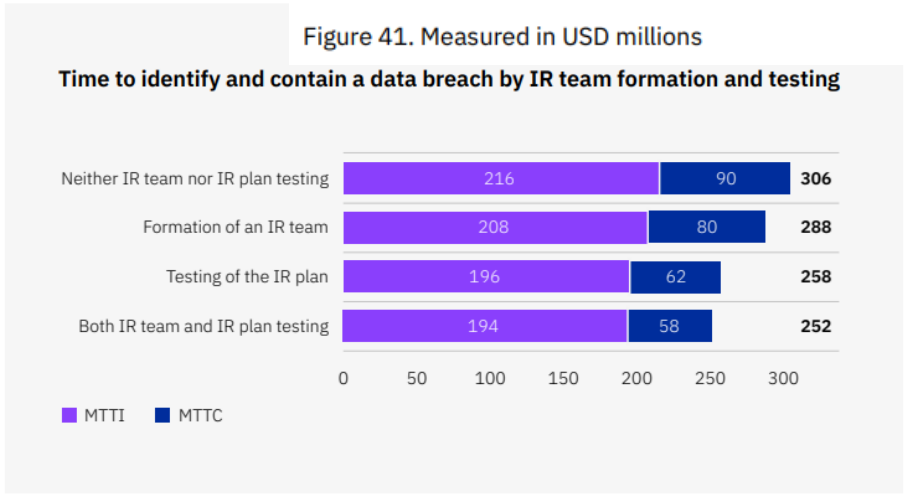


Figure 43. Measured in days

NIS2-direktivet *«kommende cyber-GDPR»*

*the **management bodies** of essential and important entities must approve the cybersecurity risk-management measures taken by those entities, oversee its implementation and **"can be held liable for infringements."***

*the **"members of the management bodies of essential and important entities are required to follow training,"** and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to **enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity**.*

Lov-prosessen tar tid

- NIS-1 ble godkjent av EU i 2016, men ikke gjeldende for EØS
- NIS-2 gjelder flere virksomheter og er strengere.
- EU-medlemmer: lov 17. oktober 2024
- Vil høyst sannsynlig innføres også i Norge
- Vil uansett gjelde for dem som handler med utlandet
- GDPR-nivå på bøter (10M € / 2% omsetning)

“samfunnskritisk”?

Energi, transport, drikkevann, bankvirksomhet, helse, digital infrastruktur, offentlig forvaltning, post, leveringstjenester, avfallshåndtering, matproduksjon, forskning ++

- I utgangspunktet med over 50 ansatte eller omsetning på mer €10M, men mindre kan også pålegges hvis de er viktige

eller

250 ansatte og omsetning på mer enn €50M

EUs krav er minstekrav. Land kan selv utvide listen.

Hva med NIS1?

Regjeringen.no

Søk

Tema Dokument Aktuelt Departement Regjering

Forsiden • Aktuelt • Pressemeldinger

Norge får sin første lov om digital sikkerhet

Pressemelding | Nr: 38 – 2023 | Dato: 05.05.2023

Regjeringen har lagt fram et forslag til lov om digital sikkerhet. Loven skal bidra til å styrke den digitale sikkerheten i virksomheter som har særlig betydning for samfunnet.

- Ble sendt til Stortinget i Norge 5. mai
- Mer frivillig basert, ikke tvang ved ansvarsbrudd
- Leverandørkjede og risiko er viktig
- Begrensede sektorer (energi, transport, helse, bank, finans, vann, digital infrastruktur)

...samarbeid, CSIRT, DNS og gjensidig revisjon

Article 21

Cybersecurity risk-management measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

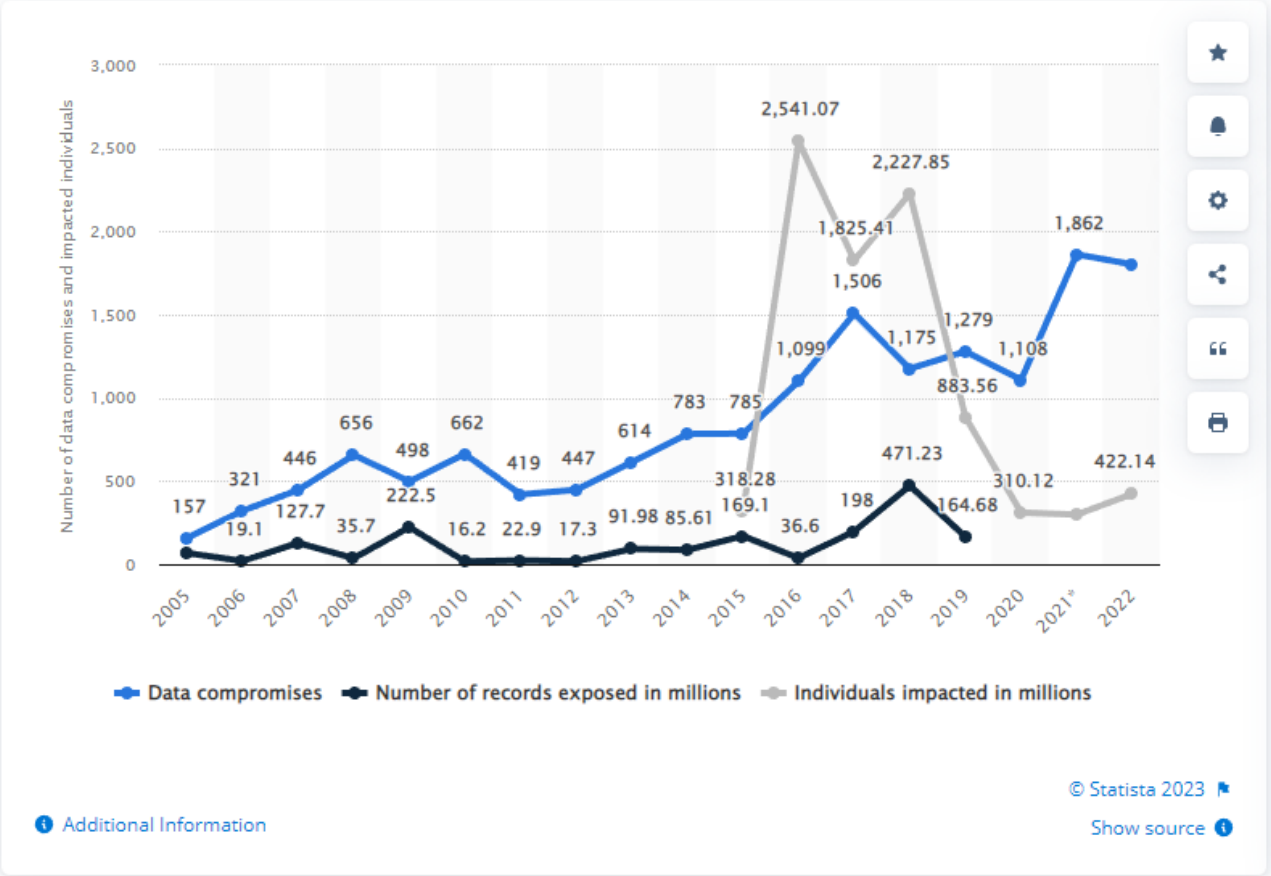
(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Hva vil NIS2 kreve?

