



Alt handler om risiko – hvordan overleve et cyberangrep?

Roger Ison-Haug

PEDAB

Her er vi



- 26 års erfaring
- 9 land
- Omsetning 2018: 1,4 mia nok
- Vekst: 24,2% y/y
- 130 ansatte

3 FOKUSOMRÅDER

INFRASTRUCTURE

SECURITY

DATA & ANALYTICS

VÅRT BIDRAG

Vi knytter sammen



Forretningskompetanse



Teknisk kompetanse



Nye teknologier



Egne og andres løsninger



Agile forretningsmodeller

Vi forenkler



det samlede økosystem og
tilpasser det til hver enkelt
kunde og marked

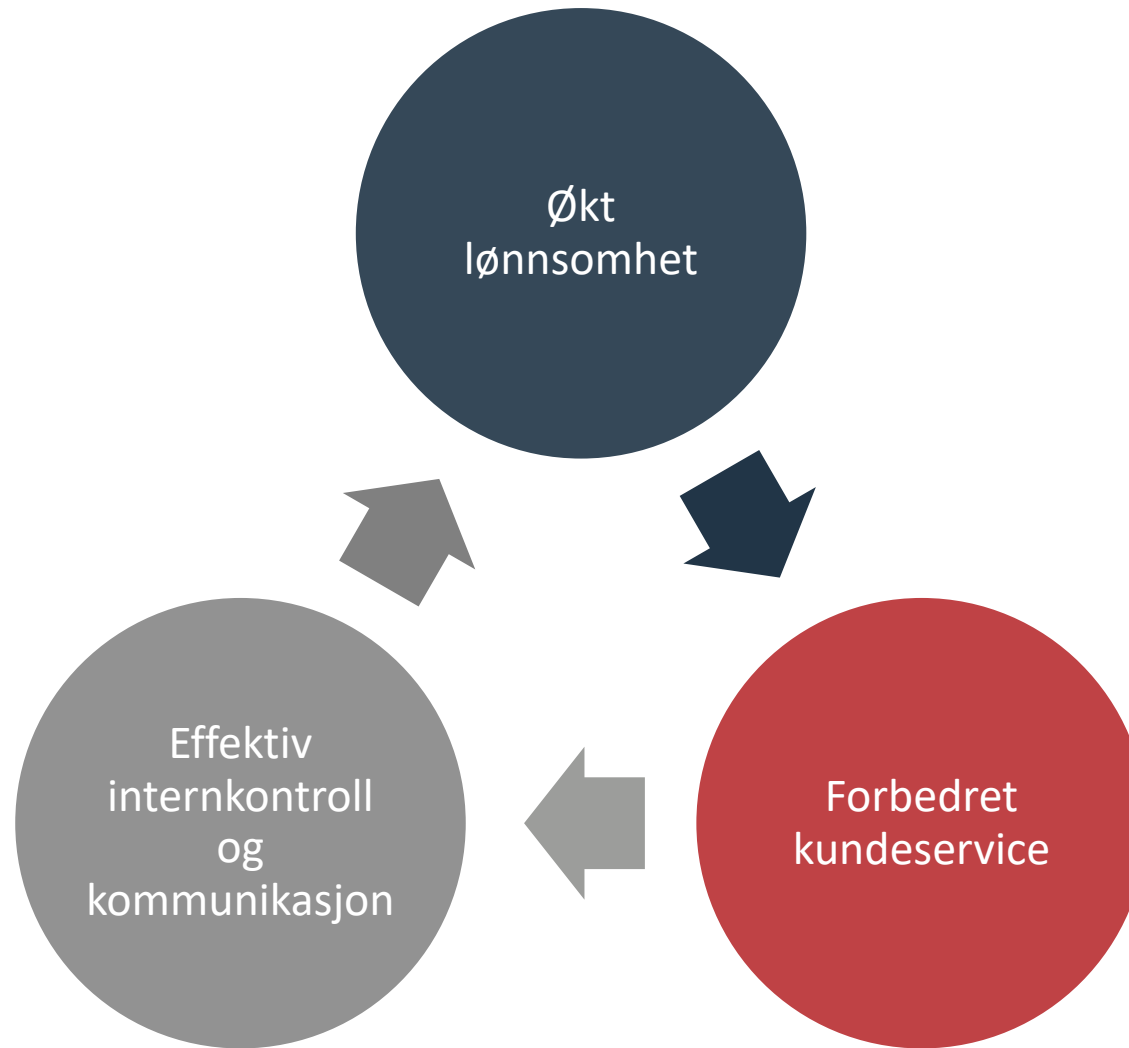
Vi transformerer og akselererer vekst



hos både kunder og
partnere



Hvorfor investerer det i IT?



Din organisasjons risikobilde

Utsiktede eksterne trusler.
Dette er trusler mot en organisasjon som tilfeldigvis er et resultat av organisasjonenes forhold til eksterne parter

Utsiktede interne trusler,
tilfeldige handlinger fra innsidere som kan ha negativ innvirkning på organisasjonens systemer, nettverk og data - som følge av uaktsomhet eller menneskelig feil.



Ondsinnede eksterne trusler,
bevisst forsøk fra utenforstående til å få uautoriserte tilgang til organisasjonens kritiske informasjonssystemer.

Ondsinnede interne trusler,
bevisste handlinger begått av innsidere som har til hensikt å få uautorisert tilgang til kritiske systemer.

