- Digitaliseringens betydning for revision af IT- og cyberrisici

- ISA 315 som primær regulering af IT i finansiel revision

AALBORG UNIVERSITET
CAND.MERC.(AUD.)
Cecilie Rosenkjær – 20166444
Jonas Emborg Bunk Jensen - 20165847

Dato: 31. maj 2021
Antal anslag: 221.052
Vejleder: Peter Thor Kellmer

Abstract

In the recent years and the foreseeable future IT-system plays an increasingly important role in businesses. Consequently, this development has brought an increase in cybercrime and IT-related risk in general. Still, the international Standard on Auditing (ISA) 315 remains relatively unchanged. Therefore, this paper seeks to examine whether ISA 315 is sufficiently recent, to enable auditors to effectively gather suitable audit evidence regarding IT.

This is done by describing the general development in cybercrime, cybersecurity, and appropriate IT customs. Additionally, the IT-related actions contained in the ISA's are summarized and followed by an overview of the COBIT 5 and COSO frameworks. This summation and overview are used to analyze two surveys respectively dealing with auditing of IT and the opinions of businesses on cybercrime. Also analyzed is the increasing importance of IT- and cybersecurity in relation to the auditing risk model, COSO compared to COBIT 5 and ISA 315 compared to the revised ISO/IEC 27002. Moreover, the auditing process is evaluated with a focus on IT-auditing, with the objective of finding how auditing of IT can be implemented in the overall process. Throughout the entirety of this paper, information from multiple interviews is applied to enhance the validity of the paper. The analysis finally determines multiple measures of improvement, including but not limited to: Updating ISA 315, entering references to ISO-standards in ISA 315 and increasing the IT-competence of auditors. This leads to the part of illuminating the issue, which discusses whether cybersecurity should be part of the auditing tasks and if IT-auditing reasonably can become a larger part of the overall audit. In summation it is found that businesses themselves should have the primary responsibility for making sure that their cybersecurity is sufficient. To elaborate, auditing as a concept concerns itself with the past, while cyberrisk is an eventual problem. Regarding IT-auditing becoming a more substantial part of overall auditing it is inferred that there is a gap in the interpretation of ISA 315 between the IT-auditors and the financial auditors. Therefore, it is concluded, that increasing IT-oriented awareness and competence among financial auditors likely will have the biggest effect.

Concludingly, the continuous technological development results in widespread business application of IT-systems. This leads to an increase in IT- and cyberrisk, which furthers the need to take these aspects into account during auditing. Consequently, various measures reducing businesses vulnerability to cybercrime have been developed and are recommended to use in combination with proper IT customs. Finally, because of the this change IT-auditing should be normalized to a greater extent.

Kapitel 1

Indledning & Metode

Dette kapitel omfatter den indledende del af specialet, som har til formål at introducere specialets problemstilling samt hvilken metode der er anvendt til at løse denne. Kapitlet indeholder indledning, problemfelt, problemformulering, metode og afgrænsning.

1 Indledning

Danmark er et af de mest digitale samfund i verden, hvor IT i stigende grad indgår i danske virksomheder. I 2020 anvendte 93 pct. af virksomhederne hjemmesider eller sociale medier (Erhvervsministeriet, u.å.; Danmarks Statistik, 2020). Denne udvikling har medført en topposition i EU, når det kommer til brugen af digital teknologi. Ifølge Dansk Industri er årsagen til dette, at Danmark er EU's mest digitaliseringsparate samfund, med en stærk position inden for udviklingen af teknologiske løsninger inden for blandt andet sundhed, administration, uddannelse, cybersikkerhed, mv.
Dette er en position, som Dansk Industri mener, at Danmark skal fastholde, med det formål at sikre EU's digitale fremtid, og at sikre, at europæiske virksomheder har de bedste vilkår, for at konkurrere med virksomheder i lande som USA og Kina (Dansk Industri, u.å.).

Danmarks position inden for digital udvikling og det danske samfunds afhængighed af internettet, medfører en større sårbarhed over for digitale trusler, herunder cyberkriminalitet. Denne trussel er en tendens, som generelt har været stigende i forbindelse med den øgede brug af teknologi. Cyberkriminalitet er under konstant udvikling og tilpasning til verdenssituationen, som Covid-19 krisen er et eksempel på, hvor cyberkriminelles aktiviteter har ændret sig, med det formål at udnytte den globale krise (Center for cybersikkerhed (a), 2020, s. 3). Center for cyberkriminalitet (Red. CFC) er en national IT-sikkerhedsmyndighed, netsikkerhedstjeneste og nationalt kompetencecenter for cybersikkerhed, etableret i 2012, som en del af forsvarets efterretningstjeneste. Ifølge CFC' Trusselsvurdering 2020 er truslen fra cyberkriminalitet vurderet til at være høj, og det vurderes at truslen om målrettede ransomware-angreb mod danske myndigheder og virksomheder er stigende (Center for cybersikkerhed (a), 2020, s. 3).
Det er ifølge Danmarks statistik især store virksomheder, som oplever brud på IT-sikkerheden, hvor hver tredje i 2019 blev ramt af et sikkerhedsbrud (Danmarks Statistik, 2019). Denne udvikling har fået flere af de store virksomheder til at øge investeringerne i IT-sikkerhed (Dansk industri, 2019).

Den stigende digitalisering har endvidere påvirket revisionen og en del af revisorers opgaver er blevet digitaliserede, hvorfor der stilles spørgsmålstegn ved revisorers fremtidige arbejde (Gath & Jepsen, 2018). Dette kan dog give anledning til nytænkning for revisorernes arbejde, herunder med formål om at øge fokusset på revision inden for IT, som på nuværende tidspunkt kun er en lille del af revisorernes opgaver. Hertil gælder, at revisor skal danne sig et overblik

over virksomhedernes IT-anvendelse samt vurdere om virksomhedens anvendelse af IT er betydelig (ISA 315). Der kan argumenteres for at denne indgangsvinkel ikke længere er tilstrækkelig og at der kræves en forandring og opdatering af revisors arbejde samt krav til revisor i forbindelse med revision af IT i virksomhederne.

2 Problemfelt

På nuværende tidspunkt bliver revisionen af IT-systemer primært reguleret ved ISA 315. Derimod reguleres IT som en del af revisors sædvanlige identifikation og vurdering af risici ud fra ISA 315, og revisors reaktion på de vurderede risici ud fra ISA 330. Spørgsmålet er om denne generelle regulering af IT kan fortsætte med at være tilstrækkeligt i en tid hvor virksomhederne i stigende grad bliver digitaliseret (Liempd, Kristensen, Wickstrøm, & Haug, 2020)?

Ifølge Liempd et al. (2020) er der et stort uudnyttet potentiale i revisionsbranchen, når det kommer til anvendelsen af nye digitale teknologier, der på sigt kan have stor forretningsmæssig betydning for revisorerne, som følge af omfattende automatisering. Det tyder på, at både revisorerne og deres kunder inden for en overskuelige fremtid, vil gennemgå en væsentlig udvikling, hvor digitalisering og IT vil spille en større rolle end hidtil. Revisors anvendelse af ny teknologi, kan for revisor betyde indtrædelsen i en helt ny rolle, hvortil der kræves nye kompetencer og arbejdsmetoder (Gath & Jepsen, 2018). På samme måde forventes virksomhedernes stigende anvendelse af ny teknologi samt IT, at stille nye krav til revisors kompetencer, som måden hvorpå revisor forstår virksomheden og dens omgivelser.

Tidligere formand for FSR Peter Gath og adm. direktør Charlotte Jepsen påpeger: ” Vi skal kunne forstå, håndtere og vurdere ny teknologi og processerne omkring. IT-revision er i dag et speciale. Det bliver mainstream.” (Gath & Jepsen, 2018).

En Ph.d.-afhandling af Peter Birkholm Laursen (2001) giver en mulig forklaring på, hvorfor IT-revision fortsat er et speciale i revisionsbranchen. Laursen (2001) beskriver hvordan de analyserede dokumenter, herunder dagældende revisionsvejledning (RV) 14 og 17, primært varetager aktørernes økonomiske egeninteresse ved beskrivelsen af intern kontrol som begreb. Med fokus på revisionsstandarderne bliver disse således af mere generel karakter, da dette minimerer kravene til revisors arbejde. Selvom overgangen fra RV 14 og 17 til ISA 315 samt

330 anses som en forbedring, kræves det af revisor kun at opnå forståelse af de interne kontroller m.v. direkte knyttet til regnskabsaflæggelsen, jf. ISA 315, 18. I forlængelse heraf omhandler revisors erklæring udelukkende det konkrete resultat, og ikke kvaliteten af den interne kontrol som helhed eller ledelsens styring heraf (Laursen, 2001).

Der kan på baggrund af ovenstående argumenteres for, at det er i revisors egeninteresse at stille højere krav til sig selv i forhold til IT-revision, hvilket eksempelvis kan gøres ved proaktiv udstedelse af regulering eller udvidelse af eksisterende revisionsstandarder. Argumentet tager udgangspunkt i omfanget af den kompetencemæssige omstilling, der antages at være ved skiftet til et fokus på IT-revisionen. Derfor kan der stilles spørgsmål til hvorvidt de nuværende krav til IT-revisionen, er tilstrækkelige i forhold til revisors kompetencer til at opnå egnet revisionsbevis i sammenhæng med den stigende digitalisering. Herunder hvilken betydning den indledningsvist nævnte trussel af cyberkriminalitet kan have på revision generelt. Dette leder frem til nedenstående hypotese og problemformulering.

2.1 Problemformulering

- *Hypotese: Revisionsstandarderne er ikke ajourført tilstrækkeligt til at afdække det stigende behov for revision af IT, hvorfor revisor ikke opnår tilstrækkeligt egnet revisionsbevis.*

- *Hovedspørgsmål: Hvilken diskrepans findes der mellem det stigende behov for revision af IT og de IT-relaterede krav i ISA 315, hvordan kan dette forbedres?*

    - *Underspørgsmål 1: Hvilke andre IT-relaterede standarder og modeller kan være relevant for revisors håndtering af IT?*
    - *Underspørgsmål 2: Hvilken udvikling er der inden for cyberkriminalitet og -sikkerhed, og hvordan påvirker denne revisionen?*
    - *Underspørgsmål 3: Hvordan kan virksomhederne forebygge og reducere effekten af cyberkriminalitet?*
    - *Underspørgsmål 4: Bør ansvaret for cybersikkerhed pålægges revisorerne eller virksomhederne?*

3 Metode

Dette afsnit omhandler den juridiske-, samt anden metode, som anvendes til at besvare specialets problemformulering. Afsnittet omfatter endvidere en beskrivelse af dataindsamling, herunder hvordan data indsamles og anvendes i specialet. Endeligt indgår et definitionsafsnit, som har til formål at definere mere komplicerede begreber anvendt i specialet.

3.1 Juridisk metode

Specialet tager udgangspunkt i den retspositivistiske tilgang. Denne retsteori omfatter hvad der er gældende ret på et givent område og hermed ikke det moralske aspekt. Det vil sige, at der i denne tilgang ikke er sammenhæng mellem rettens gyldighed og hvad der er godt eller dårligt på det pågældende område (Tvarnø & Nielsen, 2017, s. 333).

Retspositivismen stræber efter sikker viden og dermed sandheden inden for hvad der er gældende ret, hvilket blandt andet skabes ud fra empiriske undersøgelser af fakta, hvilket kommer til udtryk gennem specialet, hvor der søges efter en sandhed inden for gældende ret gennem det generelle og konkrete niveau (Tvarnø & Nielsen, 2017, s. 333).
I specialet vil det generelle fortolkningsniveau komme til udtryk gennem definitioner samt redegørelser af cyberkriminalitet og -sikkerhed, samt regulering og etik inden for revision af IT. Dette vil blive sammenfattet med COSO-, COBIT- samt revisionsrisikomodellen, med formål om at opnå et højere empirisk niveau i specialet.
Det konkrete niveau opstår ved, at gældende regulering og skik analyseres samt fortolkes i forhold til situationer der kan opstå med udgangspunkt i specialets problemstilling. Endvidere anvendes den retsdogmatiske metode, som omfatter en systematisering, fortolkning samt beskrivelse af standarderne for at undersøge gældende regulering. Fortolkningen inden for retsdogmatikken vil blive foretaget på et generelt og konkret niveau (Tvarnø & Nielsen, 2017, s. 29).
Projektets primære retskilder er ISA 315 og ISA 300, som understøttes af andre anvendte retskilder samt litteratur, herunder tidsskrifter, artikler mv. Dette følger retsdogmatikkens tanker om læren om normen, som i specialet omfatter hvordan den gældende regulering påvirker specialets problemstilling (Tvarnø & Nielsen, 2017, s. 29).

3.2 Deduktiv metode

Specialets metodiske fremgangsmåde er deduktiv. Dette skyldes, at der er taget udgangspunkt i en teori samt generelle antagelser, som forsøges testet gennem observationer (Arbnor & Bjerke, 2009, s. 93). I specialet opstilles en hypotese, om at gældende revisionsstandarder ikke er tilstrækkelige i henhold til den teknologiske udvikling. Hypotesen omfatter endvidere, at revisors udførelse af IT-revision samt inddragelse af IT-revision ligeledes ikke er tilstrækkelig, da udviklingen efter antagelsen, har medført et behov for øget revision inden for IT. Denne hypotese testes gennem analysen af de udvalgte teorier, samt specialets empiri, bestående af kvalitativt og kvantitativt data, samt lovgivning, artikler, standarder mv. Dette gøres med formål om efterfølgende at falsificere eller verificere hypotesen (Arbnor & Bjerke, 2009, s. 56).

3.3 Spørgeskema

Dette afsnit omfatter en kort beskrivelse af formålet med spørgeskemaundersøgelsen samt en beskrivelse af hvordan der er taget stilling til validiteten og reliabiliteten i spørgeskemaet.

Spørgeskemaet som er udarbejdet i programmet 'SurveyXact', har til formål at undersøge hvordan revision af IT samt IT- og cyberrisici håndteres blandt revisorerne. Derudover er formålet at undersøge om ISA-standarderne ifølge revisorerne har fulgt med udviklingen inden for anvendelsen af IT og om der er behov for en ændring af standarderne, samt flere tiltag i forbindelse med IT-revision.

3.3.1 Reliabilitet og validitet

For at sikre pålideligheden i spørgeskemaundersøgelsen, er der på forhånd fastlagt en strategi til indsamling af stikprøven (Darmer et al., 2010, s. 244). Denne omfatter, at der er udarbejdet et spørgeskema, hvor det er lagt vægt på formulering samt forståeligheden af spørgsmålene, med formål om at sikre at respondenterne forstår meningen med de enkelte spørgsmål, samt at der ikke opstår misforståelser under besvarelsen af skemaet. Der har ligeledes været fokus på en overskuelig opsætning i skemaet, for at undgå at respondenterne, finder spørgeskemaet uoverskueligt og dermed falder fra undervejs i besvarelsen.

Der er efterfølgende foretaget en udvælgelse af respondenter til undersøgelsen. Hertil er der søgt at skabe en stor stikprøve, for at underbygge generaliserbarheden i undersøgelsen. Derudover er der foretaget en geografisk udvælgelse, hvor der er udvalgt respondenter fra forskellige dele af landet, med formål om at få en bred forståelse.
Forinden ibrugtagen af spørgeskemaet er der foretaget test heraf, for undgå misforståelser samt fejlfortolkninger mv., denne test er foretaget ved at lade personer, som ikke arbejder inden for det specifikke fagområde, gennemlæse skemaet og give feedback på hvordan spørgsmålene opfattes af dem (Darmer et al., 2010, s. 244).

Reliabilitet kan være svær at opnå i en samfundsvidenskabelig undersøgelse. Dette skyldes at de ydre omstændigheder er under konstant udvikling, hvorfor den samme undersøgelse udført på et senere tidspunkt, højst sandsynligt ikke vil give samme resultat (Darmer et al., 2010, s. 245).

3.4 Interview

I specialet anvendes det semistrukturerede interview. Denne tilgang er valgt for at sikre for en dybere og mere fleksibel samtale, hvor der er mulighed for nye og opfølgende spørgsmål (Darmer et al., 2010, s. 220). Der er på forhånd udarbejdet en interviewguide, bestående af en række spørgsmål, som tager udgangspunkt i specialets problemstilling. Interviewguiden giver respondenterne muligheden for at danne sig en holdning til interviewets indhold, inden det foretages (Kvale og Brinkmann, 2015, s. 185). Dette kan styrke kvaliteten af besvarelsen, da respondenten kan opnå en indsigt, som ikke havde været mulig, såfremt guiden ikke var tilsendt forinden. Det kan ligeledes medføre, at respondenten som repræsenterer en virksomhed, kan have forberedt sig på at give politisk korrekte svar.
For sikre at interviewet lever op til det etiske ansvar, bliver respondenterne bedt om at tage stilling til, hvorvidt interviewet må optages, samt om de vil fremgå anonymt i specialet.

Interviewdataene anvendes til analyse af speciales centrale dele. Dette foretages gennem en deduktiv tilgang, hvor interviewet er opbygget efter specialets hypoteser, med det formål at verificere eller falsificere disse.

3.4.1 Respondenter til interviews

Respondenterne er udvalgt på baggrund af deres faglige ekspertise og viden inden for specialets problemstilling. Der er foretaget fire interviews af forskellige fagpersoner fra henholdsvis Danske Bank, Beierholm, Deloitte og Aalborg Universitet. Interviewene fremgår som lydfil i bilag, dog ikke interview af Dorthe Tolborg fra Danske Bank, da lydfilen grundet bankens IT-sikkerhedsforanstaltninger ikke kunne forlade bankens systemer, derfor fremgår interviewet som et referat i bilag.

IT-Chef i Danske Bank, Dorthe Tolborg

Dorthe Tolborg er uddannet revisor og har specialiseret sig i IT. Hun har tidligere arbejdet som IT-revisor hos KPMG, Deloitte og PwC. Endvidere har hun været revisionschef hos Codan. På nuværende tidspunkt har hun stillingen Chief Audit Executive samt medlem af Revisorrådet og eksamensudvalget, og civil censor ved mundtlig revisoreksamen.

IT-revisor og ekstern lektor, Hans Henrik Berthing

Hans Henrik Berthing er uddannet revisor med speciale i IT og har arbejdet som IT-revisor i Beierholm og Arthur Andersen. Han har endvidere arbejdet som IT-revisionschef hos Post Danmark. På nuværende tidspunkt har han sit eget revisionsfirma Verifica, som har speciale inden for IT-revision, risikostyring, compliance strategy samt governance. Derudover er han ekstern lektor på Aalborg Universitet, hvor han underviser i revision og har fagansvaret.

Director Risk Assurance hos PwC, Thomas Gi Scharf

Thomas Gi Scharf er uddannet revisor med speciale i IT. Han har tidligere være intern revisionschef i KMD. På nuværende tidspunkt er han Director Risk Assurance ved PwC.

Manager hos Deloitte, Mikkel Hede Olsen

Mikkel Hede Olsen er uddannet revisor, hvor han startede hos KPMG med fokus på revision af helt store virksomheder. Senere har han specialiseret sig i startup tech virksomheder og formue virksomheder. Derudover er han ved at uddanne sig som statsautoriseret revisor. På nuværende tidspunkt er han manager hos Deloitte, hvor han udfører revision af helt store virksomheder, men primært foretager rådgivning af tech virksomheder samt formue virksomheder.

3.4 Definitioner og begrebsafklaring

Dette afsnit har til formål at definere begreber, som anvendes i specialet.

Cybersikkerhed:

Cybersikkerhed dækker over IT-sikkerhed for netværksforbundne IT-systemer. Netværket kan være isoleret eller forbundet til andre netværk som for eksempel internettet (Center for cybersikkerhed (c), u.å., ¶ ordforklaringer).

IT-sikkerhed:

IT-sikkerhed dækker over informationssikkerhed for data, der behandles i IT-systemer. IT-systemer omfatter hardware og software og kan være både uafhængige eller forbundet med andre systemer i et netværk (Center for cybersikkerhed (c), u.å., ¶ ordforklaringer).

Kryptering:

Defineres som kodeteknikker, der får information til at fremstå uforståelig for tredjepart og på den måde kan hemmeligholdes. Kryptering bruges ofte til at sikre information, der skal sendes via ikke-sikre kommunikationskanaler som f.eks. internettet. Kryptering gør, at budskabet ikke kan blive læst og forstået af uvedkommende. Kryptering anvendes ligeledes af hackere, med formål om at utilgængeliggøre data for dataejeren, eksempelvis for at kræve en løsesum for at dekryptere data (Center for cybersikkerhed (c), u.å., ¶ ordforklaringer).

Revisor:

Anvendelsen af begrebet revisor i specialet dækker over finansielle revisorer. IT-revisorer omtales uden undtagelse som IT-revisor.

Risikoappetit:

Risikoappetit omfatter det samlede niveau for risiko, som en virksomhed er parat til at påtage sig, for at realisere virksomhedens overordnede mål (PwC, u.å., ¶ Risikostyring i en krisetid).

VPN-løsning:

VPN er et program eller en app, som kan anvendes til at forbinde til internettet. VPN gør det muligt at surfe mere sikkert og privat på internettet. Det omfatter, at internetfærden bliver

krypteret, således at internetudbyderen og hackere ikke kan følge med i hvad der foretages på internettet (It-borger, 2020, ¶ Hvad er en VPN og hvorfor gør det dig ekstra sikker på nettet?).

WPA og WPA2:

WPA står for Wi-Fi protected Access og sikrer det trådløse netværk ved at kryptere de data der overføres via netværket. WPA2 er en nyere sikkerhedskontrol, som er designet til at korrigere nogle af de sikkerhedshuller der er i den oprindelige WPA (Computerviden, u.å., ¶ Hvad er forskellen mellem WPA & WPA2).

4 Afgrænsning

Specialets fokusområde omfatter hvordan reguleringen inden for IT-revision kan være manglende, i forbindelse med revision et regnskab. Det antages at alle andre områder end IT af revisionen er fyldestgjort, således at specialets opmærksomhed primært vil være på de IT-relaterede bestanddele. Der er i den sammenhæng taget udgangspunkt i større virksomheder, samt online virksomheder og andre virksomheder, hvor omsætningen i større grad er omfattet af IT. Dermed er der afgrænset fra mindre virksomheder, hvor IT ikke spiller en stor rolle, samt virksomheder som ikke har ressourcer til IT-sikkerhed. Der er endvidere afgrænset fra at se på regler i henhold til IT- samt cybersikkerhed i PIE-virksomheder samt andre virksomheder, hvor der gælder særlige regler, herunder branche- og virksomhedsspecifikke regler. Dette skyldes, at der i specialet er et mere generelt perspektiv, for at afdække behovet i de virksomheder, hvor der ikke er særlige krav og regulering.

Ovenstående antagelse kommer særligt til udtryk hvor revisionsstandarderne samt anden relevant lovgivning beskrives. Visse generelle dele af den eksisterende regulering vil også omfatte IT-relaterede elementer. Her vil de områder med større betydning for specialets fokusområde beskrives med henblik på at fremhæve disses relevans til IT-området. Endvidere tager specialet udgangspunkt i dansk revision, hvorfor dansk lovgivning anvendes som den primære retskilde i sammenhæng med revisionsstandarderne. Dette betyder hovedsageligt, at specialet ikke direkte vil kunne overføres og anvendes i international henseende, uden potentielle ændringer.

Specialets håndtering af cyberkriminalitet er hovedsageligt virksomhedsorienteret. Dermed vil specialet ikke behandle alle typiske former for cyberkriminalitet, da flere af disse oftest er rettet

mod privatpersoner, hvilket ikke vurderes at være relevant i forhold til problemstillingen. Derimod søger specialet at beskrive det trusselsbillede som de fleste almene virksomheder står overfor i nutiden og fremadrettet.

På baggrund af specialets fokus på at IT skal indføres som en del af den generelle revision, er der afgrænset til en kort redegørelse af COBIT-modellen. Formålet med anvendelsen af modellen i specialet, er at underbygge teorien om, at der ikke er nok fokus på IT i revisors arbejde. Der er i denne sammenhæng ligeledes et afgrænset fokus på ISO-standarderne, som anvendes til fremhæve ISA 315's mere uspecifikke fokus på IT, og dertil bruges som led i forbedringsforslag

Kapitel 2

Cyberkriminalitet & Cyber- og informations-sikkerhed

Dette kapitel omfatter redegørelser af cyberkriminalitet og cyber- samt informationssikkerhed. Kapitlet har til formål at belyse behovet for cybersikkerhed i virksomheder.

5 Cyberkriminalitet

Dette afsnit omfatter en definition af begrebet samt en redegørelse af relevante og aktuelle typer af cyberkriminalitet. Endvidere har afsnittet til formål at klarlægge behovet for øget sikkerhed i virksomheder.

Cyberkriminalitet omfatter forbrydelser udført online, hvor gerningsmanden anvender særlig viden omkring cyberspace samt computerteknologi til at begå forbrydelsen (Holt og Bossler, 2016, s. 6). Udtrykket dækker over en lang række kriminelle aktiviteter, som imidlertid kan inddeles i tre kategorier, herunder 'Computerindholdsforbrydelser' og 'Computerintegritets-forbrydelser' (Det kriminalpræventive råd, 2018, s. 3).

Computerassisterede forbrydelser er forbrydelser med et økonomisk formål og omfatter blandt andet handlinger som identitetstyveri, betalingsmisbrug, nethandelsmisbrug mv., hvor de kriminelle ofte anvender metoder som phishing for at opnå dette.
Computerintegritetsforbrydelser omfatter forbrydelser som anvendes til at angribe IT-systemer gennem ddos-angreb, malware, ransomware mv. Denne type forbrydelse kategoriseres som cyberangreb og er ofte rettet mod virksomheder eller myndigheder og har typisk økonomiske eller politiske formål (Det kriminalpræventive råd, 2018, s. 3).

5.1 Cyberangreb

Cybertruslen mod Danmark anses som værende alvorlig, da denne især har økonomiske eller politiske konsekvenser. Truslen fra cyberangreb er generelt vurderet til at være meget høj, herunder er der en stigende trussel fra målrettede ransomware-angreb mod danske myndigheder og virksomheder (Center for cybersikkerhed (d), 2020, s. 3).

Cyberangreb anvendes af forskellige aktører og har dermed forskellige formål. Nedenstående afsnit har til formål, at redegøre for forskellige cyberangreb som især er aktuelle for virksomheder og som kan have store konsekvenser for de berørte.

5.1.1 Phishing

Ved et phishing-angreb forsøger hackerne at manipulere en person til at videregive personlige oplysninger. Dette gøres ved, at hackerne sender e-mails, SMS'er eller lignende med links, som i tilfælde hvor ofrene klikker på linket, enten downloader malware eller ofret bliver ledt til en falsk hjemmeside, med det formål at forsøge at franarre personlige oplysninger. Phishing-angreb kan have til formål at ramme mange tilfældige eller målrettet enkeltpersoner eller organisationer.

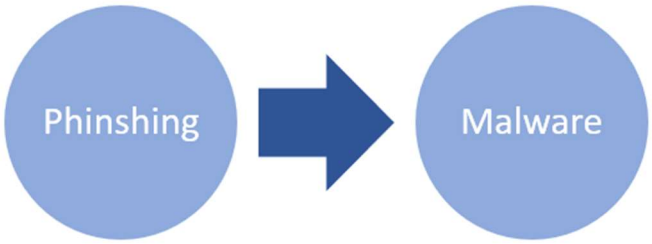
De mest almindelige phishing-forsøg bliver ofte fanget af IT-systemer eller medarbejdere, men de mere avancerede phishing-angreb er mere komplicerede at opdage. Dette skyldes, at hackerne har målrettet e-mailen således, at virksomheden eller medarbejderen manipuleres til at tro, at afsenderen er en af ofrets egne kontakter. Dette gøres eksempelvis gennem "e-mail thread hijacking", hvor hackerne udsender en mail i en igangværende tråd mellem offeret og en kontakt (Center for cybersikkerhed (d), 2020, s. 7). Selskabet Danish Agro oplevede i april 2020 et cyberangreb, som startede med en e-mail thread hijacking. Dette skete ved, at hackerne overtog leverandørernes IT-system og sendte en phishing-mail fra leverandøren i en igangværende mailkorrespondance og på den måde fik adgang til, at installere hackersoftware i selskabets system.

5.1.2 Social Engineering

Social Engineering er en teknik hvor hackere anvender psykologiske metoder, for at få offeret til i god tro at udføre en handling, som vedkommende ellers ikke ville have gjort. Dette kan eksempelvis være, hvor vedkommende afgiver loginoplysninger eller videregiver informationer om organisationen, som kan have konsekvenser (Center for cybersikkerhed (c), u.å., ¶ Ordforklaring). Denne teknik anvendes blandt andet gennem phishing.

5.1.3 Malware

Malware er ondsindede program koder og dækker over en række software som foretager skadelige og andre uønskede handlinger på offerets computer, eksempelvis ved brug af virus, ransomware mv. (Det kriminalpræventive råd, 2018, s. 16).



Figur 1 - Illustration af malware - Kilde: Egen tilvirkning

Som figur 1 illustrerer, kan malware fremkomme gennem phishing, hvor et offer åbner et link eller en vedhæftet fil i en mail og på den måde giver hackere mulighed for at overvåge computeren og dermed få adgang til personlige og økonomiske oplysninger (Det kriminalpræventive råd, 2018, s. 6).

5.1.4 Ransomware

Ransomware er en metode cyberkriminelle anvender for at opnå en typisk økonomisk løsesum, ofte i form af Kryptovaluta. Dette kan ske ved brug af en virus, som krypterer filer, så det ikke er muligt at få adgang til indholdet på computeren. Efter krypteringen udsendes en meddeles omkring løsesummens størrelse samt tidsfristen for betalingen (Det kriminalpræventive råd, u.å., ¶ Ransomware). Phishing er en metode, som hackerne eksempelvis anvender for at få adgang til systemer, hvorigennem malware bliver downloadet og i nogle sammenhænge udvikler sig til ransomware, som er en form for malware.

Figur 2 - Illustration af ransomware - Kilde: Egen tilvirkning

Tidligere var ransomware-angreb udviklet til at ramme så mange virksomheder som muligt, med det formål at opnå en mindre løsesum. Disse angreb foregår ofte via større phishing-angreb, som krypterer de pågældende maskiner direkte ved levering. I de seneste par år, er der sket en udvikling i ransomware-angrebene, hvor hackerne målretter angrebene mere mod de

enkelte virksomheder, hvor det er muligt for hackerne at opnå en større løsesum. Denne form kan have alvorlige konsekvenser for samfundsvigtige funktioner, hvis følsomme oplysninger lækkes i forbindelse med et angreb, samt alvorlige konsekvenser for virksomhedens fortsatte drift (Center for cybersikkerhed (g), 2020, s. 5).

5.1.5 DDos-angreb

DDos står for Distributed Denial of Service og er en betegnelse der anvendes om en metode som overbelaster hjemmesider. Dette gøres ved, at en hacker kontrollerer en masse computere og får dem alle til at tilgå samme hjemmeside på samme tid og konstant, således at hjemmesiden overbelastes og andre ikke kan få adgang til siden (Det kriminalpræventive råd, 2018, s. 15).
DDos-angreb kan være relativt simple at udføre og kræver ofte ikke meget planlægning eller teknisk viden. Dermed er denne trussel høj, da der ikke kræves meget af hackerne at foretage et sådant angreb (Center for cybersikkerhed (a), 2020, s. 23).

6 Cyber- og informationssikkerhed

På baggrund af udviklingen inden for cyberangreb, hvor et stigende antal virksomheder bliver udsat for dette, er det særligt relevant at sikre, at cybersikkerheden er tilstrækkelig og under konstant udvikling. Nedenstående afsnit har til formål at redegøre for tiltag, som kan reducere risikoen for cyberangreb mod virksomheder. På nuværende tidspunkt er nedenstående krav ikke gældende for andre virksomheder end PIE-virksomheder, men kravene kan anvendes til at påpege hvilke områder, som kan være relevante at indføre sikkerhedsforanstaltninger på i relation til IT- og cybersikkerhed generelt i virksomheder.

6.1 National strategi for cyber- og informationssikkerhed

I forbindelse med den stigende tendens til cyberangreb mod virksomheder samt myndigheder er informations- og cybersikkerhed blevet mere aktuelt. Informationssikkerhed er en betegnelse for de samlede foranstaltninger, der anvendes til at sikre informationer i forhold til fortrolighed, integritet og tilgængelighed. Cybersikkerhed omfatter beskyttelse mod sikkerhedsbrud, hvilket kan opstå som følge af angreb mod data eller systemer (Finansministeriet, 2018, s. 7).

Regeringen har indført tiltag i form af en national strategi for cyber- og informationssikkerhed. Denne strategi har til formål at sikre. at borgere, virksomheder og myndigheder er rustet til at modstå cyberangreb og dermed reducere risikoen for sikkerhedsbrud, som kan have alvorlige konsekvenser for samfundet (Finansministeriet, 2018, s. 10). Den nationale strategi for cyber- og informationssikkerhed fra 2015-2016 indeholdt en implementering af den internationale sikkerhedsstandard ISO27001 samt krav om et systematisk og professionelt tilsyn med informationssikkerheden i staten (Finansministeriet, 2018, s. 11).

I den nationale strategi for cyber- og informationssikkerhed for 2018-2021 er der blandt andet blevet indført tekniske minimumskrav for statslige myndigheder, som omfatter en række krav, der er specificeret i henhold til forskellige områder af myndighedernes IT-anvendelse, herunder klienter/PC, mail, mobiltelefoner, netværk og websider (Sikkerdigital, u.å., ¶ Tekniske minimumskrav for statslige myndigheder).
Disse krav omfatter blandt andet, at der skal implementeres firewall på alle klienter, hvilket skal være med til at mindske chancen for malware-spredning. Der skal benyttes en VPN-løsning for at tilgå internettet via en arbejdscomputer fra eksterne netværk. For at undgå kompromittering af data i forbindelse med tab eller tyveri af computere, skal der foretages en kryptering af harddiske. Anvendelse af mail-relays må kun foregå med autentifikation. Dette øger sikkerheden og dermed reduceres risikoen for misbrug af mail-server til spredning af malware og spam. Myndighedernes arbejdsnetværk skal være krypteret med minimum WPA2, som er mere sikkert end WPA (Sikkerdigital, 2019, s. 1-2).

Kravene som stilles til myndighederne, har til formål at mindske risikoen for cyberangreb samt kompromittering af data, som kan have samfundsmæssige konsekvenser. Kravene er minimumskrav og dermed skal myndighederne samtidig foretage egne risikovurderinger og implementere yderligere sikkerhedstiltag tilpasset den enkelte myndighed (Sikkerdigital, u.å., ¶ Tekniske minimumskrav for statslige myndigheder).

6.2 Cyber- og informationssikkerhed i virksomheder

Som udgangspunkt er der ingen generel regulering til cyber- og informationssikkerhed i virksomheder, dog med undtagelse af databeskyttelsesloven, som stiller nogle krav til håndteringen af personlige data, jf. databeskyttelsesloven. Virksomheder der har særlig

samfundsvigtig karakter, kan dog efter anmodning, blive tilsluttet netsikkerhedstjenesten hos Center for cybersikkerhed, jf. CFCS § 3, stk. 3. Endvidere kan Center for cybersikkerhed stille et påbud til virksomheder af særlig samfundsvigtig karakter, om at blive tilsluttet netsikkerhedstjenesten, med henblik på montering af netværkskommunikation, jf. CFCS § 3, stk. 4.

Der er dog en række anbefalinger til virksomheder det formål at mindske risikoen for cyberangreb. CFC anbefaler blandt andet, at virksomheder har styr på den basale IT-sikkerhed i henhold til opdatering af systemer og applikationer, segmentering af det interne netværk, antivirus, brugerkonti- og adgang samt login. Derudover bør virksomheder sikre fjernadgang med fler-faktor autentifikation og kryptering, mv. (Center for cybersikkerhed (g), 2020, s. 4). Et andet tiltag som kan reducere risikoen for cyberangreb, er at uddanne medarbejdere således, at de i mange tilfælde kan identificere forsøg på cyberangreb, før det udvikler sig. Dette kan gøres ved at informere medarbejdere om, hvad phishing-mails er, samt hvordan det kan skade virksomheden eller myndigheden, herunder hvordan en mistænkelig mail kan identificeres og håndteres. Derudover er det vigtigt, at medarbejderne er bevidste om, hvordan download af software, usb-sticks eller lignende skal håndteres, for at undgå at der downloades malware eller ransomware mv. Endeligt bør det fremgå, hvor medarbejderne skal henvende sig, i tilfælde hvor en medarbejder har åbnet et link eller tilgået en mistænkelig hjemmeside. Det er endvidere vigtigt, at medarbejderne især er opmærksomme på e-mail thread hijacking og social engineering, hvor det kan være svært at opfange mistænkeligheder (Center for cybersikkerhed (g), 2020, s. 8-9).

Den nationale strategi for cyber- og informationssikkerhed for 2018-2021 omfatter nationale tiltag, som har til formål at sikre, at virksomheder er rustet mod cyberangreb. Hertil gælder, at der opsættes en national sikkerhedsmyndighed, som skal samarbejde med relevante myndigheder samt virksomheder, for at reducere risikoen for cyberangreb (Finansministeriet, 2018, s. 14).

Kapitel 3

God IT-skik, regulering og begrebsrammer

Dette kapitel indeholder redegørelser af god IT-skik, IT-elementer i ISA-standarderne samt udvalgte begrebsrammer. Formålet med kapitlet er at skabe et overblik og disse retningslinjer som de finansielle revisorer kan anvende under revision af IT.

7 God IT-skik

Følgende afsnit fremhæver en række anbefalinger til hvordan virksomheder kan håndtere og integrere IT som en central del af virksomhedens processer. Derudover belyses kravene som stilles til revisors ageren i henhold til godskiksreglerne, herunder revisorloven § 16. Endeligt er formålet med afsnittet at skabe forståelse for, hvilke IT-relaterede områder revisor bør være opmærksom på under en revision.