Styring **av informasjonssikkerhet**

- Risikoanalyser
- Sikkerhetspolicies
- Rutiner for hendelseshåndtering
- Kontinuitetsplaner, motstandsdyktighet, katastrofeplaner
- Håndtering av leverandørkjede
- Personellsikkerhet
- **Riktig sikkerhetsopplæring!**



adaptiva
a glasspaper company

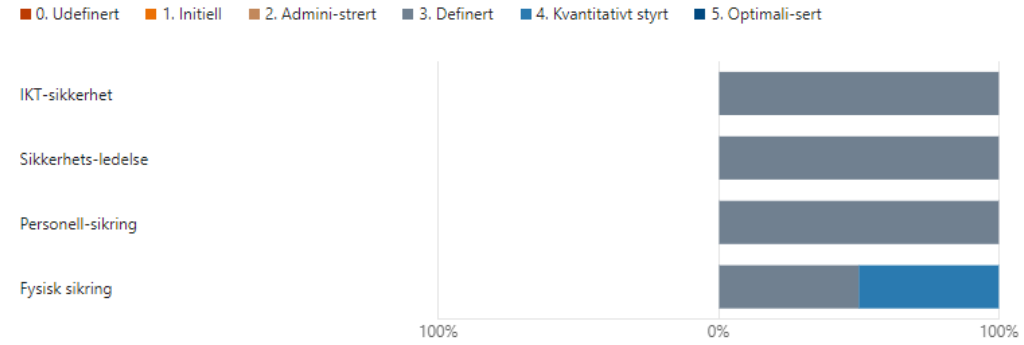
Modenhet

Bruk av NSMs grunnprinsipper

Krav i NIS2

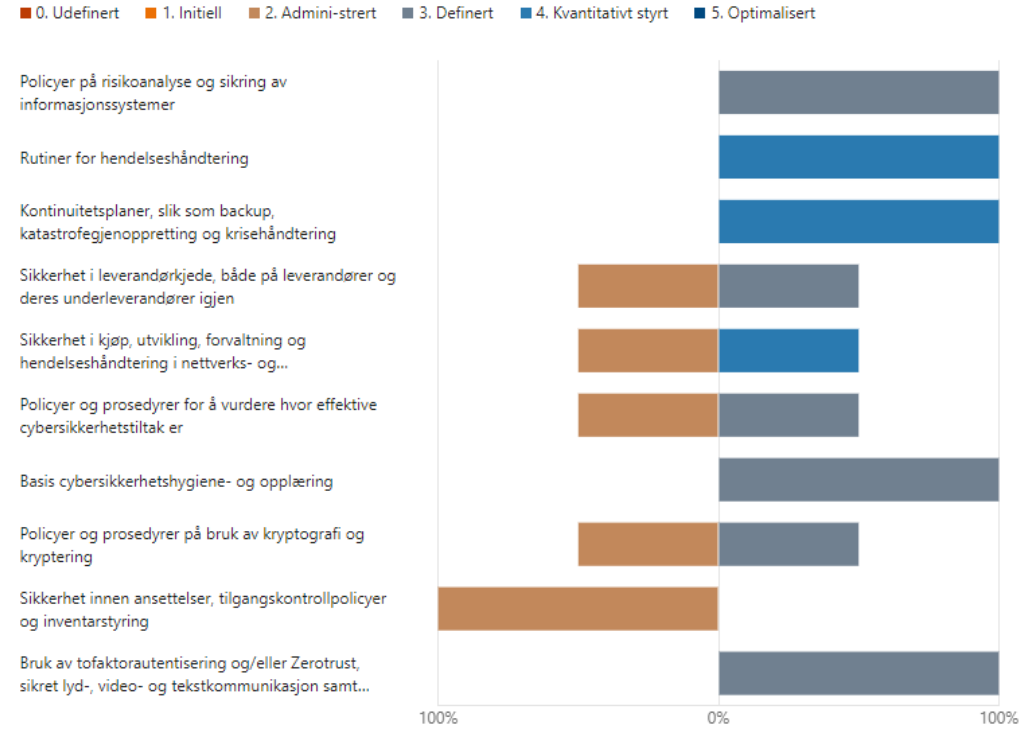
1. Bruk av NSMs grunnprinsipper

More Details



2. NIS2-kravene og dagens modenhet

More Details



adaptiva
a glasspaper company

Oppsummert: OK(-ish)