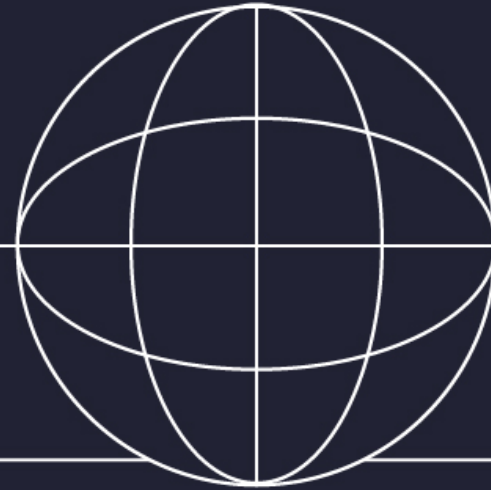
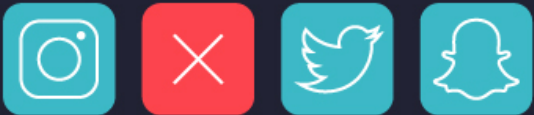
Antallet hendelser øker

Approximately

24,000

MALICIOUS

mobile apps are
blocked every day



IoT attacks were up

600%
IN 2017

Ransomware attacks are
growing more than

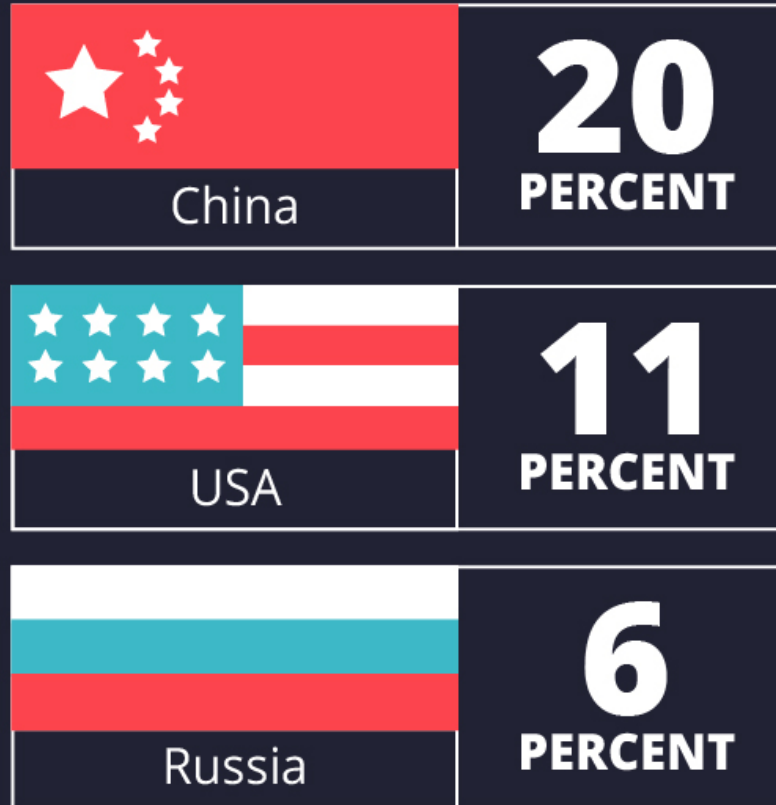
3 5 0

PERCENT

ANNUALLY

Hvor kommer angrep fra?

