Cybersikkerhet på internrevisjonens agenda

07. desember 2022

The Institute of Internal Auditors Norway

Innhold

1. Hvorfor er cybersikkerhet et viktig tema for internrevisjonen?

2. Hvordan få kontroll på cybersikkerhetsrisikoen?

3. Hvordan bruke internrevisjon for å styrke cybersikkerheten

Avsluttende diskusjon og erfaringsdeling

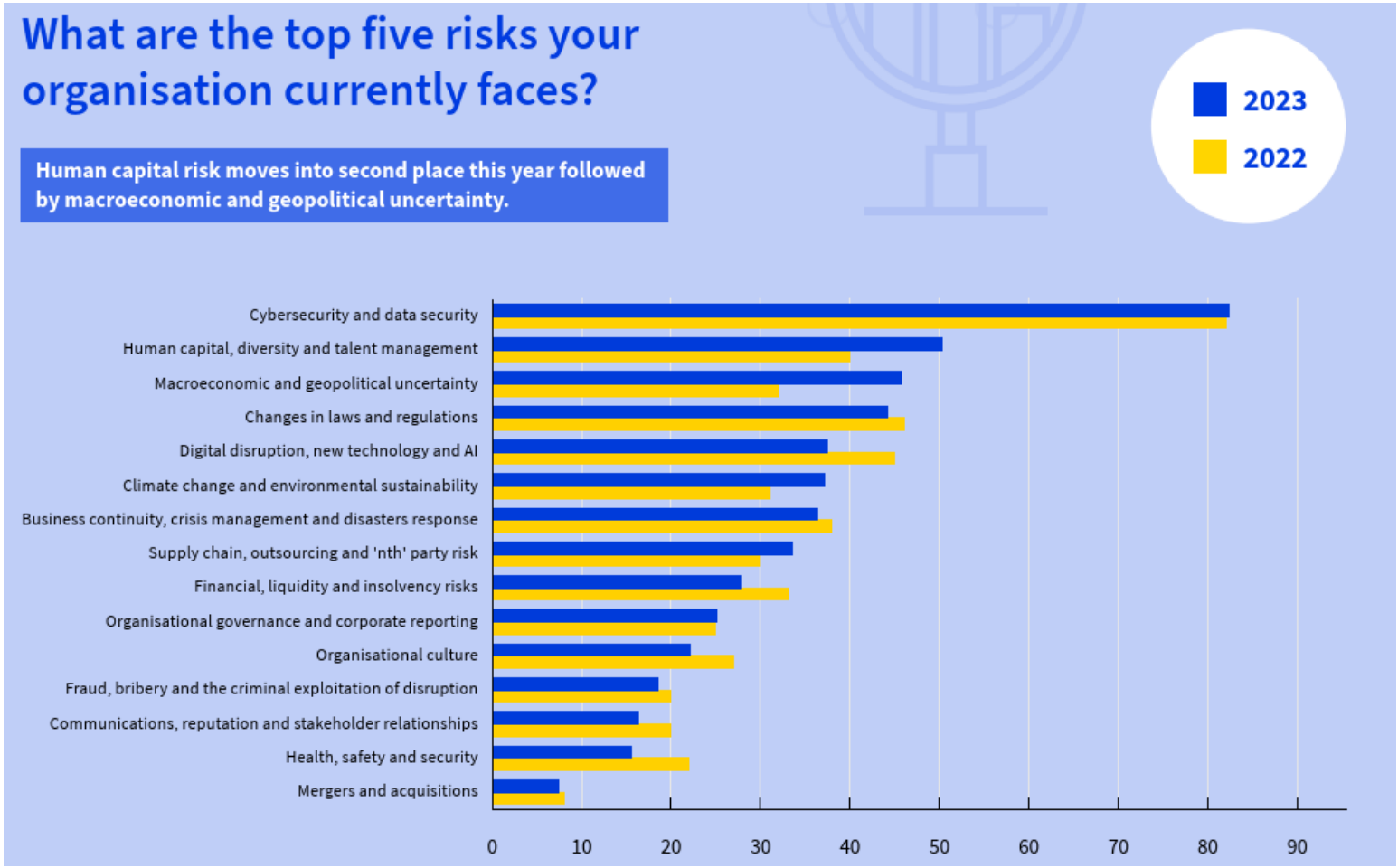
Hvorfor er cybersikkerhet et viktig tema for internrevisjonen?

For de aller fleste norske virksomheter bør cyberrisiko være en sentral «topprisiko»

En risikobasert internrevsjon bør brukes aktivt til å sørge for at ledelse og styre har forståelse av den reelle sikkerhetstilstanden i virksomheten.