- **NSM Grunnprinsipper: CMMI nivå 3, definerte prosesser**
- **NIS2**
  - Policyer på risikoanalyse og sikring av informasjonssystemer
  - Rutiner for hendelseshåndtering
  - Kontinuitetsplaner, slik som backup, katastrofegjenoppretting og krisehåndtering
- **NIS2 *OK-ish:***
  - Basis cybersikkerhetshygiene- og opplæring,
  - Bruk av tofaktorautentisering og/eller Zerotrust, sikret lyd-, video- og tekstkommunikasjon samt sikrede krisekommunikasjons-kanaler der dette er nødvendig

Oppsummert: *Ikke helt OK*

- Sikkerhet i leverandørkjede
- Sikkerhet i kjøp, utvikling, forvaltning og hendelseshåndtering i nettverks- og informasjonssystemer
- Policyer og prosedyrer for å vurdere hvor effektive cybersikkerhetstiltak er
- Policyer og prosedyrer på bruk av kryptografi og kryptering
- Sikkerhet innen ansettelser, tilgangskontrollpolicyer og inventarstyring

adaptiva
a glasspaper company

Prioritering av tiltak

adaptiva
a glasspaper company

Teknisk sikring alene gir liten effekt

- Ansvaret for sikkerhet kan ikke delegeres bort
- Sikkerhetsstyring er en forutsetning for at teknisk sikkerhet skal bli en suksess

Sikkerhetsstyring:

Riktig restrisiko balansert mot ressursbruk og ytelse i verdiskapende prosesser

Hva med:

DSBs funn om manglende oppdatering av risikorapporter?

Kompetanse om Cyber-risikoanalyser?

Veiledning om og utveksling av risiko og tiltak med prioritering og veiledning?

Teknisk fagfelt der de som jobber innen det ikke alltid kan forklare hva de gjør

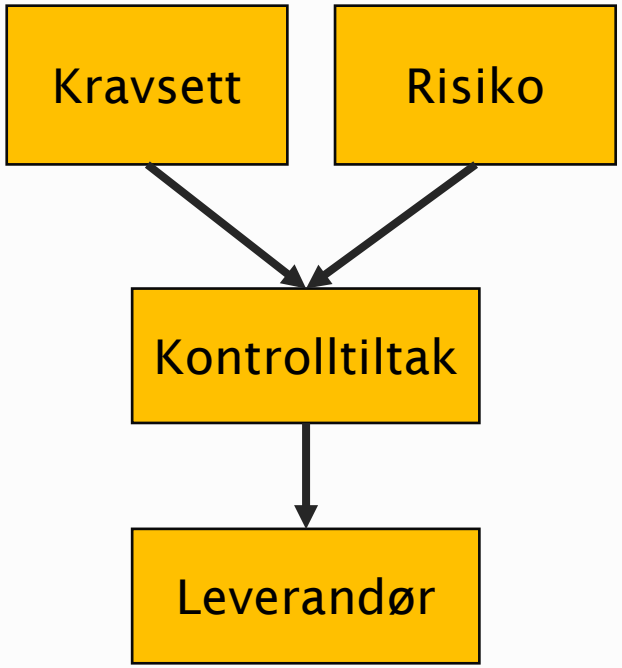
Leverandørkontroll

Mer enn Åpenhetsloven

adaptiva
a glasspaper company

Samle krav og still videre

- Samle alle krav og relevante risikoreduserende kontrolltiltak
  - Sikkerhetsmål og –strategi fra informasjonsikkerhetspolicy
  - Regulatoriske krav (sikkerhets- og personvernlover, åpenhetslov ++), kundekrav, bransjekrav, standarder
  - Tekniske- og organisatoriske krav fra fagpersonell
  - Resultater fra risikovurderinger
- Sammenstill hva som må stilles videre til underleverandør – og deres underleverandører
- Sikre at *avtaleverket* tar høyde for kravene
- *Vurder om leverandørene må være sertifisert*



Sikre riktig tjenestenivå

...at en har systemer og innarbeidet praksis som sikrer avtalt leveranse og etterlevelse av krav

adaptiva
a glasspaper company

Leverandørrevisjon

Risikoaksept styrer i hvilken grad en revidere

Starte å få oversikt

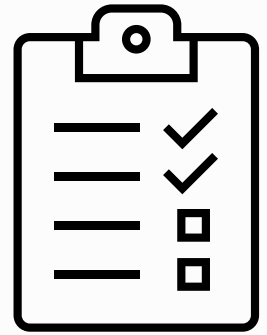
- Hvilke leverandører har en?
- Hvilke verdier håndterer leverandørene?
- Hvilke avtaler finnes? Er kravene gjenspeilet i disse?
- Avsjekk med om risikovurderingene tar høyde for leverandørene

Mulig resultat:

- Nye krav til leverandører og reforhandling/utskifting
- Gjennomføring av leverandørrevisjon

Verktøy:
status/rapporter fra leverandør

- Verifikasjon av at kunden får det som er avtalt
  - Antall og typer av hendelser i periode
  - Overholdelse av krav til oppdateringer og samsvar på utstyr
  - Ytelse på leverte tjenester
  - Resultat av intern/eksternrevisjoner
  - Resultat fra risikovurderinger, oppfølging av disse
  - Resultater fra øvelse på beredskaps- og katastrofeplaner
  - Resultater fra revisjon av underleverandører
- *Fra leverandør: avsjekk på om kunden kjøper riktig nivå av tjenester*