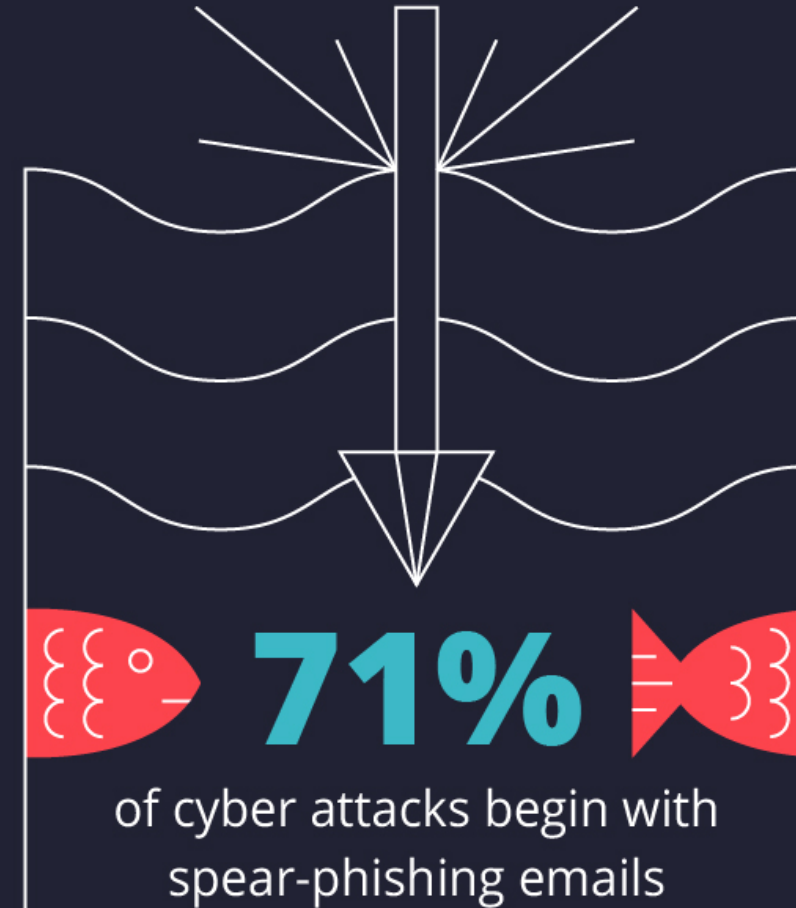
Sources of cyber attacks in 2017



Microsoft Office formats
such as Word, PowerPoint
and Excel make up

38%

**OF MALICIOUS FILE
EXTENSIONS**



IBMs CEO on Hackers

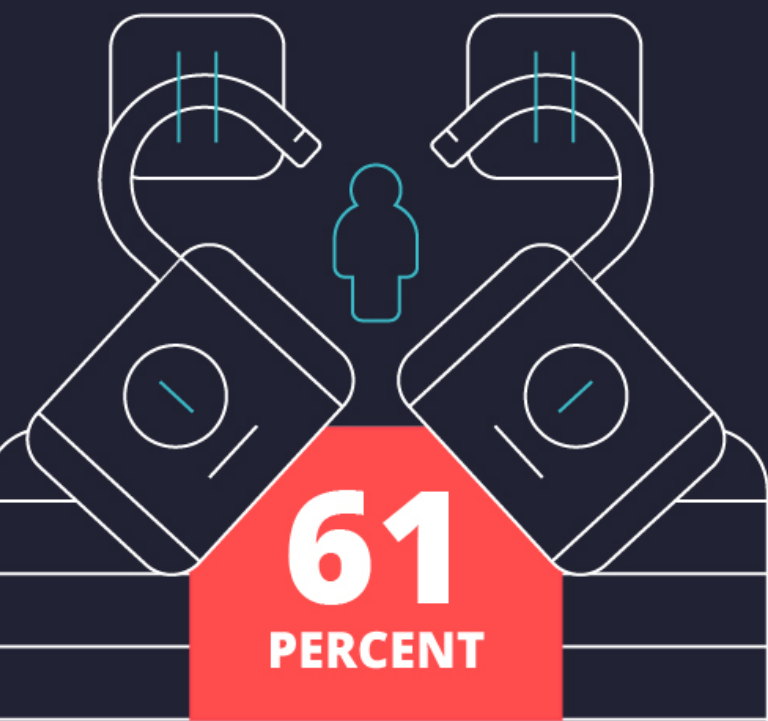


“
Cyber Crime is
the greatest
threat to every
company in the
world”

Ginni Rometty

Forbes (IBM Security Summit)

Hvem rammes?



