The background of the entire page is an aerial photograph of a soccer field. A large, white number '10' is painted on the grass, with its top extending towards the top of the frame. The field is surrounded by a line of trees and a field of golden grass in the foreground. The sky is a clear, bright blue.

Rapportering
om interne
kontrol- og
risikostyrings-
systemer
i årsrapporten

ADVISORY

Rapportering om interne kontrol- og risikostyringssystemer i årsrapporten

ADVISORY



Kapitel 1	Indledning	5
Kapitel 2	Lovgivningen og dens konsekvenser	7
2.1	Ledelsens ansvar for at beskrive hovedelementerne i virksomhedens interne kontrol- og risikostyringsystemer i forbindelse med regnskabsafslæggelsesprocessen	8
2.2	Beskrivelse af intern kontrol og risikostyring i årsrapporten	8
2.3	Revisors kontrol af beskrivelse af intern kontrol og risikostyring	9
2.4	Internationale krav til rapportering vedrørende intern kontrol og risikostyring	9
2.5	Ikrafttræden	10
2.6	Lovgivningens konsekvenser	11
Kapitel 3	Ledelsens ansvar for det interne kontrolsystem	12
3.1	Bestyrelsens og direktionens ansvar	12
3.2	Revisionsudvalg	13
3.3	Anbefaling for god selskabsledelse	14
Kapitel 4	Intern kontrol og risikostyring	15



Kapitel 5	Opbygning af et internt kontrolsystem	17
5.1	Interne kontrolsystemer	17
5.2	Organisering af opgaven med opbygning af et systematisk og integreret kontrolsystem	18
5.3	Analyse af det nuværende kontrolmiljø	19
5.4	Fastlæggelse af metodik	20
5.5	Fastlæggelse af omfang og identifikation af risici	21
5.6	Fastlæggelse af hensigtsmæssige kontroller	24
5.7	Risiko- og kontrolmatrix	26
5.8	Beskrivelse af kontrolsystem	27
5.9	Forbedringstiltag	29
5.10	Overvågning af virksomhedens interne kontrol- og risikostyringssystemer	30
5.11	Intern revision	33
Kapitel 6	Praktiske problemstillinger	34
Kapitel 7	Afslutning	35
Bilag 1	Eksempel på rapportering i årsrapporten	37
Bilag 2	COSO-Framework	41
Bilag 3	Vurdering af interne kontrol- og risikostyringssystemer	45



4 KPMG • Rapportering om interne kontrol- og risikostyringssystemer i årsrapporten

Kapitel 1

Indledning

Folketinget vedtog den 3. juni 2008 en række ændringer til årsregnskabsloven (L100). Ændringerne omfatter blandt andet et krav om, at børsnoterede virksomheder og statslige aktieselskaber skal beskrive hovedelementerne i deres interne kontrol- og risikostyringssystemer i forbindelse med regnskabsafslæggelsesprocessen.

Kravet er baseret på ændringer til EU's 4. og 7. selskabsretlige direktiver.

De nye regler omtales ofte som "EURO-SOX". Årsagen er sammenligningen med kravene i US-SOX (Sarbanes-Oxley Act). Disse krav er imidlertid væsentligt mere omfattende end de EU-baserede krav. US-SOX kræver f.eks. test af kontrollernes effektivitet over tid, herunder at virksomhedens ledelse og revisor afgiver en erklæring herom i virksomhedens årsrapport.

I EU er det alene et krav at beskrive *hovedelementerne* i virksomhedens interne kontrol- og risikostyringssystemer vedrørende regnskabsafslæggelsesprocessen.

De nye regler medfører øget fokus på dokumentation af intern kontrol og risikostyring i virksomhederne. Som udgangspunkt kan dette øgede fokus på dokumentation ses som øget bureaukrati, men baseret på erfaringer fra andre lande vil et velfungerende og dokumenteret kontrolsystem i højere grad kunne understøtte opnåelsen af forretningsmæssige mål.