7.1 Etik og god skik, revisor og IT

Når revision og andre erklæringsopgaver udføres af revisor, er der en række krav til hvordan revisor forventes at agere. Det forventes at revisor handler etisk og i overensstemmelse med nogle specifikke krav, der tilsammen udgør reglerne for god revisorskik (Bøg & Kiertzner, 2007, s. 13-14). International Federation of Accountants (IFAC) har formuleret fem etiske principper, der fungerer som retningslinjer i revisors hverdag, og samtidig indgår integreret i lovgivningen. De fem principper omfatter integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed samt professionel adfærd (Bøg & Kiertzner, 2007, s. 20-23). Principperne kan findes i revisorlovens § 16, stk. 1:

Revisor er offentlighedens tillidsrepræsentant under udførelse af opgaver efter § 1, stk. 2. Revisor skal udføre opgaverne i overensstemmelse med god revisorskik, herunder udvise den nøjagtighed og hurtighed, som opgavernes beskaffenhed tillader. God revisorskik indebærer desuden, at revisor skal udvise professionel skepsis, integritet, objektivitet, fortrolighed, professionel adfærd, professionel kompetence og fornøden omhu ved udførelsen af opgaverne.

Kravene der stilles til revisor bør anses i sammenhæng med Selskabsloven § 361, stk. 1 og 2, eftersom at revisor kan blive erstatningspligt ved uagtsom ageren. Uddybende følger ansvarsgrundlaget den almindelige culparegel, hvormed erstatningspligten kan blive gældende ved simpel uagtsomhed. I forlængelse heraf vil et erstatningsansvar omfatte de påregnelige skader, som har direkte sammenhæng med illegale handlinger og undladelser foretaget af revisor (Karnov, SLL § 361. note 1640).

De ovenstående principper og krav der stilles til revisor kan siges at være af generel karakter, og dermed være gældende i alle områder af revisors arbejde. På baggrund af problemstillingen i dette speciale vil de generelle etiske og godskiksregler ikke uddybes yderligere, da disse

antages at blive efterlevet af revisor. Derimod vil der fokuseres på revisors rolle og ansvar i forhold til IT samt virksomheders anvendelse heraf.

7.2.1 Hvorfor god IT-skik?

Det er virksomheden og ledelsen heraf, der har ansvaret for opretholdelsen af god IT-skik (Mogensen et al., 2011, s. 5-6). Anvendelsen af IT varierer mellem de enkelte virksomheder, og kan have stor sammenhæng med virksomhedens succes. Den stigende vigtighed af IT betyder, at ledelsen i større grad bør have en forståelse af, hvordan IT påvirker virksomheden samt hvilke risici og muligheder den medfører. Derfor er der lavet en række anbefalinger til god IT-skik i et samarbejde mellem FSR, ISACA, Foreningen af Interne Revisorer og Dansk IT (Mogensen et al. 2011).

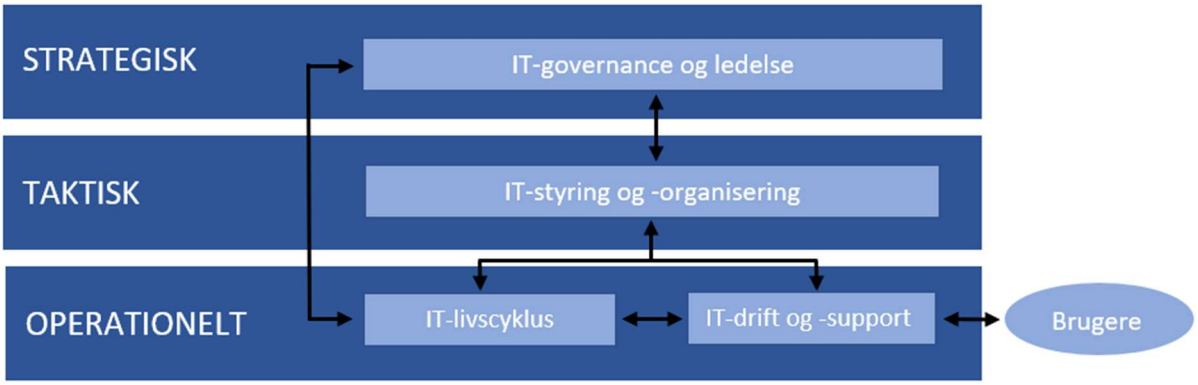
Det forventes at revisor, som led i at forstå virksomheden, jf. ISA 315, under en revision kan drage nytte af disse anbefalinger ved den IT-relaterede risikovurdering. Gennem en forståelse af kravene til god IT-skik bør revisor således være bedre stillet ved vurdering af en virksomheds IT og de dertilhørende risici.

7.2.2 Ledelsens ansvar

God IT-skik omfatter først og fremmest et kendskab til mulighederne ved IT, hvordan virksomheden er afhængig af IT, hvilke risici der er forbundet med IT-anvendelse og ansvar ved brug af IT-ressourcer. Dette indebærer at udvikling og implementering af IT forekommer med virksomhedens strategi som målsætning. Hertil bør beslutningsprocesser foregå systematisk med inddragelse af de relevante parter. Endvidere bør der være en klar rollefordeling af ansvar og opgaver i forbindelse med anvendelsen af IT. Dette skal i sammenhæng med uddannelse af medarbejderne sikre, en balance mellem opgaver, råderum samt kontrol. (Mogensen et al., 2011, s. 5).

Ledelsens primære ansvar i forbindelse med god IT-skik er at skabe sammenhæng mellem virksomhedens forretning og IT-afdeling. Ifølge anbefalingerne bør IT-processor inddeles i fire

følgende områder, hvortil ledelsen skaber rammerne i form af langsigtede strategier og mål (Mogensen et al., 2011, s. 6-7):



Figur 3 - Illustration af opdeling af virksomhedens IT-processer - Kilde: Mogensen et al., 2011

IT-governance og ledelse omhandler de øverste ledelsesprocesser, der udformer virksomhedens overordnede strategi, hvilket er styrende i forhold til målretningen af de øvrige IT-processer. IT-styring og -organisering omhandler styringen af virksomhedens IT-ressourcer. IT-livscyklus indebærer anskaffelse, implementering, udfasning mv. af virksomhedens IT-systemer. Endeligt omhandler IT-drift og -support, at anvendelsen af IT-systemerne foregår i overensstemmelse med de fastsatte rammer (Mogensen et al., 2011, s. 7).

Når den øverste ledelse fastlægger IT-strategien, bør den underbygges af aktiviteter og rammer på det taktiske- og operationelle ledelsesniveau. Dette gøres for at sikre en reel implementering af IT-strategien i virksomheden. På det strategiske niveau behandles blandt;

- Visioner og pejlemærker
- Styring, organisering og politikker
- Kompetencer
- Risikostyring og informationssikkerhed
- Økonomi

På det taktiske niveau operationaliseres IT-strategien gennem konkrete politikker, der skal bidrage til skabelsen af en kultur, som opfylder strategien bedst muligt. Yderligere bør handlingsplaner udarbejdes, således medarbejdere kan prioritere opgaver. Ved det operationelle niveau defineres processer, procedurer, instrukser og manualer, hvilket bør klargøre samt effektivisere de daglige rutiner (Mogensen et al., 2011, s. 32).

Det anbefales at virksomheden internt kan; ”dokumentere hvordan opgaver på tværs af ansvarsområder håndteres, og det bør være klart, hvem der er ansvarlig for de enkelte dele i processen” (Mogensen et al. 2011, s. 7). I forlængelse heraf kan ledelsen anvende forskellige modeller, som eksempelvis COSO eller COBIT, til systematisering af ovenstående.

7.2.3 IT-risikovurdering og -informationssikkerhedspolitik

Området der forventes at have størst relevans for revisor, er virksomhedens IT-risikovurdering samt -informationssikkerhedspolitik. I modsætning til revisors risikovurdering, som primært fokuserer på regnskabsrelaterede risici, bør virksomheden analysere samtlige IT-relaterede risici ved de forskellige forretningsmæssige processer. Dette gælder både interne samt eksterne begivenheder, der kan påvirke virksomhedens strategi (Mogensen et al., 2011, s. 33).

En effektiv risikovurderingsproces bør være organisatorisk forankret, hvortil der udpeges en ansvarlig for processen. Denne proces bør være koordineret med virksomhedens øvrige risikovurderingsprocesser, og bør gentages løbende i forbindelse med ændringer af trusselsbilledet. Identificerede risici anbefales at vurderes i overensstemmelse med en godkendt model, hvilket tilknyttes en passende mitigeringsplan. Disse risici er ofte inden for følgende kategorier:

- Menneskelige fejl og manglende efterlevelse af procedurer
- Systemfejl
- Driftsproblemer
- Personafhængighed
- Uautoriserede eller kriminelle interne aktiviteter
- Eksterne angreb
- Uforudsete konsekvenser af ændringer

Som det tidligere er beskrevet, udgør phishing, malware, ransomware og DDoS-angreb eksempler på trusler virksomheder typisk kan blive udsat for. Derfor anbefales informationssikkerhedspolitik at indgå, som en integreret bestanddel af forretningsprocesserne, anvendelsen af teknologi samt den generelle kultur blandt medarbejderne. Formålet er at sikre at medarbejdernes ageren stemmer overens med virksomhedens vurderede informationssikkerhedsniveau. Denne sikkerhedspolitik bør anses i sammenhæng med de udførte risikovurderingsprocesser, således de mest væsentlige risici afdækkes. Endeligt bør

informationssikkerhedspolitikken ligeledes klargøre de helt basale sikkerhedsregler og -foranstaltninger. Ligesom risikovurderingen, bør sikkerhedspolitikken ajourføres ved en frekvens der er hensigtsmæssig i forhold til trusselsbilledet.

8 Standarder

Nedenstående afsnit redegør for revisionsstandarder, som omfatter IT-området under en revision. Eftersom IT indgår integreret i standarderne, fokuserer afsnittet udelukkende på de punkter, som er særlig relevante for revisionen af IT, hvorfor større bestanddele af standarderne ikke inddrages.

8.1 ISA 315

I forbindelse med IT-revision udgør ISA 315 en helt central del af den gældende regulering. IT-revision indgår som et integreret element i ISA 315, hvorfor følgende afsnit vil fremhæve punkter i standarden, der er relevante for revisionen af IT. Dermed er afsnittet ikke udtømmende, hvortil det antages, at de generelle forhold i standarden opfyldes af revisoren.

Ligesom ved den generelle revision er målsætningen for IT-revision, i henhold til ISA 315, at revisor skal identificere og vurdere risici for fejlinformation på regnskabs- og revisionsmålsniveau, som opstår i sammenhæng med IT. Dette gøres gennem forståelse af virksomheden og dens omgivelser, herunder med særligt fokus på anvendelsen af IT baserede procedurer og systemer.

Et væsentligt element i forståelsen af virksomheden og dens omgivelser, indebærer en forståelse af de interne kontroller. Det er udelukkende de kontroller der er relevante for revisionen, som revisor skal opnå indsigt i. Dermed er det ikke alle kontroller der er relevante, uafhængigt af om de er relateret til regnskabsaflæggelsen, jf. ISA 315, 12.

I afsnit A63 beskrives generelle fordele der medfølger brugen af IT, som en del af virksomhedens interne kontrol. Eksempler på disse er:

- Konsistent brug af foruddefinerede forretningsmæssige regler samt behandling af store mængder transaktioner og data
- Forbedre rettighederne, tilgængeligheden og nøjagtigheden af information

- Muliggør yderligere analyse af informationer.
- Bedre mulighed for overvågning af virksomhedens aktiviteter, samt formindske risikoen for omgåelse af de interne kontroller.
- Større mulighed for effektiv funktionsadskillelse ved indførelse af sikkerhedskontroller.

Omvendt indebærer anvendelsen af IT også specifikke risici, hvilket benævnes i afsnit A64. Disse er eksempelvis:

- Tillid til systemer eller programmer, som behandler data unøjagtigt, behandler unøjagtige data eller begge dele.
- Uautoriseret adgang til data, som kan medføre ødelæggelse eller ugyldige ændringer af data. Dette kan have konsekvenser for bogføringen, og er særligt gældende i tilfælde hvor mange har adgang til en fælles database.
- Sandsynlighed for at IT-medarbejder får adgangsrettigheder, som overgår det der er nødvendigt, for at medarbejderen kan udføre sin funktion. Dette nedbryder funktionsadskillelsen.
- Uautoriseret ændring af data i stamfiler, systemer eller programmer. Endvidere upassende manuel indgriben.

Udover selve de interne kontroller skal revisor opnå en forståelse af virksomhedens kontrolmiljø, jf. ISA 315, 14. Selvom dette krav ikke er direkte relateret til IT eller giver vejledning heromkring, vurderes det at have en afgørende betydning for forståelsen af virksomhedens IT-baserede kontroller. Det uddybes i A77, at; ”kontrolmiljøet omfatter ledelsesfunktionerne og den daglige ledelses og den øverste ledelses holdninger, opmærksomhed og tiltag vedrørende virksomhedernes interne kontrol og dens betydning i virksomheden. […]” (ISA 315, A77). Elementer i kontrolmiljøet beskrives under A78, hvor nedenstående indgår:

- Kommunikation og håndhævelse af integritet og etiske værdier
- Forpligtelse til kompetence
- Den øverste ledelses deltagelse
- Den daglige ledelses holdninger og ledelsesstil
- Organisationsstruktur
- Tildeling af beføjelser og ansvar

- Personale og praksis

Af ovenstående punkter vurderes forpligtelse til kompetence, daglige ledelses holdninger og tildeling af ansvar, som de mest betydningsfulde for forståelsen af kontrolmiljøet i forhold til IT. Der kan argumenters for at særlige kompetencer er påkrævet, for at kunne forstå samt bearbejde de risici, der medfølger ved anvendelsen af IT. Ligeledes kan den daglige ledelses holdning, til hvorvidt IT har en betydning for virksomheden påvirke i hvor høj grad de IT relaterede procedurer efterleves. Endeligt sikrer en hensigtsmæssig fordeling af ansvar, at dataene i IT-systemerne ikke tilgås af uautoriserede medarbejdere, og er dermed med til at bevare dataenes integritet samt nøjagtighed.

Afsnit 21, omhandlende kontrolaktiviteter der er relevante for revisionen, påpeger særskilt at revisor skal opnå forståelse af, hvordan virksomheden har reageret på IT-relaterede risici. Disse risici uddybes i A107-109, hvortil kontrollerne generelt indføres som modsvar på risiciene nævnt i afsnit A64. Overordnet anses kontroller over IT-systemer som effektive, når de opretholder informationernes integritet og sikkerheden af data, som systemet behandler, jf. ISA 315, A107. I forlængelse heraf kan de IT relaterede kontroller inddeles i IT-kontroller og applikationskontroller.

De generelle IT-kontroller omfatter politikker og procedurer, som vedrører mange applikationer og understøtter, at applikationskontroller fungerer effektivt, jf. ISA 315, A108. Dette gøres ved, at sikre kontinuerlig og sikker drift af informationssystemer.

Eksempler på generelle IT-kontroller omfatter blandt andet:

- Drift af datacentre og netværk.
- Programændring og adgangssikkerhed.
- Anskaffelse, udvikling og vedligeholdelse af systemsoftware og applikationssystemer.

Det beskrives i ISA 315, A108, at disse kontroller typisk indføres som modsvar til de ovenstående nævnte risici i henhold til afsnit A64.

Endelig er der applikationskontroller, der beskrives i A109. Disse er manuelle eller automatiserede procedurer, som anvendes til at behandle transaktioner i individuelle applikationer, og anvendes typisk i de øvrige interne kontroller. Hovedformålet med applikationskontrollerne er, at sikre pålideligheden af bogføringen, hvilket gøres ved at sikre

at transaktioner reelt har fundet sted, er godkendte samt nøjagtigt registreret og behandlet. Dermed hænger applikationskontroller tæt sammen med virksomhedens konkrete finansielle data. Følgende er eksempler på applikationskontroller (RevisionsMemo - IT-revision, u.å.):

- Kontrol af matematisk nøjagtighed af beregninger.
- Vedligeholdelse og gennemgang af balanceposter og råbalancer.
- Manuel opfølgning af afvigelsesrapporter.

8.1.1 ISA 315 Bilag 1 – Interne kontrolelementer

I forlængelse af de IT-relaterede elementer i ISA 315, vil enkelte særligt relevante punkter i bilag 1 ligeledes belyses. Bilaget omhandler uddybende forklaringer af de interne kontrolelementer, som løbende er beskrevet igennem ISA 315.

Størstedelen af punkterne beskrevet i bilaget, kan relateres til en virksomheds IT-baserede kontroller, dog vurderes det, at nogle områder har større betydning for IT-kontroller end andre, hvorfor disse fremhæves. Under virksomhedens risikovurderingsproces beskrives eksempler på risici relevante for regnskabsaflæggelsen. Hertil kan punkterne nye medarbejdere, nye eller opdaterede informationssystemer, hurtig vækst samt ny teknologi have ekstraordinær indflydelse på en virksomheds IT-kontroller. Fælles for disse risici er først og fremmest, at de ved deres forekomst sandsynligvis kræver en grad af kompetenceudvikling i virksomheden. For det andet antages ovenstående omstændigheder, med undtagelse af nye medarbejdere, væsentligt at kunne ændre en virksomheds regnskabsaflæggelsesproces. Endvidere kan der ved udviklingen af nye teknologier med sandsynlighed opstå fejl samt IT-relaterede mangler, som kan gøre en virksomhed sårbar over for cyberangreb m.v.

Afslutningsvist defineres et informationssystem i bilaget i følgende citat: ”Et informationssystem består af infrastruktur (fysisk infrastruktur og hardwarekomponenter), software, mennesker, procedurer og data. Mange informationssystemer anvender informationsteknologi (IT) i udbredt grad.” (ISA 315 Bilag 1, 5.) Tilsvarende beskrevet i tidligere afsnit, er et informationssystem overordnet set relevant for regnskabsaflæggelsen når det sikrer eksistensen samt korrektheden af transaktioner og finansielle data, jf. ISA 315, Bilag 1, 5.

8.2 ISA 330 – Revisors reaktion på vurderede risici

I forlængelse af ISA 315, udgør ISA 330 endvidere en central del af reguleringen i forhold til IT-revision. Ligesom foregående afsnit tages der udgangspunkt i, at øvrige dele af standarden er opfyldt af revisor, hvorfor kun de IT-relaterede elementer behandles.

Når revisor reagerer på vurderede risici, jf. ISA 330, kan der skelnes mellem IT-baserede risici og løsningsmuligheder. Uddybende kan der ved en virksomheds anvendelse af IT opstå forskellige risici, men samtidig kan IT også være behjælpelig i udformningen af revisionshandlinger. Risiciene forbundet med IT er beskrevet i de forrige afsnit, og er særligt relevant for revisors vurdering af om revisionsbevis fra tidligere revisioner passende kan benyttes, jf. ISA 330, 13. Endnu en udfordring kan opstå i de tilfælde, hvor en virksomhed udelukkende dokumenterer og opbevarer transaktioner i et IT-system, hvilket kan forhindre effektive substanshandlinger og dertil nødvendiggøre test af kontroller, jf. ISA 330, A24.

Vurderer revisor, at der er væsentlig risiko for fejlinformation på revisionsmålsniveau, skal yderligere revisionshandlinger relateret til årsagen bag den specifikke risiko udføres, jf. ISA 330, 6-8. Omfanget af den ekstraordinære revisionshandling fastlægges efter væsentligheden, den vurderede risiko samt graden af sikkerhed planlagt, jf. ISA 330, A15. I forlængelse heraf påpeges der i afsnit A16, hvordan IT-baserede revisionsteknikker gør det muligt for revisor effektivt at lave tests af en hel population frem for stikprøver. Tilsvarende kan ensartetheden ved IT-databehandling reducere nødvendigheden af applikationskontroller, så længe disse er programmerede, jf. ISA 330, A29. En programmeret kontrol antages kontinuerligt at virke ensartet, så længe der ikke er foretaget ændringer i programmet eller de data programmet anvender. Dermed kan revisor, når først applikationen vurderes til at virke hensigtsmæssigt, nøjes med at teste hvorvidt (ISA 330, A29):

- Der ikke er foretaget ændringer af applikationen, uden at disse ændringer er blevet kontrolleret.
- At den godkendte udgave af applikationen benyttes til behandlingen af transaktioner.
- At andre relevante generelle kontroller er effektive.

Det påkræves ved test af kontroller, at revisor fastslår, hvorvidt de undersøgte kontroller er afhængige af indirekte kontrollerer, og dokumenterer funktionaliteten af de indirekte kontroller, jf. ISA 330, 10. Dette er væsentligt for IT-revision, da generelle IT-kontroller typisk

er en afgørende indirekte kontrol ved brugen af applikationskontroller, jf. ISA 330, A30. I forlængelse heraf kan revisionsbevis for implementeringen af en programmeret applikationskontrol, som følge af ensartetheden ved IT-databehandling, endvidere give bevis for kontrollens effektivitet, når denne ses i sammenhæng med funktionaliteten af en virksomheds generelle kontroller (ISA 330, A31).

8.3 ISAE 3402

ISAE 3402 er en standard omfattende en ekstraordinær erklæring der anvendes vedrørende kontroller, som leveres af en outsourcing leverandør, til en brugervirksomhed. Erklæringen udføres af revisor ved enten leverandøren af kontrollerne eller dennes kunder. Ydelsen der erklæres omkring, skal være relevant for den pågældende brugervirksomheds interne kontroller med forbindelse til regnskabsaflæggelsen. Dermed er erklæringen begrænset i forhold til brugervirksomhedens overordnede IT-sikkerhed og de dertilhørende risici (Mogensen et al., 2018; RevisionsMemo - ISAE 3402, u.å.).

Erklæringer efter ISAE 3402 afgives enten som type 1- eller type 2-erklæring. Type 1 erklæringen omfatter en beskrivelse af udformningen samt implementeringen af serviceleverandørens interne kontroller. Uddybende kræves en skriftlig udtalelse fra serviceleverandøren om at systembeskrivelsen er retvisende, og udformet samt implementeret den anførte dato. Yderligere skal udtalelsen bekræfte at kontrollerne, knyttet til de beskrevne kontrolmål, er hensigtsmæssigt udformet. Endeligt indebærer type 1-erklæringen en erklæring af serviceleverandørens revisor, der giver en høj grad af sikkerhed angående de ovenstående forhold. Type 2-erklæringen omfatter det samme som type 1-erklæringen, med tilføjelse af at de beskrevne kontroller har fungeret effektivt i den anførte periode. Endvidere en beskrivelse af de udførte test af kontroller og resultaterne heraf (RevisionsMemo – ISAE 3402, u.å.).

Type 1-erklæringen anvendes typisk ved erklæringsopgaver før implementeringen, ved den indledende vurdering af kontroller. Omvendt anvendes type 2-erklæringen normalt i forbindelse med erklæringsopgaver omhandlende i forvejen implementerede kontroller, hvor revisor kan foretage test af disse (RevisionsMemo – ISAE 3402, u.å.). Modtagerne af en ISAE 3402 erklæring er normalvis den øverste ledelse, den operationelle ledelse og revisoren hos brugervirksomheden. Den øverste ledelse i brugervirksomheden kan overordnet bekræfte hvorvidt aftalen med serviceleverandøren overholdes på de områder, som inddrages i

erklæringen. Den operationelle ledelse kan få en forståelse for, hvorledes services og systemer leveres samt sikkerhedsniveauet heraf. Endeligt kan revisor hos brugervirksomheden få kendskab til risici tilknyttet regnskabsaflæggelsen på baggrund af de leverede services og systemer (Mogensen et al., 2018).

8.4 Kommunikation med ledelsen

De følgende afsnit redegør for revisionsstandarderne omhandlende revisors kommunikation med den daglige- og øverste ledelse. De generelle krav til revisor behandles i begrænset omfang, hvorimod der hovedsageligt fokuseres på kommunikation i relation til IT-anvendelse, -kontroller og -risici. Formålet med afsnittet er at skabe en forståelse for, hvordan revisor skal reagere yderligere på identificerede IT-risici.

8.4.1 ISA 260

Med udgangspunkt i ISA 260 påkræves revisor at kommunikere med den øverste ledelse for at skabe overblik over den planlagte revisions omfang. Dette gøres ligeledes med henblik på at sikre en effektiv tovejskommunikation, hvor revisor lettere kan indhente relevant information samt opnå en bedre forståelse af virksomheden. Yderligere skal revisor videregive de observationer, som har betydning for ledelsens ansvar for at føre tilsyn med regnskabsaflæggelsen (ISA 260, afsnit 9).

Kommunikation vedrørende IT indgår ikke direkte i ISA 260, dog antages dette at være omfattet af de generelle bestemmelser og vejledninger i standarden. Revisor skal som før nævnt kommunikere det planlagte omfang og den tidsmæssige placering af revisionen jf. ISA 260, 15. Herunder skal revisor kommunikere til ledelsen omkring identificerede betydelige risici, hvilket kan være IT-relateret, og hvorfor særlige revisionsmæssige overvejelser er relevante. Kan revisor hjælpe ledelsen med at forstå risiciene, vil ledelsen have bedre mulighed for at opfylde sit ansvar med tilsynsførelse af regnskabsaflæggelsen jf. ISA 260, A12.

Afsnit A13 giver eksempler på områder, der kan kommunikeres omkring, herunder forekommer punkterne; revisors tilgang til intern kontrol samt arten og omfang af nødvendige specialiserede kompetencer. Disse er to eksempler hvor revisor særligt kan diskutere risiciene forbundet med anvendelsen af IT i virksomheden. I forlængelse heraf, kan revisor drøfte

ledelsens syn på virksomhedens interne kontroller, overordnede mål og strategi. Dette kan hjælpe revisor med at vurdere sammenhængen mellem virksomhedens strategi i forhold til anvendelsen af IT, se afsnit 7 om god IT-skik.

Krav om revisors kommunikation vedrørende IT-risici kan til dels også gøres gældende med udgangspunkt i ISA 260, 3, 16(e) og A33-A36, hvorunder revisor skal gøre ledelsen opmærksom på ethvert andet betydeligt forhold relevant for tilsynsførelsen af regnskabsaflæggelsen. Yderligere forhold er et vidt begreb, men med fokus på anvendelsen af IT, forventes revisors bekymringer at bidrage til virksomhedens strategiske ledelse og forpligtelse til at udvise ansvarlighed.

8.4.2 ISA 265

ISA 265 anses som en specificering af ISA 260, hvor denne omhandler krav i forhold til kommunikationen af mangler af virksomhedens interne kontrol. Denne revisionsstandard vurderes overordnet at være mere relevant i forhold til kommunikation vedrørende revision af IT, eftersom IT typisk anvendes som en bestanddel af den interne kontrol.

I ISA 265 defineres mangel i intern kontrol som:

1. *En kontrol er udformet, implementeret eller anvendt på en sådan måde, at den ikke rettidigt kan forebygge eller opdage og korrigere fejlinformationer i regnskabet, eller*
2. *Der mangler en kontrol, der er nødvendig for rettidigt at forebygge eller opdage og korrigere fejlinformationer i regnskabet (ISA 265, afsnit 6(a)).*

Når revisor konstaterer mangler i den interne kontrol, kan revisor diskutere omstændighederne for disse mangler med det relevante niveau i den daglige ledelse jf. ISA 265 A1. Dermed kan revisor potentielt opnå en forståelse af, hvorfor de pågældende mangler er opstået. Hertil nævnes i ISA 265 A2 eksempelvis afvigelser, som opstår på grund af fejlinformation, der ikke forebygges eller rettes af de passende IT-kontroller.

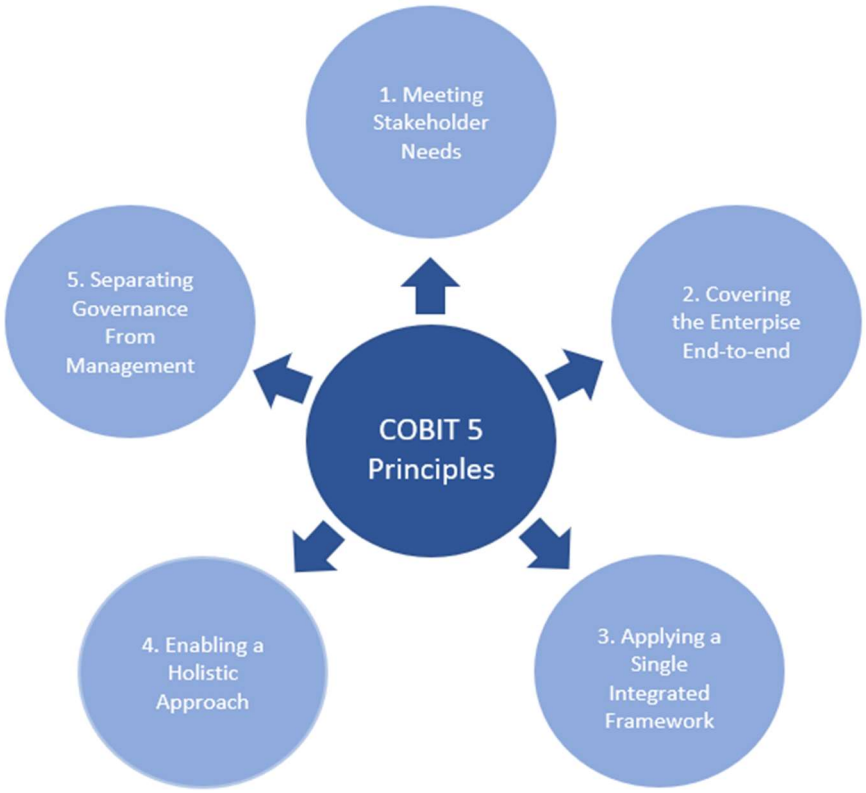
9 Teoriafsnit

Dette afsnit omfatter en redegørelse af COBIT 5 framework, COSO-kuben samt revisionsrisikomodellen.

9.1 COBIT 5 framework

COBIT 5 er en model som anvendes af virksomheder til strategisk IT-governance og -management. Modellen har til formål at hjælpe virksomheder med at nå målsætninger for styring af virksomheds-IT samt at skabe optimal værdi ud fra IT, ved at opretholde en balance mellem at realisere fordele og optimere risikoniveauer og ressourceforbrug. COBIT muliggør styring af virksomheds-IT på en holistisk måde, da modellen omfatter en fuld end-to-end forretning og IT-funktionelle ansvarsområder under hensyntagen til interne og eksterne interessenters IT-relaterede interesser.

Modellen er generisk og nyttig for alle størrelser af virksomheder, kommercielle, ikke-kommercielle og virksomheder i den offentlige sektor (ISACA, 2012, s. 2). COBIT 5 omfatter fem principper til styring og ledelse af virksomheds-IT.



Figur 4 - Illustration af COBIT 5 - Kilde: ISACA, 2012

1. Princip: Meeting stakeholders needs

Dette princip omfatter forretningsværdiskabelse gennem brug af IT, med formål om skabe værdi for virksomhedernes interessenter. Eftersom betydningen af værdiskabelse for interessenter kan være forskellig og i nogle tilfælde modstridende, er det vigtig at ledelsen overvejer hvilke værdiskabelsesbehov, som virksomheden skal opfylde. Hertil skal fordelene-, risiciene- og ressourcevurderingerne i de forskellige behov overvejes. Det anbefales, at der stilles spørgsmålene (ISACA, 2012, s. 17):

- For hvem er fordelene?
- Hvem bærer risikoen?
- Hvilke ressourcer kræves?

2. Princip: Covering the Enterprise End-to-end

Princippet om at dække virksomheden End-to-end omhandler at informationen i COBIT 5 omfatter governance samt management, hvor alle funktioner og processer i virksomheden dækkes. Dermed fokuserer COBIT 5 ikke alene på IT-funktionen, men ligeledes på information og relaterede teknologier, hvilke behandles som aktiver, der skal håndteres som ethvert andet aktiv i virksomheden. Modellen sikrer en holistisk og helhedsorienteret tilgang til governance og management af IT baseret på aktiver (ISACA, 2012, s. 23).

3. Princip: Applying a single integrated framework

COBIT 5 er en enkel og integreret ramme, som stemmer overens med andre samt nyeste relevante standarder og rammer, hvorfor den giver virksomheden mulighed for at bruge COBIT 5, som den overordnede integreringsmodel for styring og ledelse.

4. Princip: Enabling a holistic approach

Effektiv governance og management af virksomheds-IT kræver en holistisk tilgang under hensyntagen til flere interagerende komponenter. COBIT 5 definerer 7 kategorier af aktiver, som understøtter implementeringen af et omfattende styrings- og ledelsessystem til virksomheds-IT, herunder (ISACA, 2012, s. 2; 27):

- *Principper, politikker og rammer,* som er et redskab til at definere den adfærd som anvendes til praktisk vejledning til den daglige ledelse
- *Processer,* beskriver en række organiserede aktiviteter og kutymer for at opnå og fastholde virksomhedens mål, samtidig med at processerne anvendes til at producere resultater, med formål om at opnå de IT relaterede mål.
- *Organisatoriske strukturer,* er de vigtigste beslutningsenheder i en virksomhed.
- *Kultur, etik og adfærd,* af individerne er tit en undervurderet succesfaktor i governance- og managementaktiviteterne.
- *Information,* er udbredt i enhver organisation og inkluderer al information, som produceres samt anvendes af virksomheden. Information er nødvendig for at holde en organisation kørende. På det operationelle niveau er information meget ofte det vigtigste produkt af virksomheden.
- *Tjenester, infrastruktur og applikationer,* omfatter infrastruktur, teknologi og applikationer, som tilfører informationsteknologi og tjenester til virksomheden.
- *Personer, færdigheder og kompetencer,* omfatter de personer, som er nødvendige for at alle aktiviteter kan færdiggøres succesfuldt og sørger for at korrigere handlingerne samt træffe de rigtige beslutninger.

5. Princip: Separating Governance from Management

COBIT 5 skelner tydeligt mellem governance og management. Dette skyldes, at de to områder omfatter forskellige typer aktiviteter og kræver forskellige organisationsstrukturer samt tjener forskellige mål (ISACA, 2012, s. 3).

Governance

Governance sikrer, at interessenternes behov, betingelser og muligheder evalueres for at fastsætte om virksomhedsmålene opnås og for at fastsætte en retning gennem prioritering, beslutningstagning samt overvågning af ydeevne og overholdelse af aftalte retningslinjer og må (ISACA, 2012, s. 31).

Management

Management omfatter planlægning, opbygning, kørsel samt overvågning af aktiviteter i overensstemmelse med den retning, der er fastlagt af ledelsesorganet for at nå virksomhedens mål (ISACA, 2012, s. 31).

COBIT 5's fem principper har sammenlagt det formål at virksomheden får mulighed for at opbygge en effektiv ramme for governance og management, som optimerer informations- og teknologiinvesteringer og -brug til gavn for virksomhedernes interessenter (ISACA, 2012, s. 2).

9.2 COSO

COSO's begrebsramme omfatter strategier til behandling af intern kontrol og danner grundlag for internationale standarder for intern kontrol. Begrebsrammen definerer intern kontrol som en proces, der finder sted i alle lag af en virksomhed. Tidligere har revisors fokus på interne kontroller været rettet mod regnskabsmæssige transaktioner, denne tilgang har ændret sig til, at revisor fokuserer på interne kontroller i alle lag af virksomheden. Hertil gælder ledelseskontroller som specifikke kontroller på transaktionsniveau. Dermed skal revisor have fokus på områder som udgør en væsentlig risiko (Davidsen, 2008, s. 13-14).

COSO ERM (Enterprise Risk Management) har til formål at guide virksomheder til at håndtere usikkerheden forbundet med risici og muligheder, samt at forbedre evnen til værdiforøgelse. Den største værdiforøgelse opnås, ved at ledelsen udarbejder strategier og mål for hvordan virksomheden skaber en optimal balance mellem vækst, målopfyldning og mulige risici. Derudover opnås værdiforøgelse, når ledelsen udnytter virksomhedens ressourcer på en effektiv og virkningsfuld måde (COSO, 2004, s. 4).

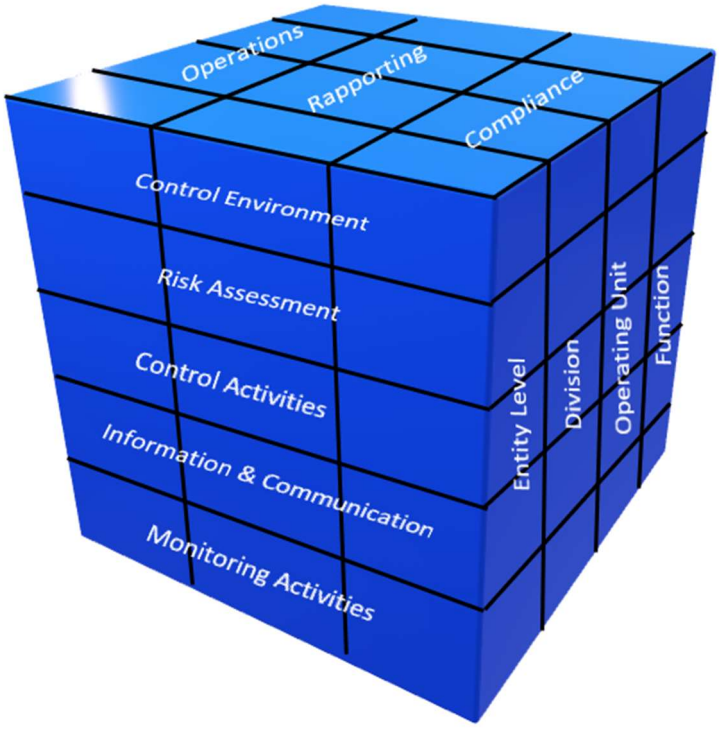
Enterprise Risk Management defineres som følgende:

"Enterprise Risk Management er en proces, som en virksomheds bestyrelse, ledelse og andet personale bruger til at udvikle strategier på tværs af virksomheden og identificere potentielle begivenheder, som kan have indflydelse på virksomheden. Virksomheder anvender enterprise risk management til at håndtere risikoappetit og til på en fornuftig måde at forsikre, at virksomhedens mål bliver opfyldt".

Enterprise Risk Management anses som værende en vedvarende proces, som anvendes gennem hele virksomheden samt på alle niveauer heraf. Modellen anvendes til strategiudvikling på tværs af virksomheden og har til formål, at identificere potentielle begivenheder, som kan

påvirke virksomheden, samt til at håndtere risici ud fra virksomhedens risikoappetit. Endvidere er modellen skabt til målopfyldelse i én eller flere kategorier (COSO, 2004, s. 4).