61
PERCENT

of breach victims in 2017
were businesses with
UNDER 1,000 EMPLOYEES



The United States ranks highest

with **18.2%**

of all ransomware attacks



RANSOMWARE

attacks on the healthcare
industry are expected to

QUADRUPLE
by 2020

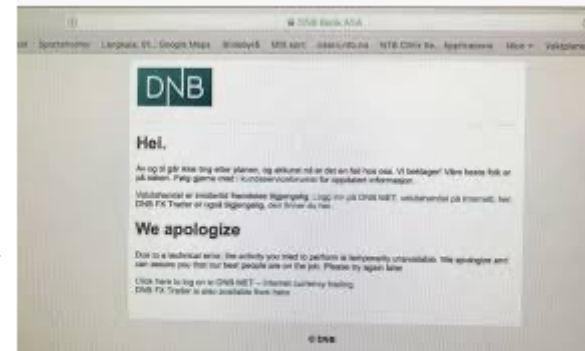


PATCHING

Havet av blåskjermer hos DNB kunne vært unngått, mener ekspert



Bergen kommune får straffegebyr på 1,6 millioner kroner etter sikkerhetsbrist



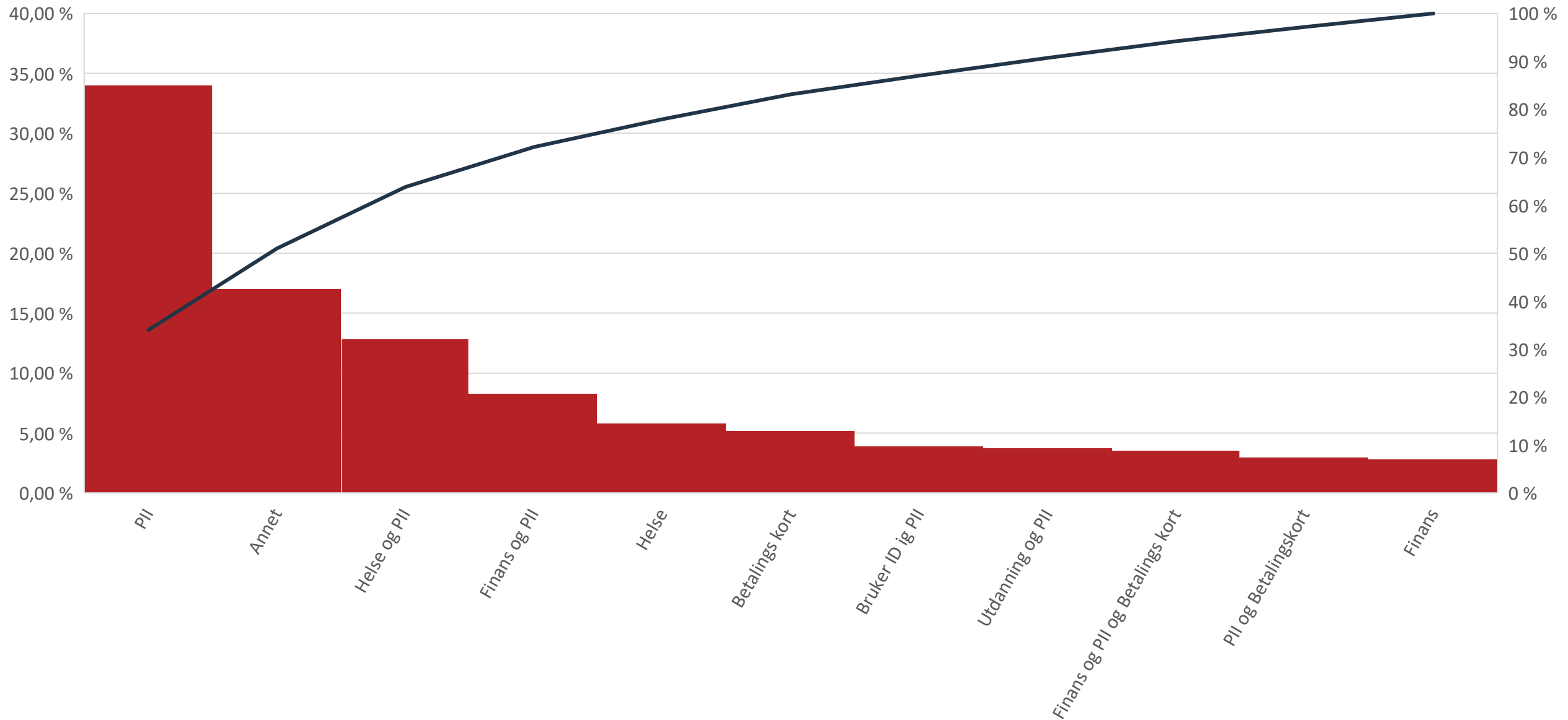
Beklager, vi fikk ikke logget deg inn

Det er vår feil, ikke din. Og vi jobber med å løse problemet så fort vi kan.

[Prøv igjen](#)

PEDAB

Datalekkasjer



Det er tre hovedrisiko

- ✓ **Forretningsoperativ risiko:** Potensialet for direkte eller indirekte tap som skyldes svikt i viktige forretningssystemer, prosesser, prosedyrer eller personer.
- ✓ **Omdømmerisiko:** Potensialet for tap eller skade som følge av skade forårsaket en organisasjons omdømme eller offentlige image.