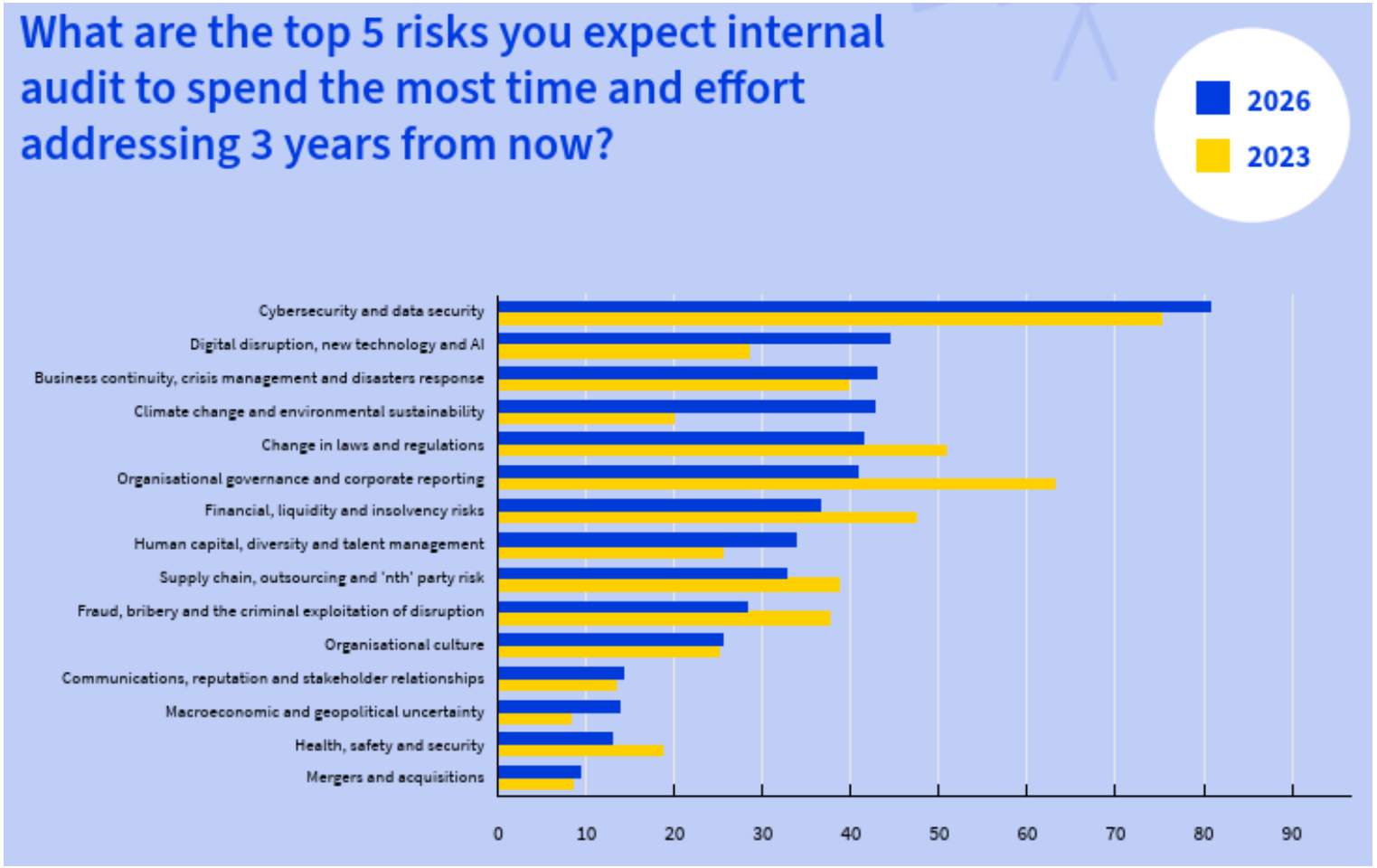
Denne innsikten er sentral for å jobbe mot et tilfredsstillende cybersikkerhetsnivå for deres virksomhet.

Hva mener internrevisjonsledere i Europa er de største truslene i dag?



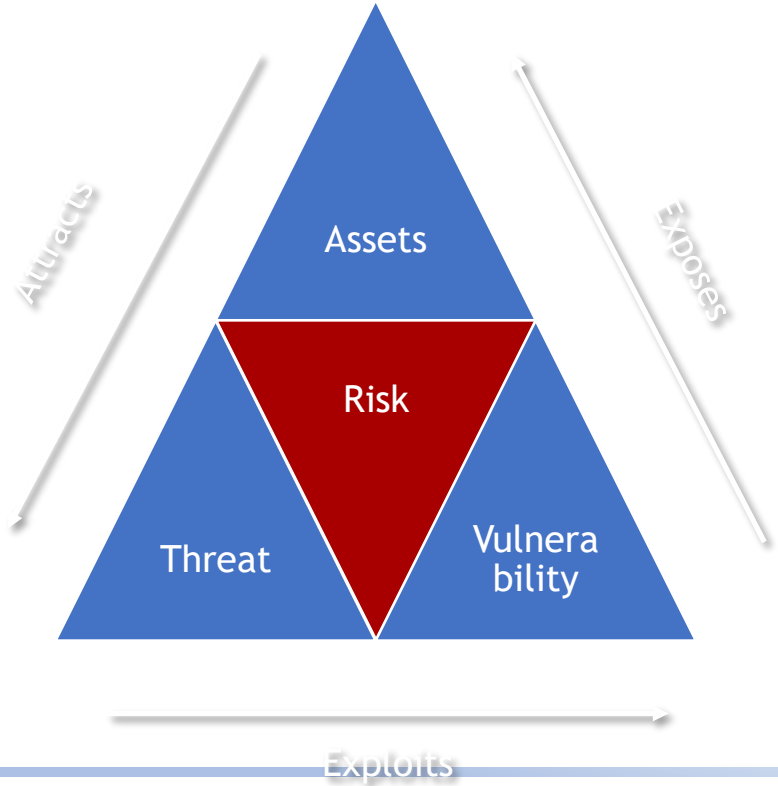
- Risk in Focus 2023, utgitt av ECIIA
  (European Confederation of Institutes of Internal Auditing)

Og hva vil være de risikoene internrevisjonen vil bruke mest ressurser på om 3 år?