Denne publikations formål er at redegøre for de nye krav i årsregnskabsloven til beskrivelsen af hovedelementerne i virksomhedens interne kontrol- og risikostyringssystemer for regnskabsafslæggelsesprocessen samt beskrive vigtigheden af intern kontrol og risikostyring, herunder fordele ved effektive interne kontrol- og risikostyringssystemer.

Publikationen omfatter en praktisk proces for systematisk opbygning af virksomhedens interne kontroller, herunder hvorledes virksomhedens interne kontroller kan dokumenteres og overvåges. Processen er baseret på vores erfaringer fra danske og internationale virksomheder.

I Bilag 1 er givet et eksempel på en beskrivelse i årsrapporten af en virksomheds hovedelementer i interne kontrol- og risikostyringssystemer.

I Bilag 2 er en kort beskrivelse af den internationalt anerkendte begrebsramme for intern kontrol baseret på COSO (Committee of Sponsoring Organization).

Advisory
Marts 2009

Kapitel 2

Lovgivningen og dens konsekvenser

Den 3. juni 2008 vedtog Folketinget en ændring af årsregnskabsloven, hvorefter børsnoterede virksomheder og statslige aktieselskaber, efter § 107 b i ledelsesberetningen, skal beskrive *hovedelementerne i virksomhedens interne kontrol- og risikostyringssystemer i forbindelse med regnskabsaflæggelsesprocessen*.

§ 107 b. En virksomhed, som har værdipapirer optaget til handel på et reguleret marked i et EU/EØS-land, skal medtage en redegørelse for virksomhedsledelse, der omfatter følgende:

- 1) Oplysning om, hvorvidt virksomheden er omfattet af en kodeks for virksomhedsledelse, med henvisning til den kodeks, virksomheden i givet fald er omfattet af.
- 2) Angivelse af, hvor den i nr. 1 omhandlede kodeks er offentligt tilgængelig.
- 3) Angivelse af, hvilke dele af den i nr. 1 omhandlede kodeks virksomheden fraviger og grundene hertil, hvis virksomheden har besluttet at fravige dele af kodeksen.
- 4) Angivelse af grundene til, at virksomheden ikke anvender den i nr. 1 omhandlede kodeks, hvis virksomheden har besluttet ikke at anvende kodeksen.
- 5) Henvisning til eventuelle andre kodekser for virksomhedsledelse, som virksomheden har besluttet at anvende i tillæg til eller i stedet for den i nr. 1 omhandlede kodeks, eller som virksomheden frivilligt anvender, med angivelse af tilsvarende oplysninger som de i nr. 2 og 3 anførte.
- 6) Beskrivelse af hovedelementerne i virksomhedens interne kontrol- og risikostyringssystemer i forbindelse med regnskabsaflæggelsesprocessen.**
- 7) Beskrivelse af sammensætningen af virksomhedens ledelsesorganer og deres udvalg samt disses funktion.

Redegørelsen skal afspejle de aktuelle forhold og skal være tilpasset den enkelte virksomheds konkrete situation og karakteristika, som f.eks. størrelse, kompleksitet og struktur.

Ordet "*hovedelementerne*" understreger, at der skal gives en overskuelig beskrivelse i hovedpunkter om centrale forhold i eksisterende risikostyringssystemer og interne kontrolforanstaltninger i relation til regnskabsaflæggelsesprocessen.

For virksomheder, som udarbejder koncernregnskab, gives redegørelsen for modervirksomheden og koncernen samlet.

Beskrivelsen af hovedelementerne i virksomhedens interne kontrol- og risikostyringssystem i forbindelse med regnskabsaflæggelsesprocessen bør ifølge lovens bemærkninger omfatte:

- *Procedurer eller systemer, som virksomheden har indført i forbindelse med risikostyringen, herunder hvorledes direktionen løbende identificerer og styrer risici for væsentlige fejl i regnskabsaflæggelsen*
- *Interne kontrolsystemer, som er indført i virksomheden til sikring af, at væsentlige fejl i regnskabsaflæggelsen bliver imødegået, opdaget og korri-geret.*

Det understreges således, at der er tale om "væsentlige fejl i regnskabsaflæggelsen". Ved væsentlige fejl forstås fejl, som kan udmønte sig i en rettelse af regnskabet. Væsentlighed er op til den enkelte virksomhed at fastlægge, da væsentlighedsniveau er forskelligt fra virksomhed til virksomhed.