Ifølge COSO-rammen er der en direkte sammenhæng mellem virksomhedens mål og intern kontrol. Kuben består af tre sider, hvoraf den ene udgør tre elementer, som er med til at muliggøre målopfyldelsen for virksomheden, herunder kategorierne drift, rapportering og overholdelse af lovgivningen (Davidsen, 2008, s. 217). COSO består endvidere af en side, som omfatter virksomhedens interne kontrolsystem, målsætninger og de enkelte forretningsenheder/-aktiviteter (Davidsen, 2008, s. 206).



Figur 5 - Illustration af COSO ERM - kilde: Davidsen, 2008

Endeligt består COSO af en side som omfatter fem komponenter der anvendes i virksomhedens interne kontrol, herunder:

Control Environment (Kontrolmiljø):

Virksomhedens interne miljø udgør fundamentet for risikohåndtering, ved at tilføre disciplin og struktur. Det interne miljø definerer hvorledes risici identificeres, vurderes og håndteres. Denne komponent påvirker anvendelsen af kontrolaktiviteter, overvågningsaktiviteter samt informations- og kommunikationssystemer i virksomheden. Endvidere omfatter det

virksomhedens etiske værdier, kompetencer og udvikling af personalet, samt ledelsesstilen i virksomheden (Davidsen, 2008, s. 218).

Risk Assessment (Risikovurdering):

Vurdering af virksomhedens interne kontroller, med formål om at identificere eksisterende risici samt at fastsætte et acceptabelt risikoniveau for virksomheden. Formålet er at sikre, at de mulige begivenheder ikke påvirker målopfyldelsen. Dette gøres ved, at ledelsen tager udgangspunkt i tidligere begivenheder, som medfører en mere objektiv tilgang end ved en tilgang der er baseret på subjektive skøn (Davidsen, 2008, s. 219).

Control Activities (Kontrolaktiviteter):

Kontrolaktiviteter er de principper og procedurer, som anvendes til at afdække mulige risici i virksomheden. Aktiviteterne udføres gennem hele virksomheden, på alle niveauer og i alle funktioner og er et led i processen om at nå virksomhedens mål. Aktiviteterne omfatter under normale omstændigheder en politik for hvad der skal gøres, samt procedurer for udførelse af denne politik (Davidsen, 2008, s. 219).

Information and communication (Information og kommunikation):

Der er behov for informationer til at identificere, vurdere samt reagere på risici, med henblik på at nå virksomhedens mål. Dette omfatter kommunikation af informationer, som er relevante for de enkelte mål. Der anvendes henholdsvis eksterne og interne kilder for at afdække informationerne, hvilke kan fremkomme i kvantitativ og kvalitativ form. Informationerne gør det muligt, at tilpasse risk management i forhold til ændrede forhold i virksomheden (Davidsen, 2008, s. 219).

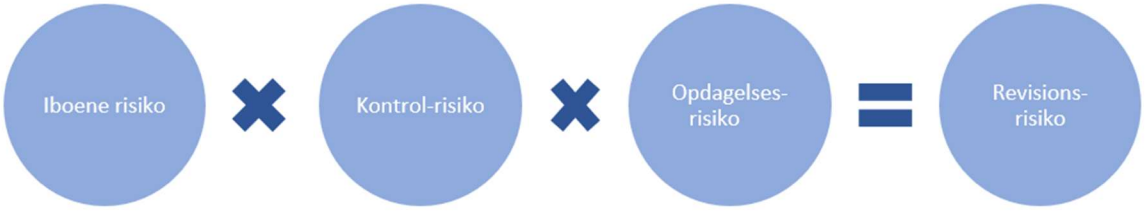
Monitoring Activities (Overvågningsaktiviteter):

Tilstedeværelsen og kvaliteten af risk management processen overvåges over tid, for at sikre, at de anvendte metoder er optimale. Overvågningen kan foregå på to måder, herunder via løbende aktiviteter samt via enkeltstående evalueringer, som udføres på fastlagte tidspunkter (Davidsen, 2008, s. 220).

9.3 Revisionsrisikomodellen

Modellen omfatter risikoen for, at der forekommer væsentlige fejl i regnskabet, som revisor ikke har opdaget, herunder revisionsrisikoen. Ifølge modellen er den iboende risiko, kontrolrisikoen samt opdagelsesrisikoen et udtryk for revisionsrisikoen, som maksimalt må udgøre 5 pct.

Den iboende risiko omfatter risikoen for, at der forekommer væsentlige fejl i regnskabet, som revisor ikke har fundet, kontrolrisikoen omfatter risikoen for at væsentlige fejl ikke forhindres eller rettes af den interne kontrol og opdagelsesrisikoen omfatter risikoen for, at væsentlige fejl ikke opdages under revisionen (Samuelsen et al., 2019, s. 189-190).



Figur 6 - Illustration af Revisionsrisikomodellen - Kilde: Egen tilvirkning

Det er revisors opgave at nedbringe revisionsrisikoen til et acceptabelt niveau, således at revisor med høj grad af sikkerhed kan konkludere, at regnskabet er aflagt i overensstemmelse med den gældende regulering samt at regnskabet giver et retmæssigt billede (Samuelsen et al., 2019, s. 190).

Kapitel 4

Analyse

Dette kapitel indeholder en analyse af væsentlige områder for problemstillingen. Formålet er at belyse hvordan den stigende trussel fra cyberangreb kan have en effekt set fra et revisionsmæssigt perspektiv. Endvidere er formålet at belyse diskrepansen ved reguleringen til IT-revision samt anvendelsen heraf blandt finansielle revisorer.

10 Introduktion til analyse

For at skabe en forståelse af de relevante forhold i reguleringen og den overordnede udvikling i cyberkriminalitet samt IT-sikkerhed, laves en analyse af forhold som vedrører dette. Udgangspunktet for analysen er en egen udarbejdet spørgeskemaundersøgelse, hvor en række revisorer er blevet spurgt om deres holdning til blandt andet IT-revision, risici og ISA-standardernes indhold omkring IT.

I analysen bliver elementerne i revisionsrisikomodellen sammenholdt med typiske risici der kan observeres under IT-revisionen. Dertil vurderes hvordan eksterne trusler som cyberkriminalitet kan inddrages i revisionsrisikomodellen. Dette gøres på baggrund af statistik vedrørende virksomhedernes brug af IT-sikkerhed efter antal ansatte og CFC's vurdering af trusselsniveauet mod danske virksomheder.

Endvidere identificeres potentielle revisionsmuligheder med udgangspunkt i anbefalingerne om god IT-skik. Her fokuseres særligt på virksomhedens kultur i relation til IT-sikkerhed generelt, herunder revisors forståelse af kontrolmiljøet. Dernæst analyseres PwC's Cybercrime Survey 2020, hvori virksomhederne adspørges omkring oplevelser med cyberkriminalitet og holdninger til IT-sikkerhed. Undersøgelsen tager udgangspunkt i PAVA-konceptet udviklet af PwC, hvormed besvarelserne er struktureret efter hvilket sikkerhedsområde af virksomheden de vedrører. I forlængelse heraf anvendes besvarelserne til at vurdere virksomhedernes prioriteter i forhold til IT-sikkerhed, og dermed finde handlinger revisor vil kunne foretage til at opnå forståelse af virksomheden.

Der vil ydermere fremgå en komparativ analyse af COSO og COBIT med formål om, at skabe en forståelse af anvendelsen af de to modeller til IT-revision. COSO's tilgang til intern kontrol med fokus på at identificere og mindske risici anvendes til at understøtte behovet for IT-revision, som en generel del af revisionsprocessen. COBIT's IT fokuserede perspektiv, anvendes til at understrege det fortsatte behov for IT-revisorer i mere komplekse sammenhænge.

Derudover analyseres revisionsprocessen, med formål om at sætte processen i relief til udviklingen i anvendelsen af IT, samt risikoen for cyberangreb. Her er fokusset på planlægningen, den løbende revision samt afslutningen, hvor IT-revision anses som værende relevant.

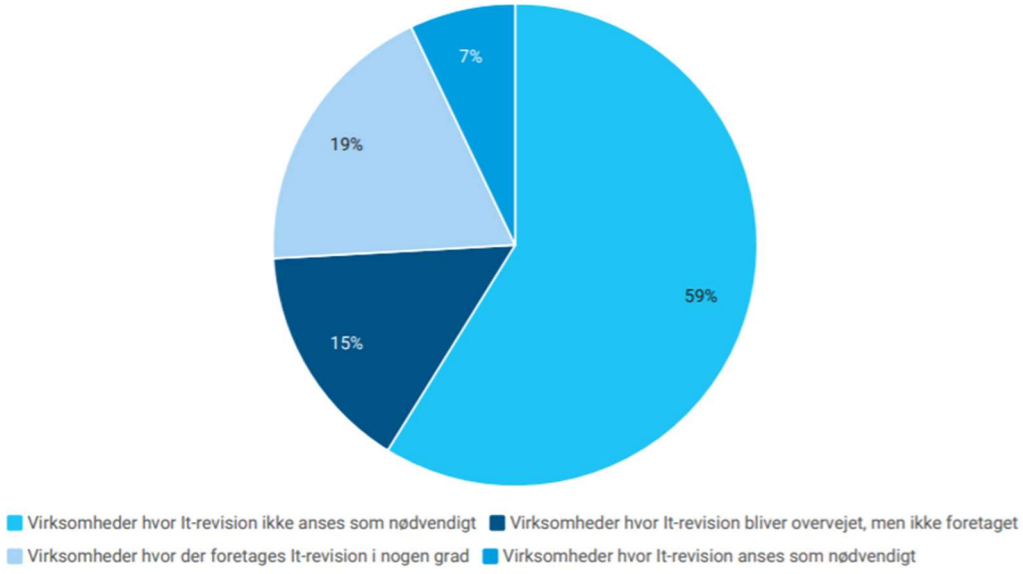
En af besvarelserne i det eget udarbejdede spørgeskema foreslår, at der i ISA-standarderne kan udarbejdes henvisninger til andre standarderne, eksempelvis ISO-standarderne, hvorfor der vil indgå en sammenligning af de overordnede elementer i ISA 315 med ISO 27002, som er en foranstaltningsorienteret standard. Formålet med ISO 27002 er at nedbringe IT-relaterede risici hos virksomhederne, hvorfor den kan give revisor et indblik i hvilke foranstaltninger der kan og bør findes i nogle virksomheder.

Endeligt opsamles analysen med belysning af hvilke konkrete konsekvenser et succesfuldt cyberangreb kan have for en virksomhed. Til dette formål benævnes Daarbak og Mærsk, som begge har lidt økonomiske tab under cyberkriminalitet. Yderligere fremhæves hvordan cyberangreb har udviklet sig i sine metoder og udformninger, hvortil der sættes fokus på Center for Cybersikkerheds anbefalinger til hvilke tiltag en virksomhed kan implementere for at gøre sig mindre attraktiv over for cyberangreb. Afslutningsvist opsamles kort hvordan cyberkriminalitet som trussel overfor virksomhederne har relevans for revisor og revisors rolle fremadrettet.

11 Spørgeskemaanalyse

Spørgeskemaundersøgelsen blev udsendt til 1.117 revisorer i forskellige revisionsfirmaer med geografisk adspredelse, hvoraf 67 respondenter deltog i undersøgelsen, hvilket svarer til cirka 6 pct., hvilket anses som værende tilstrækkeligt til at generalisere i henhold til specialets problemstilling. I forbindelse med analyse af undersøgelsen, vil data indgå i en indholdsanalyse, hvor der forsøges at tolke på respondenternes besvarelser.

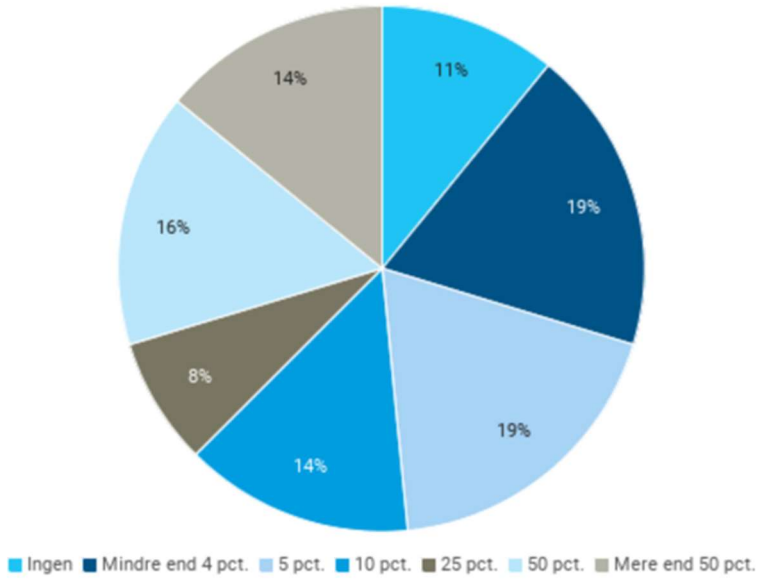
Figur 7 belyser i hvilket omfang revisorerne overvejer IT-revision i forbindelse revision af virksomheders regnskaber.



Figur 7 - Hvilke af følgende virksomheder har du oftest som kunde?

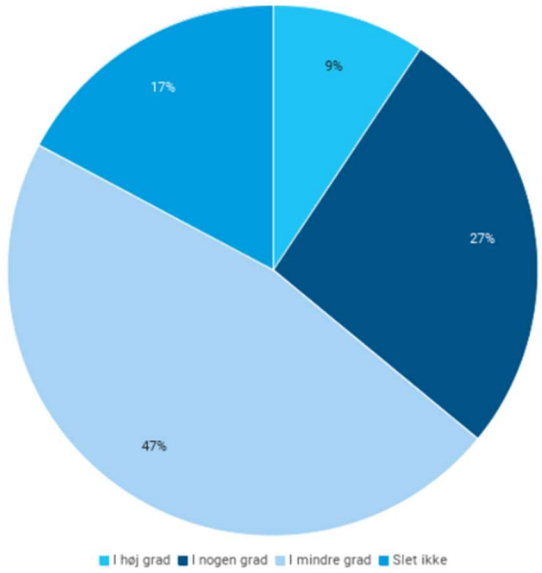
Over halvdelen af revisorerne udfører revision af virksomheder, hvor IT-revision ikke anses som værende nødvendigt. Dette kan være problematisk i henhold til udviklingen inden for cyberkriminalitet, hvortil det anses som en stor risiko for virksomhederne at blive ramt af et cyberangreb, hvorfor revisorerne i større omfang bør inddrage IT-revision. Dette understøttes af Berthings udtalelse om at IT-revision, bør indgå i revision af alle virksomheder (Berthing, 2021). Endvidere kan det være nødvendigt at undersøge virksomhedens IT- samt manuelle systemer, med formål om at mindske fejl, som leder til en større eksponering i henhold til cyberangreb.

Endvidere understøttes ovenstående af figur 8, som belyser revisorernes holdning til hvor mange af virksomhederne, hvor IT-revision ikke er påkrævet, men alligevel bør overvejes. 33 pct. mener at 50 pct. eller derover af ovenstående virksomheder, bør overvejes IT-revision i forbindelse med revisionen.



Figur 8 - Hvor mange af disse kunder, falder ind under kategorien, virksomheder hvor IT-revision ikke er krævet, men bør overvejes?

Der er dog 60 pct. af revisorerne, som mener at dette kun bør overvejes i 10 pct. eller mindre af virksomhederne. Dette kan indikere, at revisorerne ikke har kendskab til udviklingen i forbindelse med IT- og cyberrisici (Berthing, 2021). Eftersom dette udgør en væsentlig risiko i en stor andel af virksomhederne.



Figur 9 - I hvilken grad anvender du IT-relaterede revisionshandlinger i forbindelse med revision?

Ifølge figur 9 udfører 17 pct. af revisorerne ingen IT-revisionshandlinger i forbindelse med revision. Hvor 47 pct. udfører IT-revisionshandlinger i mindre grad. Dette stemmer overens med holdningen om, at IT-revision ikke er relevant i så stor en andel af virksomhederne.

Kontroleelementer- og områder ved IT-revision		
Funktionsadskillelse	Adgangskontroller	Virksomhedens omsætning
Beskyttelse af systemer	Opbevaring af persondata	Risikovurderingsproces
Interne kontroller	Forretningsgange	Momskoder
Backup procedurer	Virksomhedens processer	Afhængigheden af IT i den daglige drift
Overholdelse af lovgivning	Kontrolmiljø	Vurdering af operationel effektivitet af kontroller
IT-sikkerhed	Fysisk sikring	Anvendelsen af IT i bogføring samt regnskabsudarbejdelsen

Tabel 1 - Hvilke fem elementer/områder er vigtigst at kontrollere i forbindelse med IT-revision?

Revisorerne anser ifølge undersøgelsen elementerne/områderne i ovenstående tabel som de vigtigste at kontrollere i forbindelse med IT-revision. Overordnet anser revisorerne IT-sikkerhed til at mindske besvigelser og svindel i virksomhederne i henhold til salg, omsætning mv., som en væsentlig faktor i forbindelse med IT-revision. Derudover er IT-sikkerhed som helhed et vigtigt element, herunder adgangskontroller, beskyttelse af systemer, opbevaring af persondata mv.
Vurdering af kontroller, kontrolmiljø, -aktiviteter, mv. anses ligeledes som vigtige elementer i henhold til IT-revision. I denne sammenhæng er det relevant at undersøge om virksomheden anvender IT til bogføring samt regnskabsudarbejdelse, med formål om at sikre, at der ikke er fejl i systemerne og dermed fejl i regnskabet.

Det anses endvidere som en væsentlig del af IT-revision, at vurdere virksomhedens backup procedurer. Dette skyldes, at det kan have afgørende betydning for virksomheden, hvor stærk en backup der er, da dette kan være med til at sikre, at et vellykket cyberangreb på virksomheden, medfører at driften ikke kan fortsættes (Berthing, 2021).

Den fysiske sikring af virksomhedens server er ligeledes vigtig, for at sikre virksomheden mod cyberangreb. Dette omfatter sikring af 'serverrummet', samt sikring af data som smides ud i form af post, dokumenter, medier mv. Årsagen er, at såfremt cyberkriminelle får adgang til dette, kan det medføre, at personen får adgang til virksomhedens systemer eller andet materiale, som kan have konsekvenser for virksomheden.

De største IT- og cyberrisici		
Hacking/cyberkriminalitet	Manglende IT-kontroller	Mangler i virksomhedens processer
IT-fejl	Adgangskontroller	Mangler i henhold til IT-sikkerhed
Backup	Nedbrud	Manglende kompetencer
Menneskelige fejl	Going Concern	Svindel/besvigelser

Tabel 2 - Hvilke tre risici relateret til IT og cyberkriminalitet, mener du er de største?

Kategorierne i tabel 2 omfatter de risici, som revisorerne anser som de største risici forbundet med IT og cyberkriminalitet. Hacking bliver i undersøgelsen anset som en af de største risici. Dette skyldes, at en stor andel af besvarelserne omfatter hacking i en eller anden form.

Eksempelvis ved phishing, hacking af ordresystem så virksomheden ikke kan modtage ordrer, nedbrud som følge af hacking mv. Dermed anses, det til at være relevant virksomhederne forsøger at mindske risikoen for cyberangreb, da et angreb kan medføre alvorlige konsekvenser for virksomhederne. Andre former for cyberkriminalitet bliver ligeledes anset som en stor risiko i forbindelse med IT, herunder nævnes eksempler som tyveri af identitet, tyveri af data, indbrud i netbank mv.

Mangler i virksomhedernes IT-sikkerhed, processer og IT-kontroller er ifølge revisorerne ligeledes placeret højt i forbindelse med risici, som relaterer sig til IT og cyberkriminalitet. På baggrund af dette, kan der argumenteres for at det er væsentligt, at virksomhederne har fokus på sikkerheden, samt kontrollerne forbundet med IT. Virksomhedens størrelse, i henhold til om det er muligt for virksomheden at have tilstrækkelige IT-kontroller, kan være en udfordring og kan derfor skabe en stor risiko for de mindre virksomheder.

IT-fejl anses ydermere som en af de større risici og kan sammen med ovenstående om IT-kontroller og -sikkerhed, anvendes til at argumentere for behovet for IT-revision. Dette skyldes, at IT-revision kan mindske risikoen for fejl. Eftersom revisor kan opdage fejlen og rapportere til ledelsen, som dermed får muligheden for at rette den fejl, som kan lede til en øget risiko for fejl i regnskabet.

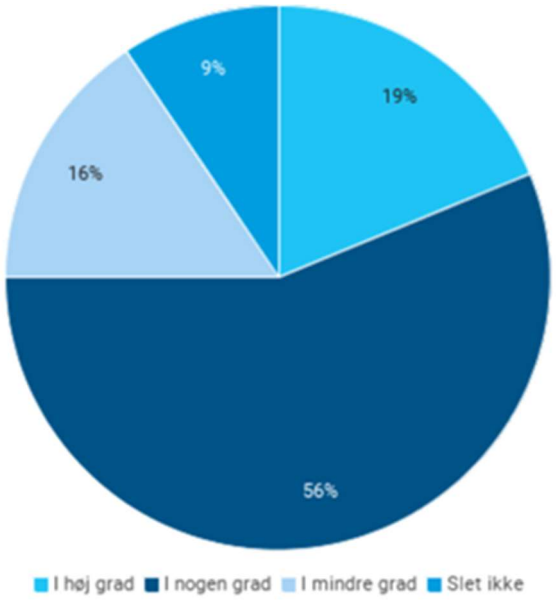
Adgangskontroller anses endvidere som en væsentlig faktor, for at mindske risikoen for cyberangreb, hvorfor det anses som vigtigt, at virksomhederne har særlig fokus herpå. Dette skyldes, at manglende samt utilstrækkelige adgangskontroller, kan medføre, at adgangen til virksomhedens system er let tilgængeligt for de cyberkriminelle, hvilket medfører en større risiko for angreb.

Menneskelige fejl samt manglende kompetencer er ifølge undersøgelsen væsentlige i henhold til risici forbundet med IT og cyberkriminalitet. Dermed anses det som værende nødvendigt, at virksomheder er særligt opmærksomme på dette.

Back-up anses som en væsentlig faktor i forbindelse med IT-sikkerhed. Årsagen til dette er at angreb, hvor virksomheden ikke kan få adgang til vigtige data, driften mv. i værste fald kan medføre going concern, hvilket ligeledes er en risiko som nævnes blandt revisorerne.

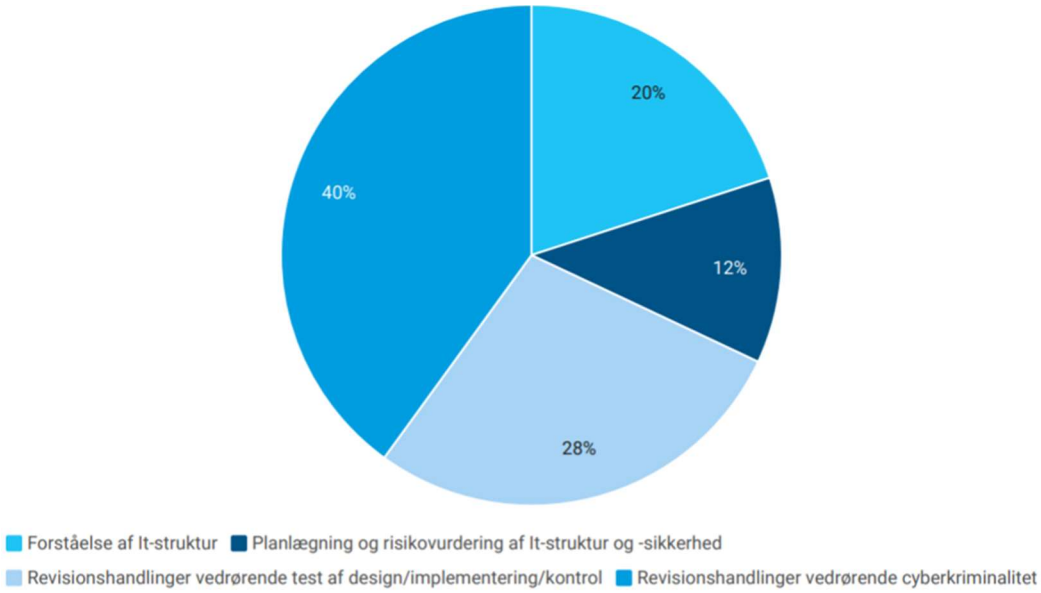
Endeligt er besvigelser og svindel ligeledes områder der opfattes som en stor risiko i forbindelse med IT, herunder risikoen for regnskabsmanipulation samt svindel med data,

hvilket kan medføre, at det retvisende billede af regnskabet trues og dermed skaber et behov for IT-revision for at mindske risikoen.



Figur 10 - I hvor høj grad mener du, at ISA 315 er fyldestgørende til identifikation af IT-relaterede risici?

Ovenstående indikerer, at langt over halvdelen af revisorerne mener, at ISA 315 kun i nogen grad er fyldestgørende i forbindelse med identifikation af IT-relaterede risici. Derudover mener 25 pct. at standarden i mindre grad eller slet ikke er fyldestgørende. Dermed kan der argumenteres for, at standarden på nuværende tidspunkt ikke er tilstrækkelig, således at revisorerne mener, at den alene er tilstrækkelig til at afdække risici i forbindelse med IT. På baggrund af dette, kan der argumenteres for, at der er en sammenhæng mellem manglerne i standarden og det at revisorerne ikke overvejer samt anvender IT-revision i forbindelse med revision i langt de fleste virksomheder. Endvidere tyder antallet af besvarelse til dette spørgsmål, som var markant højere end en del andre tekstspørgsmål, på at der er et behov, som ikke bliver dækket.



Figur 11 - Såfremt du ikke mener, at standarden er fyldestgørende, hvilke områder vurderer du, at der er mangler?

Figur 11 belyser nogle af de områder, som revisorerne mener mangler i ISA 315 i forbindelse med identifikation af IT-relaterede risici. 'Revisionshandlinger vedrørende cyberkriminalitet' anses, som en væsentlig mangel i ISA 315. Dette skyldes, at 40 pct. af revisorerne mener, at denne mangler i standarden.

28 pct. af revisorerne mener, at 'Revisionshandlinger vedrørende test af design/implementering/kontrol' ligeledes mangler i standarden. Dette indikerer, at der anses for at være behov for IT-revisionshandlinger i form af test af design/implementering samt test af IT-kontroller.

20 pct. mener, at ISA 315 mangler at give en forståelse af IT-struktur, hvilket tyder på, at en væsentlig andel af revisorerne mangler en hel klar forståelse af hvordan IT skal håndteres. Endvidere mener 12 pct., at standarden mangler mere uddybende omkring planlægning og risikovurdering i forbindelse med IT. Dette kan understrege behovet for awareness blandt revisorerne.

Nedenstående tabel omfatter yderligere elementer anses som mangler i standarden. Hertil nævnes revision af generelle IT-kontroller, samt at standarden helt generelt ikke følger med udviklingen. Argumentet for dette er, at udviklingen er konstant samtidig med, at standarden ikke er opdateret i 9 år.

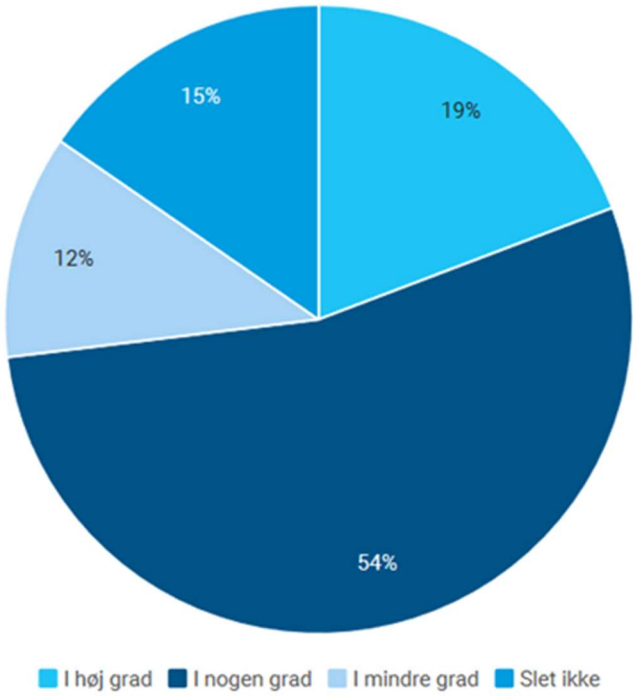
Andre områder som ikke er fyldestgjorte i ISA 315
Revision af generelle IT-kontroller
Følger generelt ikke med udviklingen

Tabel 3 - Er der yderligere områder i ISA 315, som ifølge dig ikke er fyldestgørende?

Som det fremgår af tabel 4 nedenfor, er der enkelte, som mener, at ISA 315 dækker revisors opgaver tilstrækkeligt, hvortil det nævnes, at standarden skal anvendes som teorigrundlag og ikke en konkret angivelse af IT-revisionshandlinger. På baggrund af denne besvarelse, skal revisorerne anvende standarden til vejledning i forbindelse med IT-revision. Der kan dog på baggrund af Figur 10 argumenteres for, at der mangler en forståelse af IT-revision blandt revisorerne, som giver udfordringer i henhold til at tolke standarden.

Andre bemærkninger om ISA 315
Anvendes som teorigrundlag
Halter efter virkeligheden
Dækker tilstrækkeligt til forskellige revisionsopgaver

Tabel 4 - Har du andre bemærkninger omkring ISA 315 vedrørende IT-revision?



Figur 12 - I hvor høj grad mener du, at ISA-standarderne generelt følger med udviklingen omkring stigende anvendelse af IT i virksomhederne?

Et væsentligt flertal af respondenterne mener, at ISA-standarderne generelt set følger med den stigende anvendelse af IT i virksomhederne. Kun 27 pct. Mener, at standarderne i mindre grad eller slet ikke er opdateret tilstrækkeligt. Såfremt det konkluderes, at revisors håndtering af IT- og cyberrisici er manglende, så indikerer denne besvarelse, at det sandsynligvis ikke er som følge af indholdet i standarderne. Dermed virker det mere sandsynligt, at eventuelle mangler vil forekomme på baggrund af hvordan standerne tolkes. Dette stemmer overens med den holdning Berthing udtrykte i interviewet, hvor han påpegede at det tydeligt beskrives i standarderne, at IT medfører risici for regnskabet. Derfor er Berthing enig i, at standarderne udfylder den rolle de skal i relation til formålet med dem, og at det udelukkende er de finansielle revisorer der har ansvaret for korrekt tolkning af standarderne. Samtidig påpeges det, at kendelser til revisornævnet er nødvendige, for at Erhvervsstyrelsen anerkender, at IT skal være en del af kvalitetskontrollen.

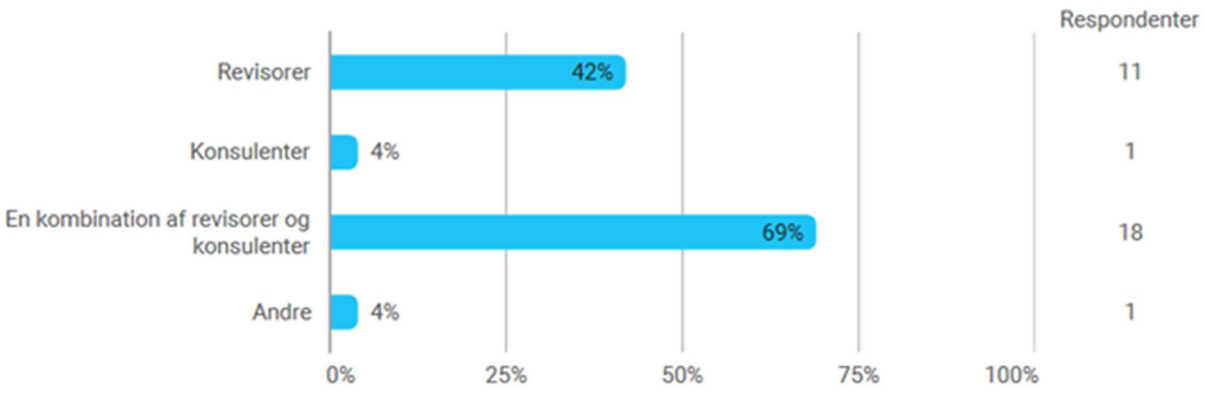
IT mangler i ISA standarderne
Revisionshandlinger/mål direkte målrettet cyberkriminalitet samt direkte målrettet generelle it-kontroller.
Fordrer anvendelse på den korrekte og relevante måde jf. tidligere svar.
Henvisninger til eksempelvis ISO 27001 standarder, så der er andre der tager stilling til udviklingen i it-sikkerhedsnormerne.
ISA standarderne kan jo overordnet ikke følge med IT udviklingen, men med fortolkning og revisionsansvar er det reelt en dårlig undskyldning. Dokumentationskravene bør jo blot øges for at overholde standardkravene, selvom standarden ikke ændres.
En forståelse af at virksomhedens omgivelser ikke nødvendigvis favner it miljøet og it-omgivelser.

Tabel 5 - Såfremt du vurderer, at der er mangler i ISA-standarderne i henhold til IT-revision, beskriv hvad der ifølge dig bør indgå.

Ovenstående tabel oplister de mangler og forbedringer der ifølge respondenterne bør indgå i ISA-standerne. Besvarelserne kan tolkes og opdeles i kategorierne:

1. Indførelse af specifikke handlinger målrettet mod cyberkriminalitet.
2. Henvisninger til eksterne standarder, der vedligeholdes af eksperter, eksempelvis ISO 27001.
3. Forbedre den generelle tolkning af ISA-standarderne, ved at øge dokumentationskrav for at overholde standardkravene.

Der kan skelnes mellem disse kategorier ud fra hvorvidt der fordres ændringer i ISA-standarderne. Første kategori kræver direkte ændringer i standarderne, anden kategori søger indirekte ændringer ved indførelse af henvisninger til alternative vejledninger og tredje kategori nødvendiggør ingen ændringer. Således udgør kategorierne tre forskellige perspektiver på hvordan revisors håndtering af cyberkriminalitet og IT kan forbedres. I forlængelse heraf, kan perspektiverne anses som grundlaget for udarbejdelsen af potentielle løsningsforslag.



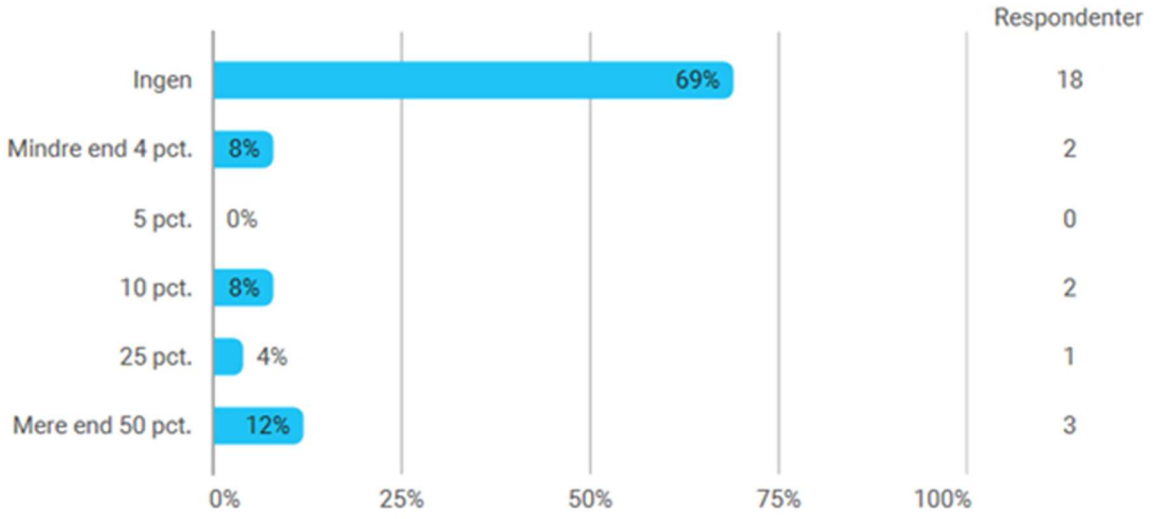
Figur 13 - Hvem mener du, skal foretage IT-revision

Diagrammet viser, hvem respondenterne mener skal foretage IT-revision. Heraf fremgår det at et overvældende flertal er enige, at i revisor bør indgå i IT-revisionen, enten alene eller i samarbejde med konsulenter. Af disse to muligheder mener flest, at både revisor og konsulenter skal være en del af IT-revisionen. Besvarelsen her kan tolkes som et udtryk for, at revisor alene ikke altid kan afdække kompleksiteterne af en virksomheds IT-systemer. Dette kommer også til udtryk i det efterfølgende spørgsmål.

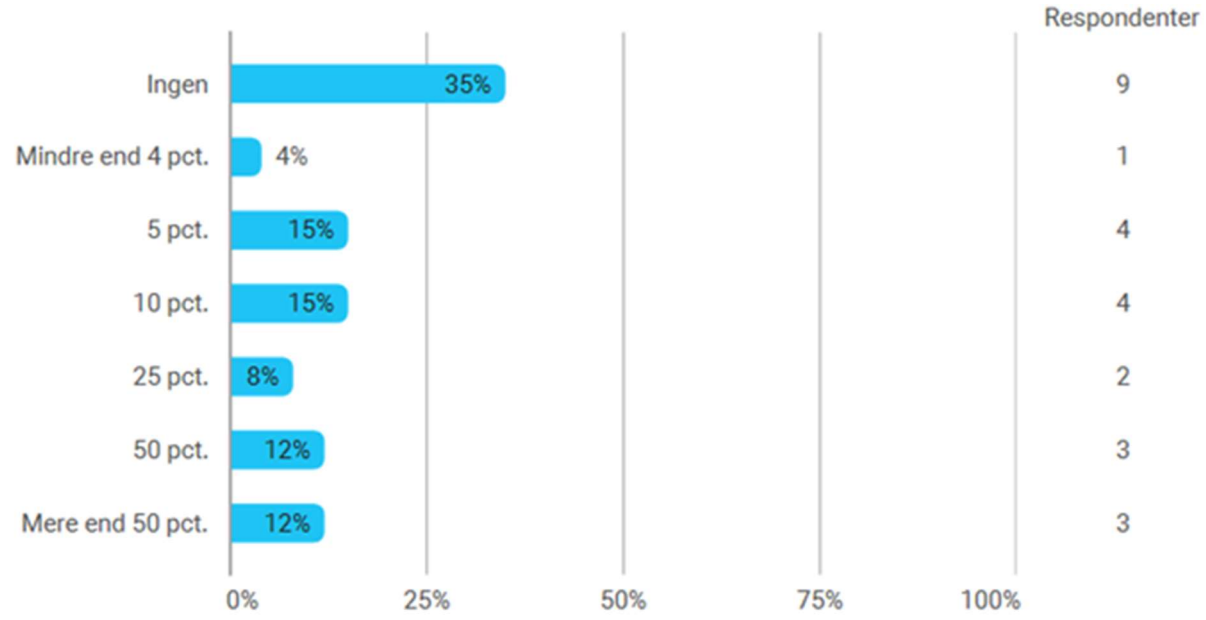
Andre som skal foretage IT-revision
Revisionsvirksomhedens egne IT-revisorer/specialister
Den finansielle revisor har ikke nødvendigvis det fulde indblik i en virksomhedssikkerhed eller indsigt i IT

Tabel 6 - Såfremt du mener, at andre skal foretage IT-revision, så uddyb gerne.