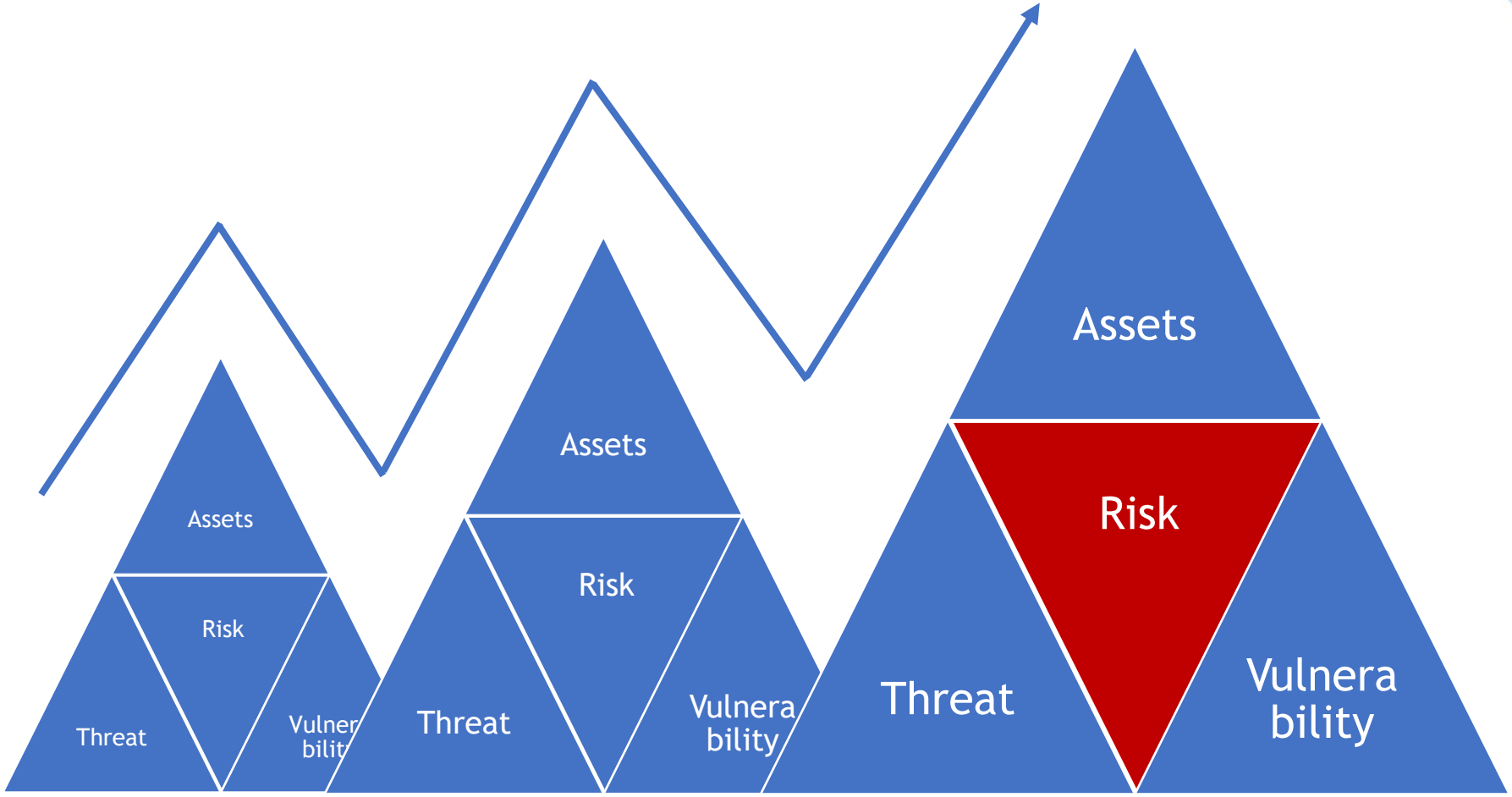


- Risk in Focus 2023, utgitt av ECIIA
  (European Confederation of Institutes of Internal Auditing)

Hva er cyberrisiko?



Hvorfor øker risikoen?



Hva må vi beskytte oss mot?

"Cyberangrep har blitt hverdagskost"

- **Gjennomsnittlig kostnad ved dataangrep er 43 MNOK**
- **Stadig flere angrep starter via leverandørkjeder**
- **75% av alle angrep starter med en phishing-epost eller trykk på link**
- **Ransomware er «dominerende» angrepstype**
- **Gjennomsnittlig løsepenge-sum er 5,7 MNOK**
- **77% av ransomware-angrep er i kombinasjon med trusler om å publisere data**
- **12% av rammede virksomheter betaler løsepenger**
- **Bare 8% av disse får faktisk gjenopprettet all data**
- **77% av virksomheter har planverk for håndtering av cybersikkerhetshendelser**

Kilder: ENISA, norton.com, techtarget.com, pandasecurity.com, statista.com, veeam.com, Sophos.com, varonis.com

NRK TV NRK RADIO NRK

Humor Distrikt Mer

Innlandet Tips oss Radio TV Langlesing Klassequizen 2020/2021

Østre Toten har vært uten datasys måned etter hacking

ØSTRE TOTEN (NRK): PST mener dataangrep er en av de største truslene i 2021. I Østre Toten innrømmer ordføreren at sikkerheten ikke var god nok.

KREVENDE JOBB: Over 1000 PC-er måtte gjenopprettes i Østre Toten etter at noen tok seg inn bak brannmurene til kommunen, sletta alle sikkerhetskopier og krypterte alle data.
FOTO: ANDERS BAKKERUD LARSEN / NRK

E24 AKSJELIVE BØRS E24+ TIPS OSS

DATAANGREP

Norfund ble svindlet for 100 millioner: – Dette er dobbelt så stort som Nokas-ranet

Det statseide Norfund har tapt 100 millioner kroner i et digitalt angrep, opplyser de onsdag.

Russisk cybergruppe angriper Norge

Onsdag morgen varslet den russiske hackergruppen Killnet et dataangrep mot Norge, melder Dagbladet.