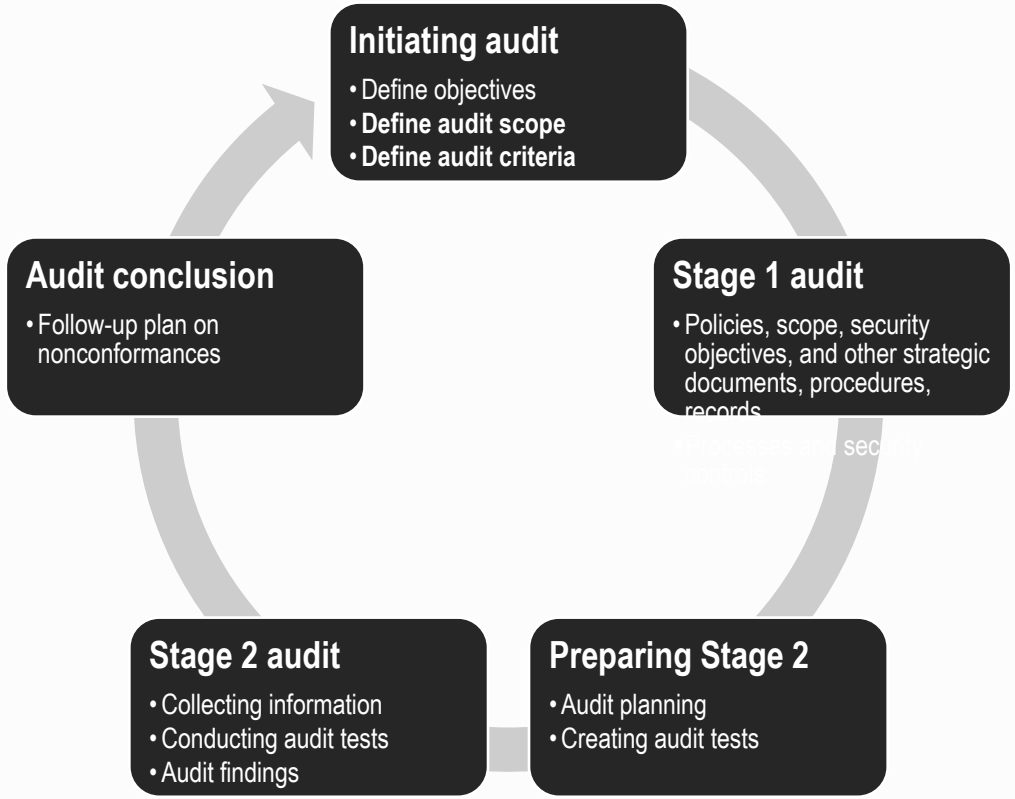


Verktøy: leverandørrevisjon

Hvor sterkt krav om bevis på samsvar kreves det?

- Spørsmålsliste (tilpasset egenerklæring)
- Annenpartsrevisjon
- Uavhengig revisjon av nøytral tredjepart

Områder: organisasjon, tekniske systemer, prosedyrer, prosess, produkt



Utfordring: utforming av spørsmål på riktig nivå og analyse av svar krever fagkompetanse