Der skal ikke gives oplysning om interne kontrol- og risikostyringssystemer, som ikke knytter sig til "regnskabsaflæggelsen". Regnskabsaflæggelse skal forstås bredt og omfatter ikke blot udarbejdelse af årsrapporten, men hele processen fra disponering, modtagelse af bilag og registreringer i bogholderiet til udarbejdelse af årsrapporten.

Årsregnskabsloven angiver kun overordnede krav til beskrivelsen. Det forventes, at der inden for en kort årrække vil udvikle sig en "best practice" herfor. Denne "best practice" vil påvirkes af udviklingen – i bl.a. EU-lande som UK, Tyskland, Frankrig osv.

2.1 Ledelsens ansvar for at beskrive hovedelementerne i virksomhedens interne kontrol- og risikostyringssystemer i forbindelse med regnskabsaflæggelsesprocessen

Bestyrelsen og direktionen har ansvaret for, at oplysningerne opfylder lovgivningens generelle kvalitetskrav og grundlæggende forudsætninger til årsrapporter, herunder at oplysningerne er relevante og pålidelige.

Det skal sikres, at der er dokumentation for oplysningerne i årsrapporten, f.eks. i form af direktionsgodkendte politikker, dokumenterede risikostyringssystemer og procedurer samt interne kontroller for væsentlige og risikofyldte områder relateret til regnskabsaflæggelsen, herunder identificerede risici for besvigelser og fejl i regnskaberne.

2.2 Beskrivelse af intern kontrol og risikostyring i årsrapporten

Beskrivelsen af hovedelementerne i virksomhedens interne kontrol- og risikostyringssystemer skal i henhold til årsregnskabsloven fremgå af ledelsesberetningen eller eventuelt i et bilag hertil.

Interne kontroller og risikostyring i forbindelse med regnskabsaflæggelsesprocessen er ikke defineret i lovgivningen. Det er regnskabsaflæggelsesprocessen relateret til årsrapporten, halvårsregnskaber og kvartalsrapporter, der

tilgår "markedet", der har særlig interesse. Placeres oplysningerne i et bilag, skal der være en henvisning hertil i ledelsesberetningen, og det skal tydeligt fremgå af bilaget, at det udgør en del af ledelsesberetningen.

I årsregnskabsloven er der hjemmel til, at Erhvervs- og Selskabsstyrelsen kan bestemme, at beskrivelsen af hovedelementerne i virksomhedens interne kontrol- og risikostyringssystemer ikke medtages i ledelsesberetningen, hvis ledelsesberetningen indeholder en henvisning til virksomhedens hjemmeside, hvor beskrivelsen er offentliggjort. Erhvervs- og Selskabsstyrelsen forventes at fastsætte nærmere regler herom, herunder om virksomhedens opdatering af oplysningerne på hjemmesiden og revisors pligter i forbindelse med de oplysninger, som offentliggøres på hjemmesiden.

Uanset om ledelsen vælger at give beskrivelsen i ledelsesberetningen, i et bilag til ledelsesberetningen eller på hjemmesiden, er det ledelsens ansvar, at virksomheden giver de krævede oplysninger. Ledelsens ansvar for at årsrapporten aflægges i overensstemmelse med lovgivningen omfatter også oplysninger, som virksomheden vælger at give på hjemmesiden, efter de regler som udstedes af Erhvervs- og Selskabsstyrelsen.

2.3 Revisors kontrol af beskrivelse af intern kontrol og risikostyring

Revisor skal i forbindelse med revisionen påse, at oplysninger i ledelsesberetningen er i overensstemmelse med oplysningerne i årsregnskabet og koncernregnskabet. Revisor skal afgive en udtalelse herom i revisionspåtegningen.

