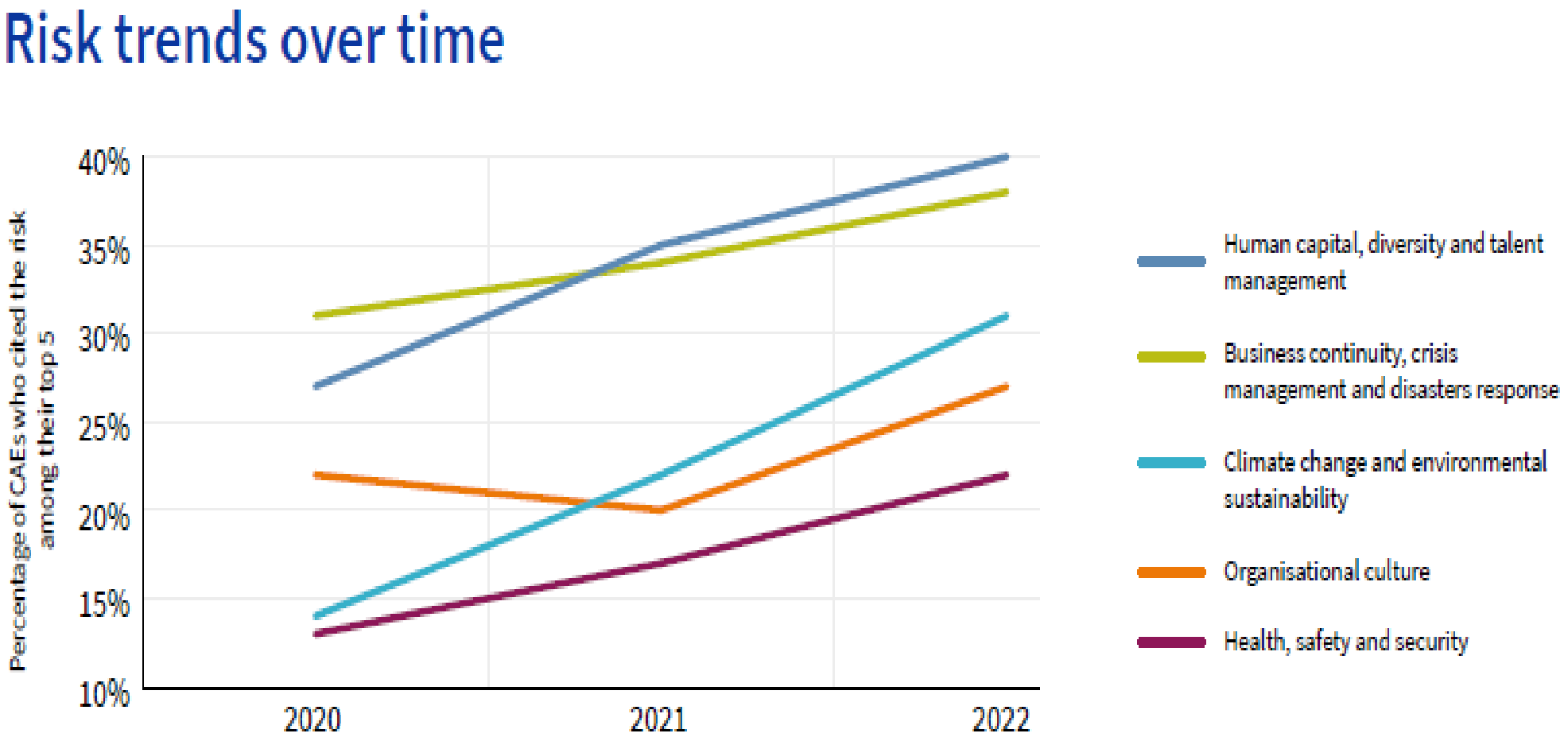
transcendent group GOVERNANCE RISK COMPLIANCE