De to kategorier i tabel 6 er udformet på baggrund af de centrale budskaber i besvarelserne. Af disse to kategorier omhandler omkring 65 pct. inddragelse af IT-revisor til håndtering af virksomhedernes IT. Dette underbygges generelt af, at den finansielle revisor ikke altid har det nødvendige kendskab til IT, hvilket også er det centrale i den anden kategori af besvarelser. Der kan her argumenteres for, at forbedring til håndtering af IT kan ske i forhold til inddragelse af IT-revisor eller udvidelse af finansielle revisors kompetencer.



Figur 14 - Hvor ofte afgiver du 3402 erklæringer i forbindelse regnskabsaflæggelse?

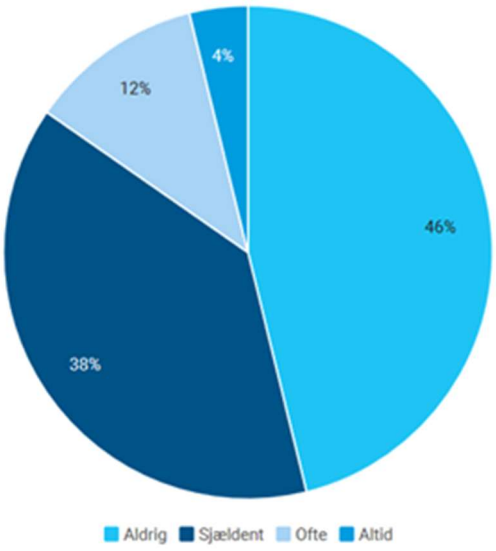


Figur 15 - Hvor ofte har du anvendt en 3402 erklæring fra en anden revisor som dokumentation til at underbygge IT?

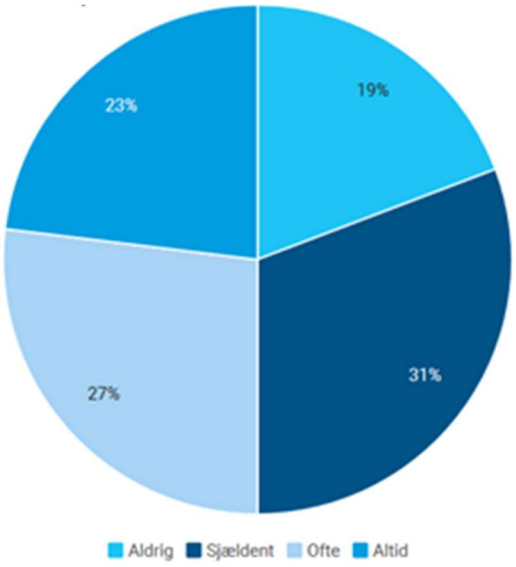
De to ovenstående diagrammer viser henholdsvis hvor ofte respondenterne afgiver 3402 erklæringer i forbindelse med regnskabsaflæggelse, samt hvor ofte de har anvendt 3402 erklæringer fra en anden revisor som dokumentation til at underbygge IT. For det første fremgår det, at et overvejende flertal af respondenterne ikke selv afgiver 3402 erklæringer, med

77 pct. der aldrig eller ved under 4 pct. af opgaver afgiver erklæringen. Omvendt kan det påpeges, at 12 pct. af respondenterne afgiver 3402 erklæringer, ved over halvdelen af opgaver. Dette giver en indikation af, at de fleste revisorer ikke selv udarbejder 3402 erklæringer, hvorimod de revisorer, som udarbejder erklæringen, gør det ofte.

I henhold til hvor ofte 3402 erklæringer udarbejdet af andre revisorer anvendes, er fordelingen mere lige mellem respondenterne. 35 pct. anvender ikke erklæringen, hvor 41 pct. anvender erklæringen mellem under 4 pct. og op til 25 pct. af opgaver og 24 pct. anvender erklæring i mindst 50 pct. af opgaver.

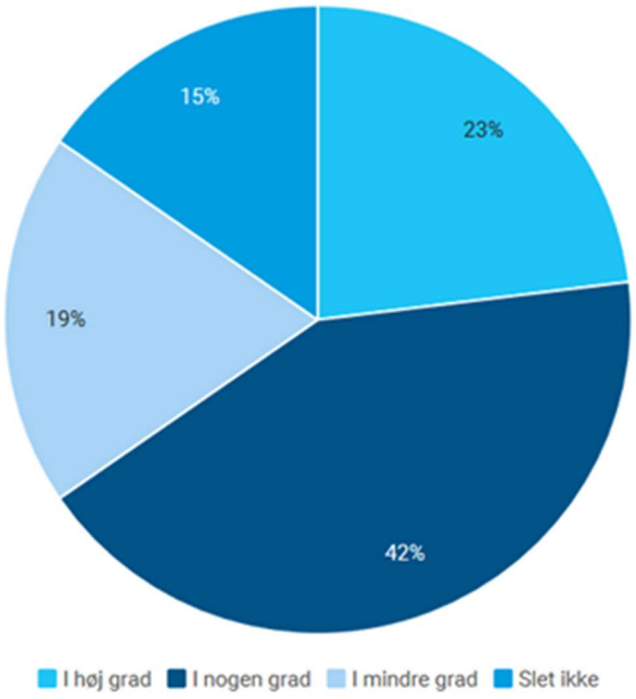


Figur 16 - Bør revisor rapportere særskilt om revision af IT i revisionspåtegningen?



Figur 17 - Bør revisor rapportere særskilt i protokollen om usikkerhed ved IT?

Ifølge respondenterne kan det i figur 16 observeres, at revisor sjældent bør rapportere særskilt om revision af IT i revisionspåtegning, hvor 84 pct. svarede sjældent eller aldrig. Omvendt mener 12 pct. at der ofte bør rapporteres særskilt og 4 pct. mener at der altid bør rapporteres. I figur 17 omhandlende hvorvidt revisor bør rapportere særskilt i protokollen om usikkerhed ved IT, er respondenterne splittede. 19 pct. svarede aldrig, 31 pct. sjældent, 26 pct. ofte, og 23 pct. mener at, der altid bør kommunikeres særskilt i protokollen. Ud fra disse to diagrammer kan der argumenteres for, at der er uenighed og usikkerhed om hvordan mangler ved IT skal håndteres. Der synes at være enighed om, at revisionspåtegningen ikke er værktøjet, hvorunder IT skal placeres. Dette kan også være et muligt tegn på, at revisorerne ikke ønsker at bære ansvaret for de IT-relaterede risici, eftersom fejlagtige revisionspåtegninger kan have betydelige konsekvenser. Sådan en sammenhæng stemmer overens med den splittede holdning omkring hvorvidt der skal rapporteres særskilt i protokollen. Én tolkning af den relativt lige fordeling kan være, at revisorerne overordnet har en interesse i at behandle de IT-relaterede risici, selvom der er usikkerhed om hvordan dette gøres mest hensigtsmæssigt.



Figur 18 - Hvor meget mener du, at IT-revision bør indgå som en del af den generelle revision?

Figur 18 belyser hvor ofte IT-revision, ifølge respondenterne, bør indgå som en del af den generelle revision. Det kan i dette diagram belyses, at 15 pct. mener IT-revisionen slet ikke bør indgå i den generelle revision. De resterende 85 pct. er af den holdning, at IT-revisionen i forskellig grad bør indgå, hvorunder 42 pct. har svaret 'i nogen grad' og omkring 20 pct.

henholdsvis 'i høj grad' samt 'i mindre grad'. For at få en bedre forståelse af Figur 18, bør figuren holdes i relation til nedenstående tabel, som uddyber grundlaget for besvarelsen af forrige spørgsmål.

Bør indgå i den generelle revision	Bør ikke indgå i den generelle revision
Øget anvendelse af IT i virksomhederne. IT er en vigtig komponent i forretningskoncepter og/eller regnskabsgenerering i de fleste virksomheder	Standardiserede systemer, som er pålidelige, reducere behov for IT-revision
For at give et retvisende billede af et regnskab, er det nødvendigt at forstå virksomhedens IT-systemer i forhold til revisors It-systemer	Små virksomheder, hvor betryggende funktionsadskillelse ikke er muligt
Stigende anvendelse af IT-revision generelt	Ikke relevant for alle virksomhedstyper

Tabel 7 - Forklar kort hvorfor du mener eller ikke mener, at IT bør indgå mere i den generelle revision.

Det hyppigste svar der taler for inddragelse af IT-revision, omhandler den øgede anvendelse af IT i virksomhederne. Der argumenteres for, at IT i stigende grad har en central rolle blandt virksomhedernes kunder, hvorfor det vil være naturligt i samme grad at øge anvendelsen af IT-revision. På den anden side påpeges det med største andel besvarelser, at det ikke er alle typer af virksomheder, hvor IT-revisionen vil være relevant. I forlængelse heraf fremhæves særligt små virksomheder, der typisk vil have et standardiseret IT-system og samtidig ikke har mulighed for at implementere effektiv funktionsadskillelse. Opsummerende kan der sandsynligvis identificeres en sammenhæng mellem størrelsen/typen af virksomhed og opfattelsen af hvorvidt IT-revision er nødvendigt.

11.1 Delkonklusion

På baggrund af spørgeskemaanalysen kan det konkluderes, at over halvdelen af revisorerne reviderer virksomheder, hvor IT-revision ikke vurderes at være nødvendigt. Med udgangspunkt i den konstante udvikling af cyberkriminalitet kan den lave grad af IT-revision, på sigt udgøre en risiko for virksomhederne og revisors evne til at opnå egnet revisionsbevis. Endvidere mener 33 pct. af revisorerne, at ved 50 pct. eller mere af de reviderede virksomheder, hvor IT-revision

ikke kræves, alligevel bør overvejes. På den anden side mener 60 pct. af revisorerne, at IT-revision kun bør overvejes ved under 10 pct. af virksomhederne. Dette kan indikere manglende kendskab til udviklingen i relation til IT blandt revisorerne, da der med den udbredte anvendelse af IT i en stor del af virksomhederne medfølger risici. Det kan yderligere i besvarelserne ses, at 17 pct. af revisorerne aldrig udfører IT-relaterede revisionshandlinger, mens 47 pct. gør det i nogen grad. Denne besvarelse stemmer overens med den generelle holdning, om at IT-revision sjældent er relevant ved revision af de fleste virksomheder.

Spørgeskemaundersøgelsen viser fortsat, at revisorerne anser områder der reducerer svig, som et af de vigtigste elementer i IT-revisionen. Derudover prioriteres elementer af IT-sikkerheden, som eksempelvis adgangskontroller, beskyttelse af systemer, opbevaring af persondata mv. Endeligt anses vurdering af henholdsvis kontrolmiljø, virksomhedens backupprocedurer samt den fysiske sikring af virksomhedens servere. I forbindelse med kontrolmiljøet er det relevant at undersøge hvorvidt virksomheden anvender IT, som en del af bogføringen samt regnskabsaflæggelsen. Backupprocedurer kan have stor betydning for virksomhederne, som følge af et succesfuldt cyberangreb kan nedlægge en virksomhedsdrift i en længere periode uden sådanne procedurer. Den fysiske sikring af virksomhedens server, herunder hensigtsmæssig afskaffelse af data, kan hindre cyberkriminelle i at få adgang til virksomheden gennem disse. Eksempler på sårbare data er dokumenter, post, medier mv.

De største risici relateret til IT og cyberkriminalitet er ifølge revisorerne er blandt andet hacking, mangler i IT-kontroller, IT-fejl, adgangskontroller og menneskelige fejl. Phishing, hacking af ordresystem mv. kan have alvorlige omsætningsmæssige konsekvenser for virksomhederne og udgør derfor en alvorlig risiko. Ligeledes beskrives IT-fejl som en betydningsfuld risikofaktor, hvorudfra der argumenteres for nødvendigheden af IT-revision. Adgangskontroller anses ligeledes som et vigtigt element af IT-revisionen, som kan medføre risici. Uddybende kan mangler i virksomhedens adgangskontroller betyde, at de cyberkriminelle lettere kan tilgå virksomheden. Fortsat anser respondenterne menneskelige fejl samt manglende kompetencer blandt de største risici med henblik på cyberkriminalitet og IT-risici. I forlængelse heraf indgår besvigelser og svindel som en stor IT-relaterbar risiko. Manipulation af data og regnskab kan have afgørende konsekvenser for det retvisende billede, uanset om denne er grundet menneskelige fejl eller tilsigtet svig. Endeligt kan Backupprocedurer have kritisk indflydelse på virksomhedens evne til at genoptage driften efter et succesfuldt cyberangreb.

Besvarelsen til hvorvidt respondenterne mener, at ISA 315 er fyldestgørende til identifikation af IT-relaterede risici, viser at væsentlig mere end halvdelen af respondenterne mener ISA 315 i nogen grad er fyldestgørende. Yderligere anser 25 pct. af revisorerne, at standarden i mindre grad eller slet ikke er tilstrækkelig. Derfor kan der argumenteres for, at ISA 315 ikke alene kan anvendes til fyldestgørende at identificere IT-relaterede risici. Det kan supplerende argumenteres, at der er sammenhæng mellem mangler i ISA 315 og observationen, at revisorerne sjældent hverken anvender eller overveje at anvende IT-revision i de fleste revisioner

Ud af fire potentielle mangelområder i ISA 315, mener 40 pct. af revisorerne, at revisionshandlinger vedrørende cyberkriminalitet er manglende. Af de resterende revisorer mener 28 pct. at 'revisionshandlinger vedrørende test af design/implementering/kontrol' er manglende, 20 pct. at der er mangler ved 'forståelse af IT-struktur' og 12 pct. svarer 'planlægning og risikovurdering af IT-struktur og -sikkerhed'. Overordnet kan besvarelsen af dette spørgsmål indikere et behov for vejledning til håndtering af revision af IT og virksomheders cybersikkerhed, samt awareness omkring IT generelt. Respondenternes yderligere holdning til mangler omfatter primært 'revision af generelle IT-kontroller' og at standarden 'følger generelt ikke med udviklingen'. ISA 315 blev sidst ajourført 2013, hvilket sammenlignet med den konstante teknologiske udvikling kan være grundlaget for denne holdning. Revisorernes andre bemærkninger omkring ISA 315 omfatter, at den bør anvendes som teorigrundlag og ikke som en konkret angivelse af IT-revisionshandlinger. Enkelte mener standarden tilstrækkeligt dækker de forskellige revisionsopgaver.

Tilsvarende ISA 315 mener flertallet af respondenterne, at ISA-standarderne generelt følger med udviklingen af den stigende IT-anvendelse i virksomhederne. Dette indikerer, at manglende håndtering af IT-revision sandsynligvis ikke er på grund af mangler i standarden, men derimod som følge af tolkning af standarderne. Det fremgår af lignende besvarelse vedrørende ISA 315, at revisorerne blandt andet opfatter revisionshandlinger målrettet cyberkriminalitet, henvisninger til eksterne standarder og øget dokumentationskrav for revisor, som generelle mangler i ISA-standarderne. Dermed kan der vurderes til at være et behov for at IT-revision omfatter vurdering af cybersikkerhed i nogen grad. Svarende til spørgsmålet om ISA-standarderne kan inddeles i tre kategorier til forbedringer i forhold til ISA-standarderne. Den første er direkte ændringer i standarderne, den anden er indirekte ændringer ved henvisninger til eksterne standarder og den tredje kræver ingen ændringer.

Flertallet af respondenterne mener hovedsageligt, at IT-revision skal udføres af enten revisor alene eller i samarbejde med konsulenter. Respondenterne uddyber, at revisionsvirksomhedens egne IT-revisorer bør foretage IT-revisionen, eftersom den finansielle revisor ikke nødvendigvis har de nødvendige kompetencer i forhold til kompleksiteten af virksomhedens IT-systemer. For bedre at afdække IT-risici samt cybersikkerhed kan der argumenteres for, at IT-revisor bør inddrages oftere eller at den finansielle revisors kompetencer tilpasses.

Ved spørgsmålene omhandlende 3402 erklæringer fremstår det, at 69 pct. af respondenterne aldrig afgiver denne erklæring. Hertil afgiver 12 pct. 3402 erklæringer ved mere end halvdelen af opgaver. I henhold til anvendelse af 3402 erklæringer udarbejdet af andre revisorer anvender 35 pct. den ikke, 41 pct. anvender den 4-25 pct. af gangene og 24 pct. anvender erklæringen i mindst halvdelen af opgaver.

De næste to spørgsmål i undersøgelsen omhandler særskilt rapportering omkring IT i henholdsvis revisionspåtegningen og protokollen. Her forekommer det, at 86 pct. af respondenterne mener, at IT sjældent eller aldrig skal rapporteres særskilt i revisionspåtegningen. I henhold til rapportering i protokollen er besvarelserne relativt lige fordelt med 20-30 pct. på både altid, ofte, sjældent samt aldrig. Der kan ud fra disse besvarelser tolkes, at der blandt revisorerne er uenighed og usikkerhed omkring hvordan mangler ved IT skal håndteres. Endvidere kan enigheden om, at der ikke skal rapporteres i revisionspåtegningen indikere, at revisorerne ikke ønsker at bære det endegyldige ansvar, da fejlagtige revisionspåtegninger kan medføre betydelige konsekvenser.

Afslutningsvist spørges respondenterne om deres holdning til hvor meget IT-revision bør indgå som en del af den generelle revision. Her mener 15 pct., at IT-revision slet ikke bør indgå i den generelle revision. Flertallet af respondenterne fordeler sig dog således, at 42 pct. svarer 'i nogen grad' mens omkring 20 pct. svarer henholdsvis 'i høj grad' og 'i mindre grad'. Besvarelserne af disse to spørgsmål uddybes yderligere med kommentarer fra respondenterne. Argumenterne for øget inddragelse af IT-revision omfatter, at IT i stigende grad anvendes samt udgør en væsentlig komponent i flere virksomheder. I forlængelse heraf, at det retvisende billede nødvendiggør en forståelse af virksomhedens IT-systemer og dennes samspil med revisors IT-systemer. Argumenterne imod inddragelsen af IT-revision er primært, at pålidelige og standardiserede systemer reducerer behovet herfor. Derudover, at IT-revision ikke er relevant for alle virksomhedstyper, særligt små virksomheder, hvor effektiv funktionsadskillelse ikke er muligt.

12 Revisionsrisiko

I følgende afsnit sammenholdes elementerne i revisionsrisikomodellen med de risici der medfølger den stigende anvendelse af IT i virksomhederne og den stigende trussel for cyberkriminalitet. Modellens elementer analyseres enkeltvis med fokus på hvordan IT relaterede risici kan påvirke iboende-, kontrol- og opdagelsesrisiko hver især. Endeligt gives i afsnittet et indblik i hvor hyppigt forskellige sikkerhedsforanstaltninger anvendes i forhold til størrelsen af virksomheden.

Generelt set er målsætningen for en revision at opnå en høj grad af sikkerhed svarende til en accept af 5 pct. risiko for væsentlige fejl. Sammenholdes denne målsætning med den stigende grad af kompleksitet i IT-sikkerhed og cyberangreb, kan der stilles spørgsmålstegn ved hvordan revisors risikovurdering påvirkes. Med udgangspunkt i antagelsen om at IT, i stigende omfang udgør en central del af flere virksomheder, forventes det at IT vil blive et alment aspekt i revisors risikovurderingsproces. Udviklingen i cyberkriminalitet kan betyde at både iboende-, kontrol- og opdagelsesrisiko i nogle tilfælde vil være større under en enhver revision, uddybende fremgår nedenfor.

12.1 Iboende risiko

Den iboende risiko som tidligere beskrevet påvirkes af transaktionernes karakteristika, kompleksitet samt graden af skøn mv. forventes at stige ved den vækstende trussel fra cyberangreb. Dette kommer af, at et eksternt cyberangreb ikke kan antages at være begrænset til enkelte regnskabsposter, men derimod omfatte hele systemer samt de bagvedliggende data. Danish Agro eksemplet i afsnit 5.1.1 demonstrerer, hvordan denne form for iboende risiko reelt kan forekomme. På baggrund af ovenstående anses den IT-baserede risiko at være størst i virksomheder med få gennemgribende IT-systemer, hvori store mængder data er samlet og alle kan påvirkes ved ét ekstern gennembrud. Et eksempel kan også være i forvejen etablerede virksomheder med en lav grad af fokus på IT-sikkerhed, som ikke er opdaterede eller dannede i forhold til det skiftende trusselsbillede, og dermed vil være mere udsatte overfor phishing eller social engineering. Uddybende kan en virksomheds mailsystem eller sociale medier være en af mange indgangsvinkler for gerningsmænd.

12.2 Kontrolrisiko

Kontrolrisikoen forventes at have stor betydning for virksomhedernes evne til at imødekomme truslen i forbindelse med den konstante teknologiske udvikling. Både kompleksiteten af de interne kontroller og cyberangreb er stigende, hvilket kræver nye kompetencer for både medarbejdere og revisorer. Med udgangspunkt i anbefalingerne for god IT-skik bør der være en gennemgående sammenhæng i virksomhedens anvendelse af IT og overordnede strategi samt forretningsproces. Dermed omhandler kontrolrisiko som problemstilling en omfattende kompetenceudvikling blandt virksomheder og ansatte. Tages der udgangspunkt i spørgeskemaundersøgelsen anser respondenterne blandt andet IT-fejl, adgangskontroller og menneskelige fejl, som nogle af de største IT-relaterede trusler.

En dybere forståelse af IT bør styrke virksomhedens evner til at opdage generelle risici samt cyberangreb. Respondenterne i spørgeskemaundersøgelsen mener, at nogle af de vigtigste IT-områder at kontrollere omfatter: Kontrol af omsætning i forhold til svig, kontrolmiljøet, virksomhedens backup-procedurer samt fysisk sikring af serverer. Politikker eller handleplaner sigtet mod en konsekvent behandling af IT-baserede transaktioner samt virksomhedens andre IT-systemer kan forebygge væsentlig fejlinformation. Ligeledes kan funktionsopdeling af både personer og systemer reducere risikoen for, at en enkelt person, intern såvel som ekstern, kan få adgang til en kritisk mængde data. Mulighederne og risici forbundet med den interne kontrol bør stemme overens med den enkelte virksomheds behov.

Antal ansatte	0-49	50-99	100-249	250+
Foretager kryptering af data, filer eller e-mails	49	66	77	88
Har backup af data til en alternativ geografisk placering (Inkl. Cloud)	81	90	93	95
Har adgangskontrol til virksomhedens netværk	81	93	95	98
Har VPN	61	83	91	96
Foretager risikoanalyse	49	65	74	85
Foretager tests af IT-sikkerhed	45	63	71	84
Havde brud på IT-sikkerheden i foregående kalenderår	9	13	19	31
Stigende niveau for investeringer i IT-sikkerhed i foregående kalenderår	33	45	48	63
Har dokumentation om forholdsregler, aktiviteter og procedurer vedr. IT-sikkerhed	52	74	83	95

Tabel 8 - Virksomhedernes brug af IT-sikkerhed efter branche, alle virksomhedsbrancher (Private, ikke-finansielle byerhverv) - Kilde: Danmarks Statistik, 2020

Omfanget af den enkelte virksomheds IT-systemer, bør naturligt hænge sammen med kompleksiteten samt mængden af de data, herunder transaktioner, som virksomheden foretager. Ud fra denne påstand, vil der typisk være en sammenhæng mellem størrelsen af virksomheden og omfanget af IT-anvendelsen. I forlængelse heraf må risikoen for at fejlinformation ikke opdages eller rettes være større i en stor virksomhed, som følge af den samlede mængde data. Dette må alt andet lige, nødvendiggøre et større behov for IT-sikkerhed i den pågældende virksomhed, hvilket ligeledes kan anskues i ovenstående tabel. I tabellen er opstillet en række handlinger, som forskellige størrelser af virksomheder har foretaget for at øge IT-sikkerhedsniveauet. Yderligere indeholder tabellen den procentvise mængde virksomheder, der har haft brud på IT-sikkerheden, øget investeringen i IT-sikkerhed og har en dokumenteret procedure vedrørende IT-sikkerhed.

Når revisor foretager risikovurderingen af virksomheder med betydelig IT-anvendelse, skal bestemte risici overvejes. Disse er først og fremmest, hvorvidt der er risiko for økonomiske tab ved utilsigtet reduktion af IT-kapaciteten. For det andet, risikoen for at ødelæggelse af data kan forhindre aflæggelse og revidering af årsregnskabet. Slutteligt risiko for fejl i de systemer, der leverer data til regnskabet (RevisionsMemo – IT-revision, u.å.). Med udgangspunkt i ovenstående tabel vil revisor oftest vurderer kontrolrisikoen som værende høj i de store virksomheder, hvoraf 31 pct. oplevede brud på IT-sikkerheden, trods hyppigste anvendelse af IT-sikkerhedsforanstaltninger.

12.3 Opdagelsesrisiko

Det sidste element af revisionsrisikomodellen er opdagelsesrisikoen, som omhandler risikoen for at revisor under revisionen ikke opdager væsentlig fejlinformation. Opdagelsesrisikoen udgør den ukendte størrelse i revisionsrisikomodellen. Endvidere er der en omvendt sammenhæng mellem at risici for væsentlig fejlinformation opstår og opdagelsesrisikoen, hvor opdagelsesrisikoen er lav ved en stor risiko for fejlinformation. Samtidig kan opdagelsesrisikoen aldrig reduceres til nul, da revisor ikke gennemgår samtlige transaktioner i en virksomhed (RevisionsMemo – Opdagelsesrisiko, u.å.).

Opdagelsesrisikoen forventes i høj grad at være stigende grundet den konstante udvikling inden for cyberangreb. Center for Cybersikkerhed (2020, (b)) vurderer, at truslen fra

cyberkriminalitet samt cyberspionage imod danske virksomheder er meget høj. Ligeledes påpeger CFC (2020, (a)) beskrivelse af ransomware-angreb, at gerningsmænd har et bredt udvalg af angrebsmetoder. Dette talrige udvalg af metoder, for at opnå adgang til virksomheden, kan vanskeliggøre både revisors og virksomhedens egne chancer for at opdage væsentlig fejlinformation. Effektiviteten af stikprøver antages også at reduceres såfremt en ekstern gerningsmand har gennemgribende adgang til virksomhedens IT-systemer, og dermed væsentligt kan ændre eller ødelægge data. Denne fleksibilitet skaber risiko for at enkelte såvel som flere regnskabsposter påvirkes i forskelligartet grad, hvilket kan gøre konsekvenserne af sådan et angreb uigennemskuelige, set fra et revisionsmålsperspektiv.

Yderligere kan det påpeges, at en grundlæggende fejl i et IT-system vil påvirke samtlige data, som dette system behandler (Olsen, 2021). Eksempelvis hvis en virksomhed anvender estimatbaserede transaktioner, og systemet der skal udregne disse estimater er programmeret forkert, så vil alle disse transaktioner bogføres med en fejlagtig værdi.

12.4 Delkonklusion

Opsummerende kan øget risiko identificeres i alle elementer af revisionsrisikomodellen i forbindelse med den stigende trussel fra cyberkriminalitet. Den iboende risiko er større i kraft af en ny naturlig risiko ved at drive virksomhed i form af cyberangreb. I forlængelse heraf vil et sådant cyberangreb sandsynligvis påvirke hele systemer, som typisk håndterer data relevante for et flertal af regnskabsposter. I henhold til kontrolrisikoen pålægges virksomhederne et behov for konstant at udvikle sine interne kontroller for at stå stærkt overfor potentielle cyberangreb. Formår virksomheden ikke at udvikle sine kontroller, herunder sine medarbejder, i tilstrækkelige grad, vil kontrolrisikoen stige. Ligeledes kan der identificeres en sammenhæng mellem virksomhedens størrelse og mængden af brud på IT-sikkerheden. Endeligt betyder de mange angrebsmetoder, at opdagelsesrisikoen ligeledes er stigende, da revisor gennem stikprøver ikke kan afdække alle transaktioner.

13 Revisionshandlinger med udgangspunkt i IT- og cybersikkerhed

Afsnittet omhandler hvordan revisor kan opnå forståelse af virksomhedens IT-sikkerhed gennem forståelse af virksomhedens kultur. Afsnittet søger dermed at belyse hvordan revisor ved forståelse af kravene til god IT-skik, kan vurdere en virksomheds IT-sikkerhedsmæssige indsats og dermed risikoniveauet. Yderligere analyseres PwC's cybercrime survey for få et indblik i virksomhedernes holdning og handlinger til cybersikkerhed. Forståelse af udviklingen i virksomhederne forventes at bidrage til at rette revisors opmærksomhed mod de IT-områder, som oftest er sårbare.

13.1 God it-skik og risici forbundet med kontrolmiljøet

Under interviewet med Dorthe Tolborg blev der nævnt eksempler på hvordan et cyberangreb kan forekomme, hvoraf et af disse var resultatet af menneskelige fejl. Der kan argumenteres for, at et IT-system ikke er bedre end de mennesker, som bruger det. Selvom systemet kan være avanceret og på et højt teknologisk niveau, vil det sandsynligvis stadig være sårbart over for hackere, som får adgang gennem medarbejdernes oplysninger. Som Tolborg påpegede, kan en uopmærksom medarbejder nemt trykke på det forkerte link, hvorfra den kriminelle hurtig kan anskaffe sig password og lignende information.

Dette aspekt af IT-sikkerheden er af stor relevans for både revisor og virksomhederne, da grundlæggende IT-relateret uddannelse af medarbejdere alt andet lige, må være mindre omkostningstungt end investering i komplekse IT-systemer. Med udgangspunkt i god IT-skik anbefalingerne, bør der være en kritisk masse til opretholdelsen af kompetenceområdet, hvor mangel heraf bør føre til overvejelser omkring kompetenceudvikling mv. (Mogensen et al., 2011, s. 19). Yderligere administrative og informationssikkerhedspolitiske tiltag som virksomheden kan foretage, er uddybet i afsnit 7 om God IT-skik.

For revisor opstår relevans i fremgangsmåden til vurdering af det IT-relaterede kontrolmiljø. Forståelse af kontrolmiljøet udgør en væsentlig del af kravene i ISA 315, og kan være med til at give revisor en god indikator på kontrolrisikoniveauet i en pågældende virksomhed. Dette antages at være særligt gældende i henhold til IT, da det ikke nødvendigvis kræver samme tekniske kompetencer at forstå kontrolmiljøet i forhold til selve de IT-relaterede kontroller. Eksempelvis opnås revisionsbevis for kontrolmiljøet typisk gennem forespørgsler samt inspektion af dokumenter og vurdering af ledelsens reaktion på den interne revisions

observationer af mangler i den interne kontrol jf. ISA 315, A79-A80. Ud fra revisors konklusion på kontrolmiljøet forventes det, at revisor kan identificere hvor der er størst risici forbundet med den pågældende virksomheds IT- og cybersikkerhed. Denne konklusion kan være at der overordnet forventes at være mangler i IT-systemet, at der er manglende IT-kompetencer blandt medarbejderne eller at det er en kombination af begge, som skaber væsentlige risici.

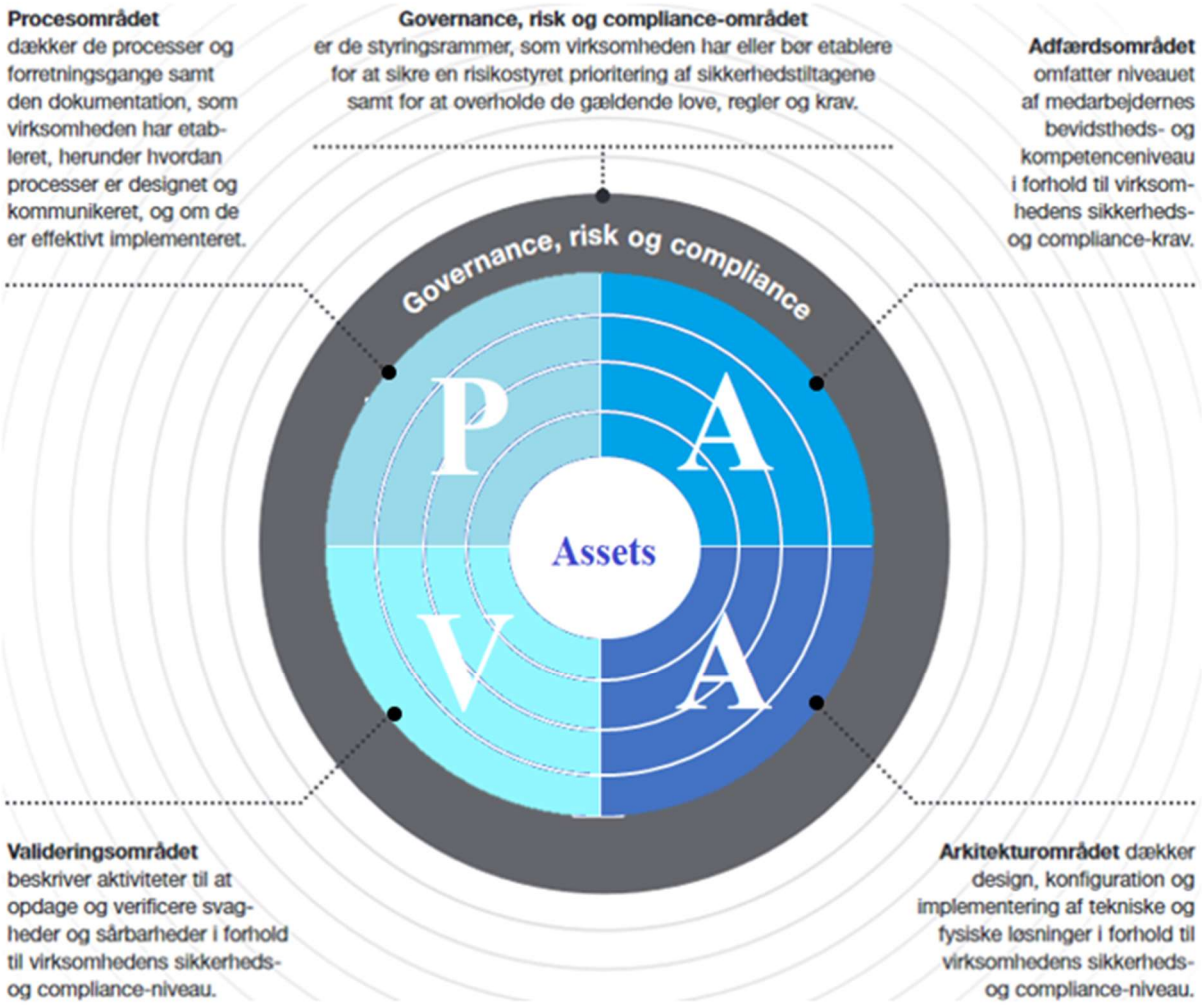
13.2 PAVA-konceptet

PwC har i forbindelse med deres Cybercrime Survey udviklet PAVA-konceptet med formålet om at skabe en fælles forståelse mellem virksomhedsledere og fagfolk, der arbejder med sikkerhed (Nielsen et al., 2020). Konceptet omfatter elementerne:

- Procesområdet
- Valideringsområdet
- Adfærdsområdet
- Arkitekturområdet
- Governance, risk og compliance-området

PwC beskriver konceptet som en generisk kommunikations-, vurderings-, samt rapporteringsmodel, og kan derfor anvendes af forskelligartede standarder og frameworks. PAVA-konceptet redegøres ikke dybdegående, men gennemgås i forbindelse med resultaterne af PwC's Cybercrime Survey 2020. Formålet med denne fremgangsmåde er at skabe en perspektivering af undersøgelsens resultater, samtidig med at skabe en forståelse af hvordan resultaterne kan være relevant for revisor.

Undersøgelsens 326 respondenter består af danske virksomhedsledere, IT-chefer og sikkerhedsspecialister. Respondenterne er fordelt med 67 pct. i den private sektor, 22 pct. i den offentlige- og 11 pct. i den finansielle sektor. Endvidere defineres større virksomheder ved mindst 200 ansatte, og mindre virksomheder omvendt, med under 199 ansatte. Undersøgelsen belyser, er at antallet af IT-relaterede hændelser er det højeste i fire år, hvor 58 pct. af respondentvirksomhederne har oplevet mindst én hændelse.



Figur 19 - Illustration af PAVA-konceptet - Kilde: PwC, 2020

"Governance, risk og compliance-området er de styringsrammer, som virksomheden har eller bør etablere for at sikre en risikostyret prioritering af sikkerhedstiltagene samt for at overholde de gældende love, regler og krav" (Nielsen et al., 2020, s. 4). Inden for dette område omhandler undersøgelsen primært virksomhedernes syn på GDPR samt GDPR-relateret cyberkriminalitet. I henhold til god IT-skik er det lovpligtigt at beskytte personfølsomme data, hvorfor virksomhedens håndtering af GDPR-reglerne og de dertilhørende risici antages at have relevans for revisor. Undersøgelsen viser et fald i at lovkrav og regulering anses som den største trussel for virksomheden, i relation til cybersikkerhed, fra 41 pct. i 2018 til 15 pct. i 2020. Samtidig er antallet af hændelser, hvor personfølsomme data utilsigtet er blevet delt steget fra 17 pct. i 2018 til 38 pct. i 2020 (Nielsen et al., 2020, s. 10; 16-17). Udviklingen i virksomhedernes perspektiv kan i sammenhæng med det stigende antal hændelser, være en indikation på at virksomhederne i højere grad forstår alvoren af cyberkriminalitet.