Revisors udtalelse omfatter sammenhængen mellem ledelsesberetningens oplysninger og forhold, som revisor er blevet opmærksom på i forbindelse med sin revision. Det forudsættes ikke, at revisor foretager særlige handlinger for at fremskaffe sådanne oplysninger. Der er alene tale om oplysninger, som revisor i forvejen er kommet i besiddelse af i forbindelse med revisionen af årsrapporten.

Indeholder ledelsesberetningen en henvisning til en hjemmeside, hvor beskrivelsen af virksomhedens interne kontrol og risikostyring fremgår, omfatter revisors udtalelse også oplysningerne på hjemmesiden.

2.4 Internationale krav til rapportering vedrørende intern kontrol og risikostyring

Turnbull Guidance (UK)

De nye danske krav svarer i hovedtræk til de krav, der i nogle år har været gældende for børsnoterede virksomheder i UK med udgangspunkt i "The Combined Code" og Financial Reporting Council's rapport fra oktober 2005 "Internal Control: Revised Guidance for Directors on the Combined Code".

Der er dog den væsentlige forskel, at der i UK tillige skal gives oplysning vedrørende risikostyring og intern kontrol i relation til "compliance" (overholdelse) i relation til love og retningslinjer samt styring af operationelle og strategiske risici. Omfanget af kravene i UK er således større end i Danmark.

Danske virksomheder kan finde støtte til arbejdet med interne kontrol- og risikostyringssystemer i forbindelse med regnskabsafslæggelsesprocessen blandt andet i "The Turnbull Guidance".¹

Sarbanes-Oxley Act

Virksomheder, der er børsnoterede i USA og omfattet af Sarbanes-Oxley-lovgivningen m.v., er underlagt strengere krav end de danske. Her kræves en egentlig *erklæring* fra ledelsen om effektiviteten af den interne kontrol samt en redegørelse for eventuelle *svagheder eller mangler* i den interne kontrol vedrørende den finansielle rapportering med en konklusion på resultatet af ledelsens vurdering af effektiviteten i virksomhedens interne kontrol.

I USA kræves endvidere, at den uafhængige revisor afgiver en *revisorerklæring* om effektiviteten. Der er *ikke* krav herom i Danmark. Figuren nedenfor illustrerer de væsentligste ligheder og forskelle mellem US-SOX og de europæiske krav (EuroSox):

	EURO SOX	US SOX-404
Implementering	Den øverste ledelses ansvar	Den øverste ledelses ansvar
Omfang	Intern kontrol med regnskabsafslæggelsen	Intern kontrol med regnskabsafslæggelsen
Evaluering af effektiviteten	Revisionsudvalgets/bestyrelsens ansvar	Den øverste ledelses ansvar
Beskrivelse	Beskrivelse af hovedelementerne i de interne kontroller forbundet med regnskabsafslæggelsen	Skriftlig årlig erklæring fra ledelsen om effektiviteten af interne kontroller forbundet med regnskabsafslæggelsen
Ekstern revision	Ingen uafhængig gennemgang	Uafhængig gennemgang af interne kontrollers effektivitet

2.5 Ikrafttræden

Ændringerne til årsregnskabsloven trådte i kraft den 1. september 2008 og har virkning for regnskabsår, der begynder den 1. september 2008 eller senere. I virksomheder med kalenderårsregnskab får ændringerne således betydning for årsrapporterne for 2009.

Kravet om at revisor skal afgive en udtagelse om ledelsesberetningen træder tilsvarende i kraft for regnskabsår, der begynder den 1. september 2008 eller senere.

¹ Guidance kan findes på <http://www.frc.org.uk/corporate/internalcontrol.cfm>

2.6 Lovgivningens konsekvenser

Der vil formodentligt gå nogle år, før danske børsnoterede virksomheder vil have udviklet "best practice" på området. I mellemtiden kan inspiration derfor hentes fra lande, der i flere år har haft bestemmelser, der minder om de foreslåede, eksempelvis UK.