Webinar:
Aktuella granskningsområden

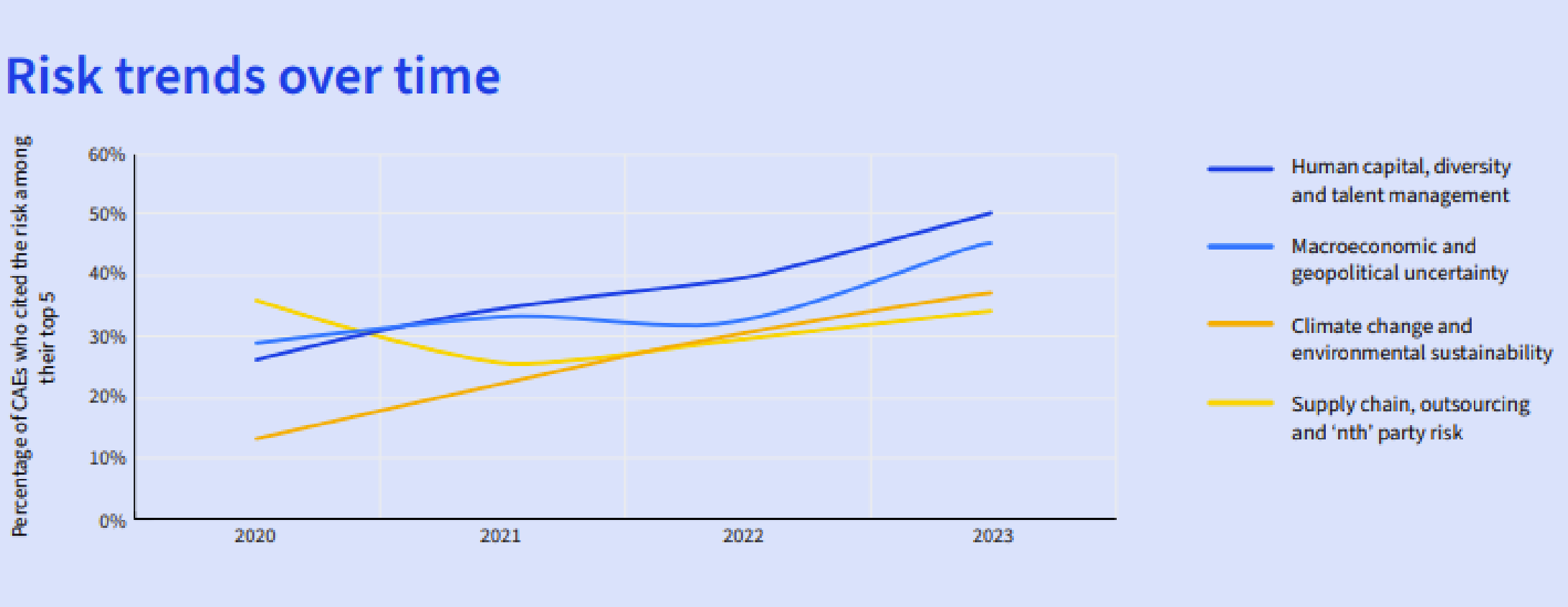
2022-10-28

Charlotte Eklund
Magnus Thyllman

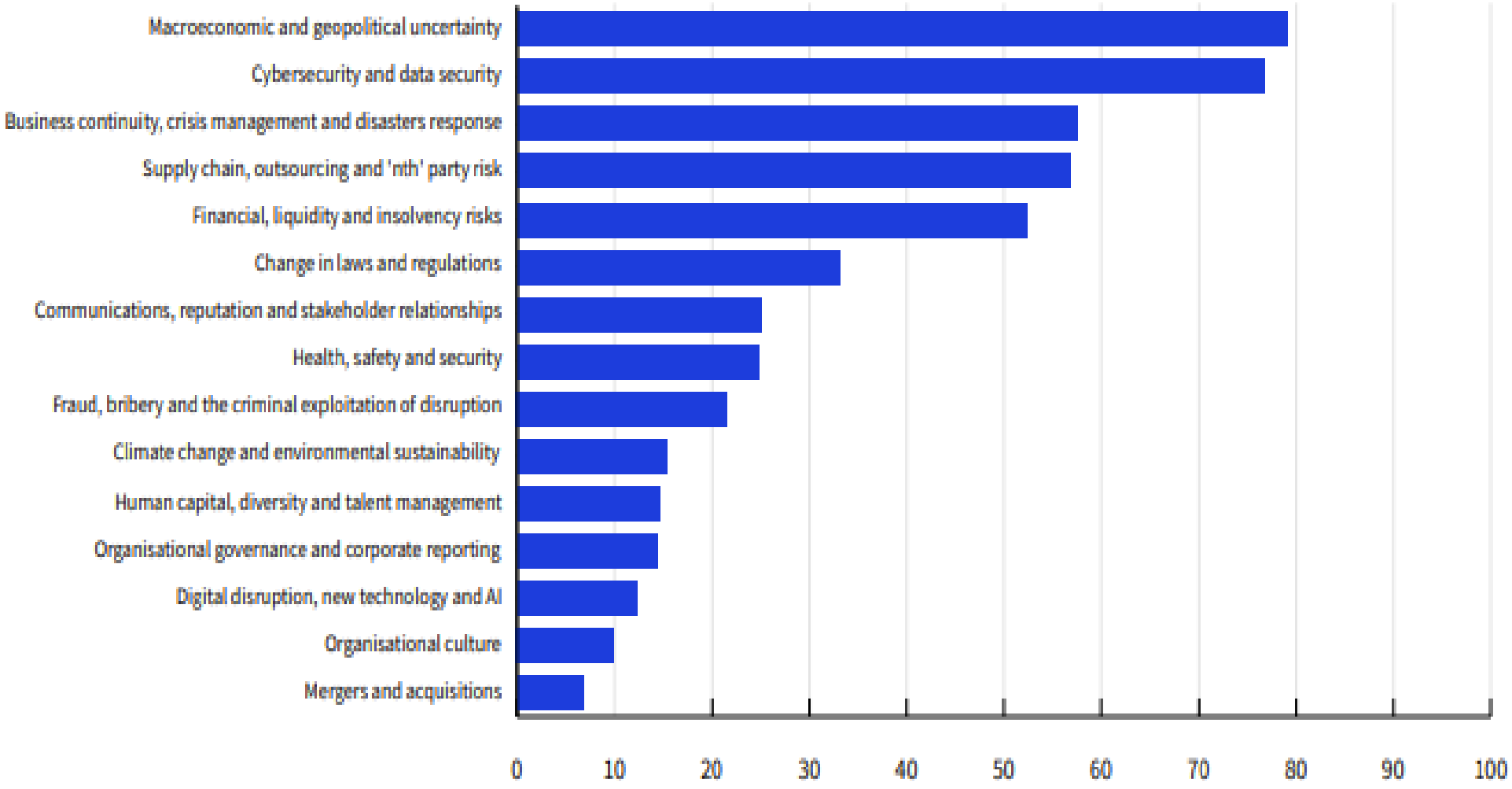
Hämtat från Risk in Focus 2022



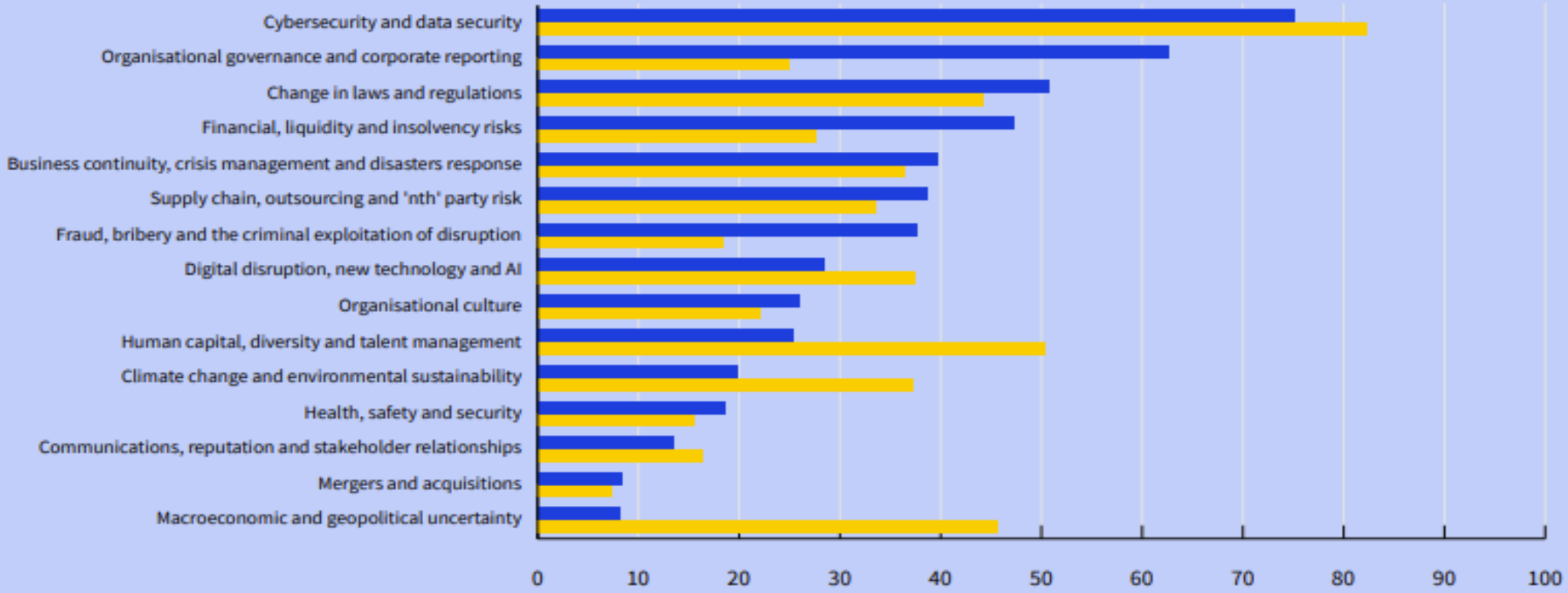
Hämtat från Risk in Focus 2023



What top five risks has the War in Ukraine had the most impact on?



What are the top 5 risks on which internal audit spends most time and effort?



En omvärld i förändring

En ökande riskbild

Antagonistiska hot från många håll

- Organiserad brottslighet
- Statliga aktörer
- Aktivister
- Enskilda hackers

Nedbrutna risker

- Störningar i kritisk verksamhet
- Offentliggörande av känslig information
- Informationsstöld
- Utpressning (Ransomware)
- Rykte/varumärkesrisk

Skydd av säkerhetsskyddskänslig eller samhällskritisk verksamhet

- Hur väl organiserat och systematiskt är säkerhetsskyddsarbetet?
- Har verksamheten infört rutiner, processer och förutsättningar för efterlevnad av säkerhetsskyddsförordningen och säkerhetsskyddslagen?
- Finns verksamhet som omfattas av NIS-direktivet?
- Utgå från lagkrav och interna styrdokument

Cybersäkerhet/IT-säkerhet

- Finns IT-säkerhetsregler med krav på skyddsåtgärder definierade?
- Hur beslutas vilka skyddsåtgärder som är nödvändiga (baseras dessa på informationsklassning)?
- Har ändamålsenliga skyddsåtgärder införts?
- Hur mäts och utvärderas det egna skyddet?
- Finns tillräcklig förmåga att identifiera och hantera intrång?
- Görs regelbundna penetrationstestning/sårbarhetsanalyser?
- Finns fokus på awareness?