- ✓ **Juridisk og overholdelsesrisiko:** Potensialet for tap eller skade som følger av rettslige skritt mot en organisasjon for brudd på lovgivningen eller myndighetskrav.

For mange forsøger å selge «månedens løsning»

SECURITY MANAGEMENT AND COMPLIANCE

Managed Security Service Providers



SIEM



Security Training



Governance, Risk and Compliance



INFRASTRUCTURE SECURITY

Data Masking



Enterprise Network Firewalls



Intrusion Prevention Systems



Network Access Control



Unified Threat Management



CYBER SECURITY

Secure Web Gateways



Network Forensics



Threat Intelligence Services



ENDPOINT SECURITY

Secure Email Gateways



Data Loss Prevention



Endpoint Protection & Anti-virus



Endpoint Threat Detection & Response



APPLICATION SECURITY

Application Security Testing



Web Application Firewalls



Application Control



CLOUD SECURITY



MOBILE SECURITY



IDENTITY AND ACCESS MANAGEMENT

User Authentication



Identity Governance and Administration



SECURITY PARTNERS



SECURITY ORGANIZATIONS



SECURITY CONFERENCES



ANALYST HOUSES



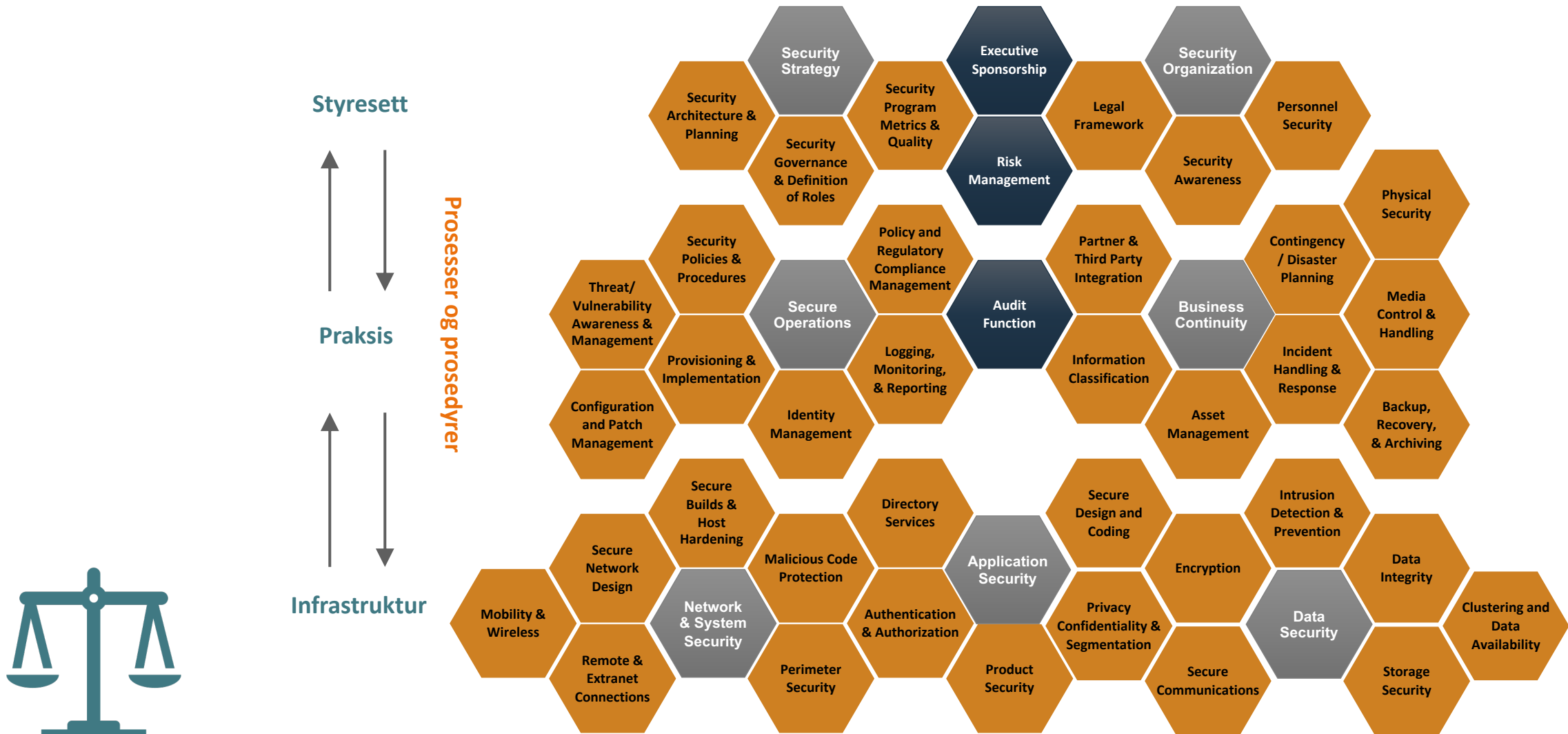
Konsekvenser:

- ✓ Silobasert. Ofte gode løsninger, men de henger ikke sammen
- ✓ Tidkrevende
- ✓ ULV! ULV!
- ✓ Veldig dyrt
- ✓ Ofte kompliserte og tunge å benytte for ansatte/kunder
- ✓ Uløste sikkerhetsproblemer, ofte ubevisst

Trender innen datarisiko



IT-sikkerhetsinitiativer kontra risikoreduksjon



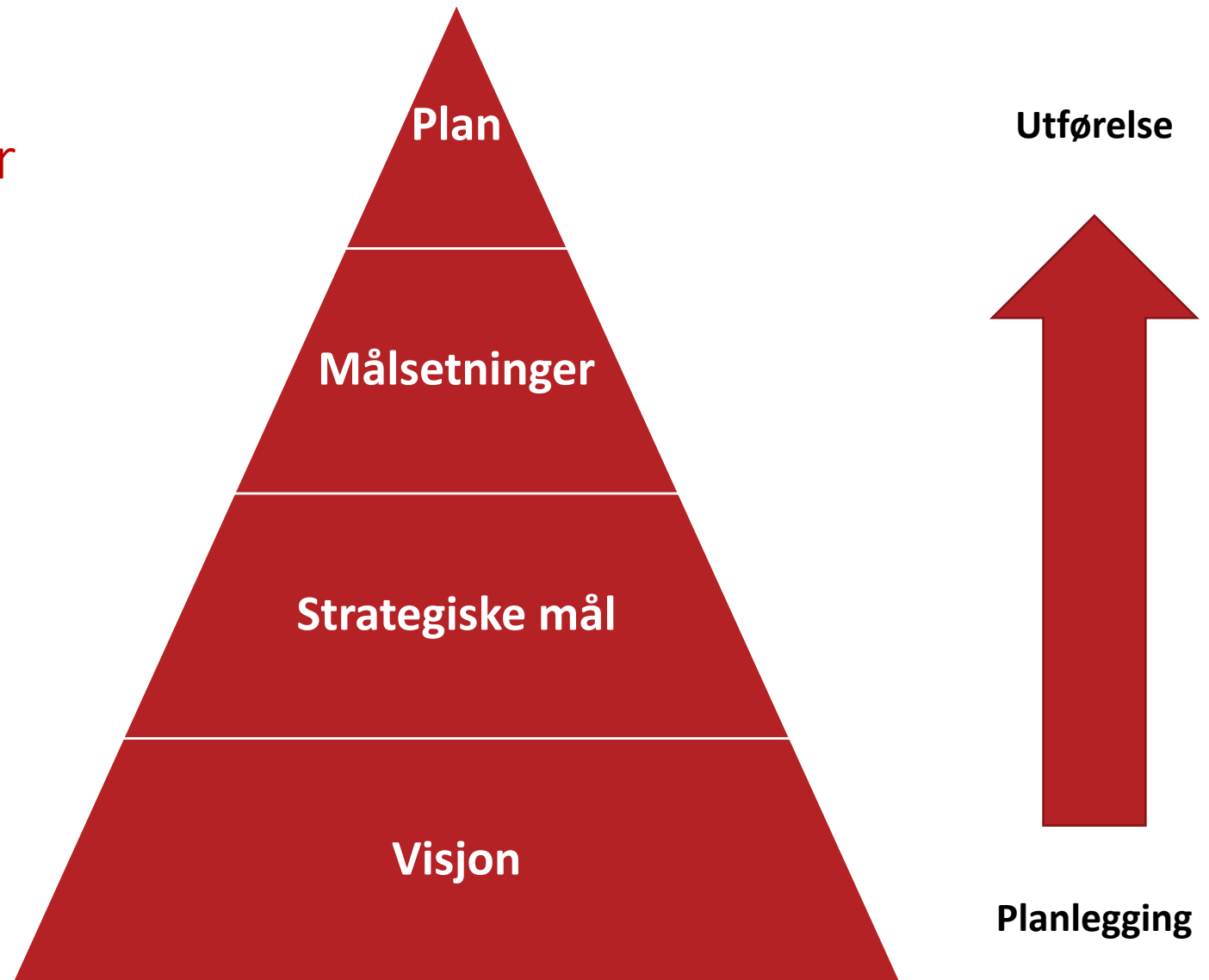
Velg en metode
Jobb mot en standard

Hvorfor velge en standard

Jobb mot noe som er velprøvd

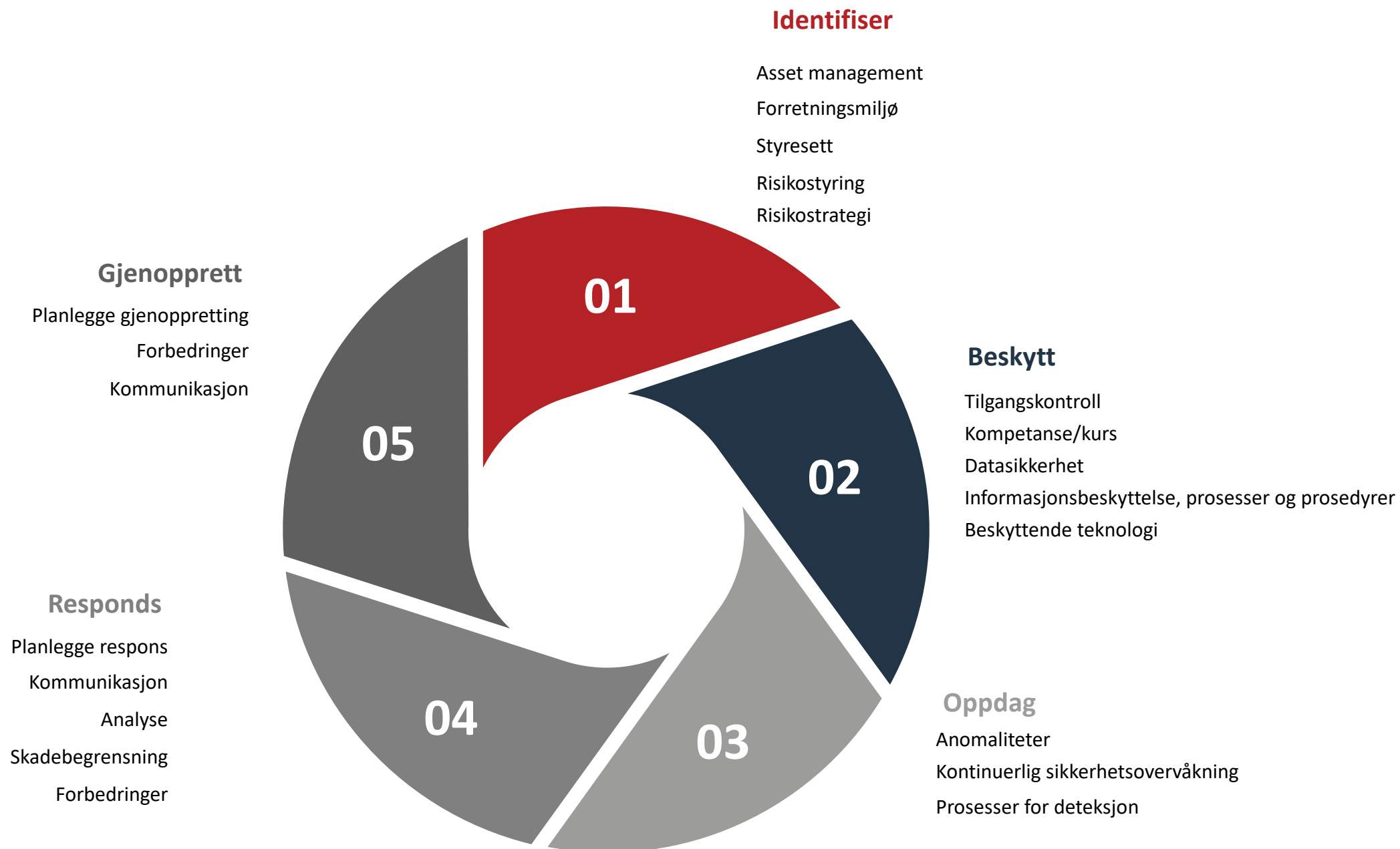
- ✓ Overblikk – sikrer at alt og alle er med
- ✓ Strukturert tilgang – ingenting glemmes
- ✓ Klar kommunikasjon – på tvers av hele organisasjonen, samt opp til styret
- ✓ Transparens vedrørende risiko om de beslutninger som tas
- ✓ Gjennomprøvede prosesser og beste praksis
- ✓ Jevnlig/kontinuerlig trening og bevisstgjøring
- ✓ Identifisering av hvilke oppgaver som skal løses in-house og hvilke som kan flyttes ut
- ✓ Sertifisering så samarbeidspartnere kan forholde seg til deres sikkerhetssystem/-tanke sett

Relasjon mellom visjonen,
strategiske mål og målsetninger
som er inkludert i strategien