Et væsentligt skridt på vejen vil være at fastlægge omfanget af de oplysninger, der skal gives i årsrapporten, og det grundlag, der skal være, for at kunne afgive disse oplysninger.

Det dokumentationsgrundlag, der skal anvendes til brug for ledelsens rapportering om virksomhedens risikostyringssystemer og interne kontroller i forbindelse med regnskabsaflæggelsen, kan være omfattende.

Med henblik på at kunne demonstrere, at virksomheden har effektive risikostyringssystemer og interne kontroller, skal de fleste virksomheder dokumentere og formalisere virksomhedens risikostyring og interne kontroller. Virksomhederne vil således i større omfang end tidligere skulle dokumentere deres risikostyringsproces og væsentlige processer og kontroller relateret til regnskabsaflæggelsen.

Virksomhederne skal bruge ressourcer på at implementere denne dokumentation og kontrollere overholdelsen. Ledelsen skal sikre, at der sker opfølgning på svagheder og mangler i de interne kontroller.

Ledelsen må endvidere sikre sig, at der periodisk (formentlig mindst en gang årligt) sker en bekræftelse af, at de godkendte rammer, politikker, instrukser m.v. er overholdt.

Særligt for de større danske børsnoterede virksomheder og statslige aktieselskaber kan der være tale om en ikke ubetydelig opgave. Opgaven kan være særlig omfattende i perioder med væsentlige virksomhedsovertagelser, implementering af nye it-systemer, omstruktureringer, organisationsændringer m.v.

Med den relativt korte implementeringsfrist anbefales det, at virksomhederne allerede nu påbegynder arbejdet med fastlæggelse af de informationer, der skal gives i årsrapporten for 2009, samt med struktureringen af det interne kontrolsystem for at sikre, at ledelsen i forbindelse med aflæggelsen af årsrapporten i 2009 kan give de krævede oplysninger på et relevant, pålideligt og veldokumenteret grundlag.

Kapitel 3

Ledelsens ansvar for det interne kontrolsystem

3.1 Bestyrelsens og direktionens ansvar

I henhold til aktieselskabsloven skal bestyrelsen implementere en forsvarlig organisering af virksomheden, herunder regnskabsfunktion, interne kontroller, it-organisation, budgettering og særlige risici.

Bestyrelsen skal påse, at bogføringen og formueforvaltningen kontrolleres på en efter virksomhedens og koncernens forhold tilfredsstillende måde.

Direktionen skal sørge for, at virksomhedens bogføring sker under iagttagelse af lovgivningens regler herom, og at formueforvaltningen foregår betryggende.

De nye bestemmelser i årsregnskabsloven ændrer ikke ved kravene i aktieselskabsloven.

I forbindelse med regnskabsafleggelsen er det bestyrelsens ansvar – gennem sit tilsyn med direktionen – at sikre, at virksomheden etablerer og vedligeholder interne kontroller, der giver høj grad af sikkerhed om

- pålideligheden af regnskabsafleggelsen, og
- overholdelse af relevant lovgivning og anden regulering af relevans.

Bestyrelsen bør ved varetagelsen af sit tilsyn overveje direktionens mulighed for at

- tilsidesætte kontroller eller for i øvrigt at
- udøve upassende indflydelse i regnskabsafleggesprocessen.

Bestyrelsen angiver "the tone at the top" og dermed virksomhedens overordnede holdning til risici, hvilket styrker direktionens engagement i at etablere en kultur, der bygger på ærlig og redelig adfærd, samt til etablering af stærke interne kontroller bl.a. i forbindelse med regnskabsafleggelsen.

Direktionens ansvar omfatter etablering og vedligeholdelse af kontroller, der understøtter virksomhedens mål om at udarbejde en årsrapport eller anden finansiel rapportering, der giver et retvisende billede, samt styring af risici, som kan resultere i væsentlig fejlinformation i regnskabsafleggelsen. Sådanne interne kontroller reducerer, men eliminerer ikke, risiciene for fejl.