Første centrale element af PAVA-konceptet er procesområdet. Dette element omhandler *" […] de processer og forretningsgange samt den dokumentation, som virksomheden har etableret, herunder hvordan processer er designet og kommunikeret, og om de er effektivt implementeret."* (Nielsen et al., 2020, s. 4). I henhold til procesområdet viser PwC's undersøgelse en udvikling i formen af cyberangreb, hvor 35 pct. af phishingangreb er relateret til COVID-19. I forlængelse heraf har 29 pct. af de adspurgte virksomheder oprettet særligt cyber-beredskab i forbindelse med COVID-19 (Nielsen et al., 2020, s. 12). Med fokus på god IT-skik har ledelsen, som beskrevet i afsnit 7, ansvaret for sammenkoblingen af virksomhedens overordnede strategi og anvendelsen af IT. Det antages i denne kontekst, at den øverste ledelse i enhver virksomhed, hvor det er relevant, har overvejet og drøftet de potentielle risici der medfølger af COVID-19. For revisor kan forespørgsel vedrørende COVID-19 tiltag, vise hvorvidt den pågældende virksomhed har taget stilling til disse risici. Yderligere kan revisor undersøge om der er implementeret procedurer eller processer, der hjælper medarbejderne med at undgå cyberangreb sigtet netop mod de ansatte, som eksempelvis phishingangreb. Er virksomheden tilstrækkeligt forberedt på phishingforsøg og lignende med en dokumenteret procedure, er det måske ikke nødvendigt at foretage ekstraordinære handlinger på baggrund af COVID-19-situationen.

Undersøgelsen af PwC viser fortsat, at virksomhederne netop er blevet bedre til at dokumentere sikkerheds- og lovgivningskrav i de interne retningslinjer, procedurer og vejledninger. Særligt de større virksomheder får dokumenteret sikkerhedskravene mv., hvor 44 pct. svarer at 75 pct. af disse er dokumenteret. Kun 13 pct. af de større virksomheder har dokumenteret mindre end 25 pct. I de mindre virksomheder fordeler graden af dokumentation sig således, at 33 pct. har dokumenteret mere end 75 pct., hvorimod hele 22 pct. har dokumenteret under 25 pct (Nielsen, M. et al., 2020. S. 13). Ud fra denne fordeling kan der argumenteres for, at de større virksomheder i højere grad efterlever kravene til god IT-skik, hvorfor mindre virksomheder, alt andet lige, vil være mere eksponeret overfor cyberangreb.
I forlængelse heraf påpeger PwC: *" […] virksomheder i stigende grad ønsker at veri-ficere, om deres politikker og retningslinjer er tilstrækkeligt forankret og efterlevet i organisa-tionen – og ikke blot er publiceret med en forventning om, at alle medarbejdere så efterlever dem."* (Nielsen et al., 2020, s. 13). Ud fra PWC's erfaring kan endnu et område, hvor revisor kan rette forespørgsler, således være mod virksomhedens verificering af at sikkerhedspolitiske tiltag reelt er blevet implementeret.

Adfærdsområdet af PAVA-konceptet omhandler medarbejdernes bevidsthed samt kompetencer relateret til virksomhedens sikkerhed (Nielsen et al., 2020, s. 4.). Ifølge undersøgelsen betyder den fortsat stigende trussel fra cyberkriminalitet, at der i samme grad er behov for at øge medarbejdernes bevidsthed på området. I PwC's undersøgelse er respondenterne blevet adspurgt: *"Hvilke af følgende tiltag gør din virksomhed brug af i forbindelse med GDPR-, cyber- og informationssikkerheds-awareness?"* (Nielsen et al., 2020, s. 14). Uddybende sammenlignes tiltagsformerne fra de seneste 12 måneder, med de kommende 12 måneder. 74 pct. af virksomhederne har i det seneste år foretaget envejskommunikation, som en del af deres bevidsthedssøgende tiltag. Sammenlignet med de kommende 12 måneder, planlægger 57 pct. af virksomhederne at anvende envejskommunikationen, hvilket udgør et fald på 27 pct. Denne udvikling kan anses som et tegn på, at virksomhederne ikke længere vurderer at envejskommunikation skaber den ønskede effekt. De andre tiltagsformer, som indgår i undersøgelsen, er E-learning, klasseundervisning og gamification. Gamification er en metode, hvor elementer der typisk anvendes i spil bruges til at fordre en bestemt slags handling blandt kunder eller medarbejderne. Udviklingen i anvendelsen af disse typer tiltag fra forrige år til det kommende år er minimal, hvormed der ved E-learning er et fald på 5 pct., ingen ændring i klasseundervisning og en 3 pct. stigning i gamification. Implementering af tiltag der skal øge medarbejdernes bevidsthed og kompetencer i forhold til IT-sikkerhed kan, være et område revisor kan lave forespørgsler til med henblik på risikovurderingen. Dette kommer af, at der alt andet lige må være en sammenhæng mellem medarbejdernes sikkerhedsrelaterede bevidsthed samt kompetencer og risici for succesfulde cyberangreb.

Næste område af PAVA-konceptet er valideringsområdet, som omhandler *"Aktiviteter til at opdage og verificere svagheder og sårbarheder i forhold til virksomhedens sikkerheds- og compliance niveau"* (Nielsen et al., 2020, s. 4). Det kan argumenteres, at valideringsområdet udgør det væsentligste område i forhold til at reducere effekten af et succesfuldt cyberangreb. I forlængelse heraf udtaler Berthing (2021) følgende, om IT-revisions virkning på cyberkriminalitet:

"*Jeg tror ikke, at IT-revision mindsker cyberkriminalitet. Cyberkriminalitet den rammer alle, den rammer hele tiden, og det er blot noget der bliver større og større. IT-revisionen den er jo lidt på bagkant, så det der nok gør det mere robust, mere resilience for virksomhederne, det er*

i virkeligheden en god IT-sikkerhedsstyring, IT-sikkerhedsstrategi, IT-sikkerhedspolitik og awareness […]".

Med udgangspunkt i citatet, må det derfor erkendes, at fuldstændig beskyttelse mod cyberkriminalitet ikke er muligt, hvorfor det er væsentligt at have fokus skadeinddæmning. Uddybende oplevede 31 pct. af respondenterne at blive ramt af cyberkriminalitet eller informationssikkerheds hændelser som følge af leverandør fejl, hvilket antages at være uden for virksomhedens egenkontrol. Derfor vurderes det potentielt at have afgørende betydning for virksomhederne, at have implementeret inddæmmende eller segmenterede tiltag, for at reducere spredning af et eventuelt cyberangreb. Endvidere kan det være lige så væsentligt for virksomheden at have en backup plan, hvormed mistede data kan gendannes eller erstattes på anden vis.

PwC's undersøgelse viser, at antallet af phishingangreb aldrig har været større, hvor 79 pct. har været udsat herfor, hvilket fortsat nødvendiggør fokus på medarbejdernes awareness samt kompetencer. Samtidig mener henholdsvis 72 pct. og 69 pct. af virksomhederne, at organiserede kriminelle og ansatte/insideres ubevidste handlinger, udgør de største IT-relaterede trusler. Ifølge PwC kan der identificeres en sammenhæng mellem begge disse trusler og den stigende mængde phishingangreb. Phishingforsøg er pr. definition afhængige af menneskelige fejl, hvilket er noget organiserede kriminelle i stigende grad forsøger at udnytte (Nielsen et al., 2020, s. 17). Overordnet kan revisor under en revision, som nævnt, undersøge medarbejdernes opmærksomhed på IT-kriminalitet samt hvorvidt awareness-træning er prioriteret. Ligeledes kan det have betydning for den IT-relaterede risikovurdering, at undersøge hvad virksomheden har implementeret af backup planer og inddæmmende tiltag.

Det sidste element i PAVA-konceptet, og dermed PwC's undersøgelse, er arkitektur-området. Dette element omhandler *"design, konfiguration og implementering af tekniske og fysiske løsninger i forhold til virksomhedens sikkerheds- og compliance-niveau"* (Nielsen et al., 2020, s. 4). Til denne del af undersøgelsen har PwC spurgt ind de højest prioriterede investeringer inden for cyber- og informationssikkerhed. Ligesom resten af undersøgelsen ender fokus primært på medarbejderne samt deres kompetencer og bevidsthed, hvor 54 pct. af respondenterne har awareness-træning som en af de højeste prioriteter. Yderligere er henholdsvis privilegeret adgangsstyring (PAM) og 'identity & access management' (IAM) højt prioriteret af 30-32 pct. af respondenterne. PAM og IAM handler overordnet om fordeling og kontrol af adgang til en virksomheds infrastruktur. Forståelse af en virksomheds mere tekniske

IT-sikkerhedsrelaterede implementeringer forventes at kræve inddragelsen af en IT-revisor, da den finansielle revisor ikke kan forventes at have de nødvendige kompetencer på området.

13.3 Delkonklusion

Opsummerende kan det fastslås ud fra både interviewet af Tolborg og PwC's Cybercrime Survey 2020, at cyberkriminalitet i høj grad søger at udnytte menneskelige fejl. Ligeledes ser fokus ud til at være rettet mod det menneskelige aspekt fra virksomhedernes side, hvor den primære investering i cybersikkerhed omhandler medarbejdernes awareness og kompetencer. PwC's undersøgelse viser, at 58 pct. af virksomheder har været udsat for sikkerhedshændelser, hvilket er det højeste i fire år. Yderligere har 70 pct. af virksomheder oplevet forsøg på phishing angreb, hvorunder 35 pct. af disse er relateret til COVID-19. I forhold til virksomhedernes fokus på medarbejderne fremgår det, at 69 pct. af respondenterne mener, at ansattes ubevidste handlinger udgør en af de største IT-relaterede trusler. I forlængelse heraf er den højest prioriterede investering i cyber- og informationssikkerheds af 54 pct. af virksomhederne, investering i awareness-træning.

Med udgangspunkt i undersøgelsen samt anbefalingerne i god IT-skik kan der identificeres flere områder med potentiel relevans for revisor og revision af IT. Særligt det store fokus på medarbejdernes kompetencer øger værdien af at få indsigt i det IT-relaterede kontrolmiljø. Forståelse af kontrolmiljøet er en væsentlig del af ISA 315, og forventes at have betydelig indflydelse på revisors risikovurdering i henhold til cybersikkerhed. Gennem forespørgsler og inspektion af dokumenter bør revisor få en generel forståelse af virksomhedens IT-kontrolmiljø. På baggrund af Cybercrime Survey 2020, kan der gives eksempler på områder revisor kan undersøge og kontrollere. Disse er blandt andet, undersøgelse af procedurer der hjælper medarbejderne mod phishingforsøg, verificering af sikkerhedspolitiske tiltag er implementeret og undersøgelse af backup planer mv.

14 Komparativ analyse af COSO og COBIT

Dette afsnit omfatter en analyse af COSO og COBIT, og har til formål at sammenholde de to modeller med udviklingen inden for anvendelsen af IT, samt tendensen til cyberangreb hos virksomhederne. Endvidere omfatter afsnittet en belysning af, hvor modellerne er relevante at anvende samt i hvilken forbindelse.

Udviklingen inden for anvendelsen af IT i virksomhederne, har betydet, at virksomhederne i langt højere grad, er i risiko for at blive udsat for cyberkriminalitet. Derfor er der opstået et større behov for intern kontrol af IT i virksomhederne, med formål om at mindske risikoen for at blive ramt af cyberangreb. Revisors arbejde har ligeledes udviklet sig, hvor fokusset har flyttet sig fra kontrol af regnskabsmæssige transaktioner til kontrol af alle lag i virksomheden, med fokus på områder som udgør en væsentlig risiko for regnskabet.

På baggrund af dette, kan der argumenteres for, at revisor i et omfang bør inddrage IT i revisionen af virksomhederne. Dette skyldes, at den nævnte udvikling inden for anvendelsen af IT og den stigende tendens til cyberangreb, udgør en væsentlig risiko for virksomhederne og dermed bør udgøre en væsentlig del af revisors fokus.

COSO er som tidligere nævnt en model, der anvendes til intern kontrol, som i begrebsrammen defineres således: *"Intern kontrol er en process, der finder anvendelse på virksomhedens bestyrelse, ledelse samt øvrige personale og har til formål at give en rimelig sikkerhed for, at de målsætninger, der er forbundet med drift, rapportering og overholdelse nås".* Denne definition er meget anerkendt og er blandt andet indført i ISA 315, hvor den danner grundlag for fortolkningen af intern kontrol, jf. ISA 315 pkt. 4, c. Endvidere er COSO's begrebsramme i høj grad indført i de internationale standarder (Den Europæiske Revisionsret, 2016, s. 31).

COSO's formål om at identificere potentielle begivenheder, som kan påvirke virksomheden, underbygger argumentet om, at IT bør indgå som en del af almindelig revision. Eftersom der i modellen er fokus på at identificere begivenheder, som kan påvirke virksomheden, hvilket et manglende fokus på cyberangreb samt IT-sikkerhed kan.
Begrebsrammen opdateres og tilpasses løbende, således at den harmonerer med udviklingen i virksomhederne samt tendenser som kan have betydning for virksomheden.
I 2013 blev interne kontroller af IT indført som en del af COSO, herunder i det 11. Princip:

"The organization selects and develops general control activities over technology to support the achievement of objectives" (COSO, 2013, s. 7).

Ifølge det 11. princip bør ledelsen fastsætte behovet samt forbindelsen mellem forretningsprocesser, automatiserede kontrolaktiviteter og generelle IT-kontroller. Derudover bør ledelsen udvikle kontrolaktiviteter, til at sikre fuldstændighed, nøjagtighed og tilgængelighed af IT-anvendelsen med formål om at begrænse adgangen til virksomhedens netværk til autoriserede brugere, for at beskytte aktiver mod eksterne trusler (D'Aquila, 2013). COSO blev desuden opdateret i 2017 og udvidet fra de eksisterende 17 principper til 20 principper, med et langt større fokus på cybersikkerhed. Dette skyldes udviklingen inden for cyberrisici og -management. Hvor det vurderes, at der er et større behov, for at sikre IT i virksomhederne, grundet de store konsekvenser cyberangreb kan have (COSO, 2019, s. 2).

Eftersom COSO's begrebsramme i langt højere grad har fokus på IT-kontroller, er det relevant, at revisorers fokus ligeledes ændrer sig hertil. Årsagen til dette, er at ved en implementering af mere IT-kontrol i virksomhederne, kan der opstå et større behov for at sikre, at virksomhedens kontroller lever op til det nødvendige, for at undgå cyberangreb. Kontrolbaseret revision medfører, en hurtigere identifikation af svagheder, som derfor kan rapporteres til ledelsen (Berthing, 2021).

Ifølge COSO's komponent *'Control Environment'* udgør virksomhedens interne miljø fundamentet for risikohåndtering og omfatter hvordan risici identificeres, vurderes og håndteres. Dermed er miljøet i en virksomhed, en afgørende faktor for risici forbundet med cyberangreb. Dette kan mindskes ved, at virksomheden anvender kontrolaktiviteter, overvågningsaktiviteter samt informations- og kommunikationssystemer rettet mod IT-sikkerhed. *'Control Activities'*, omfatter procedurer, som virksomhederne anvender til at afdække mulige risici. I denne komponent, er det relevant for virksomheden at indføre kontrolaktiviteter, som er målrettet IT-sikkerhed, med formål om at mindske risikoen for cyberangreb. *'Information and communication'* og *'Monitoring Activities'* omfatter kommunikation af information om mulige risici samt overvågning af tilstedeværelsen og kvaliteten af risk management processen i virksomheden. Disse to komponenter er ligesom ovenstående komponent relevante i forbindelse med IT-sikkerhed, da der er behov for at sikre, at informationsniveauet og kommunikationen omkring risici i de enkelte virksomheder. Endvidere anses det at være af stor betydning, at virksomhederne har fokus på

overvågningsaktiviteter, som har til formål at sikre, at risk management processen i virksomheden er tilstrækkelig, samt at kvaliteten og tilstedeværelsen af processen hænger sammen med risikoniveauet.

Endeligt anses komponenten *'Risk Assessment'*, ligeledes som relevant i henhold til IT-sikkerhed. Dette skyldes, at det er en nødvendighed at virksomheden vurderer de interne kontroller, som har til formål at identificere IT- og cyberrisici. Det er ligeledes relevant at fastsætte et risikoniveau, som passer til virksomheden, da dette er med til at sikre, at mulige begivenheder ikke påvirker virksomhedens målopfyldelse. Dermed kan der med fordel tages højde for vurdering af IT-sikkerhed i denne sammenhæng, da et muligt cyberangreb kan påvirke virksomhedens mulighed for at opnå fastsatte mål.

Der kan på baggrund af ovenstående argumenteres for, at der er et stort behov for intern kontrol af IT i virksomhederne. Dette behov er udledt af den stigende anvendelse af IT, hvortil det anses, som værende nødvendigt, for virksomhederne at have et større fokus herpå.
Der kan på baggrund af dette argumenteres for, at revisorers arbejde bør følge udviklingen i COSO til et større fokus på IT-kontrol. Årsagen til dette, er at ved en implementering af mere IT-kontrol i virksomhederne, kan der opstå et større behov for at sikre, at virksomhedens kontroller lever op til det nødvendige, for at mindske risikoen for cyberangreb. Dette understøttes af Tolborgs udtalelse om, at der er et behov for at IT-revision anvendes til at bekræfte at risikoen for cyberkriminalitet er reduceret til et passende niveau, eller hvis det ikke er tilfældet, at anbefale tiltag, som kan styrke cybersikkerheden (Tolborg, 2021).

COBIT 5 omfatter et specificeret fokus på IT i virksomheder. Modellen har til formål at muliggøre styring af virksomheds-IT samt at optimere risikoniveauer i forbindelse med dette. De fem principper som modellen omfatter, har tilsammen et formål om at give virksomhederne mulighed for, at opbygge en effektiv ramme for governance og management. Disse to områder vil ved en effektivisering optimere informations- og teknologiinvesteringer og -brug, som er til gavn for virksomhedens interessenter.

COBIT 5 opererer ud fra ISO-standarderne, hvoraf ISO/IEC 27001, den internationale standard for Information Security Management System (ISMS), samt ISO/IEC 27002, er fokusset i specialet. ISO/IEC 27002 har til formål at hjælpe organisationer med at opfylde alle deres

informationsrelaterede overholdelsesmål. Det vil sige, at denne standard giver virksomhederne, nogle værktøjer, til at styrke informationssikkerheden (Calder, 2013, s. 2).

ISO/IEC 27001 omfatter et ledelsessystem for informationssikkerhed. Ifølge standarden er informationssikkerhed et ledelsesansvar på linje med økonomistyring, arbejdsmiljø, service og borgerbetjening. Der stilles krav til, at der er en række styringsaktiviteter til stede, dertil gælder, at ledelsen skal engagere sig systematisk i organisationens informationssikkerhed (Sikkerdigital, u.å., ¶ Ledelsessystem for informationssikkerhed (ISMS)).
ISO/IEC 27002 er med til at sikre, at virksomheden udvælger passende foranstaltninger til beskyttelse af informationer, som led i eksempelvis etableringen af et ledelsessystem for information (ISMS) efter ISO/ICE 27001 (Dansk Standard, u.å., ¶ Whitepaper ISO/IEC 27002).

COBIT understreger, at IT-revision kan være et specifikt og komplekst område, hvor der kan kræves særlige kompetencer, som derfor ikke er en del af almindelig virksomhedsstrategi samt en del af revisors almindelige opgaver og dermed ikke som en del af den generelle revision. Dette kan medføre en ulighed i forbindelse med den stigende anvendelse af IT i virksomhederne, hvorfor virksomheder i langt større grad er udsat for risici, som kan have store konsekvenser, såfremt drift eller økonomi er afhængig af IT-systemer. På baggrund af dette kan der argumenteres for, at der er behov for at indføre IT som en del af den generelle revision, samt som en del af virksomhedsstrategi som helhed. Dette underbygges af udviklingen i COSO i henhold til det større fokus på IT i de generelle kontroller, da det er en indikator for at behovet for IT-kontroller er stigende.

COSO's begrebsramme som omfatter intern kontrol som helhed i virksomhederne, henvender sig til den generelle revision og dermed de revisorer, som udfører denne (Berthing, 2021). Dermed kan der være behov for at revisorernes viden samt fokus på IT-kontroller til at mindske fejl i IT-systemerne samt cyberangreb, udvikles. Der kan dog på baggrund af COBIT's specifikke fokus på IT-kontroller argumenteres for, at der ligeledes er behov for IT-revisor i forbindelse med revision af virksomheder, hvor IT-systemerne er mere komplekse. Dette stemmer overens med Berthings udtalelse om at COBIT som udgangspunkt en model der anvendes af IT-revisorer med særlige IT-kompetencer. Problemstillingen kan ligge i om COBIT, ligesom IT-revisorer, anvendes tilstrækkeligt i forbindelse med revisionen (Berthing, 2021).

14.1 Delkonklusion

COSO's begrebsramme som omfatter interne kontroller i virksomheder har det formål at identificere risici samt håndterer disse ud fra virksomhedens risikoappetit. Dette skal ifølge modellen sikre målopfyldelse i virksomhederne.

COBIT har modsat COSO et mere specificeret fokus på IT, hvor modellen udelukkende omhandler virksomheds-IT. COBIT anses til at være en model, som kan og bør anvendes af IT-revisorer, i forbindelse med IT-revision af mere komplekse IT-systemer samt virksomheder med særlige krav til IT. Hvor COSO's mere brede tilgang til interne kontroller generelt i virksomheden anvendes til den finansielle revisor.

Tilgangen i COSO har gennem tiden ændret sig til at omfatte IT i højere grad. Dette skyldes den konstant stigende risiko for cyberangreb, særligt i forbindelse med at langt flere virksomheder anvender IT.
Dermed anses det som værende nødvendigt, at revisorerne har et større fokus på IT-revision, end på nuværende tidspunkt, hvor IT kun indgår i mindre grad af revisionen. Dette skyldes, at COSO's fokus på potentielle begivenheder, som kan påvirke virksomheder, anses at stemme overens med de risici, som anvendelsen af IT medfører. Hertil kan nævnes den stigende tendens til cyberangreb, hvor en stor del virksomheder har oplevet cyberangreb i mindre eller større omfang og at risikoen for cyberangreb er stigende. Dermed anses det som værende væsentligt, at IT-kontroller bliver indført, i den generelle virksomhedsstrategi samt revisionsstrategien.

15 Revisionsprocessen med udgangspunkt i IT-revision

Udviklingen indenfor anvendelsen af IT i virksomhederne, samt udviklingen i cyberkriminalitet og -risici har som nævnt skabt et større behov for IT-sikkerhed samt revision af virksomhedernes interne IT-kontroller. Med udgangspunkt i dette omfatter nedenstående afsnit revisionsprocessen i forbindelsen med IT-revision, med formål om at identificere områder, hvor IT-revision kan indgå i den generelle proces.

15.1 Planlægning

15.1.1 Inddragelse af IT-specialist

Som det fremgår af ISA 300, skal den finansielle revisor allerede overveje involveringen af specialister/eksperter i planlægningsfasen, i forbindelse med udarbejdelse af revisionsstrategien (ISA 300, A8). Dermed skal den finansielle revisor vurdere behovet, for at involvere en IT-revisor tidligt i processen. Det er endvidere den finansielle revisors ansvar at vurdere om den af revisor udpegede ekspert har de nødvendige kompetencer og færdigheder til formålet, jf. ISA 620, afsnit 9. Derfor er det nødvendigt at den finansielle revisor har viden nok, til at sikre at den rette specialist bliver involveret.

Det er ifølge Berthing nødvendigt, at revisorerne inddrager IT-revisorer generelt i planlægningen. Han mener dog ikke, at det nødvendigvis er IT-revisorer, som skal udføre IT-revisionen, da det ifølge ham er et spørgsmål om at give de finansielle revisorer de rette kompetencegivende færdigheder. Eftersom dette vil være tilstrækkeligt, til at lade de finansielle revisorer afdække IT-risici i forbindelse med udarbejdelsen af det finansielle årsregnskab.

15.1.2 Virksomheden og dens omgivelser

Revisor skal identificere og vurdere risikoen for, at der kan opstå væsentlig fejlinformation i regnskabet både på regnskabsniveau og revisionsmålsniveau. For at revisor kan dette, skal revisor udføre risikovurderingshandlinger, således at der opnås en forståelse af virksomheden og dens omgivelser. De udførte risikovurderingshandlinger er følgende (ISA 315, afsnit 6):

- Forespørgsler

- Analytiske handlinger
- Observationer og inspektion

Ovenstående risikovurderingshandlinger har til formål at skabe en forståelse af virksomhedens mål, strategier og interne kontroller med formål om at give revisor en indikator for hvor stort behovet er for revisionshandlinger på forskellige områder. I denne sammenhæng er det relevant, at revisor foretager forespørgsler som er målrettet virksomhedens IT-kontroller, for at vurdere behovet for IT-revisionshandlinger.

Forespørgsler omfatter indhentning af mundtlige samt skriftlige udtalelser fra den daglige ledelse samt andre relevante medarbejdere, som kan give revisor en forståelse af virksomheden, herunder ledelsens kendskab og forståelse for IT-kontroller (ISA 315, afsnit 6, A6-A13).

De analytiske handlinger kan være med til at identificere områder i virksomheden, som revisor ikke havde kendskab til og kan dermed bidrage til vurderingen af risici for væsentlig fejlinformation med henblik på at mindske disse (ISA 315, A7).

Endeligt har observationer og inspektion til formål, at understøtte revisors forespørgsler, hvilket sker ved, at revisor observerer virksomhedens væsentlige aktiviteter vedrørende IT i virksomheden (ISA 315, A18).

15.1.3 Virksomhedens interne IT-kontroller

Den finansielle revisor skal, jf. ISA 315, afsnit 12, opnå en forståelse af virksomhedens interne kontroller, som er relevante for revisionen. Det vil sige, at det er op til revisor at vurdere hvorvidt der er behov for udførelse af IT-revision. Ifølge Berthing bør IT-revision indgå i revision af virksomheder, i langt højere grad end hvad det gør på nuværende tidspunkt. Han mener, at finansielle revisorer ikke inddrager IT-revision samt IT-revisor i det omfang det er nødvendigt. Dette argument understøttes, af interviewet med Thomas Gi Scharf, som ligeledes mener, at IT-revision ikke anvendes i tilstrækkelig grad (Gi Scharf, 2021).

Ved opnåelse af forståelse af virksomhedens interne kontroller, skal følgende kontrolkomponenter vurderes:

- Kontrolmiljø

- Selskabets risikovurderingsproces
- Informations- og kommunikationssystemet, herunder tilhørende forretningsprocesser
- Kontrolaktiviteter
- Overvågning af kontroller

Kontrolmiljø

Revisor skal opnå en forståelse af virksomhedens kontrolmiljø, i denne sammenhæng IT-kontrolmiljø, jf. ISA 315, afsnit 14, hvilket som nævnt omfatter opmærksomheden samt tiltag vedrørende virksomhedens interne kontroller blandt ledelsen. Dermed skal revisor undersøge ledelsens kontrolbevidsthed, herunder ledelsens forståelse af virksomhedens data samt ledelsens generelle holdning til IT-kontroller, da dette kan være med til at give revisor et indblik i, hvor høj grad virksomheden anvender IT-kontroller.

Der kan argumenters for, at der er behov for særlige kompetencer, for at kunne forstå samt bearbejde de risici, der medfølger ved anvendelsen af IT. Derfor kan det være nødvendigt, såfremt det konstateres, at IT-kontrolmiljøet er for komplekst og af væsentlig betydning for regnskabsaflæggelsen, at revisor involverer en IT-revisor i revisionsprocessen.

Risikovurderingsproces

Under planlægningen skal revisor opnå en forståelse for selskabets risikovurderingsproces. Dette omfatter, at revisor skal undersøge om selskabet har udformet samt implementeret en proces, som fungerer til at identificere forretningsrisici, anslå betydeligheden af risiciene, vurdere sandsynligheder for at risiciene indtræffer og endeligt beslutte hvilke foranstaltninger der skal træffes for at håndtere risiciene (Samuelsen et al., 2019, s. 173).

I denne forbindelse er det relevant at vurdere risici ved anvendelsen af IT. Dette skyldes, at IT medfører en del risici, som nævnt i afsnit 8.1 om ISA 315. Hertil er der skabt en tillid til de anvendte systemer og programmer, som behandler data, hvilket kan være problematisk i sammenhænge hvor data er unøjagtig eller hvor unøjagtige data behandles. Der kan være tale om, at der er uautoriseret adgang til data, som kan medføre ødelæggelse eller ugyldige ændringer af data, hvilket i værste fald kan have konsekvenser for bogføringen. Der er

endvidere en mulighed for, at medarbejdere får adgangsrettigheder, som bryder funktionsadskillelsen mv.

Informations- og kommunikationssystem, herunder tilhørende forretningsprocesser

Det er vigtigt, at revisor opnår en forståelse for informationssystemerne i virksomheden, samt de dertilhørende processer, som kan være relevante for regnskabsaflæggelsen. Dette omfatter blandt andet de procedurer i IT-systemer og manuelle systemer, som anvendes til at igangsætte, registrere samt behandle virksomhedens transaktioner og hvis nødvendigt, efterfølgende overføre dem til finansbogholderiet og afslutningsvist rapportere dem i regnskabet (Samuelsen et al., 2019, s. 173).

Såfremt revisor ikke indhenter tilstrækkeligt med information, for at afdække virksomheden informations- og kommunikationssystemer, er der risiko for, at der kan opstå væsentlig fejl i regnskabet. Mikkel Hede Olsen (2021) påpeger i et interview, at en fundamental fejl i et økonomisystem kan resultere i fejl ved samtlige transaktioner, behandlet af systemet. Dette skyldes, at der kan være fejl i virksomhedens systemer, som i værste fald kan medføre, at revisor ikke kan opnå tilstrækkelig egnet revisionsbevis og dermed ikke kan dokumentere at regnskabet giver et retvisende billede.

Kontrolaktiviteter

Revisor skal opnå en forståelse af de kontrolaktiviteter, der er relevante for revisionen og som ifølge revisor er nødvendige, for at vurdere risiciene for væsentlig fejlinformation på revisionsmålsniveau. Hertil skal revisor, udføre yderligere revisionshandlinger til at afdække de vurderede risici. Dermed skal der opnås en forståelse af virksomhedens kontrolaktiviteter, så revisor får en forståelse for, hvordan virksomheden har reageret på IT-relaterede risici (ISA 315, afsnit 20-21).

Overvågning af kontroller

I forbindelse med revisionen skal der opnås en forståelse af de handlinger, som ledelsen udfører for at overvåge, at selskabet har de rette interne kontroller, som er relevant for regnskabsaflæggelsen, herunder de aktiviteter som er relevante for revisionen. Endvidere skal revisor opnå en forståelse af, hvilke tiltag virksomheden anvender til udbedring af mangler i de interne kontroller. Det er hertil relevant at sikre, at virksomheden overvåger IT-kontroller, da disse er med til at mindske risikoen for fejl i IT-systemerne, som kan medføre fejl i regnskabet. Endvidere er det relevant, at revisor tager stilling til, om virksomheden har fokus på IT-sikkerhed.

15.1.4 Generelle IT-kontroller og applikationskontroller

Som tidligere nævnt omfatter de generelle IT-kontroller politikker samt procedurer, som vedrører mange applikationer og de anvendes i høj grad til at håndtere de risici, som kan opstå ved anvendelsen af IT i virksomhederne. Endvidere har de til formål at sikre, at applikationskontroller fungere effektivt (ISA 315, A108).

Revisor kan med fordel undersøge, i hvilket omfang virksomheden anvender risikostyring i henhold til IT-risici samt cybersikkerhed. Dette kan give revisor en indikator for i hvilket omfang virksomhedens IT udgør en risiko. Det kan ligeledes være relevant, at revisor har særligt fokus på virksomhedens forståelse af cyberrisici, herunder awareness blandt ledelsen og medarbejderne. Revisor kan ydermere undersøge virksomhedens risikovillighed samt hvordan virksomheden prioritere de enkelte risikoområder (Deloitte, 2019, s. 9 og 11).

Ovenstående kan medføre, at det er lettere for revisor at vurdere, hvilke applikationskontroller der skal testes, da revisor har opnået en forståelse af vigtigheden for virksomheden i henhold til de data der formidles samt anvendes, herunder i hvilken grad de er relevante for virksomheden. Dertil kan revisor foreslå forbedringer, endvidere såfremt virksomheden har vurderer sin risikoappetit, i henhold til hvad der er råd til at miste og ikke er. Dette kan medføre en mere effektiv revision, dog skal revisor være kritisk og teste kontroller, som revisor vurderer til at være relevante.

15.1.5 Risikovurdering

I forbindelse med en revision skal revisor foretage en risikovurdering. I denne sammenhæng kan det være relevant, at revisor foretager risikovurdering i henhold til IT-risici for virksomheden, eftersom potentielle fejl i IT-systemet, kan have betydning for regnskabet og virksomheden. Revisors vurdering foretages med udgangspunkt i revisionsrisikomodellen, hvor revisor forsøger at identificere konkrete risici på revisionsmålsniveau, hvoraf der foretages en vurdering af iboende risiko og kontrolrisiko, herunder den samlede risiko pr. Revisionsmål. Formålet med dette er at begrænse revisionsrisikoen til det acceptable niveau for revisionen som helhed.

Revisionsrisikoen udgør risikoen for at revisor afgiver en påtegning uden forbehold på et regnskab, som indeholder væsentlige fejl, samt risikoen for at påtegningen med forbehold gives på et regnskab uden væsentlige fejl. Revisionsrisikoen kan reduceres, ved at revisor udfører en nøjagtig vurdering af den iboende risiko, ved at reducere kontrolrisikoen gennem udvidet gennemgang og test af kontroller, samt ved at reducere opdagelsesrisikoen gennem en øget mængde substansrevision.

Den iboende risiko afhænger af virksomhedens IT-sikkerhed, herunder hvor stort et fokus virksomheden har på området og dermed er den upåvirkelig af revisor. Kontrolrisikoen er et udtryk for virksomhedens kontroller til at afdække den iboende risiko, hvilken revisor anses at have en indirekte indflydelse på, gennem test samt gennemgang heraf. Dette kan medføre en problematik i henhold til at mindske revisionsrisikoen, da revisorerne ifølge spørgeskemaundersøgelsen i lav grad udfører kontrolhandlinger i forbindelse med IT, dermed kan kontrolrisikoen ikke mindskes tilstrækkeligt og revisor kan ikke opnå en høj grad af sikkerhed for at regnskabet giver et retvisende billede. Revisors indflydelse på opdagelsesrisikoen, kan vurderes på baggrund af kompleksiteten i virksomhedens IT-systemer samt -risici forbundet med virksomheden. Det vil sige, at virksomheder, hvor IT indgår som en væsentlig del, kan opdagelsesrisikoen være høj, såfremt der tages udgangspunkt i spørgeskemaundersøgelsen.

15.2 Løbende revision

Dette afsnit omfatter løbende revision, med et udelukkende fokus på revisors reaktion på vurderede IT-risici samt kommunikationen til ledelsen i forbindelse med IT-revision

15.2.1 Revisors reaktion på vurderede risici

Revisors håndtering af vurderede risici fremgår af ISA 330 og omfatter at revisor skal imødekomme de identificerede risikofaktorer ved at tilrettelægge passende revisionshandlinger (ISA 330, afsnit 3).

Test af kontroller udføres for at opnå tilstrækkeligt og egnet revisionsbevis i tilfælde, hvor revisor forventer at kontrollerne fungerer effektivt (ISA 330, afsnit 8). Hertil gælder, at jo større tillid revisor har til kontrollernes effektivitet, desto stærkere revisionsbevis skal der opnås (ISA 330, afsnit 9). Endvidere skal der udføres test af kontroller, såfremt substanshandlinger alene ikke kan give tilstrækkeligt og egnet revisionsbevis på revisionsmålsniveau (ISA 330, afsnit 8). Dette kan opstå ved at en virksomhed anvender IT-systemer til drift, hvor der ikke udarbejdes eller opbevares dokumentation for transaktionerne på anden måde end gennem det anvendte IT-system.

I forbindelse med den tidsmæssige placering af test af virksomheders IT-kontroller er det væsentligt, at revisor vurderer omfanget af risici forbundet hertil tidligt i processen. Dette skyldes, at der kan være behov for en mere omfattende IT-revision, hvor det kan være nødvendigt med yderligere revisionshandlinger. Det kan i denne sammenhæng ifølge Berthing, være væsentligt at vurdere om det er nødvendigt, at anvende en IT-revisor til test af kontroller. Årsagen er ligeledes kompleksiteten i IT-revisionen, som kan nå ud over revisorers viden på området (Berthing, 2021).

Omfanget af de nødvendige revisionshandlinger fastlægges efter væsentligheden, de vurderede risici samt graden af sikkerhed som revisor planlægger at opnå. Hertil vurderes omfanget af stikprøvestørrelsen, hvilken som udgangspunkt er afhængig af revisors overvejelser i henhold til (ISA 330, afsnit 10, A28):

- Hvor ofte virksomheden udfører kontroller i perioden

- Hvilken form for kontroller der er tale om. Hermed da manuelle kontroller er forbundet med mere omfattende test, end automatiske kontroller. Dette skyldes, at der er en større risiko for menneskelige fejl.

Som nævnt i afsnit 6 om informations- og cybersikkerhed udgør de menneskelige fejl en stor risiko i forbindelse med IT- og cyberrisici. Dermed er det væsentligt, at revisor har fokus på, om virksomhedens kontroller er manuelle, da dette vil kræve yderligere revisionshandlinger.