Mänsklig risk - Social engineering

- Hur välutbildad är personalen kring skydd av information?
- Har utsatta roller erhållit specialanpassade utbildningar?
- Har personalens motståndskraft utvärderats med hjälp av interna tester?
- Internrevisionen kan utvärdera medvetenheten och mognaden hos personalen genom att med olika scenarios testa motståndskraften mot mänsklig påverkan genom sms, samtal, mail mm.
- Kan med fördel kombineras med utvärdering av fysiskt skalskydd/inpassering.

Hantering av leverantörer

- Hanteras beslut om outsourcing på rätt nivå?
- Har organisationen rätt beställarkompetens?
- Hantering av IT-säkerhetskrav
- Hur utvärderas leveransen? (egna uppföljningar, oberoende revisioner, ISAE-intyg)
- Hur utvärderas de operativa riskerna och leverantörsberoenden?
- Kontinuitetshantering av försörjningskedjorna
- Finns specifika krav för molntjänster?

Kris- och kontinuitetshantering

- Finns en etablerad krisorganisation och krisledningsplan?
- Arbetar organisationen systematiskt med kontinuitetsplanering?
- Finns tydliga roller och ansvar för kontinuitet och återställning?
- Har kritiska verksamhetsområden identifierats?
- Har risk- och konsekvensanalyser gjorts?
- Finns kontinuitetsplaner framtagna?
- Finns återställningsplaner (recovery plans) framtagna?

Humankapitalet – organisationens viktigaste?

Kompetensförsörjning

- Arbetar din organisation systematiskt för att säkra rätt kompetenser för framtiden?
- Hanteras frågan på rätt nivå i organisationen? Finns en uttalad ansvarig i ledningen?
- Har kartläggning av kompetensgap gjorts?
- Finns både korta och långa kompetensförsörjningsplaner? Hänger de ihop med verksamhetens mål?
- Innehåller kompetensförsörjningsplanera perspektiv som utveckling av befintlig personal, rekrytering, externa resurser, avveckling av personal osv?
- Vilken effekt har pandemin fått på möjligheten att behålla och rekrytera personal?
- Har kompetensförsörjningsstrategin anpassats?

On-boarding/Off-boarding

- Finns ett tydligt mål med on/off-boardingen?
- Finns en etablerad process för on/off-boarding?
- Finns relevant stöd för cheferna?
- Efterlevs processen?
- Uppnås önskat resultat?

Strategi för konsultanvändning

- Vilken strategi har organisationen vad gäller konsultanvändning? Är den rimlig i förhållande till hur det ser ut? Är strategin förankrad? Vilka åtgärder har vidtagits?
- Har organisationen utvärderat jävsrisker och intressekonflikter? Hanteras dessa på rimligt sätt?
- Hur har behörigheter till information, befogenheter att fatta beslut mm hanterats för konsulter?
- Hur styrs konsulternas insatser?
- Hur säkerställs överföring av know-how?
- Hur arbetar organisationen med att säkerställa business continuity - trots svårigheter att rekrytera och behålla personal och stort konsultberoende?

Organisationskultur i en förändrad värld

- Hur organisationen identifierat de nya risker som uppkommit i samband med pandemin och förändrade arbetssätt?
- Finns en strategi kring att anpassa kultur och värderingar utifrån nya förutsättningar? Från att ”ha suttit i väggarna” till att sitta – var då?
- Vilka planerade åtgärder finns för att möta nya risker relaterade till kulturen?
- Finns ett strukturerat arbete med värdegrund/värderingar i organisationen?
- Är kultur/värderingar integrerade i processer, ex kopplat till medarbetarskap, rekrytering mm?