I forbindelse med beslutninger om, hvilke interne kontroller der skal implementeres, bør direktionen overveje risikoen for, at regnskabsafleggelsen kan indeholde væsentlig fejlinformation bl.a. som følge af besvigelser.

Når bestyrelsen skal udfærdige politikker omkring intern kontrol og i den forbindelse vurderer, hvad et stærkt internt kontrolsystem i virksomhedens situation indebærer, kan følgende faktorer indgå i overvejelserne:

- Arten og omfanget af virksomhedens risici, og hvilke former for risici, der anses som acceptable for virksomheden
- Sandsynligheden for, at de pågældende risici realiseres
- Virksomhedens evne til at minimere omfanget af risici, der realiseres, og den effekt de har på virksomheden
- Omkostningerne ved at etablere bestemte kontroller i forhold til den fordel der opnås derved.

3.2 Revisionsudvalg

Revisorloven § 31 stiller krav om, at børsnoterede virksomheder skal have et revisionsudvalg, herunder er det fastlagt, hvilke opgaver revisionsudvalget i det mindste skal varetage.

§ 31. Virksomheder, som har værdipapirer optaget til handel på et reguleret marked i et EU/EØS-land, skal etablere et revisionsudvalg, jf. dog stk. 4-5 og 7-8. Revisionsudvalget skal bestå af bestyrelsesmedlemmer, der ikke samtidig indgår i virksomhedens ledelse. Mindst ét medlem af revisionsudvalget skal både være uafhængig af virksomheden og have kvalifikationer inden for regnskabsvæsen eller revision.

Stk. 2. Revisionsudvalgets opgaver skal i det mindste bestå af følgende:

- 1) At overvåge regnskabsaflæggelsesprocessen,
- 2) at overvåge, om virksomhedens interne kontrolsystem, eventuelle interne revision og risikostyringssystemer fungerer effektivt,
- 3) at overvåge den lovpligtige revision af årsregnskabet m.v., og
- 4) at overvåge og kontrollere revisors uafhængighed, jf. § 24, herunder særligt leveringen af yderligere tjenesteydelser til virksomheden.

Virksomheder vil som følge af kravene til revisionsudvalget om overvågning af regnskabsaflæggelsesproces samt interne kontrolsystemer m.v. skulle etablere et grundlag til understøttelse af revisionsudvalgets opgaver. Dette grundlag er særlig vigtigt i relation til overvågningen af, om virksomhedens interne kontroller fungerer effektivt m.v. Grundlaget for overvågningen kan med fordel tage afsæt i en vurdering af, hvilke regnskabsposter der er væsentlige og risikofyldte.

Den nye bestemmelse i revisorloven har virkning fra førstkommande ordinære generalforsamling, der afholdes efter den 31. december 2008.

3.3 Anbefaling for god selskabsledelse

“Anbefalinger for god selskabsledelse 2005” foreskriver, at danske børsnoterede virksomheder skal give en redegørelse i årsrapporten for, hvordan de forholder sig til anbefalingerne.

I relation til intern kontrol og risikostyring indeholder anbefalingerne følgende:

- Det anbefales, at bestyrelse og direktion ved udarbejdelse af selskabets strategi og overordnede mål identificerer de væsentligste forretningsmæssige risici, der er forbundet med realisering heraf
- Det anbefales, at selskabet i sin årsrapport oplyser om selskabets risikostyringsaktiviteter
- Det anbefales, at bestyrelsen mindst én gang årligt gennemgår og vurderer de interne kontrolsystemer i selskabet samt direktionens retningslinjer herfor og overvågning heraf, og at bestyrelsen overvejer, i hvilket omfang en intern revision kan bistå bestyrelsen hermed.

Disse anbefalinger fokuserer ikke alene på hovedelementerne i selskabets interne kontrol- og risikostyringssystemer i forbindelse med regnskabsaflæggelsesprocessen. Anbefalingen er således bredere end det, der anføres i årsregnskabsloven.