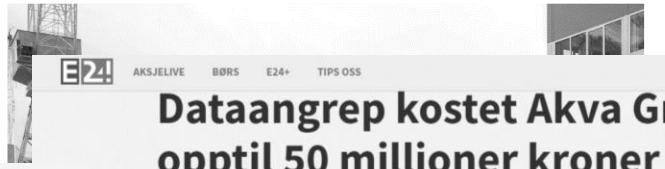
E24 AKSJELIVE BØRS E24+ TIPS OSS

Tietoevry utsatt for løsepenge-angrep: – Vi anser dette som en alvorlig kriminell handling

Verftskonsernet Vard utsatt for dataangrep

Kripos og politiet i Møre og Romsdal etterforsker et datainnbrudd hos verftskonsernet Vard.

1 min Publisert: 10.06.20 – 20.01 Oppdatert: ett år siden



E24 AKSJELIVE BØRS E24+ TIPS OSS Søk MENY

Annonse

Dataangrep kostet Akva Group opptil 50 millioner kroner

– Dette har vært en vanskelig og svært ressurskrevende situasjon, sier konsernsjef Knut Nesse.

DN Dagens Næringsliv Meny D2 Magasinet Dagens avis Kjøp DN Logg inn

Nyhetsstudio Koronaviruset Fantasyfond DN Ledelse Nyhetsbrev Siste nytt Sudoku Tips oss

Stortinget nok en gang utsatt for it-angrep

Dataangrep mot Norkart: 3,3 millioner kan være berørt

Selskapet Norkart, som leverer IT-systemer for kart- og eiendomsinformasjon, er utsatt for et dataangrep. Persondata for opp mot 3,3 millioner innbyggere er på avveier.

- ALVORLIG: Det sier administrerende direktør Leif Arne Brandsæter i Norkart om datainnbruddet.
FOTO: NRK

Svein Vestrum Olsson
Journalist

Ellen Omland
Journalist

Publisert 10. mai kl. 17:57
Oppdatert 10. mai kl. 20:59

Stortinget er nok en gang utsatt for et hackerangrep. (Foto: Aleksander Nordahl)

Det finnes grovt sett fire kategorier trusselaktører:

- Etterretningsbyråer
- Kriminelle
- Aktivister
- Terrorister

«Innsidere» faller inn under en av de fire andre kategoriene avhengig av motiv og hvem de jobber for.

Det finnes grovt sett fem kategorier for motivene deres:

- Sabotasje
- Spionasje
- Påvirkning
- Økonomisk vinning
- Infrastruktur

Her vil det ofte være noe overlapp.

For de fleste virksomheter er den mest relevante trusselen

økonomisk motiverte kriminelle

Disse aktørene bruker grovt sett tre metoder:

- Datainnbrudd
- Sosial manipulering
- Rekruttere en «innsider»

Av og til kan det være overlapp.

For å hente ut økonomisk gevinst bruker de som oftest disse fire taktikkene:

- Svindel
- Utpressing
- Digitalt tyveri
- Misbruk av datakraft

Også her kan det være overlapp.

For øyeblikket er trolig
målrettet utpressing,
også omtalt som

targeted ransomware

den farligste trusselen for de fleste virksomheter.

Diskusjon og erfaringsdeling:

Hva er deres digitale trusselbilde?
Har deres virksomhet erfart digitale angrep?

Hvordan jobbe med å få kontroll på cybersikkerhetsrisikoen?

Oversikt og kontroll på hva som skal beskyttes – før hvordan.

ETABLER OVERSIKT OVER ALLE FORRETNINGS-PROSESSER OG HVA DE ER AVHENGIGE AV

RISIKOVURDER ALLE VIKTIGE FORRETNINGSPROSESSER OG DERES AVHENGIGHETER OG IDENTIFISER OMRÅDER SOM MÅ HÅNDTERES

VELG EN STRATEGI FOR RISIKOHÅNDTERING SOM LEDERE RAPPORTERER OG BLIR MÅLT PÅ, OG HOLDT ANSVARLIG FOR

Information Security Management System

ISO

ISO/IEC 27001

The NIST Cybersecurity Framework

COBIT®

An ISACA Framework

CIS®

OWASP

Open Web Application Security Project

The Institute of Internal Auditors

IIA GTAGs – Auditing Cybersecurity Operations, Response and Recovery

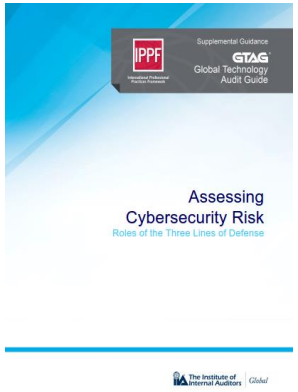
GTAG – Global Technology Audit Guides (IIA)

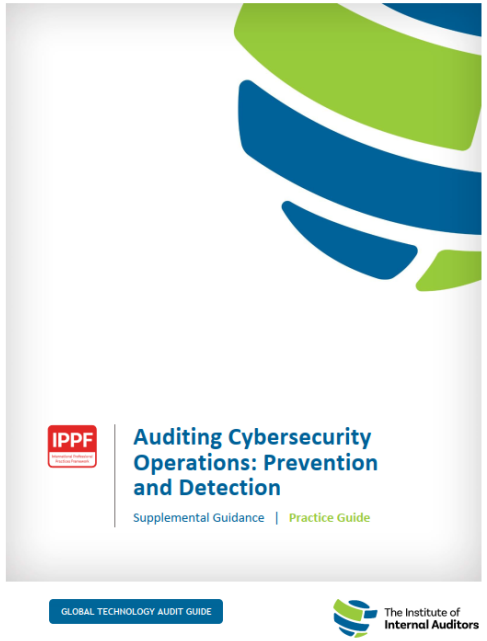
En GTAG publisert i 2016

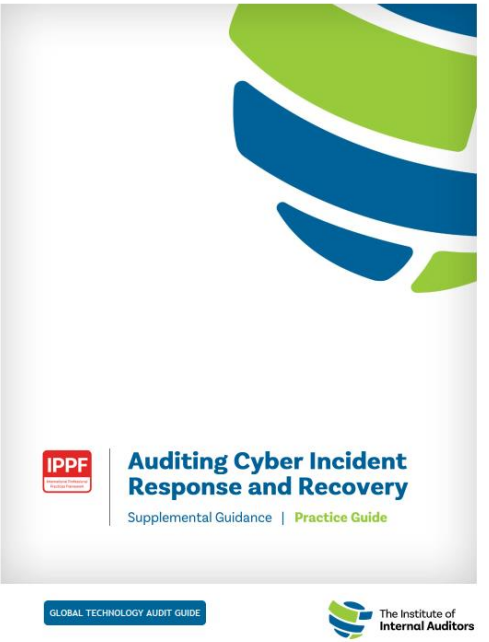
To nye GTAGs publisert i 2022

Referanser til ulike rammeverk:

- Cobit 2019
- NIST SP 800-53
- NIST CSF
- CIS Controls v8

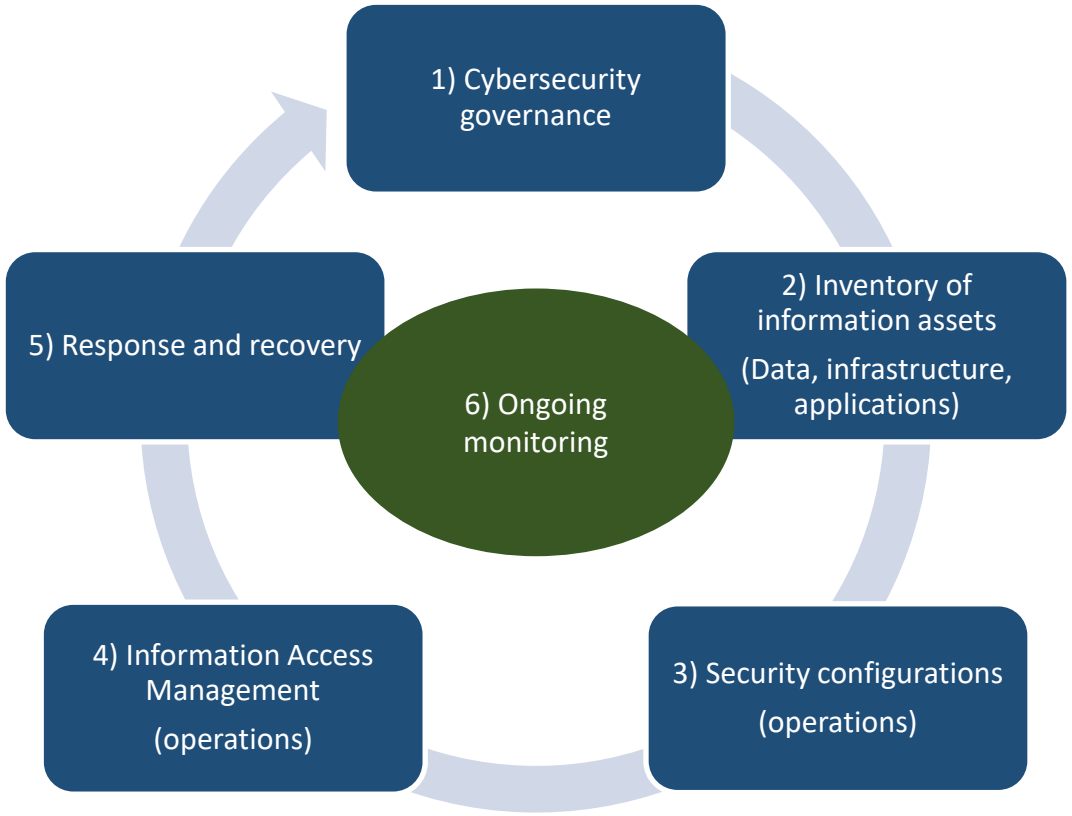






Cybersikkerhetsrevisjoner – rammeverk

GTAG – Global Technology Audit Guides (IIA)



VERIFISERES GJENNOM TEST AV SIKKERHETSTILTAK/ SIKKERHETSTESTING

Hva er beste praksis?

Det finnes en rekke standarder og rammeverk å ta utgangspunkt i:

- Internasjonalt: ISO 27001/02, NIST CSF, CIS controls, CSA Cloud Control Matrix, OWASP
- Norge: NSMs grunnprinsipper for IKT-sikkerhet v.2.0

Fordeler og ulemper ved alle:

- Noen high-level, men retningsgivende
- Noen passer best for veldig store virksomheter
- Noen er spesialtilpasset cloud eller utviklingsmiljøer

Hvilke rammeverk benytter virksomheten i dag?