adaptiva
a glasspaper company

Verktøy:
krav om sertifisering

ISO 9001
Quality

ISO 14001
Environment

OHSAS 18001
Health and safety at work

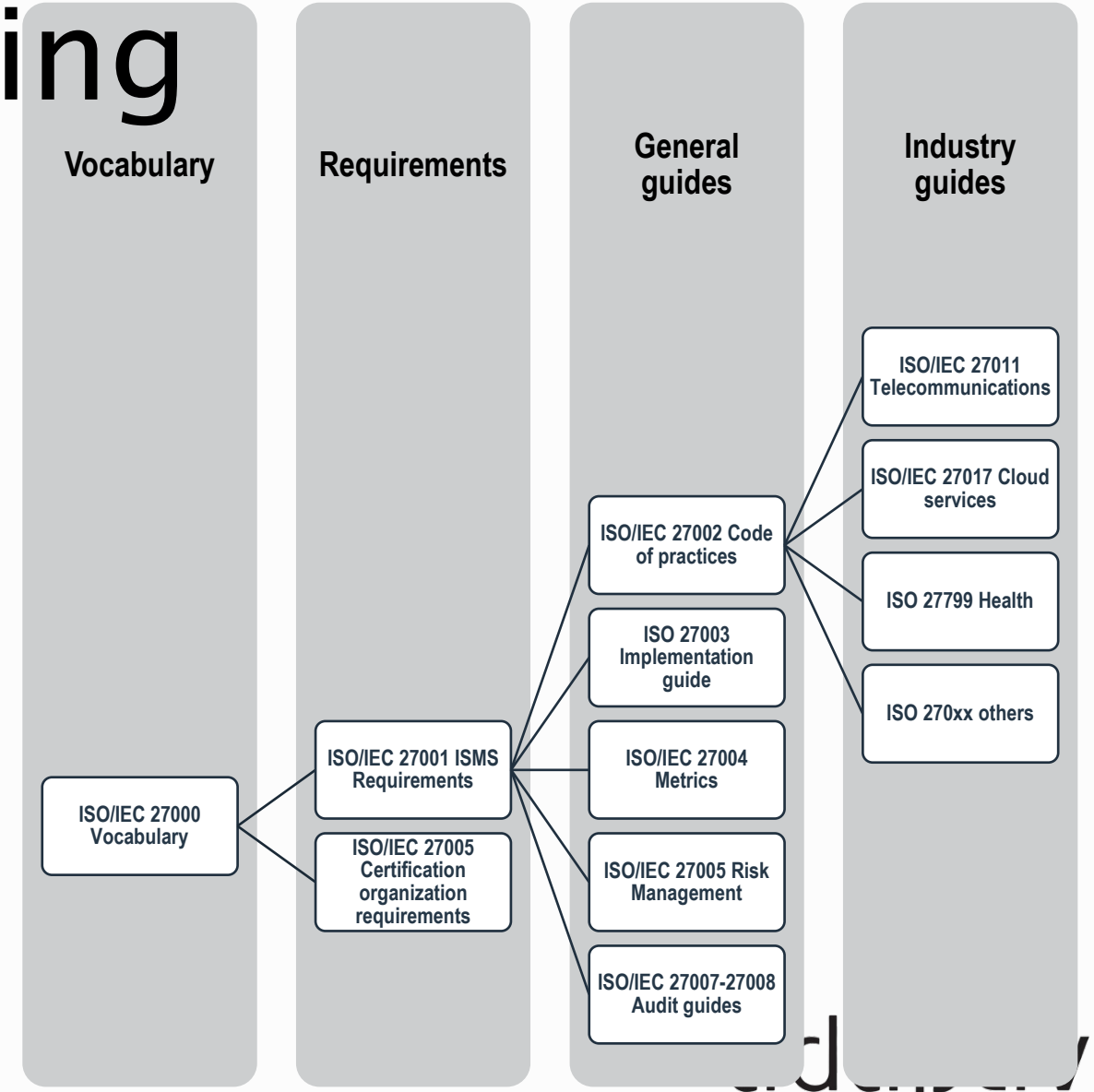
ISO/IEC 20000
IT Service

ISO 22000
Food safety

ISO 22301
Business continuity

ISO/IEC 27001
Information security

ISO 28000
Supply chain security



a glasspaper company

Rammeverk

Gjenbruk av kunnskap satt i system

adaptiva
a glasspaper company

NSM

Digital sikkerhet

Cybersikkerhet, hendelseshåndtering, kryptosikkerhet, kommunikasjonssikkerhet, NCSC, Kryptologi og forskning, informasjonssikkerhet

Personellsikkerhet

Sikkerhetsklarering, autorisasjon, adgangsklarering, personkontroll

Fysisk sikkerhet

Objektsikkerhet, luftbårne sensorsystemer, sikringstiltak

Sikkerhetsstyring

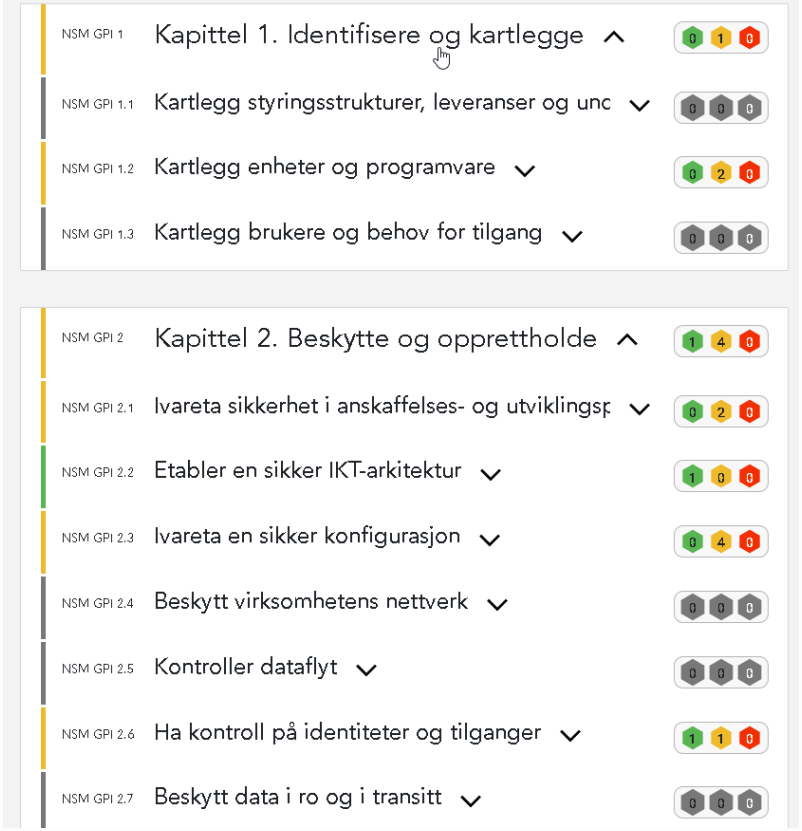
Verdivurdering, tilsyn, sikkerhetsgraderte anskaffelser, sikkerhetskultur

Faksimile: nsm.no

adaptiva
a glasspaper company

IKT prioritet 1-tiltak

1.2.3	Kartlegg enheter i bruk i virksomheten
1.2.4	Kartlegg programvare i bruk i virksomheten
2.1.2	Kjøp moderne og oppdatert maskin- og programvare
2.1.9	Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting
2.2.3	Del opp virksomhetens nettverk etter virksomhetens risikoprofil
2.3.1	Etabler et sentralt styrt regime for sikkerhetsoppdatering
2.3.2	Konfigurer klienter slik at kun kjent programvare kjører på dem
2.3.3	Deaktiver unødvendig funksjonalitet
2.3.7	Endre alle standardpassord på IKT-produktene før produksjonssetting
2.6.4	Minimer rettigheter til sluttbrukere og spesialbrukere
2.6.5	Minimer rettigheter på drifts-kontoer
2.9.1	Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata
3.2.3	Avgjør hvilke deler av IKT-systemet som skal overvåkes
3.2.4	Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn
4.1.1	Etabler et planverk for hendelseshåndtering