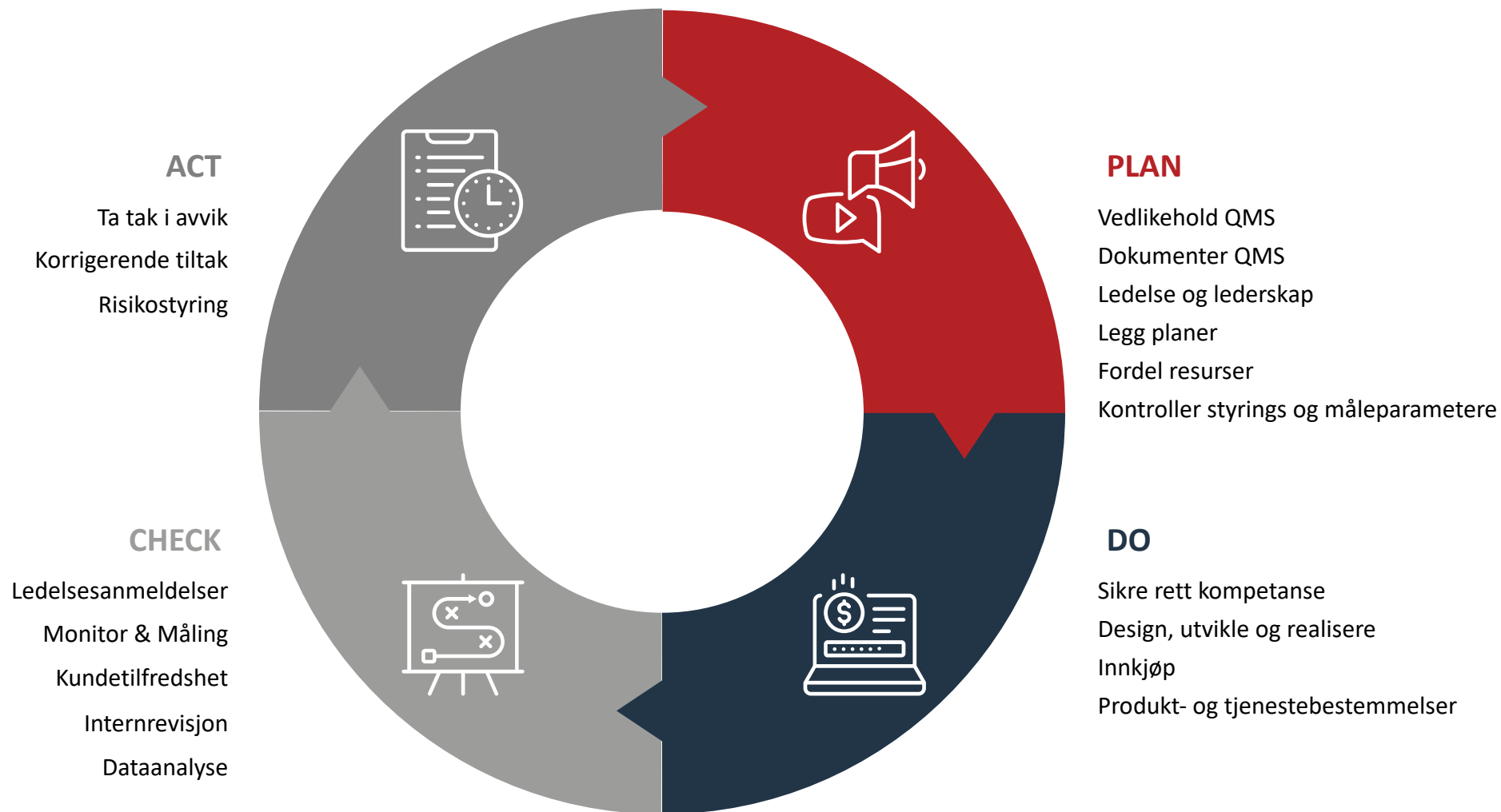
Sett deg inn i hvilken standard som passer din bedrift

- ✓ ISO / IEC sikkerhetskrollstandarder: Dette rammeverket, utgitt av International Organization for Standardization (ISO) og International Electrotechnical Commission (IEC), spesifiserer et informasjonssikkerhetsstyringssystem (ISMS) for effektiv styring av informasjonsrisiko.
- ✓ FFIEC Cybersecurity Assessment: Dette brede rammeverket ble utviklet av Federal Financial Institutions Examination Council (FFIEC) for å sikre at finansinstitusjoner har nøyaktig trusselinformasjon for å beskytte seg selv og sine kunder mot cyberattacks.
- ✓ SEC / OCIE Cybersecurity Initiative: Dette initiativet ble utviklet av U.S. Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE) for å vurdere investeringsselskapers cybersikkerhetsberedskap.
- ✓ FCC Cyber Security Planning Guide: Dette rammeverket ble utviklet av Federal Communications Commission (FCC) for å hjelpe små bedrifter med å utvikle og opprettholde retningslinjer for å beskytte kritiske forretningsdata.
- ✓ NIST Cybersecurity Framework: Dette rammeverket, opprettet av National Institute of Standards and Technology (NIST), gir implementeringsdetaljer for å håndtere cybersecurity i produksjonsmiljøet.



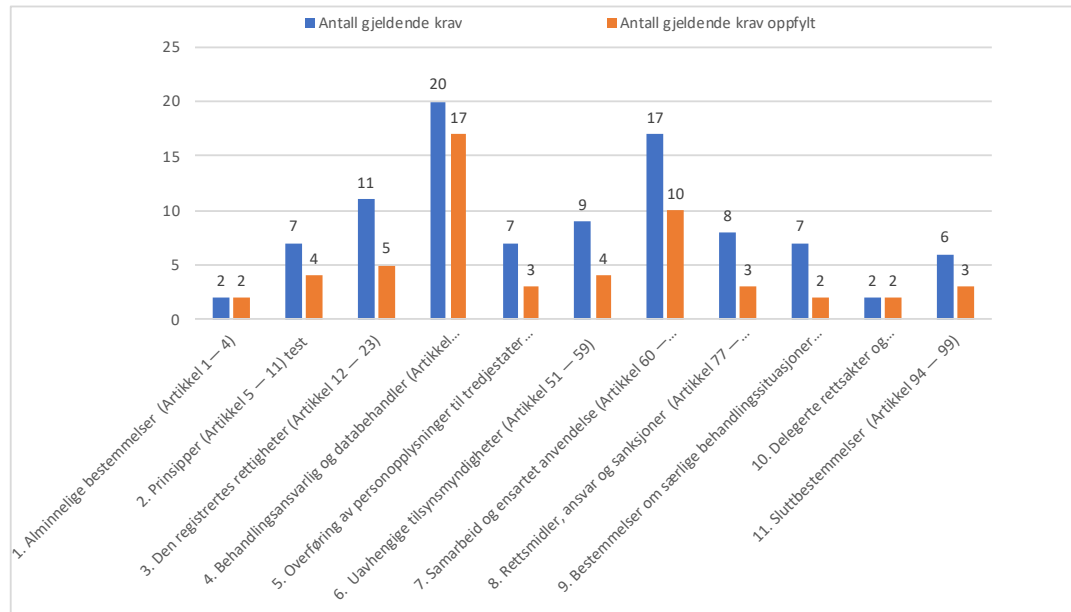
Bruk **PDCA**-syklusen for å sikre kontinuerlig forbedring av QMS