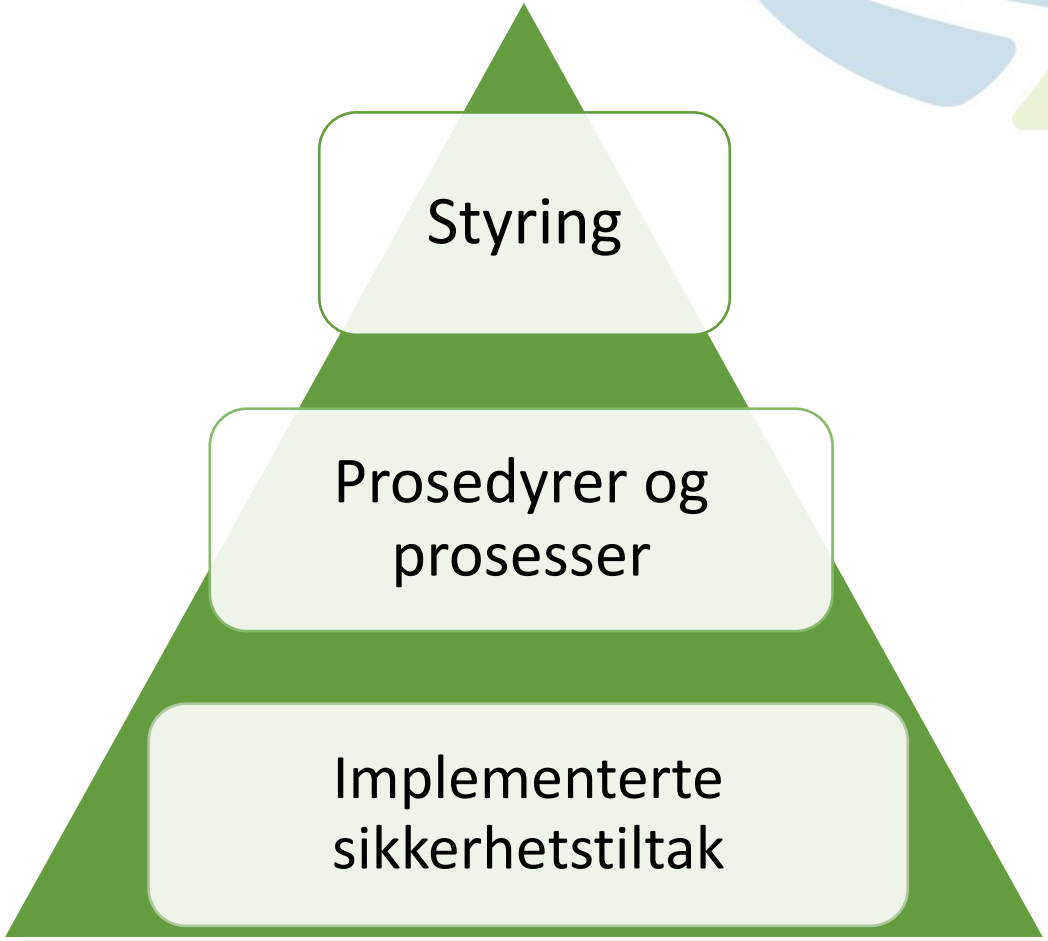
Tilpasse til virksomhetens behov

Sentralt for å forstå risikobildet:

- Forstå virksomheten og dens informasjonsverdier
- Forstå bransjen og trusselaktører
- Forstå hva som er kritiske scenarier

Oppbygging av arbeidet med cybersikkerhet i virksomheten:

- Jevn fordeling av innsats i hele trekanten
- Overslag mot styrende dokumenter vs. overslag mot implementerte sikkerhetstiltak



Diskusjon og erfaringsdeling:

Hva slags rammeverk er tatt i bruk hos dere?
Opplever dere å ha oversikt og kontroll?

Hvordan bruke internrevisjon for å styrke cybersikkerheten

Viktigheten av scoping og tilpasning

- «Cybersikkerhet» er stort og komplekst
- God scoping av revisjonen bør gjøres basert på kritikalitet og risiko
- Nøkkelpersonell bør involveres tidlig
- Revisjonen bør ta utgangpunkt i etablerte sikkerhetsmål, og bruke rammeverk som er kjent, slik at revisjonen gir verdifull innsikt og bidrag til forbedring
- Scopet bør begrenses så revisjonsprosjektet kan være konkret
- Operasjonalisere revisjonskriterier, og tilpass rammeverkene til deres behov

Erfaringer fra gjennomførte revisjoner

Identifisere og kartlegge

- Ikke identifisert informasjonsverdier og beskyttelsesbehov
- Tror de har oversikt over alt, men glemmer utkontrakterte tjenester, on-prem vs. sky
- Mange har startet på skyreisen uten å planlegge for hvordan sikkerhet skal ivaretas

Beskytte og opprettholde

- Utkontrakterer tjenester uten å stille sikkerhetskrav
- Få har sikkerhet på agendaen i anskaffelsesprosesser
- Tar i bruk M365/O365 uten å stille krav om sikkerhetskonfigurering (E5-lisenser uten at disse benyttes)

Oppdage

- Mye preventive tiltak, men lite oppdagende tiltak i form av analyser av trafikk, trender, logger etc.
- Lite løpende læring/forebygging basert på hendelser
- Lite løpende sikkerhetstesting av utviklingsmiljø og/eller produksjonssystemer