Såfremt virksomheden outsourcer væsentlige områder til eksterne leverandører, eksempelvis IT-kontroller. Skal revisor undersøge om der er en 3402 erklæring samt i hvilket omfang og hvor ofte virksomheden kommunikerer med IT-leverandøren, herunder i hvilken kontekst. Denne kontekst bør være i henhold til ændringer i virksomheden, som kan være relevant i forhold til virksomhedens IT. Endvidere kan virksomheden med fordel holde sig opdateret på antallet samt omfanget cyber indbrud og -angreb (Deloitte, 2019, s. 15).

I forbindelse med de udførte revisionshandlinger skal revisor dokumentere iagttagelser samt bemærkninger, som kan have betydning for revisors konklusion omkring virksomhedens kontroller. De gennemførte test har et formål om at konkludere om IT-kontrollerne er effektive eller ineffektive. Såfremt der er tale om ineffektive IT-kontroller, kan det betyde, at der væsentlige mangler i virksomhederne interne IT-kontrol (ISA 330, 28-30). Et eksempel herpå kan være tidligere testede IT-kontroller, som er vurderet til at være ineffektive og som ikke er udbedret af ledelsen.

I tilfælde af at revisor finder væsentlige mangler i de interne IT-kontroller, skal revisor revurdere den overordnede revisionsstrategi og tilpasse den planlagte revision efter balancedagen, udvide og risikorette revisionen samt rapportere manglerne til ledelsen (Samuelsen et al., 2019, s. 241).

15.2.2 Rapportering til ledelsen

Gennem revisionsprocessen skal revisor kommunikere med ledelsen omkring områder, der vedrører revisionen, med formål om at forstå de pågældende forhold, indhente information fra den øverste ledelse, som er relevant for revisionen samt kommunikere om forhold, som ledelsen skal have mulighed for at ændre og dermed leve op til sit ansvar (ISA 260, afsnit 4).

Det vurderes som tidligere nævnt, at IT er omfattet af de generelle bestemmelser, hvorfor revisor skal kommunikere omkring det planlagte omfang samt den tidsmæssige placering af revisionen i henhold til IT (ISA 260, afsnit 15). Denne vurdering understøttes af, at revisor jf. ISA 260, afsnit 15, skal kommunikere om de betydelige risici som revisor har identificeret. Dette skyldes udviklingen inden for anvendelsen af IT, samt omfanget af cyberangreb i virksomheder. Virksomheder kan blive udsat for cyberangreb, sikkerhedsbrud, IT-nedbrud mv., som kan have alvorlige konsekvenser på sigt. Dermed kan det give mening, at revisor spørger ind til virksomhedens cyber respons procedure, i henhold til om virksomheden har beredskabsplaner som skal være med til at sikre, at virksomheden kan håndtere situationer, hvor eksempelvis leverandører eller fragtmænd bliver ramt af cyberangreb, som kan betyde, at virksomheden ikke kan producere sine vare, eller har backup procedurer samt distribuere sine varer (Gi Scharf, 2021).

Som nævnt skal revisor rapportere til ledelsen, i tilfælde hvor det er vurderet at virksomhedens interne kontroller er mangelfulde. Dette er særligt relevant ved IT-kontroller i virksomheder, hvor omsætningen er afhængig af IT eller i virksomheder, som bliver udsat for cyberangreb i form af ransomware, hvor virksomhederne bliver afpresset til at betale store summer. Dette skyldes, at virksomheder, som er udsat for et vellykket cyberangreb i løbet af kort tid efter angrebet, kan være nødsaget til at lukke, grundet for store økonomiske tab (Berthing, 2021).

Jf. ISA 265, afsnit 11(a), skal revisor i forbindelse med kommunikation til ledelsen, beskrive manglerne samt dertilhørende potentielle konsekvenser. Særligt i situationer hvor der er kan identificeres sårbarhed over for cyberkriminalitet, kan en forklaring heraf være værdiskabende for virksomheden. Såfremt revisor kan forklare ovenstående risici og komme med løsningsforslag, vil dette muliggøre en reduktion af denne risiko.

15.3 Afslutning på revisionen

15.3.1 Fortsat drift af virksomheden

Som afslutning på revisionen skal revisor på baggrund af det opnåede revisionsbevis vurdere om virksomheden opfylder forudsætningen om going concern, herunder fortsat drift (ISA 570, afsnit 2). Revisor skal konkludere, om der er væsentlig usikkerhed i relation til begivenheder eller forhold, som kan skabe betydelig tvivl om evnen til fortsat drift af virksomheden (ISA 570, afsnit 9). Af driftsforhold som kan have betydning for om virksomheden kan fortsætte driften, kan eksempelvis være væsentlige driftstab eller forringelsen af værdien af aktiver i virksomheden (Samuelsen et al., 2019, s. 173). Hertil kan det vurderes, at cyberangreb i værste fald kan have en betydning for om virksomheden kan fortsætte driften.

15.3.2 Revisors konklusion

I forbindelse med afslutningen på revisionen skal revisor afgive en påtegning, som indeholder en konklusion om, der er opnået en høj grad af sikkerhed for, at der ikke er væsentlig fejlinformation.

Revisor kan afgive følgende konklusioner (Samuelsen et al., 2019, s. 425):

- Konklusion uden forbehold
- Konklusion med forbehold
- Afkræftende konklusion
- Ingen konklusion

Revisor skal afgive en konklusion uden forbehold, når det konkluderes, at regnskabet er udarbejdet i overensstemmelse med den relevante regnskabsmæssige begrebsramme. Konkluderes det derimod at regnskabet som helhed indeholder væsentlig fejlinformation eller er revisor ikke i stand til at opnå tilstrækkeligt og egnet revisionsbevis til at konkludere, at regnskabet som helhed ikke indeholder væsentlig fejlinformation, skal revisor afgive en konklusion med forbehold (ISA 700, afsnit 16). Den afkræftende konklusion anvendes i tilfælde hvor revisor, efter at have opnået tilstrækkeligt og egnet revisionsbevis vurderer, at fejlinformationer er både væsentlige og gennemgribende for regnskabet (ISA 705, afsnit 8). Endeligt anvendes den manglende konklusion, når revisor er ude af stand til at opnå

tilstrækkeligt og egnet revisionsbevis, og hvor uopdagede fejlinformationer kan være både væsentlige og gennemgribende (ISA 705, afsnit 9).

I forbindelse med IT-revision, kan der opstå fejl i virksomhedens IT-systemer, som eksempelvis har med bogføringen at gøre eller andre økonomiske formål. Disse fejl kan i værste fald medføre en fejl i regnskabet. Danske Banks IT-chef Dorthe Tolborg mener, at: *"Ultimativt kan det retvisende billede påvirkes, hvis IT-systemer som understøtter økonomirapporteringen, ikke er opdaterede og/eller generer fejl"*. Det er derfor relevant, at der udføres kontrol af at data overføres fra et sted til et andet fuldstændigt, nøjagtigt og rettidigt (Tolborg, 2021). Dermed kan det påvirke det retvisende billede, hvis der opstår fejl som er af et væsentligt omfang. Foretager virksomheden ikke de rette kontroller, skal revisor rapportere til ledelsen og vælger ledelsen ikke at ændre forholdene, skal revisor afgive en konklusion med forbehold.

Endvidere kan der være tale om virksomheder som har været udsat for cyberangreb, men som ikke omtaler truslen samt angrebene i årsrapporten, herunder muligheden for fortsat drift af virksomheden, skal revisor ifølge Berthing tage forbehold samt omtale dette i påtegningen.

15.4 Delkonklusion

Gennem hele revisionsprocessen er det relevant, at revisor har fokus på IT, hertil kan det være relevant at inddrage en IT-specialist allerede i planlægningsfasen, da dette kan være med til at sikre, at der tidligt i processen vurderes om virksomhedens IT er så kompleks, at det er nødvendigt med en IT-revisor. Dette betyder ikke, at det nødvendigvis er IT-revisoren, som skal udføre IT-revisionen, men derimod kan revisor i et vist omfang udføre handlingerne i forbindelse med IT. Det er dog relevant, at revisor er klædt ordentlig på til at udføre handlingerne.

Under identificeringen og vurderingen af risikoen for væsentlig fejlinformation, er det relevant at revisor foretager forespørgsler målrettet virksomhedens IT-kontroller, med formål om at vurdere behovet for IT-revisionshandlinger. I den sammenhæng kan revisor med fordel undersøge ledelsens kendskab samt forståelse for IT-kontroller. Dette skyldes, at det kan give en indikator for, i hvilket omfang ledelsen har fokus på IT-kontroller samt hvor vigtigt ledelsen vurderer IT-kontrollerne til at være. Hertil bør revisor foretage analytiske handlinger samt

observationer og inspektioner af aktiviteter vedrørende IT i virksomheden. Dette stemmer overens med at revisor skal opnå en forståelse af virksomhedens kontrolmiljø og dermed ledelsens kontrolbevidsthed. Endvidere kan denne tilgang anses som værende i overensstemmelse med revisors opgave om at opnå en forståelse af selskabets risikovurderingsproces, da der opnås en større forståelse af hvordan virksomheden håndterer de identificerede risici.

Det er især relevant i forbindelse med risici for væsentlig fejlinformation i regnskabet, at revisor er opmærksom på virksomhedens informations- og kommunikationssystemer, herunder de IT-systemer, samt manuelle processer der anvendes i virksomheden. Dette skyldes, at der eksempelvis i IT-systemerne kan opstå fejl, som overføres til regnskabet, og dermed giver et forkert billede af virksomhedens situation. Endvidere kan der opstå fejl i de manuelle processer, hvor de menneskelige fejl spiller en rolle. Revisor bør derfor overveje test og overvågning af kontrolaktiviteter i forbindelse med IT, da dette kan mindske risikoen for fejl.

Det er ligeledes relevant, at revisor kan foretage en vurdering af virksomhedens risikovillighed i forbindelse med IT-risici. Dermed kan revisor lettere vurdere, hvilke data og IT-systemer der er tilknyttet mest risici, og således prioritere sine revisionshandlinger. På baggrund af denne vurdering kan revisor overveje involveringen af en IT-revisor, hvilket kan være aktuelt, da kompleksiteten i IT-revisionen kan omfatte yderligere kompetencer inden for IT og dermed en specialist på området.

Omfanget af de nødvendige revisionshandlinger fastsættes efter væsentligheden, de vurderede risici samt graden af sikkerhed som revisor planlægger at opnå. Det kan endvidere være nødvendigt at undersøge, om virksomheden outsourcer væsentlige IT-kontroller til eksterne leverandører, med formål om at undersøge kommunikationen mellem virksomheden og leverandøren. Formålet med revisionshandlingerne er at undersøge om der er væsentlige mangler i de interne IT-kontroller. Såfremt revisor opdager væsentlige fejl, skal disse rapporteres til ledelsen, da IT vurderes til at være omfattet af de generelle bestemmelser i ISA 260 samt ISA 265. Det kan i den sammenhæng være relevant, at revisor kommunikerer med ledelsen omkring IT-risici og cyberrisici, eftersom det kan have store konsekvenser for virksomheden, hvis ikke virksomheden har fokus på disse områder.

Det vurderes endvidere, at IT-risici samt cyberangreb er en del af de generelle bestemmelser i ISA 570 om going concern. Dette skyldes, at virksomheder i værste fald kan risikere at virksomheden ikke kan fortsætte driften, såfremt den udsættes for cyberangreb. Derudover anses det som særligt relevant, at revisor gennem hele processen har fokus på virksomhedens IT-kontroller, eftersom det kan være med til at mindske IT-fejl, som kan have betydning det retvisende billede af regnskabet.

Endeligt skal revisor på baggrund af det opnåede revisionsbevis, samt vurderingen om fortsat drift afgive en påtegning med en konklusion i henhold til om der er opnået høj grad af sikkerhed for at der ikke er væsentlig fejlinformation i regnskabet. Hertil kan revisor vurdere om, der er fejl i virksomhedens IT- samt manuelle systemer, som kan medføre fejl i regnskabet, hvortil det er relevant af afgive en konklusion med forbehold, såfremt fejlen ikke rettes af ledelsen. Endvidere kan det være relevant at undersøge om virksomheden har været udsat for cyberangreb, som kan påvirke evnen til fortsat drift af virksomheden. Årsagen hertil er, at dette bør indgå i årsrapporten, da det kan have en betydning for det reelle billede af virksomheden, derfor kan revisor tage forbehold, i tilfælde hvor virksomheden ikke omtaler dette.

16 Komparativ analyse af ISA 315 og den reviderede ISO 27002

Følgende afsnit tager udgangspunkt i en besvarelse af egen spørgeskemaundersøgelse af spørgsmålet omkring hvad der bør indgå i ISA-standarderne i henhold til IT-revision. Denne besvarelse foreslår, at der bør indgå henvisninger til eksempelvis ISO 27001 standarderne, således at det er eksperter der tager stilling til udvikling i IT-sikkerhedsnormerne. Derfor søger afsnittet at skabe en overordnet sammenligning af ISA 315 og ISO 27002, hvortil den kommende opdatering af ISO-standarden analyseres i forhold til hvordan den kan anvendes af revisor.

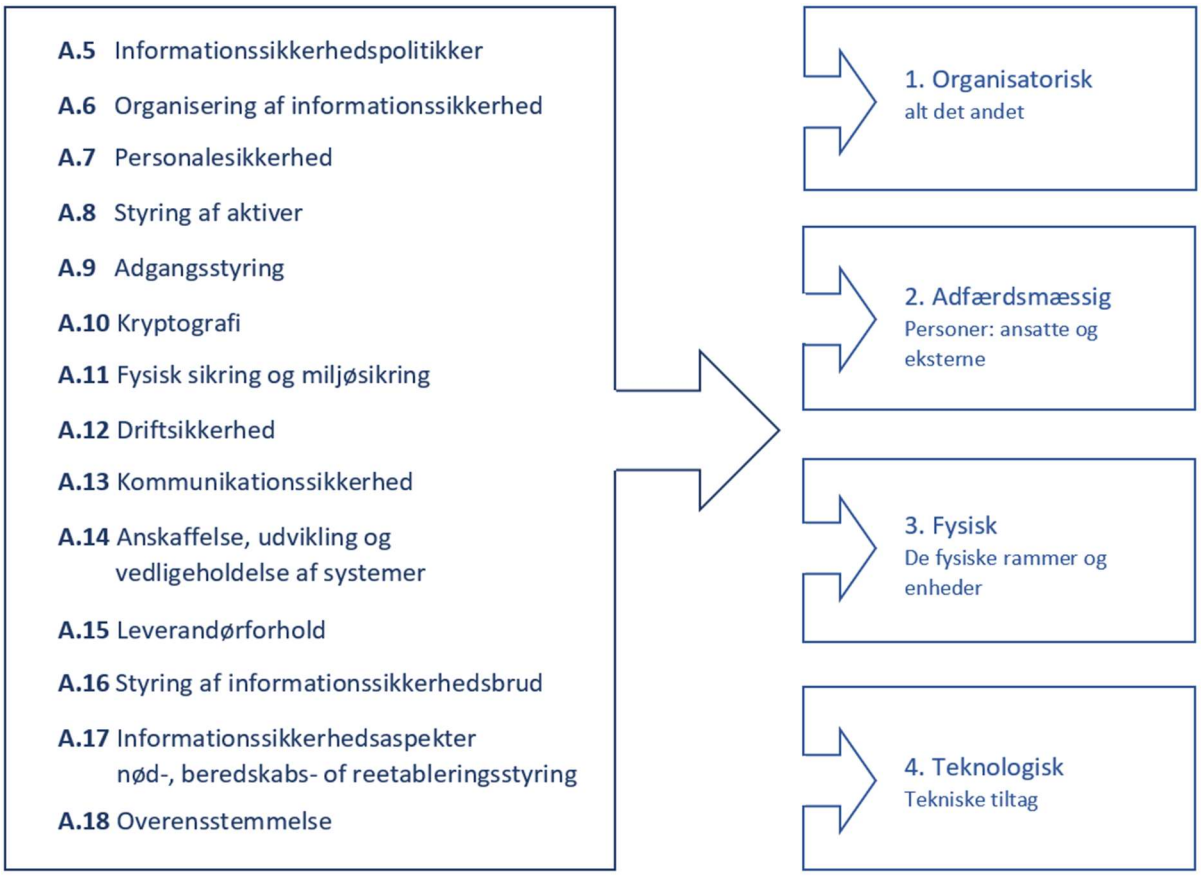
I afsnit 8.1 er det beskrevet, at ISA 315 integreret indeholder en beskrivelse af hvordan revisor skal opnå forståelse af virksomhedens IT. Den integrerede natur af denne beskrivelse betyder, at de IT-relaterede krav til revisor er relativt overordnede, da fokus primært er på den samlede forståelse af virksomheden. Grundet den stigende anvendelse af IT i virksomhederne sammenholdt med den stigende cybertrussel, kan det være fordelagtigt at udvide revisorernes kompetencer inden for IT-sikkerhed og risici. Alternativt skabe nogle mere dybdegående ressourcer

og vejledninger, således revisor lettere kan vurdere alvorligheden af cyberrisici. Dette stemmer overens med den generelle holdning i egen udarbejdet spørgeskemaundersøgelse omkring mangler i ISA 315, hvoraf 40 pct. af respondenterne påpeger mangel på handlinger målrettet cyberkriminalitet. For uddybende at forstå hvilke begrænsninger der er ved ISA 315 i relation til cyberrisici, sammenholdes standarden med Dansk Standards (2021) whitepaper om ISO/IEC 27002.

Det generelle formål med ISO/IEC 27002 i afsnit 14, hvor standarden beskrives som en vejledning til virksomheder med fokus på udvælgelse og implementeringen af foranstaltninger vedrørende informationssikkerhed. Yderligere er det væsentligt at den seneste udgave af ISO 27002 blev udgivet i 2013, hvorfor på skrivende tidspunkt revideres og forventes udgivet i løbet af 2021 (Dansk Standard, 2021, s. 2). På baggrund af den kommende opdatering, vil afsnittet tage udgangspunkt i et whitepaper, frem for den ældre udgave af standarden.

Formålet med de to standarder er forskelligartede, hvorfor standardernes fremgangsmåde til håndtering af henholdsvis IT-kontroller og foranstaltninger ligeledes er forskellig. Ud fra ISA 315 er det mest væsentligt for revisor at sikre korrektheden af IT-systemernes resultater, og dermed sikre det retvisende billede. ISO 27002 derimod er primært rettet mod virksomhederne, og søger så vidt muligt at reducere risici for cyberangreb samt konsekvenserne heraf. Det antages dog, at revisor gennem kendskab til foranstaltningerne introduceret i ISO 27002 mere effektivt kan opnå en forståelse af virksomheden i henhold til ISA 315. Den mere tematiske tilgang til foranstaltninger der medfølger opdatering af ISO 27002 vurderes lettere at kunne anvendes af den finansielle revisor.

Et mindre punkt i den opdaterede ISO-standard er ændringen i oversættelsen af ’controls’ fra det hidtidige ’kontroller’ til fremadrettet at være ’foranstaltninger’. Dermed klargøres formålet med standarden, om at det er handlinger der skal nedbringe risici som er hovedfokus, hvilket ikke nødvendigvis kommunikeres tydeligt af begrebet ’kontroller’. Den første store ændring i ISO 27002 er overgangen fra 14 kapitler til fire temaorienterede kapitler, som det ses i nedenstående figur (Dansk Standard, 2021, s. 2):



Figur 20 - Illustration af ændringer i ISO - Kilde: Dansk standard, 2021

Sammenlignes denne figur med bilag 1 i ISA 315, om bestanddelene i de interne kontrolelementer, findes:

- Kontrolmiljø
- Virksomhedens risikovurderingsproces
- Informationssystemer, herunder tilhørende forretningsprocesser, der er relevante for regnskabsaflæggelse og kommunikation
- Kontrolaktiviteter
- Overvågning af kontroller

Disse områder kan ikke nødvendigvis direkte sammenlignes, selvom der dog kan identificeres flere fællestræk. Eksempelvis:

- Organisatorisk i forhold til virksomhedens risikovurderingsproces samt overvågning af kontroller
- Adfærdsmæssig i forhold til kontrolmiljø
- Fysisk og kontrolaktiviteter

- Teknologisk og informationssystemer

Listen er ikke udtømmende, og der forventes at være flere ligheder mellem temaerne i ISO 27002 og kontrolelementerne i ISA 315. Resultatet af sådan en sammenligning er et indblik i hvilke foranstaltninger revisor sandsynligvis kan møde i gennemgangen af en virksomheds interne kontrolelementer. Opsummerende kan ISO 27002 beskrives som en væsentlig fordybelse af de sikkerhedsforanstaltninger en virksomhed kan implementere, som revisor kan undersøge i henhold til ISA 315.

Endnu en potentiel hjælp til revisors håndtering af IT-sikkerhed, er introduktion af attributter knyttet til de enkelte foranstaltninger i ISO-standarden. Fem forskellige attributter beskrives i standarden, som hver har tilknyttede værdier (Dansk Standard, 2021, s. 6-10):

Type af foranstaltning	Egenskaber for informationssikkerhed	Cybersikkerheds-koncept	Operationelle ressourcer	Sikkerhedsdomæner
Forebyggende	Fortrolighed	Identify	Generelle	Governance and Ecosystem
Opdagende	Integritet	Protect	Fysiske	Protection
Korrigerende	Tilgængelighed	Detect	System- eller programrelaterede	Defense
		Respond	Øvrige	Resilience
		Recover		

Tabel 9 - Attributter introduceret i ISO 27002:2021 - Egen tilvirkning

Ud fra disse attributter kan revisor effektivt skabe et overblik over hvilke IT-relaterede risici, som virksomheden er forberedt på. Yderligere kan det for den finansielle revisor være lettere at vurdere, hvornår det er hensigtsmæssigt at inddrage IT-revisor på baggrund af den finansielle revisors egne kompetencer. Eksempelvis kan den finansielle revisor nemt teste korrigerende foranstaltningstyper ved at simulere en hændelse hvorved korrigering er påkrævet. Derimod antages, at det typisk vil kræve ekspertviden at vurdere eksempelvis en foranstaltnings evne til at opfylde fortrolighedsattributten. Endeligt bør det nævnes at punkterne under operationelle ressourcer i tabellen blot er de fire kategorier, hvorunder der i alt er 15 attributværdier.

16.1 Delkonklusion

Overordnet har ISA 315 og ISO/IEC 27002 forskellige målgrupper og formål, selvom de kan siges at behandle ensartede emner. En bestanddel af ISA 315 omhandler hvordan revisor generelt skal opnå forståelse af virksomhedens IT, og forholder sig dermed i lav grad til cyberrisici specifikt. ISO 27002 er derimod en vejledning henvendt til virksomhederne med fokus på implementeringen af foranstaltninger, som skal reducere cyberrisici. Den seneste udgave af ISO 27002 blev udgivet i 2013, hvortil der på nuværende tidspunkt er en revidering af standarden i gang, som forventes at blive færdiggjort i løbet af 2021.

ISO 27002 overgår fra 14 kapitler til de fire tematiserede kapitler; Organisatorisk, adfærdsmæssig, fysisk og teknologisk. Disse fire kapitler kan sammenlignes med beskrivelsen af interne kontrolelementer, jf. ISA 315 bilag 1, som består af: Kontrolmiljø, virksomhedens risikovurderingsproces, informationssystemer, herunder tilhørende forretningsprocesser, der er relevante for regnskabsaflæggelse og kommunikation, kontrolaktiviteter og overvågning af kontroller. Sammenligningen af ISA 315 og ISO 27002 kan give et indblik i hvilke foranstaltninger der findes i de forskellige dele af en virksomheds interne kontroller. Dermed kan ISO-standarden anses som en uddybelse af bestemte krav i ISA 315, som kan medvirke til revisors overordnede forståelse af virksomheden.

Endeligt introducerer ISO 27002 anvendelsen af attributter, som tilknyttes de enkelte foranstaltninger. Attributterne har det formål at give en simpel og sammenlignelig beskrivelse af de enkelte foranstaltninger. Revisor kan potentielt benytte sig af attributterne til effektivt at få et overblik i henhold til hvilke cyberrisici, som virksomheden er beredt på. Yderligere forventes attributterne at være en hjælp for den finansielle revisor til, at vurdere hvornår inddragelse af IT-revisor er hensigtsmæssigt.

17 Konsekvenser af cyberangreb

Når først et cyberangreb er succesfuldt, og de kriminelle får adgang til en virksomheds systemer, kan det have enorme konsekvenser for den pågældende virksomhed. Følgende afsnit omfatter eksempler, hvor det lykkedes udefrakommende at lukke for virksomhedens IT-systemer samt hvilke økonomiske tab har medført. Yderligere omhandler afsnittet hvilke former for cyberangreb, der forekommer hyppigst, hvilken IT-relaterede trussel virksomhederne anser for størst og hvordan dette kan være relevant for revisor.

17.1 Virksomheder ramt af hackerangreb

Truslen fra cyberkriminalitet kan i sine mange former i yderste tilfælde true en virksomheds overlevelse. Hvis adgangen til kritiske systemer eller data, som er afgørende for driften fratages i en længere periode, kan det i sidste ende betyde en konkurs for den pågældende virksomhed. Ifølge SystemGruppen (2016), en IT-virksomhed der blandt andet har fokus på IT-sikkerhed, går 60 pct. af små virksomheder, som rammes af et succesfuldt cyberangreb konkurs efter seks måneder.

Konsekvenserne af et succesfuldt cyberangreb er ikke kun betydningsfulde for de små virksomheder, men kan også i væsentlig grad påvirke større virksomheder. Eksempelvis har Mærsk og Daarbak, været ramt af angreb henholdsvis d. 27. juni 2017 og 15. marts 2021. For Mærsk kom angrebet til at koste 1,3-1,9 milliarder kroner, mens angrebet på Daarbak, der standsede driften i fem dage, vurderes til at koste fire-fem millioner kroner. I artiklen fastslår direktøren af Daarbak, René Daarbak, at de selv troede de var forberedt og havde investeret i IT-sikkerhed, som dog viste sig ikke at være nok. Ligeledes har Mærsk siden angrebet arbejdet på at forbedre sikkerheden, med en klar forventning om at flere angreb vil komme i fremtiden (Fjordbak, 2021; Toft, 2017). Selvom der her blot er tale om to eksempler, kan det være en indikation på at et flertal af virksomheder står i samme situation, hvor IT-sikkerheden forventes at være tilstrækkelig. En virksomheds overvurdering af egen IT-sikkerhed kan på sigt skabe en betydelig sårbarhed, hvilket kan resultere i et længerevarende cyberangreb.

17.2 Udvikling i cyberangreb og virksomhedens muligheder

PWC's Cybercrime Survey (Nielsen et al., 2020) at 58 pct. af respondenterne har været ramt af mindst én sikkerhedshændelse i løbet af 2020, hvilket er det højeste antal hændelser i de sidste fire år. Samtidig er særligt antallet af phishingangreb steget, hvor 79 pct. af respondenterne der har været udsat for cyberangreb, vurderer at phishing har været en af angrebstyperne. Hertil har 35 pct. disse phishingangreb været relateret til COVID-19. Dermed er udviklingen i cyberkriminaliteten primært målrettet virksomhedernes medarbejdere, og deres manglende kendskab til cyberangreb. Denne udvikling underbygges af virksomhedernes egen opfattelse af hvad der er den største IT-relaterede trussel, som netop er ansattes ubevidste handlinger. Endvidere viser PwC's undersøgelse at virksomhederne ved investeringer i IT-sikkerhed i høj grad prioriterer awareness-træning (Nielsen et al., 2020, s. 18-21).

Center for Cybersikkerhed (2020) anbefaler en række basale tiltag, som virksomhederne kan foretage for at reducere risikoen for succesfulde cyberangreb. Med henvisning til afsnit 6.2, fremgår nedenfor de tekniske tiltag som anbefales af CFC (Center for Cybersikkerhed (g), 2020, s. 7):

- Opdater operativsystemer og applikationer
- Segmenter netværk og begræns trafik mellem segmenter
- Beskyt klienter med antivirus og firewall
- Styr brugerkonti og rettigheder
- Anvend sikre passwords og flerfaktorautentifikation
- Tag back-up af data og konfigurationer og test reetablering
- Etabler logning af ændringer og sikkerhedshændelser
- Beskyt fjernadgang til systemer
- Krypter data på klienter og mobile enheder samt kommunikationen over andre netværk
- Udarbejd en positivliste over applikationer

Disse ti tiltag kan i overvejende grad siges at stemme overens med både anbefalingerne i god IT-skik, COSO-modellen samt besvarelserne af PwC's spørgeskema og den egen udarbejdede spørgeskemaundersøgelse. Dette gælder særligt tiltagene vedrørende funktionsadskillelse, dokumentation af ændringer, backup procedurer og tiltag der hjælper medarbejderne. Det påpeges uddybende af CFC, at et effektivt cyberforsvar indebærer overlap af de implementerede sikkerhedstiltag. Formålet ved at have redundans indarbejdet i

cybersikkerheden er, at selvom én foranstaltning fejler, så vil yderligere foranstaltninger stadig beskytte virksomheden. Redundans i IT-sikkerheden kan i sammenspil med segmentering af data og systemer gøre det kompliceret for den cyberkriminelle at navigere i virksomheden, hvormed virksomheden generelt bliver et mindre attraktivt mål for cyberangreb (Center for Cybersikkerhed (g), 2020, s. 7).

Der kan i forbindelse med segmentering af data og systemer rettes fokus på virksomhedens egen risikoappetit, jf. afsnit 16.1.2. Med udgangspunkt i COSO-modellen, kan virksomheden kategorisere sine data efter hvor kritiske de overordnet er for virksomheden. Dermed har virksomheden mulighed for at prioritere segmentering af data, ud fra hvilke data den har råd til at miste og hvilke den ikke har. Dette vil alt andet lige betyde, at et succesfuldt cyberangreb med lavere sandsynlighed vil have indflydelse for både virksomhedens ry og drift.

Endnu et tiltag virksomhederne kan implementere, som ligeledes er et betydningsfuldt område i analysen, er awareness-træning. CFC beskriver medarbejderne som *"et første bolværk mod angreb, hvis de ved, hvad de skal gøre"* (Center for Cybersikkerhed (g), 2020, s. 8). PwC's undersøgelse understreger tydeligt, at phishingangreb er den mest udbredte metode for cyberangreb, der med tiden bliver mere og mere sofistikeret, eksempelvis ved udnyttelse af COVID-19 situationen. Derfor anbefaler CFC samtlige virksomheders medarbejdere at have kendskab til begreber som phishing-mails, social engineering og håndtering af ukendte usb-sticks (Center for Cybersikkerhed (g), 2020, s. 8-9).

Endeligt anbefales det af CFC at virksomhederne investerer ressourcer i overvågning af cyberangreb og implementering af backup-procedurer. Et ransomware-angreb indledes typisk med andre former for malware, der skal kompromittere virksomheden samt indsamle og kryptere dataene. Dette betyder, at et cyberangreb kan være undervejs i en længere periode før virksomheden påvirkes. Overvågning kan derfor føre til tidlig opdagelse af cyberangreb, hvilket kan redde virksomheden fra de værste konsekvenser. Konkrete tiltag omfatter implementering af overvågningsapplikationer, procedurer ved tegn på malware samt anvendelsen af analyseværktøjer (Center for Cybersikkerhed (g), 2020, s. 10). Lykkedes det den kriminelle at gennemføre et cyberangreb, kan backups af alle kritiske systemer og data være afgørende for eksempelvis virksomhedens fortsættelse af driften. Omvendt vil virksomheden uden backups først have mulighed for at fortsætte drift når cyberangrebet er afværget, hvilket kan tage længere tid. Det anbefales derfor af CFC at opbevare backup separat fra den daglige drift og at der oprettes en offline kopi af denne backup. Yderligere anbefales

det at beskytte backup med kryptering, password, to-faktor autentifikation og at backuppen oprettes som uforanderlige filtyper, således at dataene ikke kan redigeres efterfølgende (Center for Cybersikkerhed (g), 2020, s. 11).

17.2.1 Cyber Risk Management

Figur 21 - Illustration af Cyber Risk Management - Kilde: Deloitte, 2019

Ledelse og kultur er grundlæggende komponenter til styring af cyberrisici, som bør anvendes til at adskille pligter i jobansvar samt systemadgang, hvorfor det bør indgå som en del af virksomhedens IT-strategi. Endvidere bør der indføres en forretningsstrategi, som har fokus på IT- og informationssikkerhed på tværs af virksomheden (Deloitte, 2019, s. 8).

Det er relevant, at virksomheden forstår det nuværende cybermiljø, med formål om at tilpasse strategien, den kontinuerligt udviklende cyberkriminalitet. Ifølge Tolborg bliver teknologien, som de kriminelle anvender konstant bedre og dermed bliver muligheden for succes blandt de kriminelle større, hvilket stiller større krav til virksomhederne i henhold til fokusset på IT- og informationssikkerhed (Tolborg, 2021). På baggrund af denne udvikling anser Tolborg, at der er et behov, for at IT-revision anvendes til bekræfte at risikoen for cyberkriminalitet er reduceret til et passende niveau.

17.3 Relevans for revisor

Risikoen for et succesfuldt cyberangreb har i sig selv ikke nogen revisionsmæssig betydning, da regnskabet ikke direkte påvirkes af denne type risici. Identificeres en væsentlig sårbarhed over for cyberangreb, kan dette dog anses som et potentielt going concern problem. Hermed opstår en problematik vedrørende revisors ansvar i forhold til truslen fra cyberkriminalitet. Samtidig skal revisor være opmærksom på den generelle IT-risiko, hvorunder IT-fejl kan føre til væsentlige fejl i regnskab. Ifølge Berthing (2021) bør IT-revision indgå som en del af revisionen af næsten samtlige virksomheder, hvorfor den førnævnte problematik har stor relevans for revisor generelt.

Endvidere kan der ud fra egen spørgeskemaundersøgelse identificeres områder i ISA-standarderne, hvor der er mangler i forhold til revision af IT. Dette er særligt ISA 315, hvor der efterspørges ændringer, som kan hjælpe med håndtering af revision af IT og cybersikkerhed. Forslag til ændringerne omfatter som tidligere nævnt, direkte ændringer i standarden, henvisninger til eksterne standarder eller øget IT-kompetence hos revisorerne. Her tages der ikke højde for effektiviteten af de forskellige typer ændringer, blot hvordan de kan være relevante for revisor generelt. Yderligere illustrerer særligt PwC's spørgeskemaundersøgelse i hvor høj grad revision af IT fortsat er relevant. Endeligt afspejles den stigende betydning af IT i COSO's begrebsramme, som kontinuerligt er blevet mere IT-orienteret i sammenhæng med virksomhedernes anvendelse af IT.

Allerede ved planlægning af revisionen skal den finansielle revisor tage stilling til IT i den pågældende virksomhed. Ifølge Berthing (2021) bør IT-revisor inddrages tidligst muligt, eftersom IT-revisoren kompetencemæssigt er bedre stillet til at vurdere IT-risici i de enkelte virksomheder. I forlængelse heraf udtalte Berthing (2021), at det ikke nødvendigvis er IT-revisor der skal udføre handlingerne, da dette kan varetages af den finansielle revisor.

Med fokus på den finansielle revisors kompetencer og IT-revisionshandlinger er der i analysen fundet forskellige områder, hvor der er mulighed for forbedring. Dette gælder særligt i relation til forståelsen af en virksomheds kontrolmiljø, som kan give en indikation af cybersikkerhed i den pågældende virksomhed. Gennem kontrolmiljøet forventes det, at revisor eksempelvis kan vurdere risikoen for at der opstår menneskelige fejl, som følge af hvorvidt virksomheden har implementeret awareness-træning eller lignende. På baggrund af anbefalingerne til god IT-skik kan revisor vurdere virksomhedens generelle holdning til IT og sikkerheden heraf, hvilket kan

indikere virksomhedens sårbarhed over for cyberangreb. I forlængelse heraf skal det understreges, at cyberkriminalitet ikke fuldstændig kan forhindres eller nødvendigvis mindskes af IT-revision, som det blev påpeget af Berthing (2021). Derimod kan revisor undersøge om typiske foranstaltninger, som backup-procedurer og segregering af systemer samt data er implementeret. Disse foranstaltninger kan have stor indflydelse på hvor hurtigt virksomheden kan fortsætte driften, og kan derfor have relevans for revisor set fra et going concern perspektiv, som indledningsvist beskrevet.

I forhold til den reguleringsmæssige problematik fremstår ISA-standarderne manglende i forhold til IT, sammenlignet med elementerne i COBIT-modellen og ISO-standarderne. Sammenligningen af ISA 315 og ISO 27002 fremhæver hvordan ISA 315 har en overordnet tilgang til IT, hvorimod ISO-standarden har en mere specificeret opbygning. Dermed kan der argumenteres for enten en ændring af ISA 315, oprettelsen af ISA-standard målrettet IT eller inddragelsen af henvisninger til ISO-standarderne. Problematikken ved ændringer eller tilføjelser af revisionsstandarder er, at revisors ansvar sandsynligvis også vil blive øget. Dog kan det pointeres ud fra ISA 240 om besvigelser, at der ikke nødvendigvis tilfalder et revisoransvar, men at revisor skal forholde sig til cybersikkerhed ligestillet med besvigelser (Olsen, 2021).

Mikkel Hede Olsen (2021) er enig i ovenstående holdning, og mener at erstatningsansvar på erklæringer ikke skal øges yderligere. Selvom revisorer vil hjælpe sine kunder bedst muligt, mener Olsen (2021) ikke at det skal være lovbestemt, og påpeger at der en mangel på regulering af virksomhedernes anvendelse af IT eller mangel på samme. Sammenlignes der med andre lande som Tyskland, findes der konkrete lovkrav til blandt andet kontoplan og IT-miljø afhængig af virksomhedens størrelse (Mikkel, 2021). Ønsket om ikke at blive pålagt erstatningsansvaret kan fremhæves i egen spørgeskemaundersøgelse, hvor respondenterne i højere grad mener at kommunikation af identificerede IT-risici skal kommunikeres i protokollen, fremfor i revisionspåtegningen. Afslutningsvist opstår der hermed en problemstilling om hvor ansvaret skal placeres, således at IT samt IT-sikkerhed håndteres bedst muligt.

Kapitel 5

Diskussion & konklusion

Dette kapitel indeholder diskussionen og konklusionen. Kapitlet har til formål at diskutere og sammenholde specialet centrale elementer, samt et formål om at besvare problemstillingen i konklusionen.