Kapitel 4

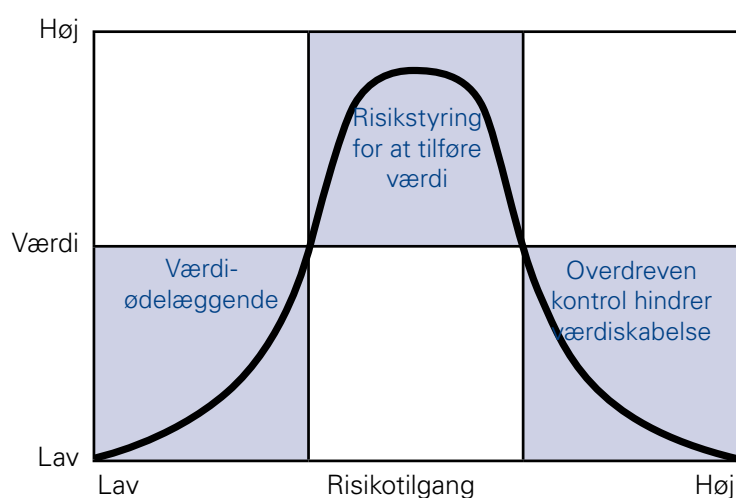
Intern kontrol og risikostyring

Formålet med intern kontrol er at styre risici, ikke at fjerne dem

Effektive interne kontrol- og risikostyringsystemer er bl.a. kendetegnet ved, at risikostyring og kontrol ikke opfattes som en administrativ byrde for virksomheden, men mere som et middel til at øge virksomhedens muligheder og reducere risikoen for tab i forbindelse med uforudsete begivenheder.

Virksomheder sætter strategiske og forretningsmæssige mål og styrer de risici, som er en trussel mod opnåelsen af disse mål. Vellykket risikostyring medvirker til at skabe øget værdi.

Formålet med intern kontrol er at styre risikoen hensigtsmæssigt, *ikke* at fjerne den, hvilket kan illustreres med nedenstående figur.



Risici findes i forskellige former, og konsekvenserne, når de realiseres, kan være positive eller negative for virksomheden. Det er essentielt, at de, der har ansvaret for virksomhedens drift, har kendskab til hensigtsmæssige metoder til at identificere, og styre, relevante risici.

Risiko kan defineres som faktiske eller potentielle begivenheder, som mindsker sandsynligheden for at opnå forretningsmæssige mål.

Intern kontrol er et væsentligt redskab til at styre risici. Andre metoder til at styre risici er, at

- overføre dem til tredjemand (f.eks. ved forsikring)
- dele dem (f.eks. ved joint venture)
- udarbejde en beredskabsplan (plan for handlinger i en krisesituation)
- afholde sig fra aktiviteter, der indebærer en uacceptabel risiko.

Som nævnt kan virksomhederne vælge at acceptere risikoen. At finde den rette balance er kernen i god ledelse, dvs. bevidst at tage risici i stedet for ubevidst at være udsat herfor.

Et velfungerende internt kontrolsystem skal kunne reagere på ændringer

Selv om fokus på risikostyring er øget i de senere år, er det ikke nyt at styre risici for at maksimere de forretningsmæssige mål. I nutidens erhvervsliv er de forretningsmæssige vilkår og virksomhedsmål imidlertid under konstant forandring. Afledt heraf ændres de risici, som virksomhederne står overfor, ligeledes konstant. Et velfungerende internt kontrolsystem skal derfor kunne reagere på sådanne ændringer og give virksomheden mulighed for at tilpasse sig hurtigere end konkurrenterne. Effektiv risikostyring og intern kontrol afhænger derfor af, at der løbende foretages en vurdering af arten og omfanget af risici.

Nogle af fordelene ved at have effektive interne kontroller og risikostyrings-systemer er:

- Tidligere udnyttelse af forretningsmuligheder
- Større sandsynlighed for at opnå forretningsmæssige mål
- Større markedsværdi
- Mere effektiv anvendelse af ledelsens tid
- Lavere kapitalomkostninger
- Færre uforudsete trusler mod virksomheden
- Mere effektiv styring af ændringer
- Klarere strategifastlæggelse.