ISO 9001, 27001/27701

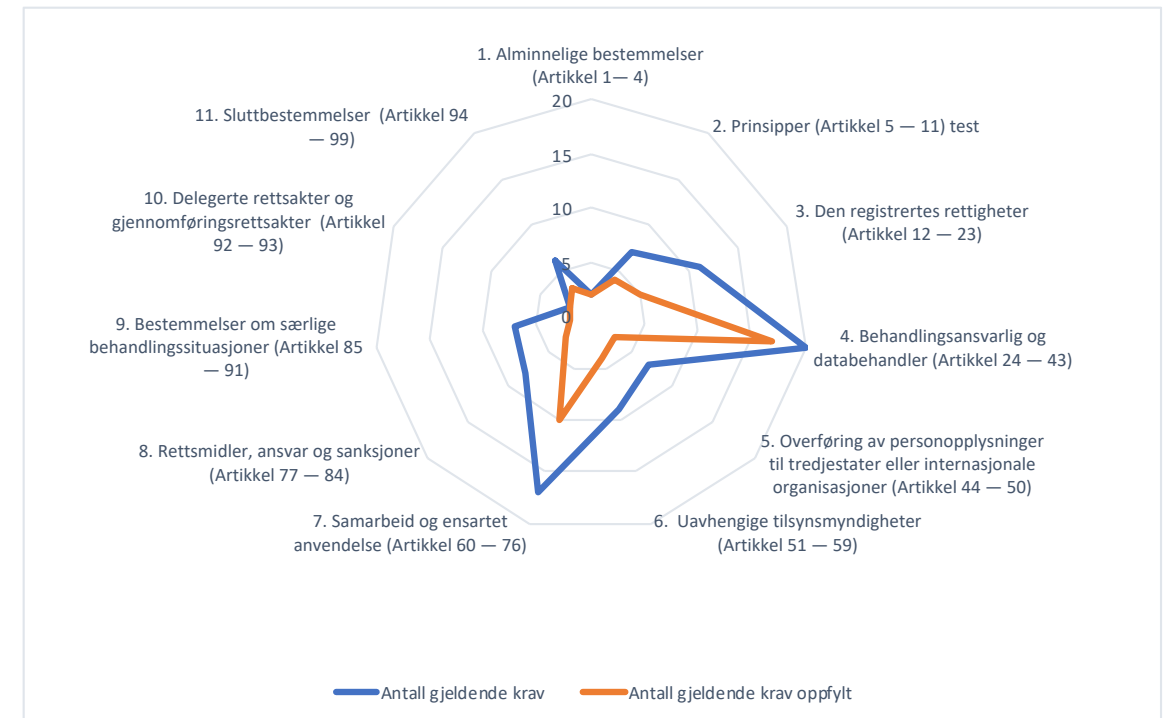


Relevante ISO standarder

- ISO 27001, 27002 og 27701, Sikkerhetstiltak og samsvar med GDPR
- ISO 19011 – Rammeverk



GDPR kapittel	Antall gjeldende krav	Antall gjeldende krav oppfylt	Samsvarsprosent
1. Alminnelige bestemmelser (Artikkel 1—4)	2	2	100,00 %
2. Prinsipper (Artikkel 5 — 11) test	7	4	57,14 %
3. Den registrertes rettigheter (Artikkel 12 — 23)	11	5	45,45 %
4. Behandlingsansvarlig og databehandler (Artikkel 24 — 43)	20	17	85,00 %
5. Overføring av personopplysninger til tredjestater eller	7	3	42,86 %
6. Uavhengige tilsynsmyndigheter (Artikkel 51 — 59)	9	4	44,44 %
7. Samarbeid og ensartet anvendelse (Artikkel 60 — 76)	17	10	58,82 %
8. Rettsmidler, ansvar og sanksjoner (Artikkel 77 — 84)	8	3	37,50 %
9. Bestemmelser om særlige behandlingssituasjoner (Artikkel 85 — 91)	7	2	28,57 %
10. Delegerte rettsakter og gjennomføringsrettsakter (Artikkel 92 — 93)	2	2	100,00 %
11. Sluttbestemmelser (Artikkel 94 — 99)	6	3	50,00 %
Total	96	55	57,29 %



Vi kan ikke velge bort IT-sikkerhet

- DPIA - vurdering av personvernkonsekvenser – artikkel 35
- Krav til systematisk helse-, miljø og sikkerhetsarbeid – Arbeidsmiljøloven §3-1
- Straffeansvar (Aksjeloven § 19)
 - Et medlem av styret, som forsettlig eller uaktsomt overtrer bestemmelsene gitt i eller i medhold av aksjeloven, straffes med:
Bøter eller under skjerpede forhold med fengsel inntil 1 år.
Det er samme strafferamme ved grov uforstand.
Medvirkning straffes på samme måte.
Det er samme strafferamme for stifter, medlem av bedriftsforsamling, daglig leder og revisor

Takk for at du deltok!

Følg med på www.pedab.no og i Pedab Norge i sosiale medier
for påmelding til neste webinar!

Er dette noe for deg?

- Hvordan starte med ISO 27001, og hvordan gjøre risikoanalyse.
 - Neste webinar er 19 November.