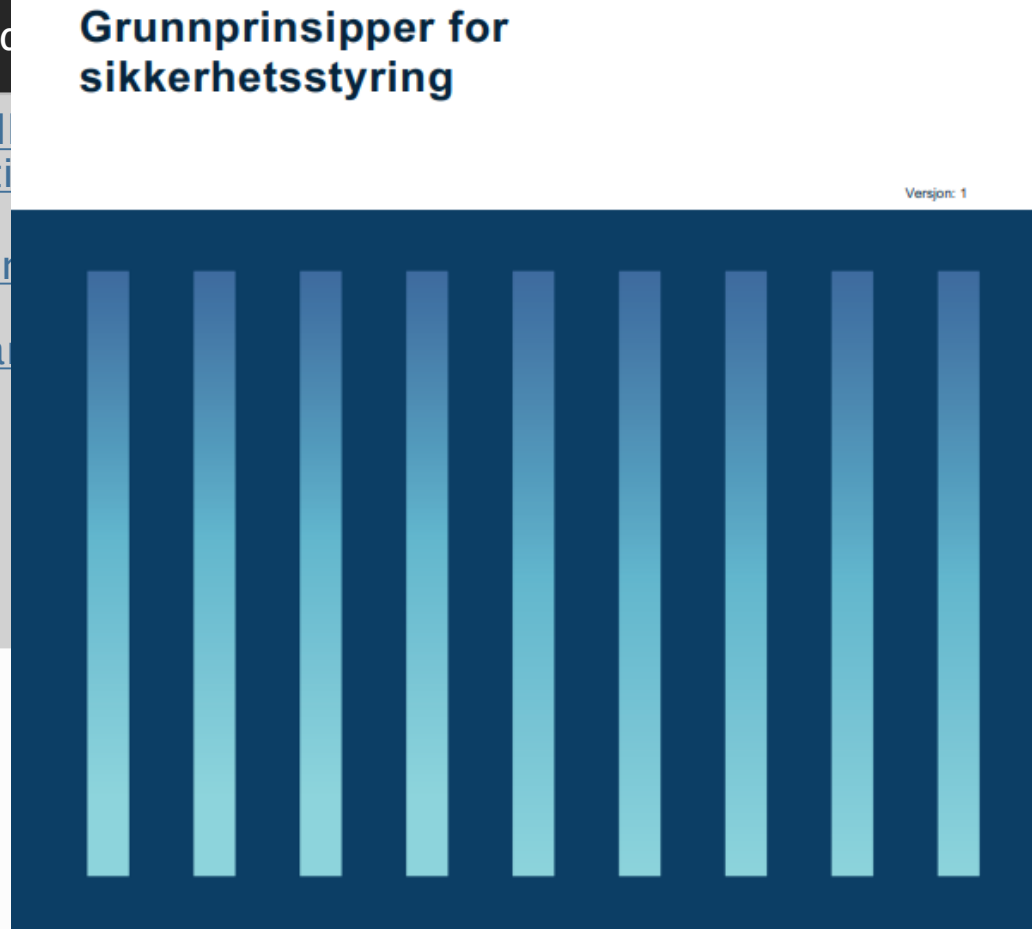


adaptiva
a glasspaper company

Sikkerhetsstyring

NASJONAL SIKKERHETSMYNDIGHET

Identifisere og kartlegge	Beskytte og opprettholde	Oppd
• 1.1 Kartlegg interne og eksterne krav • 1.2 Identifisere verdiene • 1.3 Identifiser trusler • 1.4 Avdekk sårbarheter • 1.5 Utarbeid scenario • 1.6 Kartlegg avhengigheter • 1.7 Gjennomfør konsekvensvurdering	• 2.1 Håndter identifisert risiko • 2.2 Etabler sikkerhetsorganisasjon • 2.3 Etabler styringssystem for sikkerhet • 2.4 Gjennomfør jevnlige øvelser, trening og opplæring	• 3.1 Kontroll sikkerhetsti jevnlig • 3.2 Gjennor ledelsens gjennomga



Sikkerhetsstyring: 10

NSM GPS 1.1.1	Nasjonale og internasjonale forhold og forpliktelser	Nasjonale og internasjonale forhold og forpliktelser
NSM GPS 1.1.2	Myndighetskrav, lovverk, regelverk	Myndighetskrav, lovverk, regelverk
NSM GPS 1.1.3	Bransjekrav eller -normer	Bransjekrav eller -normer
NSM GPS 1.1.4	Behov hos eksterne interessenter, kunder og leverandører	Behov hos eksterne interessenter, kunder og leverandører
NSM GPS 1.4.1	Sårbarhetsvurderinger med mål	Gjennomfør sårbarhetsvurderinger med mål om å beskrive i hvilken grad eksisterende sikkerhetstiltak vil kunne hindre en trusselaktør i å kunne påvirke virksomhetens verdier
NSM GPS 2.4.2	Planlegge og iverksette nødvendig opplæring og trening	Planlegge og iverksette nødvendig opplæring og trening slik at personer som skal utføre aktiviteter med betydning for sikkerhet tilfredsstiller og opprettholder de kravene til kompetanse som til enhver tid er gjeldende
NSM GPS 3.1.1	Sikre at det er nødvendig kompetanse i virksomheten	Sikre at det er nødvendig kompetanse i virksomheten til å gjennomføre revisjoner som er rettet mot å kontrollere sikkerhetstilstanden
NSM GPS 3.2.1	Planlegging og gjennomføring av ledelsens gjennomgåelse	planlegging og gjennomføring av ledelsens gjennomgåelse
NSM GPS 4.1.3	Det bør etableres nødvendige systemer	Det bør etableres nødvendige systemer som muliggjør varsling og rapportering av uønskede hendelser, inkludert avvik fra virksomhetens styringssystem. Systemet må også ivareta nødvendig ekstern varsling, også til myndigheter.
NSM GPS 4.1.5	Uønskede hendelser bør dokumenteres	Uønskede hendelser bør dokumenteres (eks. logg, rapporter og evalueringer) som del av virksomhetens kontrollerende dokumentasjon for forebyggende sikkerhetsarbeid. Slik dokumentasjon kan blant annet brukes i forbindelse med varsling og ved evaluering av håndteringen.