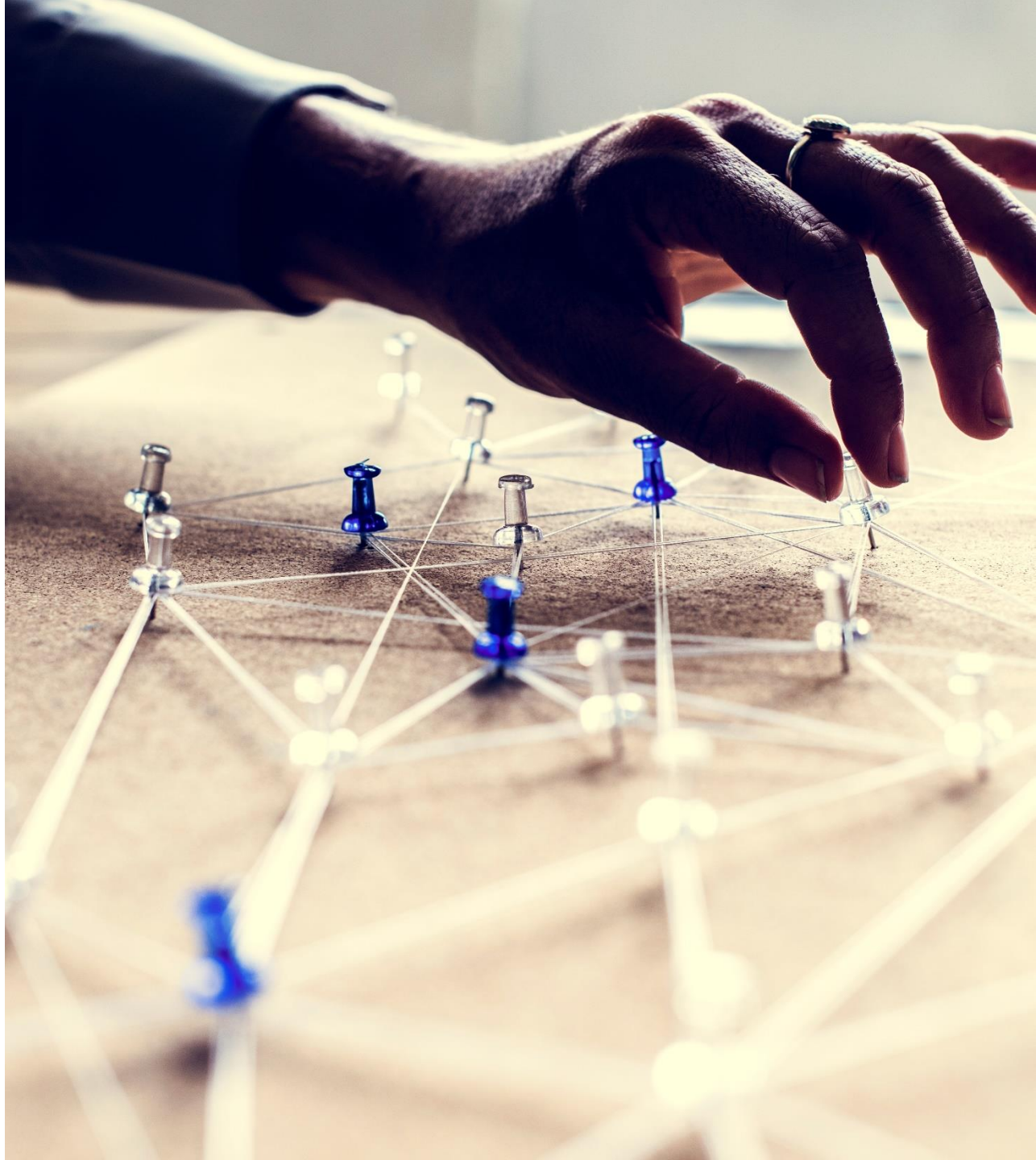
Håndtere og gjenopprette

- Veldig få har testet evnen til gjenoppretting
- Mange tror det er tilstrekkelig å ha backup
- Få har cybersikkerhetshendelser som del av beredskapsplanene og har aldri øvd på disse

Cyberangrep er dynamiske, mens cyberforsvar ofte er ganske statisk.

Vi bør derfor bort fra «listetenkning», når vi skal sjekke den reelle sikkerhetstilstanden.

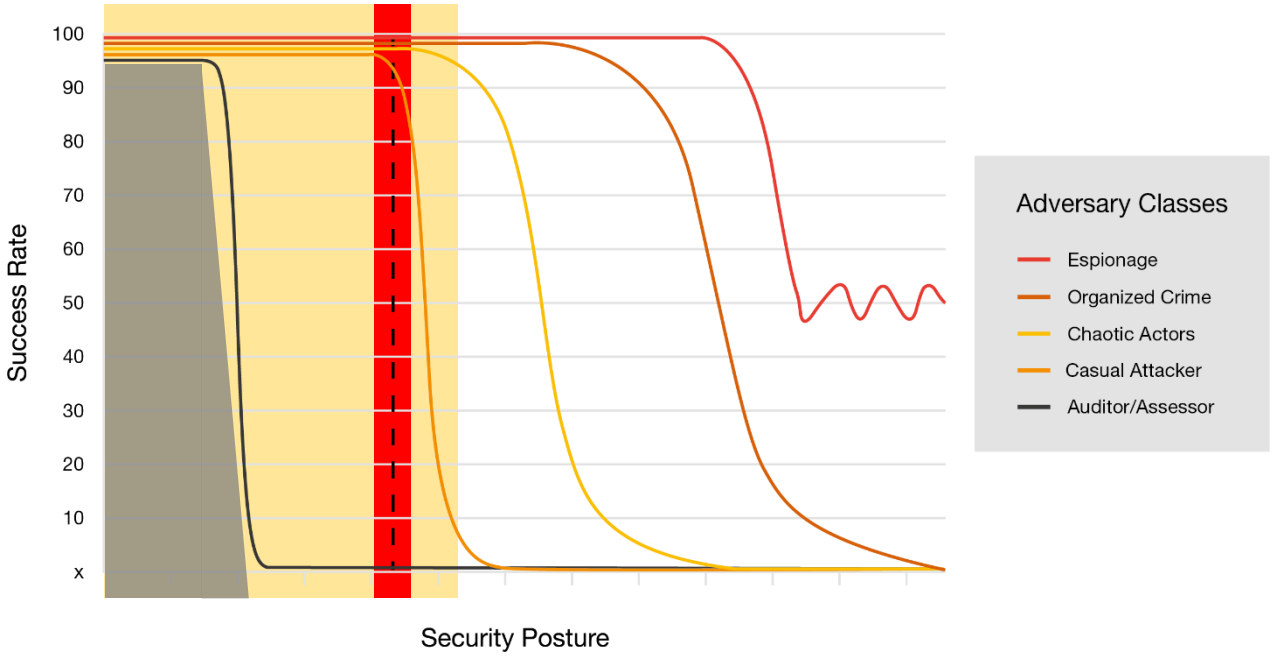
> *Defenders think in lists. Attackers think in graphs.*
> *As long as this is true, attackers win.*
>
> *– John Lambert (Microsoft)*



«Metasploit»

«Causual attacker»

«Auditor»