18 Diskussion

Specialet omhandler hvilke risici der kan opstå i forbindelse med IT, samt hvilke forskellige løsningsmuligheder der findes for at modvirke dem. For bedre at vurdere værdien samt effektiviteten af løsningsmulighederne, vil det diskuteres hvem der skal udføre tiltagende samt bære ansvaret for udførelsen heraf.

Tages der udgangspunkt i hackerangrebet på Mærsk i 2017, resulterede angrebet i et tab på omkring USD 250-300 mio. (Mærsk Årsmagasin, 17/18). Angrebet førte yderligere til stor kritik af shippingbranchen fra konsulentvirksomheden Cyberkeel, som har fokus på cybersikkerhed i shippingbranchen. Deres gennemgang af flere virksomheder i branchen fandt blandt andet svage passwords på relativt høje sikkerhedsniveauer (Asschenfeldt, 2017). Denne sikkerhedsmæssige tilstand kan anses som kritisk, set i forhold til størrelsen af de omfattede virksomheder, herunder størrelsen af de potentielle tab. I forlængelse heraf, kan der stilles spørgsmålstegn ved hvorfor der ikke er større krav til IT-sikkerhed ved virksomheder af disse størrelser. Uddybende antages, at når sådan en virksomhed bliver hårdt økonomisk ramt, så kan det have større økonomiske konsekvenser for både deres medarbejdere samt investorer. Yderligere kan det også påpeges, at investorerne som regnskabsbrugere sandsynligvis vil finde det værdiskabende, hvis IT-sikkerhed blev omtalt i årsregnskabet.

Selvom vigtigheden af hensigtsmæssig IT-sikkerhed kan virke åbenlys i store virksomheder som Mærsk, kan det i høj grad også være væsentligt i mindre virksomheder. Virksomheden Mogens Daarbak A/S, som tidligere nævnt i specialet, blev i marts 2021 ramt af et cyberangreb, hvilket stoppede driften i fem dage. Nedlukningen af driften kommer ifølge direktøren René Daarbak til at koste virksomheden fire-fem millioner kroner. Yderligere var dette angreb succesfuldt på trods af, at virksomheden anså sig selv som forberedt på denne slags angreb (Fjordbak, 2021). Dermed kan betydningen af god IT-sikkerhed også fastslås i mellemstore virksomheder, og ikke kun virksomheder på størrelse med eksempelvis Mærsk. Det faktum at cyberangrebet var succesfuldt på trods af at Mogens Daarbak A/S selv mente de var beredt, kan tyde på at der mangler retningslinjer, som virksomhederne kan sammenligne sig med. Alternativt hvis revisor i højere grad fokuserer på IT, er det muligt at sådan en sårbarhed var blevet opdaget og kommunikeret til ledelsen.

Opsummerende er disse blot eksempler på problematikker som kan afhjælpes ved øgede krav og retningslinjer til virksomhederne samt tiltag fra både revisor og virksomhederne. Dermed

bliver spørgsmålet om revisors ansvar på nuværende tidspunkt er stort nok og om øgede krav til virksomhederne vil pålægge dem for store økonomiske omkostninger?

18.1 Overvejelser omkring cybersikkerhed

I forhold til IT-revision, kan det være tvivlsomt hvorvidt revisor reelt kan behandle cybersikkerhed og -kriminalitet. Set fra et regnskabsbrugerperspektiv, kan det være relevant at omtale cybersikkerhed hermed hvilke tiltag virksomheder anvender for at mindske risikoen for angreb samt minimere effekten af et eventuelt angreb. Yderligere som det nævnes i forrige afsnit, kan cyberkriminalitet påvirke integriteten af regnskabet og dermed påvirke regnskabsaflæggelsen. I afsnit 12 omhandlende revisionsrisikomodellen omtales det hvordan et cyberangreb sandsynligvis vil påvirke et flertal af regnskabsposter samt transaktioner. Dertil beskrives hvordan de mange angrebsmetoder kan øge opdagelsesrisikoen, og udgør dermed et af de primære argumenter for relevansen af cybersikkerhed i revision. Derfor vurderes det som væsentligt at diskutere, om dette område kan og bør indføres i revision generelt. Gennem hele specialet er vigtigheden af IT samt virksomhedernes stigende anvendelse af IT pointeret kontinuerligt. Dette udgør endnu et af de primære argumenter for, hvorfor cybersikkerhed i højere grad bør indgå i revisors arbejde.

Revisors vigtigste opgave er at sikre det retvisende billede, hvorfor revisors ansvar bør tage udgangspunkt i dette. Dermed er en måde at vurdere revisors rolle i forhold til cybersikkerhed med udgangspunkt i hvordan det retvisende billede påvirkes. Olsen (2021) opdeler risici i henholdsvis forretnings- og revisionsrisici, hvorunder han kategoriserer cyberrisici i forretningsområdet. I forlængelse heraf påpeger Olsen, at hvis revisor skal tage stilling til virksomhedens forretningsmæssige risici, kan der opstilles et flertal af forskellige problemstillinger, som har større betydning end virksomhedens cybersikkerhed. Endeligt nævner Olsen, at rådgivning vedrørende cyberkriminalitet er noget revisorer kan tilbyde som en del af værditilbuddet, uden at det behøver at være et ansvarsområde. Endvidere findes der mange virksomheder der specifikt arbejder med IT-sikkerhed, hvorved de må forventes at have mere passende kompetencer sammenlignet med revisor.

Med fokus på forståelse af virksomheden i henhold til ISA 315, forekommer nogle krav, som indirekte kan give et indblik i hvor høj grad virksomheden er udsat for cyberrisici. Gi Scharf (2021) udtaler, at awareness og governance er et godt udgangspunkt for vurderingen af ekstraordinære cyberrisici. Disse to områder kan beskrives som en del af kontrolmiljøet, hvilket revisor påkræves at undersøge, jf. ISA 315, 14. Uddybende bør revisor derfor have adgang til information der muliggør forståelse af cyberrisici, under enhver revision, hvor det er relevant. Revisor kan uden yderligere kompetencer undersøge om tiltagene anbefalet af CFC eller anbefalinger i god IT-skik er implementeret i virksomheden, som nævnt i afsnit 18.2. Opnår revisor en forståelse af virksomhedens cybersikkerhed, herunder cyberrisici, bliver spørgsmålet hvordan revisor skal agere ud fra denne forståelse. I interviewene med Olsen, Gi Scharf og Berthing samt egen spørgeskemaundersøgelse er der enighed omkring, at mangler ikke skal indgå i revisionspåtegningen, eftersom det ikke falder under revisors ansvar. Med udgangspunkt i samme kilder, er der ligeledes konsensus om at mangler vedrørende cybersikkerhed skal kommunikeres til ledelsen eller noteres i protokollen.

Væsentligheden af cybersikkerhed som et element i revisionen kommer mest af alt til udtryk ud fra et going concern perspektiv. De tidligere anvendte eksempler, Mærsk og Daarbak, belyser alvorlige økonomiske konsekvenser et succesfuldt cyberangreb kan få for en virksomhed. En blanding af beredskab og held sikrede at disse to virksomheder overlevede angrebene uden at blive konkurstruet (Berthing, 2021, & Fjordbak, 2021). IT-revision kan ikke forhindre cyberkriminalitet, da revision generelt arbejder med den foregående periode, hvor cyberrisici kan siges at være fremadrettet (Berthing, 2021). Dette betyder uddybende, at revisor ikke kan tage stilling til, hvorvidt der er risiko for at virksomheden, vil blive ramt af cyberangreb. Derimod kan revisor med udgangspunkt i forståelse af de førnævnte tiltag bedømme virksomhedens beredskab på et succesfuldt cyberangreb. Endvidere kan revisor ud fra denne bedømmelse fastlægge risikoen for, at virksomheden vil lide større økonomiske konsekvenser, hvis et angreb opstår. Opsummerende kan revisor potentielt fastlægge risikoen for en going concern-problematik med afsæt i virksomhedens cybersikkerhed.

Et andet relevant faktum vedrørende revision, er at årsregnskabet er et ledelsesansvar. Det er ligeledes ledelsens ansvar, at virksomheden har et tilfredsstillende sikkerhedsniveau. Problematikken belyses af Olesen (2021) med udgangspunkt i tyske kunder, som lovmæssigt skal opfylde konkrete krav omhandlende virksomhedens økonomi. Indføres lignende lovgivning med henblik på cybersikkerhed kan der opstå en række muligheder i forhold til

håndteringen af cyberrisici. Først og fremmest vil sådan en lov give revisor belæg for at revidere en virksomheds cybersikkerhed. For det andet vil loven give et udgangspunkt for vurderingen af cybersikkerheden i den pågældende virksomhed. Ud fra dette perspektiv vil et øget ansvar hos virksomhederne føre til bedre håndteringsmuligheder af cybersikkerhed samt -risici for revisorerne. Derudover vil højere sikkerhedskrav sandsynligvis være med til at reducere den ellers stigende trussel fra cyberkriminalitet.

Såfremt virksomhederne bliver pålagt mere ansvar, bør det overvejes hvordan forskellige ansvarsniveauer fordeles på de enkelte virksomheder. Gennem empirien anvendt i specialet er det blevet klargjort, at avanceret cybersikkerhed hverken er relevant eller muligt i små virksomheder, som ikke har den nødvendige økonomi. Endnu en faktor er hvilke data de forskellige virksomheder anvender, eftersom tabet af nogle data vil have større samfundsmæssige konsekvenser end andre. Hertil vil bestemte virksomheder sandsynligvis udgøre mere attraktive mål for cyberangreb end andre, eventuelt på baggrund af potentialet for økonomisk gevinst til den cyberkriminelle eller virksomhedens samfundsmæssige betydning. Således kan det anbefales, at det største ansvar falder til offentlige- og til økonomisk større virksomheder, som på nuværende tidspunkt ikke er omfattet af krav til cybersikkerhed. Derimod vil mindre virksomheder i de fleste tilfælde kunne nøjes med standardiserede sikkerhedsforanstaltninger, der er tilknyttet mindre omkostninger. Endeligt vil der være brancher, hvor der er en større iboende risiko for cyberangreb, hvorunder et tilsvarende ansvar skal kompensere for denne risiko.

18.2 Overvejelser omkring IT-revision

Den digitale udvikling har som nævnt medført, at virksomhederne i langt højere grad er IT-baserede. Dette medfører en risiko for fejl i IT-systemerne, som kan have konsekvenser for virksomhedernes regnskab, i henhold til om det giver et retvisende billede af virksomhedens situation. Der er endvidere risiko for manipulation af IT-systemerne, som ligeledes truer det retvisende billede. På baggrund af denne udvikling, er IT-revision blevet mere væsentlig i forbindelse med revision af virksomhedernes regnskaber.
På nuværende tidspunkt indgår IT-revision i mindre grad i revision af regnskaber. Det fremgår af spørgeskemaet, at det kun anses som nødvendigt i under 10 pct. af virksomhederne. En tredjedel af revisorerne i spørgeskemaundersøgelsen mener dog, IT-revision bør indgå i mere

end 50 pct. af virksomhederne som udføres revision ved. Denne holdning deler interviewpersonerne Thomas Gi Scharf og Mikkel Hede Olsen, som begge mener, at IT-revision som udgangspunkt bør indgå i mere end 50 pct. af tilfældene (Gi Scharf, 2021; Olsen, 2021). Ifølge Gi Scharf vil et mere logisk svar på, hvornår IT-revision bør indgå være altid. Olsen (2021) er ligeledes af denne opfattelse, hvor begge parter mener, at dette ikke er muligt grundet omkostningerne forbundet med IT-revision.
Dermed kan der argumenteres for, at IT-revision ikke anvendes i tilstrækkelig grad af de finansielle revisorer, eftersom behovet alt andet lige må være stigende i forbindelse med den stigende anvendelse af IT i virksomhederne. Årsagen til dette er de risici IT medfører, som kan have konsekvenser for virksomhedens drift. Hertil vurderes det af revisorerne i spørgeskemaundersøgelsen, at manglende IT-sikkerhed generelt har stor betydning for hvor udsatte virksomhederne er for IT-fejl, som potentielt kan have betydning for regnskabet og dermed kan medføre, at regnskabet ikke giver et retvisende billede og derfor udgør en revisionsrisiko. Endvidere kan IT-systemerne anvendes til besvigelser, herunder regnskabsmanipulation samt svindel med data, hvilket endvidere kan udgøre en revisionsrisiko, som IT-revision kan mindske risikoen for.

Det kan diskuteres, hvem der skal udføre IT-revisionen, hvor ovenstående vedrørende omkostningerne forbundet med IT-revision ofte vil afgøre dette (Olsen, 2021). Årsagen hertil er at involvering af IT-revisor er for omkostningstungt for mange virksomheder. Endvidere anses det ikke som nødvendigt at inddrage IT-revisor til alle typer opgaver. De finansielle revisorer kan i et omfang udføre den nødvendige IT-revision (Berthing, 2021). Der er dog et stort gab mellem hvad der står i ISA-standarderne og hvad de finansielle revisorer udfører, hertil er det ofte C og B virksomheder, hvor Berthing er bekymret for at IT-risici bliver overset. Ifølge Gi Scharf kan revisorerne blive bedre og mere effektive i forbindelse med anvendelsen af IT-revision, hvilket han mener, vil give en bedre revision som helhed. Han henviser til at IT-revision i USA er det der driver revisionen. Omvendt påpeges det af både Olsen (2021) og Gi Scharf (2021), at revision på nuværende tidspunkt ikke er forkert, men stadig kan forbedres. Uddybende bliver den manglende IT-revision kompenseret ved substanshandlinger, hvor der på sigt kan stilles spørgsmålstegn ved om dette efterlever hurtighedskravet, jf. RL § 16 (Gi Scharf, 2021)
I spørgeskemaundersøgelsen er det belyst, at IT-revision i et vist omfang skal udføres af de finansielle revisorer, hvor 42 pct. mener at revisor skal udføre IT-revision og 69 pct. mener, at IT-revision skal udføres af henholdsvis revisor og IT-revisor.

Ifølge Olsen er det et spørgsmål om, hvorvidt revisor kan udføre IT-revision, forinden det vurderes hvem der skal udføre det. Endvidere mener han, at det ligeledes er et spørgsmål om kompleksiteten i virksomhedens IT-systemer, hvor han henviser til et beslutningstræ, som anvendes i Deloitte, for at afgøre om IT-revisor skal inddrages. Hertil mener, Berthing (2021), at det er et spørgsmål om at give revisor de rette kompetencer til at håndtere revision af IT.

Som det fremgår af ISA 315, skal revisor allerede i planlægningsfasen, vurdere behovet for involvering af IT-revisor. Berthing samt Gi Scharf, som begge har speciale i IT-revision, mener, at IT-revisor bør inddrages i planlægningen ved enhver revision. Dette skyldes, at IT-revisor kan være med til at vurdere kompleksiteten i IT-systemerne og dermed vurdere, hvor behovet er i revisionen, i henhold til om IT-revisor skal udføre IT-revisionen eller om det skal være revisors opgave. I denne sammenhæng, mener begge at det tydeligt fremgår af ISA 315, hvordan revisor skal forholde sig, samt hvornår og hvilke revisionshandlinger der skal udføres i forbindelse med IT-revision.
Der kan argumenteres for, at denne overbevisning skyldes, at både Berthing og Gi Scharf har kompetencer til IT-revision, således at de lettere kan tolke og anvende ISA 315 i forbindelse med IT-revision. Dette understøttes, af spørgeskemaundersøgelsen, som viser at størstedelen af revisorerne uden IT-speciale ikke mener, at ISA 315 er tydelig samt tilstrækkelig til at vurdere hvordan de skal forholde sig til IT-revision. Ifølge Olsen som ligeledes ikke har speciale i IT, dækker ISA 315 over en mere generel tilgang, og standarden kan derfor være svær at anvende i forbindelse med IT-revision, da det vil kræve en viden omkring området at vurdere, at det er en del af det generelle af virksomheden. Spørgeskemaundersøgelsen viser endvidere, at ISA 315 ifølge revisorerne er mangelfuld på flere områder, når det gælder IT-revision, hvoraf det vurderes at der især er behov for en simplificering samt udspecificering af hvornår og hvor meget IT-revision der skal udføres i forbindelse med revisionen. Der kan argumenteres for, at behovet for IT-revision er tæt på generel. Dette skyldes udviklingen som viser, at langt de fleste virksomheder anvender IT-systemer i en eller anden grad. Dermed kan det være relevant at mindske risikoen for IT-fejl, som kan have betydning for virksomhedens regnskab. Olsen mener ligeledes, at IT-revision bør indgå i revision af regnskaber samt at det er en væsentlig del, af langt de fleste virksomheder (Olsen, 2021). Hans udtalelse om, at ISA 315 er for generel, omfatter at han ikke mener, at IT-revision kan sidestilles med nettoomsætning, varelager mv., på baggrund af dette kan der argumenteres for, at ISA 315 favner for bredt, hvilket Olsen er overbevist om, at den gør. Årsagen til dette, er at der er en kompleksitet i revision af IT, som almindelige revisorer ikke har tilstrækkelig

uddannelse til og derfor ikke kan tolke og forstå hvordan det skal håndteres på baggrund af ISA 315. Ifølge ham, bør kendskabet til virksomheden i ISA 315 generelt defineres mere konkret om hvordan revisor skal håndtere IT-revision. Hertil kan der vurderes et behov for generelle IT-kontroller implementeret i standarden, hvilket efterspørges i henholdsvis spørgeskemaundersøgelsen samt interviewet af Olsen.

Der kan dog være behov for, at IT-revisionsdelen ikke fremgår i ISA 315, men i stedet bliver udspecificeret i sin egen ISA. Dette kan være med til at sikre, at revisorerne udfører revision af IT i langt højere grad, da en mere konkret og detaljeret standard i henhold til IT-delen, vil mindske vanskelighederne, som det vurderes, der er på nuværende tidspunkt. Denne forståelse deler Olsen, hvoraf han nævner, at den vigtigste datakilde i alle virksomheder er IT-baseret, hvorfor han er uforstående overfor, at der endnu ikke er en ISA til IT-revision, i stedet for at det er forsøgt at implementere det i flere forskellige standarder.

En anden måde, at løse problemet på, kan være at ISA 315 får implementeret henvisninger til ISO-standarderne, så revisorerne ved hvor de skal lede efter en mere detaljeret tilgang til IT-revision. Der kan dog alligevel argumenteres for, at dette ikke er tilstrækkeligt. da ISO-standarderne som udgangspunkt anvendes af IT-kompetente IT-revisorer, som anses til at blive inddraget i forbindelse med IT-revision i virksomheder med mere komplekse IT-systemer. Dermed kan der være behov, for at ovenstående omkring implementering i ISA 315 eller en ISA til håndtering af IT-revision, da der som nævnt er behov for, at revisorerne kan udføre IT-revision en nogen grad.

Ifølge Berthing skal der dog mere til, at IT-risici bliver anset som en så væsentlig del af revisionen. Han er af den overbevisning, at der er behov for kendelser i revisornævnet, for at Erhvervsstyrelsen får øjnene op for, at IT skal være en del af kvalitetskontrol. Han vurderer, at problemet ligger ved de finansielle revisorer, da det ifølge ham er dem som har ansvaret, for at sikre at IT indgår i revisionen. På trods af dette, mener han alligevel ikke, at der er noget i galt med ISA-standarderne, tværtimod, mener han at det er *"Det er klokkeklart, at IT medfører risici"*, og dermed skal indgå som en del af de generelle kontroller. Der kan argumenteres for, at denne opfattelse af at IT medfører risici, kommer af en viden, som ikke nødvendigvis er en selvfølge blandt alle revisorer.

På baggrund af ovenstående kan der argumenteres for, at der er opstået en reguleringskløft, mellem IT-revisorers forståelse af standardernes tydelighed samt det at finansielle revisorer ikke mener, at reguleringen er tilstrækkelig til udførelse af IT-revision. Dermed er det relevant at vurdere, behovet for ændringer i reguleringen for at minimere denne kløft.

18.3 Vurdering af overvejelser

I forhold til håndteringen af cyberrisici vurderes det primært at være virksomhedernes eget ansvar. Ligesom årsregnskabet kan der argumenteres for, at det først og fremmest er virksomhedernes eget ansvar at have et hensigtsmæssigt cybersikkerhedsniveau. Yderligere kan en virksomhedsorienteret lovgivning omhandlende cybersikkerhed, give revisor belæg for undersøgelse af virksomhedens cybersikkerhed. Samtidig vil en sådan lovgivning give et grundlag, som revisor kan afgive sin sikkerhedsrelaterede konklusion ud fra. Det er dog væsentligt at skelne mellem blandt andet størrelsen af virksomhederne, når dette ansvar uddeles. Mindre virksomheder kan ikke nødvendigvis bære de økonomiske omkostninger forbundet med øgede krav til cybersikkerhed. Endvidere vil øget cybersikkerhed ikke være lige relevant i alle brancher, hvorfor der også her bør differentieres i kravene til sikkerheden. Større virksomheder samt virksomheder som besidder data omkring befolkningen/kunder, bør være omfattet i større grad end andre virksomheder, da behovet for cybersikkerhed blandt denne type virksomheder som regel er stor, samt at større virksomheder økonomisk har bedre vilkår for at øge sikkerheden. Ligeledes skal kravene til mindre virksomheder afspejle deres økonomiske muligheder og deres betydning for offentligheden.

Revisionshandlingerne som revisor kan udføre i forbindelse med Cyberrisici og -sikkerhed, kan overordnet siges at være begrænsede. Revision omfatter hovedsageligt det foregående år, hvorimod risiko for cyberangreb er et fremadrettet element. I forlængelse heraf kan risikoen for et succesfuldt cyberangreb aldrig reduceres til nul, grundet den konstante teknologiske udvikling. Cyberrisici kan yderligere betragtes som en forretningsrisiko, fremfor revisionsrisici, hvorfor det ikke direkte falder under revisors ansvar. Der hvor revisors muligheder opstår er med udgangspunkt i et going concern perspektiv og med fokus på virksomhedens beredskab på forekomsten af et succesfuldt angreb. I henhold til kravene i ISA 315 skal revisor opnå en forståelse af kontrolmiljøet, hvilket med de rette revisionshandlinger kan give et indblik af virksomhedens tiltag relateret til cyberrisici. Uddybende kan revisor eksempelvis ved forståelse af virksomhedens backup-procedurer vurdere, hvorvidt et

cyberangreb vil have større eller mindre økonomiske konsekvenser og dertil medføre et going concern problem. Opdager revisor mangler i cybersikkerheden anbefales det, at revisor informerer den daglige ledelse, således at manglerne kan udbedres.

På baggrund af spørgeskemaet samt de gennemførte interviews, vurderes det at revisorernes kompetencer til at foretage IT-revision ikke er tilstrækkelige, herunder at behovet for IT-revision samt vigtigheden heraf kan være svær at vurdere, såfremt revisorerne ikke har den fornødne forståelse for udviklingen og dermed for i hvor stor en del IT indgår i de enkelte virksomheder. Dette kan medføre, at flere revisorer ikke inddrager IT i et væsentligt omfang i forbindelse med revision af virksomheder. Eksempelvis fremgår det af spørgeskemaet, at nogle revisorer ikke mener, at IT skal være en del af den generelle revision, da standardiserede systemer som ifølge dem er pålidelige og mindsker behovet. Dette kan medføre, at revisorerne overser fejl, som kan være forbundet med systemerne, og som potentielt kan medføre fejl i regnskabet og dermed true det retvisende billede. Endvidere kan der argumenteres for, at revisorerne ligeledes mangler kompetencer til at tolke standarderne til hvilke IT-baserede handlinger, der skal foretages i forbindelse med revision af virksomhedernes IT-systemer. Dette medfører en problemstilling, da det kan være nødvendigt, at revisorerne har en forståelse for hvordan IT-revision skal udføres i en vis grad. Det kan dermed være nødvendigt at sikre, at revisorerne har kompetencerne til at forstå hvordan IT-revision skal håndteres på dette niveau. Med udgangspunkt i ovenstående, kan det være relevant at sikre, at fremtidige revisorer har en større forståelse af IT-revision, hvorfor det med fordel kan indgå i større grad på uddannelserne samt gennem efteruddannelse af revisorer. Dette er med et formål om at sikre, at revisorerne får en bedre forståelse for IT-revisionens udførelse samt årsagen til nødvendigheden af denne.

Udviklingen fortsætter som nævnt med at gå i retningen af IT, hvorfor det kan være nødvendigt at foretage ændringer i reguleringen tilpasset IT-revision. Det kan konstateres på baggrund af specialets undersøgelse, at der er en diskrepans mellem IT-revisorernes samt de finansielle revisorers forståelse af tilstrækkeligheden og forståeligheden af ISA-standarderne i forbindelse med revision af IT. Det er tydeligt, at IT-revisorernes kompetencer medfører en anden forståelse af standarderne. Dermed kan der argumenteres for, at der på baggrund af manglende kompetencer og viden blandt revisorerne, er behov for ændringer i reguleringen omkring IT-revision. Eftersom IT i højere grad indgår i virksomhederne, herunder som en vigtig samt

bærende del i mange af disse virksomheder, kan der argumenteres for, at det kan være nødvendigt med en standard, som er specialiseret i IT-revision. Denne løsning kan dog kompenseres ved, at IT-delen i de forskellige standarder bliver udspecificeret i højere grad, herunder ved eksempelvis at indføre generelle IT-kontroller i standarderne. Der kan endvidere afhjælpes på området ved at henvise til ISO-standarderne, denne løsning kan være mindre relevant, da ISO-standarderne kan argumenteres for at række udover den generelle revision og dermed anvendes i højere grad til revision, som udføres af IT-revisorer, i forbindelse med revision af virksomheder, som har mere komplekse IT-systemer.

19 Konklusion

Den konstante udvikling inden for IT har medført flere muligheder for virksomhederne, og dermed også en stigende anvendelse af IT generelt. Denne udvikling har i lige så stigende grad resulteret i opstanden af nye trusler, som virksomhederne skal være opmærksomme på. Cyberkriminalitet har indtaget en større rolle i flere virksomhedslederes bevidsthed, hvilket understreges i PwC's spørgeskemaundersøgelse. De cyberkriminelle har mange indgangsvinkler til at angribe virksomhederne, hvor den mest anvendte i 2020 er phishingangreb. Således kan det siges, at god cybersikkerhed aldrig har været vigtigere, og vil i værste fald kunne gøre forskellen mellem konkurs og mindre økonomiske konsekvenser.

For at hjælpe virksomhederne med at varetage truslen fra cyberkriminalitet er der udarbejdet forskellige anbefalinger, standarder og begrebsrammer. I statslige myndigheder er implementeret 'den nationale strategi for cyber- og informationssikkerhed', som omfatter et flertal af minimumskrav vedrørende IT-anvendelse. Uddybende, er der generelt set ingen lovgivning vedrørende IT-sikkerhed i virksomheder som ikke er PIE virksomheder, foruden databeskyttelsesloven omhandlende personfølsomme data. I stedet kan virksomhederne benytte sig af Center for Cybersikkerheds retningslinjer til at forstå og forebygge cybertruslen. CFC samt den internationale standard ISO 27002 giver eksempler på hvilke tiltag virksomhederne kan implementere, herunder segmentering af netværk, kryptering af data og oprettelse af backup-procedurer.

Yderligere er der udarbejdet nogle vejledninger til god IT-skik, som er en ledelsesorienteret beskrivelse af hvordan hensigtsmæssig praksis bør være ved anvendelsen af IT. Denne fokusere på, at ledelsen er involveret i IT-relaterede beslutninger, eftersom IT-afdelingen overordnet har

en stor betydning for forretningsdelen af virksomheden. Formålet herved er at IT-anvendelsen bliver behandlet som en central del af virksomhedens strategi.

Med udgangspunkt i hypotesen afhænger accept af hvilket perspektiv der anvendes. Hertil kan det overordnet konkluderes, at finansielle revisorer anser ISA 315 som manglende og uspecifik i henhold revision af IT. Omvendt mener IT-revisorer dog, at ISA 315 grundlæggende indeholder den nødvendige information for tilfredsstillende at kunne afdække IT-revision.

På nuværende tidspunkt anses IT-revision som en ekstraordinær forekomst, som ikke skal indgå i flertallet af revisioner. Dette bekræftes i spørgeskemaundersøgelsen, hvor IT-revision generelt anses som sjældent at være nødvendigt. Omvendt fastslås det i interviews med revisorer, at IT-revision er relevant i over 50 pct. af revisioner, men undlades på baggrund af de økonomiske omkostninger. Det kan hermed siges, at der eksisterer en uenighed om hvordan IT-revision skal håndteres blandt revisorer. Berthing (2021) påpegede, at det ikke nødvendigvis er IT-revisor, der skal udføre IT-revisionshandlingerne, men dette derimod kan foretages af den finansielle revisor. Overordnet kan der argumenteres for, at den finansielle revisor ikke har de nødvendige kompetencer eller den rette vejledning til at håndtere revision af IT. Den primære regulering omhandlende revision af IT fremgår i ISA 315, hvis omtale af IT vurderes til at være relativt uspecifik. Dette vurderes på baggrund af spørgeskemaundersøgelsen, at der forekommer et gab mellem de handlinger, som den finansielle revisor faktisk udfører på baggrund af ISA 315 samt de handlinger, der bør udføres i forbindelse med revision af IT. Dermed anses der til at være opstået en reguleringskløft. Forbedringsmuligheder indebærer udviklingen af en selvstændig IT ISA, henvisning til eksterne standarder, eksempelvis ISO 27002 og forøgelse af awareness blandt revisorerne.

Opsummerende er betydningen af IT for virksomhederne blevet tydeliggjort, både i forhold til muligheder og til de tilknyttede risici. Denne udvikling betyder også, at IT alt andet lige, må udgøre en større bestanddel af den generelle revision. Yderligere forventes det at være værdiskabende for regnskabsbrugerne, at få indblik i hvorvidt virksomheden er sårbar over for cyberangreb. I forlængelse heraf kan et cyberangreb, udover de forretningsmæssige konsekvenser, påvirke tilgængeligheden af data relevante for revisionen. Uddybende forventes et succesfuldt cyberangreb at påvirke hele systemer i virksomheden, hvilket kan påvirke integriteten af regnskabs relevant data på tværs af regnskabsposter. Yderligere kan uforudsigeligheden af et cyberangreb have indflydelse på opdagelsesrisikoen med udgangspunkt i revisionsrisikomodellen.

Behovet for at de finansielle revisorer udfører IT-revision anses endvidere som begrundet af COSO's generelle fokus på risici i virksomhederne, som omfatter et behov for handlinger samt strategier rettet med IT samt cybersikkerhed. Den stigende anvendelse af IT i virksomhederne, øger risiko for fejl eller besvigelser rettet mod IT-systemer, og udgør potentielt en revisionsrisiko, som kan omfatte at regnskabet ikke er retvisende. Dermed anses det som værende nødvendigt, at revisorerne tager stilling til behovet for revision af IT i de enkelte virksomheder, hertil kan der argumenteres for, at det er nødvendigt at involvere IT-revisorer i planlægningsfasen, således at det hurtigere kan vurderes om der er behov for, at IT-revisor foretager revisionen af IT eller om den finansielle revisor kan varetage denne opgave. Dette vurderes til at være nødvendigt i mellemstore og store virksomheder samt virksomheder hvor IT spiller en stor rolle i henhold til driften, økonomien mv. Hertil er der tale om virksomheder, som på nuværende tidspunkt ikke er omfattet af krav til revision af IT.

COBIT's formål er specialiseret til styring af virksomheds-IT, samt IT-revision. Denne model, anvendes i høj grad i virksomheder, hvor IT indgår som en betydelig del af virksomhedens drift, omsætning mv., samt af IT-revisorer i forbindelse med revision af IT.
Det er i sammenhæng med revision af ovenstående typer virksomheder, hvor IT-revisor bør udføre IT-revisionen. Dette skyldes, at der som udgangspunkt kræves en ekspertise, der er yderliggående i forhold til den generelle forståelse, som indgår i COSO, og derfor typisk ikke kan foretages af den finansielle revisor. Argumentet for dette, er at IT-revision af komplekse systemer samt i virksomheder, hvor IT udgør en meget stor del af driften, omsætningen mv., rækker ud over de kompetencer som revisorerne har til IT-revision. Derudover omfatter finansielle revisorers arbejde andre opgaver, som er af betydning for revisionen og som stadig bør være revisorernes generelle fokus.

Med udgangspunkt i ændringerne i COSO til et større fokus på cybersikkerhed, vurderes det at der er et behov for, at virksomhederne i langt højere grad indfører sikkerhedsforanstaltninger, til at mindske risikoen fra cyberangreb samt effekten af et muligt angreb. Virksomhederne bør derfor indføre awareness-træning af sine ansatte for at sikre, at de ansatte har den fornødne viden, til i højere grad at undgå, at blive udsat for malware samt ransomware, som resultat af at en ansat har modtaget en phishing mail, som vedkommende ikke har håndteret korrekt. Der lægges vægt på, at de menneskelige fejl er en af de helt store risici, forbundet med cyberkriminalitet, hvilket understøtter behovet for awareness blandt virksomhedernes

medarbejdere. Det er ligeledes relevant, at virksomhederne sikrer adgangskontrollerne samt fysisk sikring af virksomhedens server. Endvidere anses det som nødvendigt, at virksomheder, som anvender IT-systemer, fastsætter backup procedurer som skal sikre virksomheden i forbindelse med et muligt angreb. Dette skyldes, at cyberangreb ikke kan afværges med sikkerhed, da hackerne kan få adgang, også i virksomheder med et højt cybersikkerhedsniveau. Virksomhederne kan derfor med fordel, sikre en backup af virksomhedens data, som er separat for virksomhedens generelle IT-systemer.

Der kan argumenteres for, at virksomheder hvor IT indgår som en betydelig del og dermed udgør en stor risiko for virksomheden i forbindelse med cyberangreb, bør anvende en COBIT-tilgang til virksomheds-IT. COBIT's holistiske fremgangsmåde medfører, at virksomhedens IT- samt cybersikkerhed er på et niveau, som i højere grad er tilpasset kompleksiteten i virksomhedens IT-systemer, end ved brugen af COSO's tilgang.
Det antages dog, at der med udgangspunkt i COSO's tilgang ligeledes er behov for et fokus på IT- samt cybersikkerhed i virksomheder, hvor IT indgår i mindre grad. Ud fra dette kan der argumenteres for, at revisor bør have fokus på cybersikkerhed, herunder ved at undersøge virksomhedens backup procedurer, samt om virksomheden anvender awareness. Revisor bør, såfremt der identificeres væsentlige svagheder, som øger risikoen for et succesfuldt cyberangreb, kommunikere herom til ledelsen, således at ledelsen kan tage stilling til dette. Der bør dog ikke være tale om, et revisoransvar i forbindelse med cybersikkerhed, eftersom det som udgangspunkt ikke har nogen revisionsmæssig betydning for regnskabet. Derimod kan der argumenteres for et behov for at der stilles krav til virksomheder, som er sårbare over for cyberangreb, for at sikre at virksomheder tager ansvar i forbindelse med cyberkriminalitet. Hertil anvendes Tyskland som eksempel, på baggrund af interview af Olsen (2021), hvor der stilles specifikke krav til virksomhederne i forbindelse med cybersikkerhed. Der kan være behov for at indføre krav til større virksomheder om cybersikkerhed, samt retningslinjer til mindre samt større virksomheder, som vil gøre det lettere at overskue hvordan virksomhederne kan og skal håndtere cybersikkerhed. Årsagen til dette er, at såfremt virksomhederne ikke tager stilling til cybersikkerhed, kan det have konsekvenser for investorerne samt medarbejderne, i tilfælde hvor virksomheden mister en del kapital eller i værste fald går konkurs.