Fysisk sikring: 6

NSM GPF 1.1.2	Kartlegg plassering av verdier
NSM GPF 1.3.1	Kartlegg virksomhetens sårbarheter som en del av risikovurderingen
NSM GPF 2.3.1	Utarbeid plan for gjennomføring av øvelser
NSM GPF 3.2.1	Kontroller at de fysiske sikkerhetstiltakene fungerer som forventet
NSM GPF 3.3.6	Sørg for klar rollefordeling og kommuniser dette gjennom et tydelig planverk
NSM GPF 4.1.4	Sørg for at ansatte er godt kjent med roller og oppgaver ved hendelser
NSM GPF 4.2.3	Inngå avtaler med eksterne tjenesteleverandører som kan drifte og gjenopprette sikkerhetstiltak

Personellsikkerhet: 5

NSM GPP 1.1.4	Sikkerhetsopplæring	Innfør individuelle og/eller gruppebaserte tiltak – for eksempel en tilpasset sikkerhetsopplæring for medarbeidere i utsatte stillinger.
NSM GPP 1.2.4	Sikre tilstrekkelig kompetanse	Påse at alle aktuelle kandidater har tilstrekkelig kompetanse om sikkerhet og har forstått sine plikter før de gis tilgang til virksomhetens verdier. Bekreft alltid personens identitet.
NSM GPP 2.2.1	Tilgangskontroll	Etabler tilgangs- og adgangsskiller som sikrer at medarbeidere kun gis tilganger som er nødvendige for å kunne utføre sine arbeidsoppgaver – «need to know»-prinsippet.
NSM GPP 3.1.7	Oppfølgingskurs	Gi orienteringer og hold obligatoriske oppfølgingskurs om ulike sikkerhetsutfordringer, eksempelvis sosial manipulasjon, trusselbildet og trusselen fra innsidere.
NSM GPP 3.6.2	Offboarding av medarbeidere	Sørg for at medarbeiderens tilganger til informasjon, systemer, prosedyrer og adgang til objekter eller infrastruktur sperres, fjernes og/eller slettes.

Andre rammeverk?

Krav

- Personvern, Åpenhetslov, regnskapslover, etc
- Bransjestandarder: HR Norge, Regnskap Norge, Normen
- Kunders krav
- Styre krav til IT: COBIT
- Krav til IT-sikkerhet:
  - NSM Grunnprinsipper for IKT, styring, personell
  - ISO27001, NIST, GTAG

vs

Kontroller

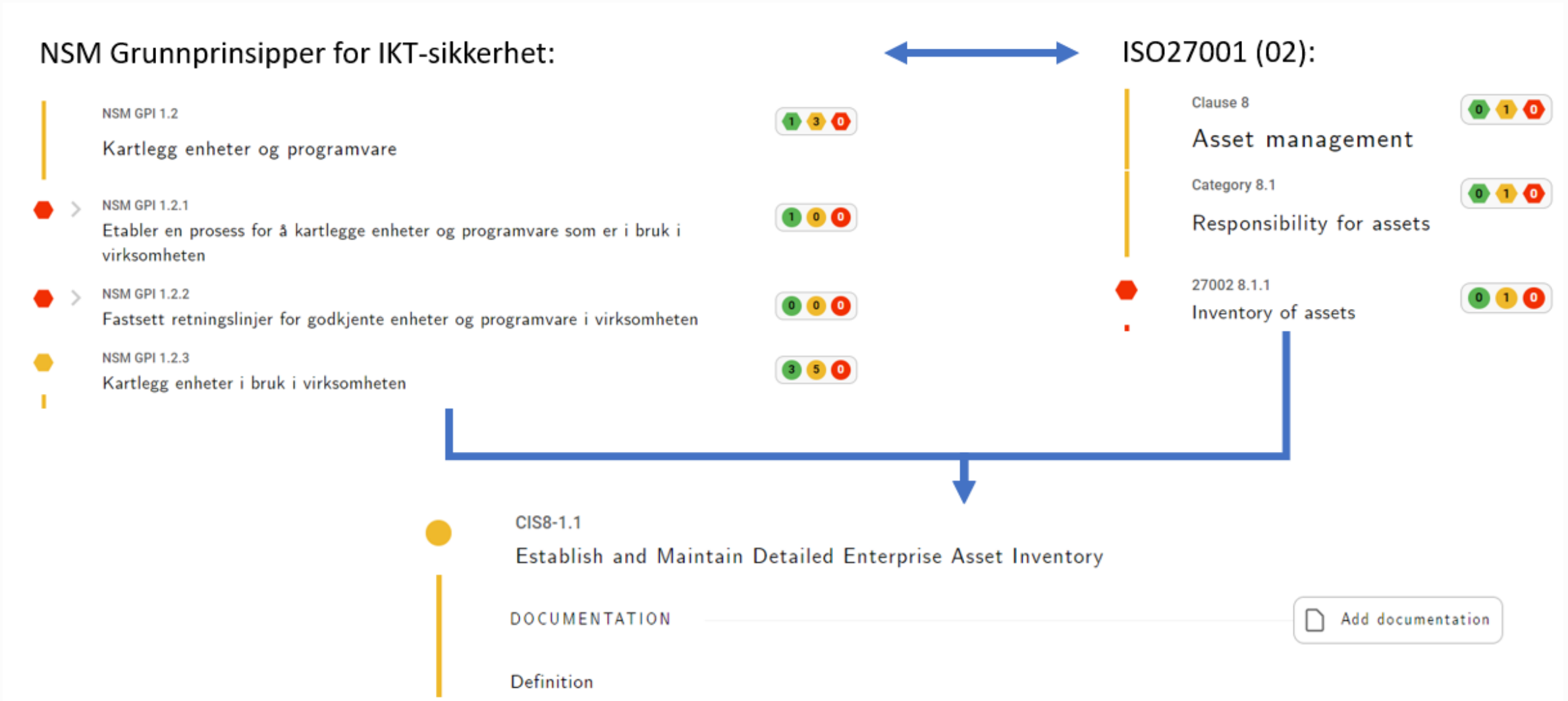
- Leverandør-praksis: Cloud adoption Framework, beste praksis til config
- (NSMs Grunnprinsipper for IKT)
- CIS-kontroller v8
- NIST 800-56
- Australsk cybersecurity-kontroller ☺