Hållbar arbetsmiljö

- **Systematiskt arbetsmiljöarbete (AFS 2001:1)**
  - Har arbetet integrerats i det dagliga verksamheten?
  - Finns en uppgiftsfördelning och delegering av arbetsmiljöansvar?
  - Görs en regelbunden analys av risker i arbetsmiljön?
  - Gör en särskilt riskanalys vid större förändringar?
  - Vidtas lämpliga åtgärder och följs dessa upp?

- **Organisatorisk och social arbetsmiljö (AFS 2015:4)**
  Finns rutiner och arbetssätt som omhändertar det som förskriften vill uppnå ex:
  - fördelning av arbetsuppgifter
  - hantering av arbetstider och arbetsbelastning över tid
  - konflikter och kränkande särbehandling

Digitalisering och agil utveckling

IT- och digitaliseringsstrategier

- Finns en fastställd strategi för digitalisering och IT som utgår från affärsstrategin?
- Har organisationen utvärderat vilka förmågor, tekniska IT-lösningar och verktyg som kommer krävas för att möta framtida behov från medarbetare och kunder?
- Har det analyserats hur mycket pengar som organisationen är villig investera i innovation och utveckling av framtida IT-lösningar?
- Finns handlingsplaner framtagna för att möta strategiska målsättningar?
- Vilka konsekvenser kan digitaliseringen få för utsatta kundgrupper?
- Digitization vs Digitalization

Agil affärsutveckling

- Hur formaliseras och förankras nya arbetssätt för verksamhetsutveckling?
- Vem äger utvecklingsmodellen och hur tillhandahålls stöd till verksamheten?
- Hur görs prioriteringar på strategisk, taktisk och operativ nivå?
- Har roller, ansvar och mandat definierats och förankrats?
- Hur utvärderas risker när man överger traditionell projektstyrning?
- Finns rutiner för fastställande och uppföljning av nyttokalkyler och business case?

Säker systemutveckling

- Finns en fastställd metodik/vägledning för säker systemutveckling med obligatoriska moment/aktiviteter?
- Görs hotanalyser för att bedöma risker med eventuella sårbarheter?
- Hur hanteras extern kod (öppen källkod) som nyttjas i utvecklingsarbetet?
- Genomförs säkerhetstestning manuellt och/eller med hjälp av automatiserade verktyg?
- Vem tar beslut om produktionssättning i det fall sårbarheter identifierats?

Granskningsområden inom hållbarhet

Hållbarhet – är verksamheten på banan?

- Nya regelverk från 2021 (disclosure- och taxonomiförordningen samt non-financial reporting directive) – omfattas din organisation av regelverken och i så fall vilka?
- Har analys av påverkan gjorts, finns en handlingsplan, styrs arbetet på rätt nivå? Hur ser strategin ut?
- Är hållbarhetsrisker inkluderade i organisationens riskanalys?
- Är hållbarhet integrerat i organisationen processer eller bedrivs arbetet separat? Vad gör övriga kontrollfunktioner, t.ex. regelefterlevnad och risk?
- Finns det processer på plats för att säkerställa att korrekt information kommuniceras till intressenter?

Oegentligheter, korruption och intressekonflikter

- Hur ser organisationens förebyggande arbete ut?
  - Finns en väl definierad kontrollmiljö
  - Har oegentlighetsrisker/intressekonflikter identifierats? Finns ett systematiskt arbete runt detta?
  - Finns lämpliga kontroller och åtgärder på plats?
  - Hur arbetar organisationen med information och kommunikation?
  - Vilken uppföljning görs?
- Bisysslor – alltid en risk – särskilt i offentlig förvaltning
  - vilka regler och rutiner finns på plats?
  - efterlevs de? Verifiera med hjälp av registeranalyser
- Whistleblow – en del av det interna kontrollsystemet
  - Finns rutiner för att ta emot och hantera ärenden?
  - Hur skyddas den som rapporterar in något?

Frågor?

Charlotte Eklund – charlotte.eklund@transcendentgroup.com
Magnus Thyllman – magnus.thyllman@transcendentgroup.com

© Transcendent Group 2021