20 Litteraturliste

Artikler:

Asschenfeldt, P. M. (2017); *Kritik af branchen efter cyberangreb på Mærsk - 12345 regnes som et ok password* https://nyheder.tv2.dk/business/2017-07-04-kritik-af-branchen-efter-cyberangreb-paa-maersk-12345-regnes-som-et-ok-password

D'Aquila, J. (2013); *COSO's Internal Control Integrated Framework Updating the Original Concepts for Today's Environment*

Fjordbak, E. (2021). *Nordjysk virksomhed nægter at betale hackere: - Jeg ønsker det ikke for min værste fjende*¸ TV 2 Nord. Tilgået den 20/04 på: https://www.tv2nord.dk/nordjylland/nordjysk-virksomhed-naegter-at-betale-hackere-jeg-oensker-det-ikke-for-min-vaerste-fjende

Toft, E. (2017). *Cyberangreb tvang Mærsk til at drive virksomhed uden it i over en uge*, Danmarks Radio. Tilgået den 20/04 på: https://www.dr.dk/nyheder/penge/cyberangreb-tvang-maersk-til-drive-virksomhed-uden-it-i-over-en-uge

Faglitteratur:

Arbnor, I., & Bjerke, B. (2009). *Methodology for creating business knowledge.* London: Sage Publications

Bøg, K. C. & Kiertzner, L. (2007). *Professionsetik for revisorer*. Viborg: Nørhaven Book

Calder, A. (2013). *ISO27001/ISO27002 - A Pocket Guide.* Cambridgeshire: IT Governance Publishing

Darmer, P., Jordansen, B., Madsen, J. A., Thomsen, J. (2010). *Paradigmer i praksis.* Randers: Damm's Forlagsbogbinderi

Davidsen, C. M. (2008). *Intern kontrol i revisionsprocessen.* København: Revifora og

forlaget Thomson A/S

Holt, J. T. Bossler, M. A. (2016); *Cybercrime in progress*

ISACA (2012); *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*

Samuelsen, M., Davidsen, C. M., Sudan, S., Parker, H. (2019). *Revision i praksis.* København: Karnov Group Denmark A/S

Moeller, R. M., (2016); *Brink's Modern Internal Auditing.* New Jersey: John Wiley & Sons. Inc

Mogensen, J. K., Lind, B., Gotfredsen, K., Joensen, T. B., Mikkelsen, N. T., Nielsen, F. S., Nielsen, K. F. & Berthing, H. H. A., (2011); *God it-skik.*

Hjemmesider:

Center for cybersikkerhed (a) (2020); *Anatomien af målrettede ransomware-angreb,* tilgået d. 4/2-21 på: https://cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

Center for cybersikkerhed (b) (2020); *Cybertruslen mod Danmark*, tilgået d. 2/2-21 på: https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/-cybertruslen-mod-danmark-2020-.pdf

Center for cybersikkerhed (c) (u.å.); *Ordforklaring,* tilgået d. 8/2-21 på: https://cfcs.dk/da/cybertruslen/ordforklaringer/

Computer viden (u.å.); *Hvad er forskellen mellem WPA & WPA2,* tilgået d. 25/2-21 på: http://www.computerdk.com/Networking/network-security/75623.html

Dansk Industri (u.å.); *Digitalisering i danske virksomheder,* Tilgået d. 2/2-21 på:

https://www.danskindustri.dk/politik-og-analyser/di-mener/digitalisering/digitalisering-af-erhvervslivet/

Dansk Industri (2019); *Flere store virksomheder tager cybertruslen alvorligt,* tilgået d. 2/2-21 på:
https://www.danskindustri.dk/di-business/arkiv/nyheder/2019/10/di-flere-store-virksomheder-tager-cybertruslen-alvorligt/

Dansk Standard (u.å.) *Whitepaper ISO/IEC 27002,* tilgået d. 18/3-21 på:
https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder/whitepaper

Danmarks Statistik (2020); *It-anvendelse i virksomheder,* tilgået d. 2/2-21 på:
https://www.dst.dk/da/Statistik/emner/uddannelse-og-viden/informationssamfundet/it-anvendelse-i-virksomheder

Danmarks Statistik (2019); *Halvdelen har oplevet it-sikkerhedsproblemer,* tilgået d. 2/2-21 på:
https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=41944

Den Europæiske Revisionsret (2016); *Forvaltning i Kommissionen - bedste praksis*, tilgået den 9/3-21 på:
https://eca.europa.eu/Lists/ECADocuments/SR16_27/SR_GOVERNANCE_DA.pdf

Det kriminalpræventive råd (u.å.); *Ransomware,* tilgået d. 4/2-21 på:
https://dkr.dk/it/ransomware/

Erhvervsministeriet (u.å.); *Digital vækst,* tilgået d. 2/2-21 på:
https://em.dk/ministeriet/arbejdsomraader/samfundsoekonomi-konkurrenceevne-og-digitalisering/digital-vaekst/

IT-borger (2020); *Hvad er en VPN og hvorfor gør det dig ekstra sikker på nettet?* tilgået d. 25/2-21 på:

https://www.it-borger.dk/sikkerhed/sikkerhedsprogrammer/hvad-er-vpn-og-hvorfor-goer-det-dig-ekstra-sikker-paa-nettet

Karnov Group (u.å.); *RevisionsMemo; Opdagelsesrisiko,* tilgået d. 16/3-21 på: https://pro.karnovgroup.dk/b/documents/7000745337

Karnov Group (u.å.); *RevisionsMemo; It-revision,* tilgået d. 8/2-21 på: https://pro.karnovgroup.dk/document/7000840748/1?frt=it-revision&hide_flash=1&page=1&rank=1

Karnov Group (u.å.); *RevisionsMemo; ISAE 3402,* tilgået d. 18/3-21 på: https://pro.karnovgroup.dk/b/documents/7000758094

PwC (u.å.); *Risikostyring i en krisetid,* tilgået d. 25/1-21 på: https://www.pwc.dk/da/services/krise-strategi/risikostyring-i-en-krisetid.html

Reciprocity (2018); *What Are the Differences Between COBIT & COSO,* tilgået d. 18/1-21 på: https://reciprocitylabs.com/what-are-the-differences-between-cobit-coso/

Sikkerdigital (u.å.); *Ledelsessystem for informationssikkerhed (ISMS),* tilgået d. 18/3-21 på: https://sikkerdigital.dk/myndighed/iso-27001-implementering/forstaa-arbejdet-med-informationssikkerhed/ledelsessystem/

Sikkerdigital (u.å.); *Tekniske minimumskrav for statslige myndigheder,* tilgået d. 9/2-21 på: https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/

Internationale Standarder om Revision (ISA) og lovgivning:

ISA 260 (2016): *Kommunikation med den øverste ledelse*

ISA 265 (2009): *Kommunikation om mangler i intern kontrol til den øverste og daglige ledelse*

ISA 300 (2009): *Planlægning af revision af regnskaber*

ISA 315 (2013): *Identifikation og vurdering af risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser*

ISA 330 (2009): *Revisors reaktion på vurderede risici*
ISA 570 (2016): *Fortsat drift (Going concern)*
ISA 620 (2009): *Anvendelse af en revisorudpeget eksperts arbejde*
ISA 700 (2016): *Udformning af konklusion og afgivelse af erklæringer om et regnskab*
ISA 705 (2016): *Modifikationer til konklusionen i den uafhængige revisors erklæring*
Bekendtgørelse af lov om Center for Cybersikkerhed (2019) - CFCS
Lov om aktie- og anpartsselskaber (selskabsloven) (2008), Karnov - SLL

Interviews:

Interview af Dorthe Tolborg, d. 25. marts 2021
Interview af Hans Henrik Berthing, d. 7. april 2021
Interview af Mikkel Hede Olsen, d. 28. april 2021
Interview af Thomas Gi Scharf, d. 29. april 2021

Rapporter:

A.P. Møller Maersk (2018); *Årsrapport 2017*
https://investor.maersk.com/static-files/c2228b56-1078-43aa-990f-8ea2b522f302

Center for cybersikkerhed (d) (2020); *Anatomien af målrettede ransomware-angreb*

https://cfcs.dk/globalassets/cfcs/dokumenter/rapporter/CFCS-rapport-anatomien-af-maalrettede-ransomwareangreb.pdf

Center for cybersikkerhed (e) (2020); *Cyber criminals rearm in the shadow of the pandemic.*
https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-threat-assessment-cyber-criminals-rearm.pdf

Center for cybersikkerhed (g) (2020); *Ransomware vejledning.*
https://cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/cfcs-ransomware-vejledning-.pdf

COSO (2019); *COSO Deloitte Managing Cyber Risk in a Digital Age.*

https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

COSO (2004); *COSO ERM Executive summary danish.* https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Danish.pdf

COSO (2013); Internal Control - Integrated Framework, *Executive Summary.* https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

Dansk Standard. (2021). *Den nye ISO/IEC 27002-standard* *https://www.ds.dk/da/om-standarder/cyber-og-informationssikkerhedsstandarder/whitepaper*

Det kriminalpræventive råd (2018); *Cybercrimefolder.* https://www.dkr.dk/media/9820/cybercrimefolder2018.pdf

Finansministeriet (2018); *National strategi for cyber- og informationssikkerhed.* https://digst.dk/media/16815/national_strategi_for_cyber-_og_informationssikkerhed_pdfa.pdf

PwC (2020); *Cybercrime Survey 2020.* https://www.pwc.dk/da/publikationer/2020/cybercrime-survey-2020.pdf

Sikkerdigital (2019); *Tekniske minimumskrav.* https://sikkerdigital.dk/media/10946/tekniske-minimumskrav.pdf

System Gruppen (2016). *IT-Sikkerhed – Omfanget og konsekvensen af IT-kriminalitet* *https://www.systemgruppen.dk/wp-content/uploads/2019/09/SystemGruppen-Omfanget-og-Konsekvensen-af-IT-kriminalitet.pdf*

Tidsskrifter:

Gath, P., Jepsen, C. (2018); *Hvordan uddanner vi til en fremtid vi ikke kender?*

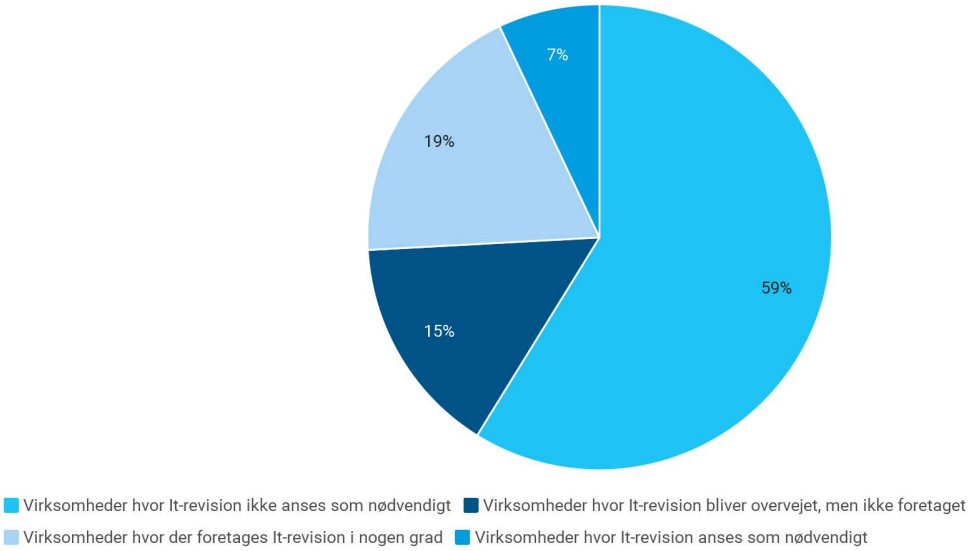
Laursen. P.B. (2001); Udviklingen i international revisionsregulering med hensyn til intern kontrol og IT-revision. *Revision & Regnskabsvæsen, 2001*(11), 32-43

Liempd, D.V., Kristensen, R.H., Wickstrøm, K.A. & Haug, A. (2020); Danske revisorers digitaliseringsparathed - er hele potentialet udnyttet? *Revison & Regnskabsvæsen, 2020*(11), 60-71

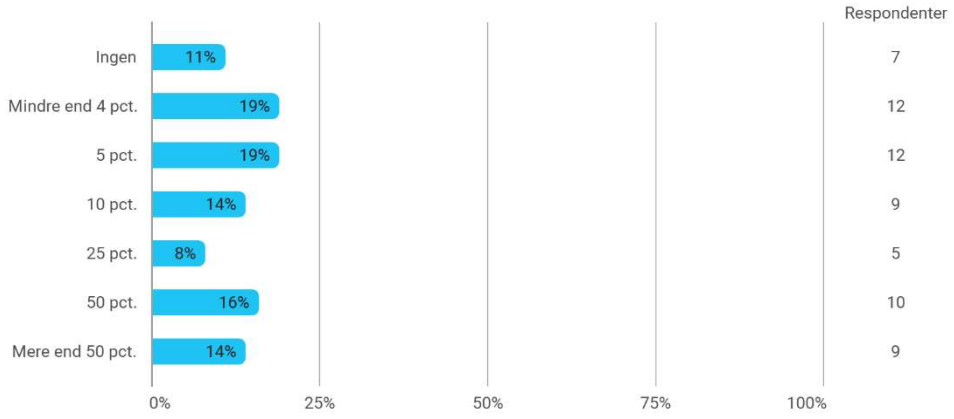
21 Bilag

21.1 Bilag 1: Spørgeskemaundersøgelse

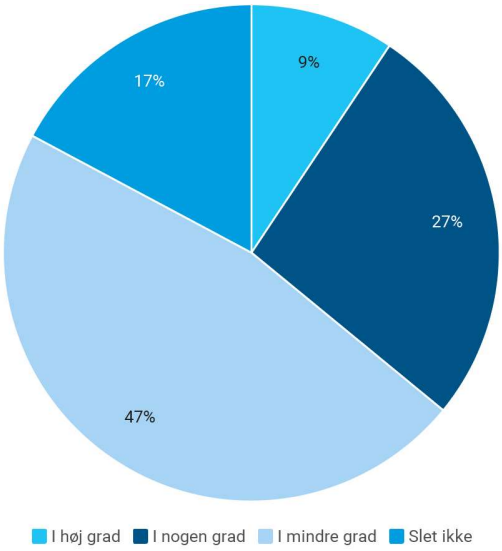
Spørgsmål 1: Hvilke af følgende virksomheder har du oftest som kunde?



Spørgsmål 2 :Hvor mange af disse kunder, falder ind under kategorien, virksomheder hvor It-revision ikke er krævet, men bør overvejes?



Spørgsmål 3: I hvilken grad anvender du it-relaterede revisionshandlinger i forbindelse med revision?



Spørgsmål 4:Hvilke fem elementer/områder er vigtigst at kontrollere i forbindelse med It-revision?

- Funktionsadskillelse
  Brugeradgange
  Opbevaring af dokumenter/koder
- Adgang til diverse systemer/koder ikke bare ligger fremme.
- Processen for ordreoprettelse-fakturering-debitor-betaling
  Processen for varekøb-lagerføring-betaling-vareforbrug-fakturering
  Processen for løn-udbetaling
- Salg
- .
- Arbejder generelt ikke med emnet, men interne kontroller/forretningsgange må ses at være relevant i den forbindelse.
- Nettoomsætning
  Varebeholdninger
  Tilgodehavender fra salg
  Likvide beholdninger og pengestrømme
  Momsområdet
- Omsætning, vareforbrug, debitorer, varelager, kreditorer
- Generelle it-kontroller
  Funktionsadskillelse
  Beskyttelse af systemer

Back-up procedurer

Rettighedstildelinger

- Omsætning

  Vareforbrug

  Lager

  Debitor

  Kreditor

- .
- ?
- Systemanvendelse

  IT-sikkerhedsmiljø

  Adgangsrettigheder

  Ændringsrettigheder

  Fysisk sikring

- Backupprocedurer

  Fysisk placering af server mv.

  Adgangskontroller

  Vedligeholdelse

  Sikkerhed, f.eks. firewall mv.

- adgangskontroller
- .
- ok
- Adgang til programmer og data

  Backup

  Transaktionssporet

  Mulighed for at ændre i kontoplan, momskoder mv.

- k
- Adgangssikkerhed

  Backup

  Funktionsadskillelse

- Vurdering af kontrolmiljøet

  Vurdering af virksomhedens risikovurderingsproces

Vurdering af kontrolaktiviteter, herunder hvilke generelle IT-kontroller der eksisterer; design, implementering og effektivitet

- Fysisk sikkerhed, back up, brugeradgange, nødplaner, change management
- Back-up
  Adgangskontroller
  Systemintegration
  Programmerede kontroller
  uddata-kontrol
- B
- Adgangskontroller, input, output og beregninger
- Er jeg ikke klar over
- Nødplaner / back-up
  Adgangskontroller både fysiske og programmerede
  Dokumentation for til rettelser
- adgangssikkerhed, ændringer, drift
- ?
- sikkerhed
  back-up
  opdatering
  licens
  brugeradgange
- Jeg laver ikke revisioner da jeg sidder som konsulent i outsourcing
- Det kommer meget an på virksomheden.
  Adgangskontroller
  Godkendelseskontroller
  ...
- Jeg er reelt lidt i tvivl om jeres spørgsmål.
- Kontrolmiljø, it-processer, afhængigheden af it i den daglige drift, overholdelse af lovgivning ved brugen af it-systemer og backup procedurer
- Revisor skal gennemgå, vurdere og eventuelt teste virksomhedens it-ressourcer, forretningsgange og it-basserede registreringssystemer med henblik på at fastslå, om disse er tilstrækkelige sikre til at revisionen kan baseres på kontrollerne.
- d

- anvendelsen af it i bogføring og regnskabsudarbejdelsen
  - vurdering af virksomhedens afhængighed i relation til it-anvendelsen
  - vurdering af det overordnede it-miljø
  - vurdering af design og implementering af kontroller
  -vurdering af den operationelle effektivitet af kontroller
- Kundens IT-system
  Bogføring
  udarbejdelse af regnskab
  Revisors eget it-system
  Lovmæssige krav i forhold til it-system
- Økonomisystem/bogføringsprogram, opbevaring af persondata, interne kontroller, tjek af adgange/brug af koder mm samt metode for backup.
- Indbyggede kontroller
- Adgangskontroller
  Ændringskontroller
- Hvilke tre risici relateret til IT og cyberkriminalitet, mener du er de største?
- .
- Pas
- Hacking af ordresystem, så virksomheden ikke kan modtage eller administrere ordrer

  Hacking af betalinger/bank via medarbejdere

  generelle manglende processer omkring godkendelsesflow i virksomheden
- Hacking
  IT-Fejl
  Menneskelige fejl
- Misbrug af aktiver
  Overstatement af nettoomsætning
  Overstatement af aktiver
- hvidvask, besvigelser
- Medarbejdernes adfærd
  Adgangskontroller
  Back-up

- ??
- .
- ?
- Nedbrud pga. hacking
  Tyveri af data
  Indbrud i netbank
- For dårlige adgangskontroller
  Ubetænksomme brugere
  Travlhed
- .
- ok
- sikkerhed
  backup
  adgang
- k
- Angreb ude fra
- Manglende prioritering fra ledelsens side i forhold til sikring
  Ingen mulighed for effektive kontroller som følge af virksomhedernes størrelse
  Underforsikring
- Risiko for uautoriseret adgang til data og likvider
  Risiko for svindel med mail-data og andet, der fører til falske betalinger
  Risiko for nedbrud og manglende mulighed for at komme op at køre igen
- H
- Manglende fokus på kontroller. For stor integration af systemer, så det bliver uoverskueligt.
- Har jeg ikke en holdning til
- Phishing etc.
  manglende adgangskontrol
- adgangssikkerhed, drift, ændringer af it
- ?
- hacking
  blokerer adgang
  miste data

- Ved ikke
- Identitetstyveri

  Regnskabsmanipulation

  Going Concern

  Jeg er reelt lidt i tvivl om jeres spørgsmål.
- Manglende kontrol af automatiserede IT-processer giver en stor risiko for utilsigtede fejl.

  Manglende systemopdateringer, som øger risikoen for cyberkriminalitet.

  Manglende kompetencer i anvendelsen af IT.
- d
- manglende adgang til virksomhedens stamdata

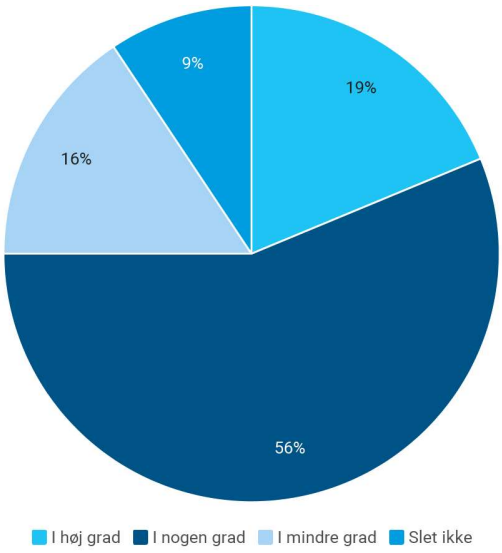
  - læk af fortrolige oplysninger

  - manglende afgang til den operationelle drift af virksomheden
- Hacking.

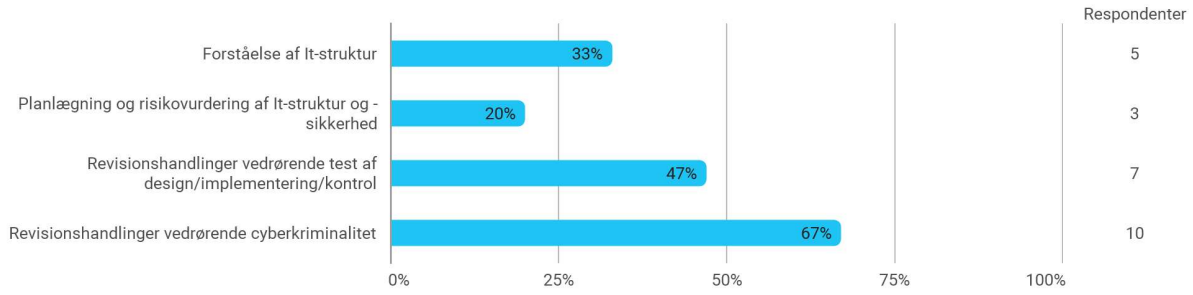
  Besvigelser.

  Svindel.
- Dårlige/deling af adgangskoder, falske mails og dårlige firewalls mm.
- Password sikkerhed
- Adgang

Spørgsmål 5: I hvor høj grad mener du, at ISA 315 er fyldestgørende til identifikation af It-relaterede risici?



Spørgsmål 6: Såfremt du ikke mener, at standarden er fyldestgørende, hvilke områder vurderer du, at der er mangler?

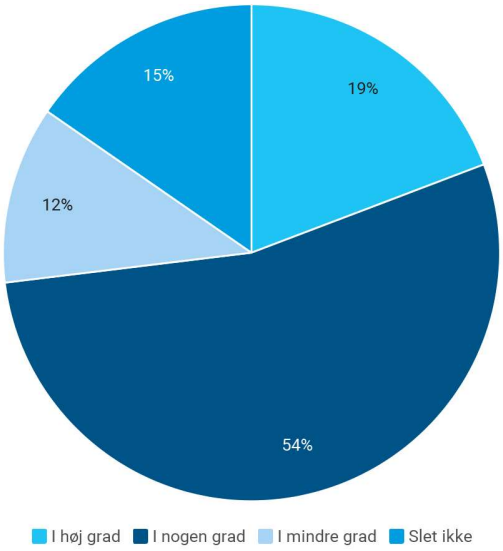


Spørgsmål 7: Er der yderligere områder i ISA 315, som ifølge dig ikke er fyldestgørende?

Revision af generelle it-kontroller

- .
- ok
- k
- Generelt sker der konstant så stor udvikling i hvad risikoen reelt er. Derfor vil en 9 år gammel revisionsstandard være udfordret
- første led SMV virker er overvejende bruger af enkle plat forme (Vismaprodukter, afløser for C5 etc.
- Jeg synes ovenstående afkrydsning spænder bredt.
- Har du andre bemærkninger omkring ISA 315 vedrørende It-revision?
- ISA 315 skal efter min opfattelse anvendes som teorigrundlag i designet af de rent faktiske og praktiske it-revisionshandlinger, og ikke opfattes som en konkret angivelse af it-revisionshandlinger.
- .
- ok
- nej
- k
- Den halter efter virkeligheden.
- det passer ikke overvejende godt til SMV
- Nej
- Jeg synes efterhånden, at man som revisor på forskellige opgaver er dækket godt ind under ISA 315.

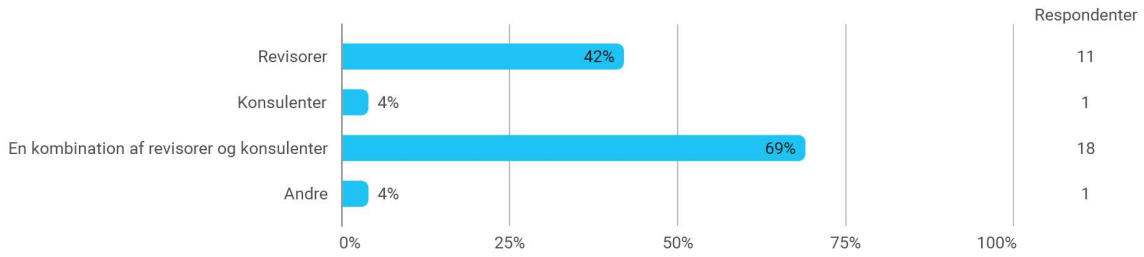
Spørgsmål 8: I hvor høj grad mener du, at ISA-standarderne generelt følger med udviklingen omkring stigende anvendelse af It i virksomhederne?



Spørgsmål 9: Såfremt du vurderer, at der er mangler i ISA-standarderne i henhold til It-revision, beskriv hvad der ifølge dig bør indgå.

- revisionshandlinger/mål direkte målrettet cyberkriminalitet samt direkte målrettet generelle it-kontroller
- Fordrer anvendelse på den korrekte og relevante måde jf. tidligere svar.
- Henvisninger til eksempelvis ISO 27001 standarder, så der er andre der tager stilling til udviklingen i it-sikkerhedsnormerne.
- .
- ok
- nej
- k
- som skrevet - SMV virker er anderledes sat op
- -
- ISA-standarderne kan jo overordnet ikke følge med IT udviklingen, men med fortolkning og revisionsansvar er det reelt en dårlig undskyldning. Dokumentationskravene bør jo blot øges for at overholde standardkravene, selvom standarden ikke ændres.
- En forståelse af at virksomhedens omgivelser ikke nødvendigvis favner it miljøet og it-omgivelser
- Kan ikke komme i tanke om noget.

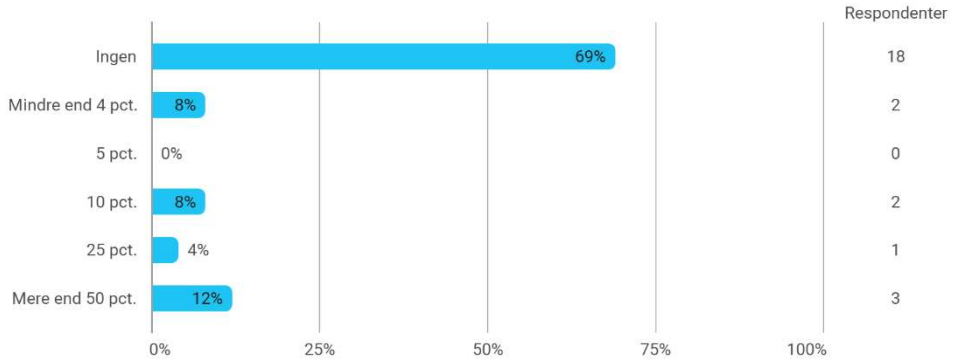
Spørgsmål 10: Hvem mener du, skal foretage It-revision?



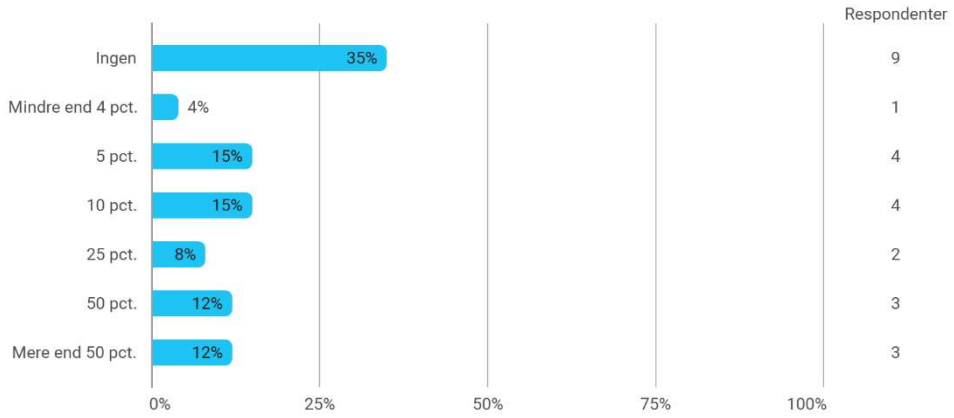
Spørgsmål 11: Såfremt du mener, at andre skal foretage It-revision, så uddyb gerne.

- har mere indgående kendskab til it
- Konkret it-revisionsteamets sammensætning må konkret bero på revisionsobjektets kompleksitet og infrastruktur.
- En generelist revisor har ikke nødvendigvis den fulde indblik i hvordan sikkerheden kan sættes op i virksomhederne
- Revisorvirksomhedens specialister/IT Auditorer
- .
- ok
- Der bør være IT revisorer involveret i dette arbejde, da der er en kompleksitet, hvor det må forventes at en bonus pater revisor kommer til kort
- Det er IT-revisorer der skal udføre IT revision.

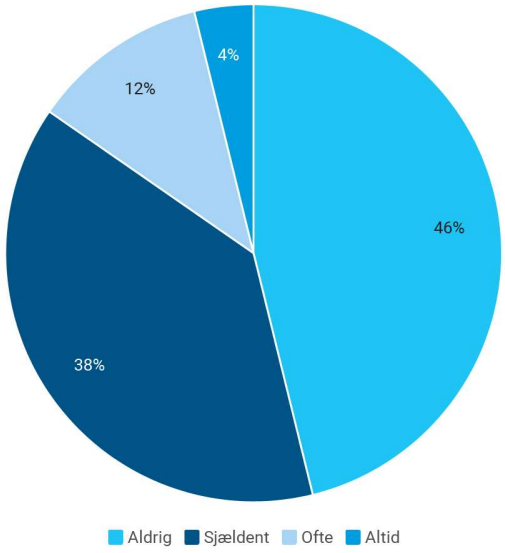
Spørgsmål 12: Hvor ofte afgiver du 3402 erklæringer i forbindelse regnskabsaflæggelse?



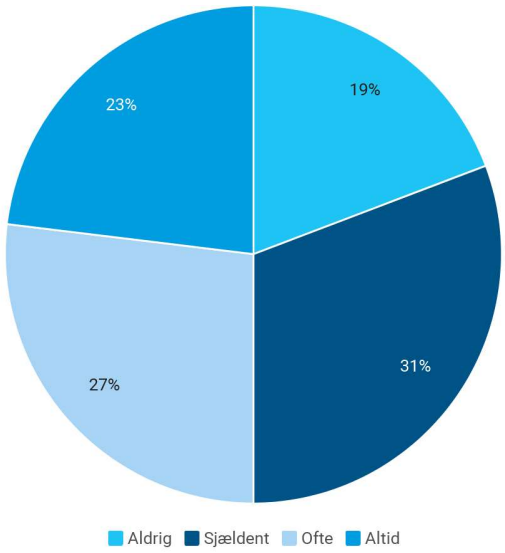
Spørgsmål 13: Hvor ofte har du anvendt en 3402 erklæring fra en anden revisor som dokumentation til at underbygge IT?



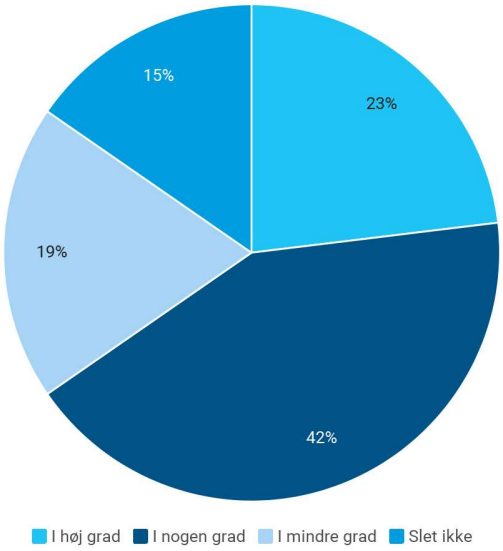
Spørgsmål 14: Bør revisor rapportere særskilt om revision af IT i revisionspåtegningen?



Spørgsmål 15: Bør revisor rapportere særskilt i protokollen om usikkerhed ved IT?



Spørgsmål 16: Hvor meget mener du, at It-revision bør indgå som en del af den generelle revision?



Spørgsmål 17: Forklar kort hvorfor du mener eller ikke mener, at It bør indgå mere i den generelle revision.

- .
- It anvendes i højere og højere grad i virksomhederne, og det er nødvendigt at revisor forstår alle processerne omkring virksomheden herunder it-anvendelsen for at revisor kan identificere risici for tilsigtede eller utilsigtede fejl i regnskabet
- I takt med at IT-revision efter min mening vinder frem i branchen børe det også være med
- It-anvendelse er næsten uden undtagelse en vigtig komponent i forretningskoncepter og/eller regnskabsgenerering i langt de fleste virksomheder og organisationer hvis årsregnskab er underlagt finansiel revision.
- IT indgår i regnskabsaflæggelsen. SMV oftest i standardiserede systemer, som er pålidelige. Dette reducerer behov for egentlig IT-revision
- It er kommet for at blive.
- Det er ikke alle virksomheder it-revision giver mening at udføre på. Er der tale om en meget lille virksomhed, hvor en betryggende funktionsadskillelse ikke er muligt, vil it-revision være unødvendigt. Det handler meget om virksomhedens type.
- It-fylder mere og mere i kundernes hverdag.
- Det er et komplekst område, med stigende digitalisering af arbejdsgange og processer
- det kommer an på virksomheden, nogle gange bør det

- ok
- kundens ansvar
- k
- Det giver ikke mening i forhold til sidste spørgsmål
- Det bør indgå i det omfang, det er relevant for den "almindelige" revision og kan sikre, at systemer og applikationskontroller fungerer
- Ingen bem.
- Ikke relevant for alle typer virksomheder
- Det er forskelligt fra virksomhed til virksomhed hvor afhængigt de er af it jeg har netop skrevet at IT bør indgå mere i den generelle revision
- Revisorer med mindre kunder ikke er bekendt med indhold af IT-revision.
- Det bør indgå hvor det giver mening. Man kan ikke sætte det op sort hvid. Kunderne er jo forskellige og deres IT-systemer er meget varierende.
- Vi skal passe på ikke at trække IT-revision ned over hovedet på virksomheder, hvor det er irrelevant, men samtidig skal det helt sikkert bruges hvor det er relevant
- Dets betydning for virksomhedens drift og interne kontrolmiljø
- Som revisor handler det om at give et retvisende billede af et regnskab. Og det kan kun foregå, hvis kundens it-systemer arbejder nogenlunde sammen med revisors it-systemer.
- Derfor skal man altid tage stilling til, hvilke it-systemer man arbejder med, og hvordan de er blevet benyttet.
- n/a

21.2 Bilag 2: Interview af Dorthe Tolborg

Referat:

Spørgsmål 1:

Vil du give en kort introduktion til din stilling og eventuelt tidligere stillinger?

Svar:

Autoriseret revisor 1995 → IT KBMG 1996 → Deloitte → PwC → Revisionschef i Codan

Spørgsmål 2:

Hvad opfatter du som de mest væsentlige forskelle på it-revision og finansiel-revision?

Svar:

Forskellen er at der er nogle andre revisionsmål. De hænger sammen og derfor er det vigtigt at revisor er kompetent til It-revisionen eller at der er et samarbejde med en It-revisor. Integritet og fortrolighed, er et større fokus inden for It-revision.

Spørgsmål 3:

Har du erfaringer inden for cyberkriminalitet i virksomheder?

Svar:

Dorthe har ikke styr på det tekniske/detaljerne i det, men har et overordnet kendskab til det

Spørgsmål 4:

Hvis ja, hvordan ser du udviklingen i henhold til cyberkriminalitet?

Svar:

I Danske Bank er cyberrisici er højt på agendaen
Risikoen bliver ved med at stige og teknologien som de kriminelle anvender bliver konstant bedre, så muligheden for succes blandt de kriminelle er større og derfor stilles der større krav til virksomhederne. Dette er en konstant udvikling på begge sider

Mange virksomheder bliver angrebet hver dag, det er bare ikke alle der ved det. Nogle virksomheder måler hvor mange gange der bliver forsøgt at opnå adgang.

Spørgsmål 5:
Hvor stort et behov mener du, der er for It-revision til at mindske cyberkriminalitet?

Svar:
Et rigtig stort behov. Cyberrisikoen (Netværkssikkerheden før i tiden) selvom det er noget vi i Danmark har arbejdet med i mange år, så er truslen stadigvæk stor/stigende.
Der er et behov, for at revidere i netværkssikkerheden og den måde vi agere på som brugere.

En medarbejder kan let få en mail og komme til at trykke på et link, som man aldrig skulle have trykket på eller medarbejder kan komme til at vise sit password, og derfra kan den kriminelle opnå adgang til virksomheden.

IT-revision er struktureret rigtig fint i dag, hvor der er tradition for at revidere generelle It-kontroller og applikationskontroller inden for de internationale standarder. Om de så gennemføres rigtig og godt nok ved hun ikke

Spørgsmål 6:
Tror du, at truslen fra cyberkriminalitet kan påvirke det retvisende billede i en revision?

Svar:
Ja ultimativt, hvis angriberen, eller den kriminelle, da der faktisk er penge involveret i det her, kan vedkommende gå ind og redigere i virksomhedens data. Det kan jo så få betydning for regnskabets korrekthed og dermed det retvisende billede.

Oplagt at kigge på styringen af oprettelsesmulighederne, logisk sikkerhed → Adgang til data kan der manipuleres med dette. Hvis systemer inden for økonomi ikke udvikles, kan det lave fejl → Kontrol af at data overføres også på rigtige tidspunkter. AP Møller Mærsk angreb (Nedlagt i flere dage, kan have betydning for going concern) (Banker er især følsomme)

Spørgsmål 7:
Vi har en teori om, at cyberkriminalitet i yderste tilfælde kan påvirke en virksomheds going concern-status, hvad er dit perspektiv på dette?

Svar:
Kriminelle som forlanger løsesum, som lykkedes med at sende mails til medarbejdere i virksomheder med links der trykkes på, så virksomhedens data låses og der ikke kan fås adgang. Dette kan have store konsekvenser for alle virksomheder, især online virksomheder kan blive påvirket, således at de går konkurs.
Dorthe har ikke hørt om at løsesummen i sig selv har betydet en konkurs, men i tanken kunne det godt ske.

Spørgsmål 8:
Tror du på, at revisor kan forebygge going concern problematikken, såfremt der udføres passende it-revisionshandlinger?

Det er ikke revisors ansvar, virksomheden skal sikre sig bedst muligt. Revisor skal forholde sig til virksomhedens it-kontrol og rapporter tilbage i henhold til fejl og mangler.

Spørgsmål 9:
Er revisionsstandarderne ifølge dig ajourført tilstrækkeligt i forhold til den stigende trussel fra cyberkriminalitet?

Der er ikke sket nogen ændringer så vidt jeg ved, siden jeg sad som revisor. Det er et spørgsmål om de er specifikke nok og om cyberrisici står nævnt konkret.

Revisionsbekendtgørelsen. Ekstern revisor skal i protokollen konkludere at It-kontrollerne er udført betryggende. Det er svært at sige hvor meget arbejde, der skal udføres, for at det betryggende. Det er vanskeligt at tyde omfanget.

Det er ikke svært at tyde omfanget i forhold til ISA 315 og 330

Spørgsmål 10:
Har du yderligere kommentarer eller perspektiver?

Svar:
Det er er relevant emne, som er vanskeligt for mange. Der er nok en del finansielle revisorer, som måske mener det er for svært et emne og derfor afholder sig fra det. Der kan være behov for oplysning er finansielle revisorer og for at It bliver en mere generel ting.

21.3 Bilag 3: Interview af Hans Henrik Berthing, se lydfil

21.4 Bilag 4: Interview af Mikkel Hede Olsen, se lydfil

21.5 Bilag 5: Interview af Thomas Gi Scharf, se lydfil