Tiltak: det du gjør for komme i samsvar/håndtere risiko

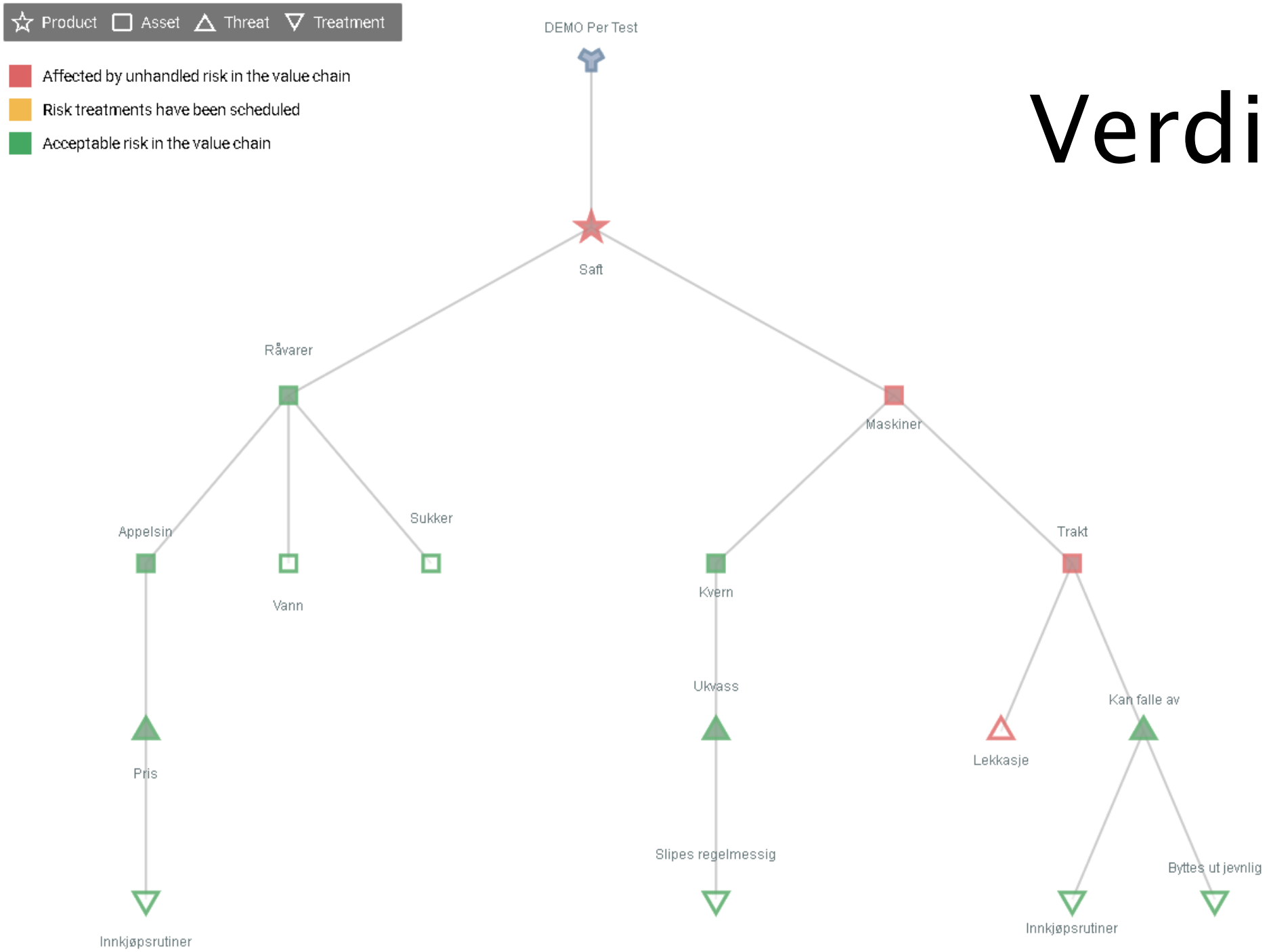
CIS Critical Security Controls

1. Inventory and control of Enterprise Assets
2. Inventory and control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continous Vulnerability Management
8. Audit Log Management
9. Email and Web browser protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3
6	6,3	Users	Protect	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	x	x	x
6	6,4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x
6	6,5	Users	Protect	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	x	x	x


NSM Grunnprinsipper for IKT-sikkerhet:
ISO27001 (02):
NSM GPI 1.2
Kartlegg enheter og programvare
1 3 0
NSM GPI 1.2.1
Etabler en prosess for å kartlegge enheter og programvare som er i bruk i virksomheten
1 0 0
NSM GPI 1.2.2
Fastsett retningslinjer for godkjente enheter og programvare i virksomheten
0 0 0
NSM GPI 1.2.3
Kartlegg enheter i bruk i virksomheten
3 5 0
Clause 8
Asset management
0 1 0
Category 8.1
Responsibility for assets
0 1 0
27002 8.1.1
Inventory of assets
0 1 0
CIS8-1.1
Establish and Maintain Detailed Enterprise Asset Inventory
DOCUMENTATION
Add documentation
Definition

Verdikjede


Product
Asset
Threat
Treatment
Affected by unhandled risk in the value chain
Risk treatments have been scheduled
Acceptable risk in the value chain
DEMO Per Test
Saft
Råvarer
Maskiner
Appelsin
Vann
Sukker
Kvern
Trakt
Pris
Ukvass
Lekkasje
Kan falle av
Innkjøpsrutiner
Slipes regelmessig
Byttes ut jevnlig
Innkjøpsrutiner

Oppsummert

- Skap forståelse for at arbeidet med NIS2-direktivet **må startes nå**.
- Videre forskning: **Hvor er vi svake? Utveksling av risikoer og fungerende kontrolltiltak?**
- Gjør ting **enkelt**: start med **NSM Grunnprinsipper for sikkerhetsstyring**, kjør **gapanalyser**
- Kjør **risikovurdering** og sett tiltakene/kontrollene dine i system
- Bygg revisjonskompetanse:
  gå fra "lykkelig uvitende" til "ulykkelig vitende":
- Gå videre med CISv8 og ISO27001!
- **Husk: si ifra til andre hva du gjør!**

company

Takk for oss!

Per Øyvind Arnesen
per@adaptiva.no
93064405

Inge Nævra
inge@adaptiva.no
41918450