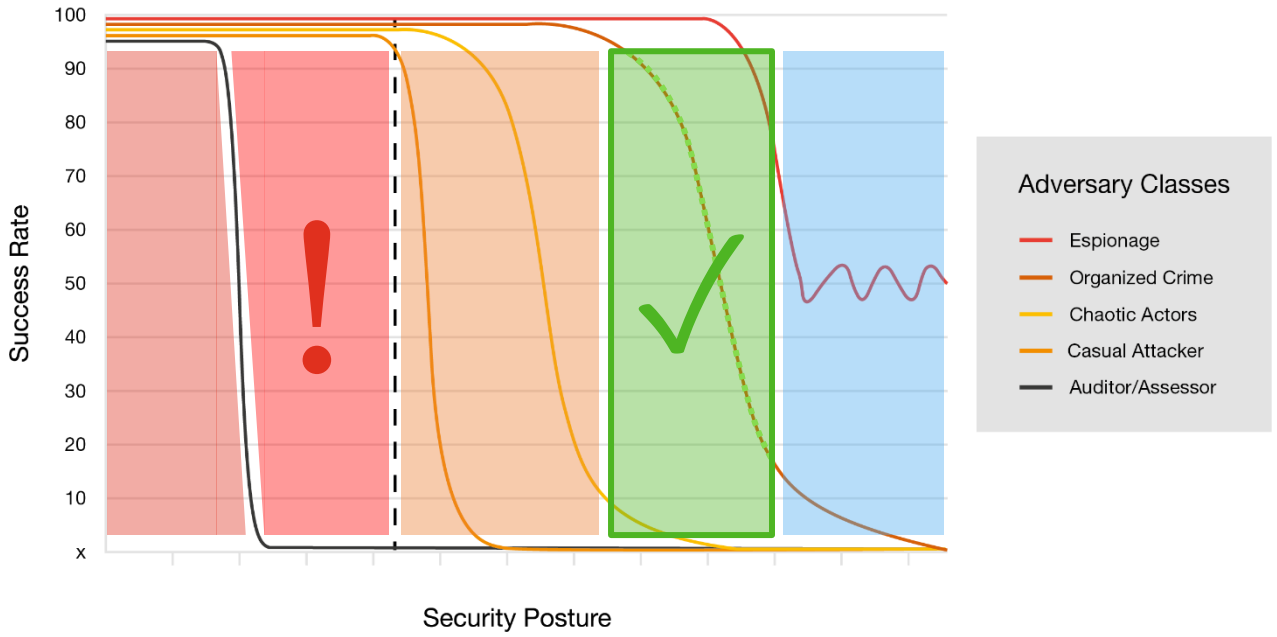


Påstand:

Revisoren er
den enkleste
«motstanderen»
å overvinne.

... og utvikler seg trolig saktere enn
de andre trusselaktøren

Det å være «compliant» sier ikke nødvendigvis noe om reell motstandsdyktighet



Dårlig og vet det.

Dårlig, men vet det ikke!

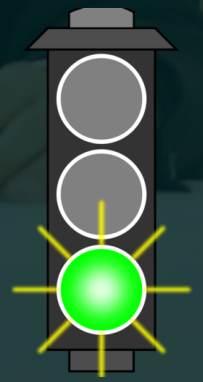
På bedringens vei.

✓ God sikkerhet.

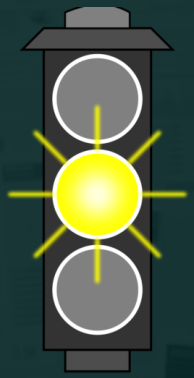
Svært god sikkerhet.

«God» ut fra trusselbildet og verdiene som skal beskyttes.

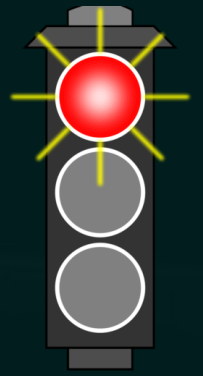
Følger vi beste praksis?



Er beste praksis implementert i hele virksomheten?



Fungerer dette etter hensikten i vår virksomhet?



Tekniske tester og verifikasjon

- **Sikkerhetstester**, både eksterne og interne, gir innsikt i sårbarheter og sikkerhetshull
- **Red-Team/TIBER-øvelser** med realistiske scenarier viser virksomhetens reelle evne til å oppdage og forhindre angrep
- **Gjennomgang av sikkerhetskonfigureringer** i sentrale systemer gir innsikt i om sikkerhetsfunksjonalitet er på og utnyttes fullt ut
- Gjennomgang av **evalueringer og forbedringstiltak** som er implementert etter faktiske hendelser gir innsikt i virksomhetens evne til læring og kontinuerlig forbedring
- **Verifikasjoner** av representativt utvalg gir innsikt i operasjonell effektivitet over tid

Våre anbefalinger

- Inkluder cybersikkerhet i internrevisjonsprogrammet
- Ha en risikobasert tilnærming
- Scope revisjonene så det er mulig å gå i dybden
- Ta utgangspunkt i rammeverk og sikkerhetsmål
- Involver nøkkelpersonell tidlig, så det er tydelig at revisjonen skal gi verdifull innsikt og bidrag til forbedring
- Inkluder dybdekompetanse på teknisk sikkerhet i revisjonsteamet
- Gjør verifikasjoner for å kontrollere faktiske forhold

Diskusjon og erfaringsdeling:

Er cybersikkerhet en del av deres revisjonsprogram?
Hva er deres viktigste erfaring etter gjennomførte revisjoner på temaet?

Ingunn Holte
Head of Advisory Services

Tlf.: 975 53 777
Epost: ingunn.holte@defendable.no

Siv Irene Aasen
Partner, Risk Advisory Services

Tlf.: 982 06 148
Epost: siv.irene.aasen@bdo.no