Det såkaldte COSO-framework (Committee of Sponsoring Organization), er internationalt den mest anerkendte og anvendte referenceramme for fastlæggelse af risikostyring og interne kontroller.

Vi har i bilag 2 givet en nærmere beskrivelse af COSO-begrebsrammen.

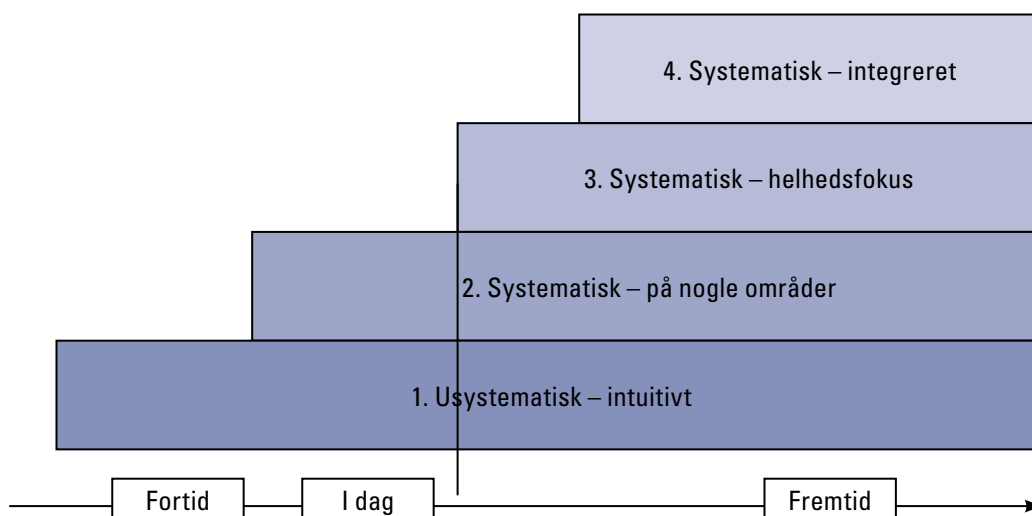
De fleste virksomheder anvender dette framework som basis for virksomhedens interne kontroller. I Holland og USA skal børsnoterede virksomheder eksempelvis anføre hvilket framework de anvender. Omkring 95 % af børsnoterede virksomheder i USA, som er underlagt SOX-404, anvender COSO som referenceramme.

Opbygning af et internt kontrolsystem

5.1 Interne kontrolsystemer

Alle virksomheder har interne kontroller til at imødegå risici. Udfordringen er derfor mere strukturering og dokumentation af kontrollerne.

De nye krav i lovgivningen indikerer, at der er behov for mere struktur og dokumentation omkring intern kontrol. Det er ikke en enkeltstående opgave, at strukturere og dokumentere de interne kontroller, men et kontinuerligt forløb for derigennem at imødegå f.eks. nye risici, ændrede arbejdsgange eller implementering af et nyt ERP-system. Illustrativt vil de fleste virksomheder over tid bevæge sig imod et integreret kontrolmiljø. Ved et integreret kontrolmiljø forstås, at interne kontrol- og risikostyringssystemer er forankret som en naturlig del af virksomhedens normale drift.



Et velfungerende internt kontrolsystem kan understøtte en virksomheds opnåelse af forretningsmæssige mål, herunder effektiv udarbejdelse af retvisende finansiell rapportering. Kontrolsystemer skal derfor betragtes som en del af de samlede ledelsesværktøjer.

En effektiv implementering af et struktureret kontrolsystem kræver, at omfanget og udformningen af kontrolsystemet tilpasses den enkelte virksomheds konkrete forhold og behov. En vellykket og styret implementering er grundlaget for en efterfølgende effektiv vedligeholdelse og løbende forbedring af det interne kontrolsystem.

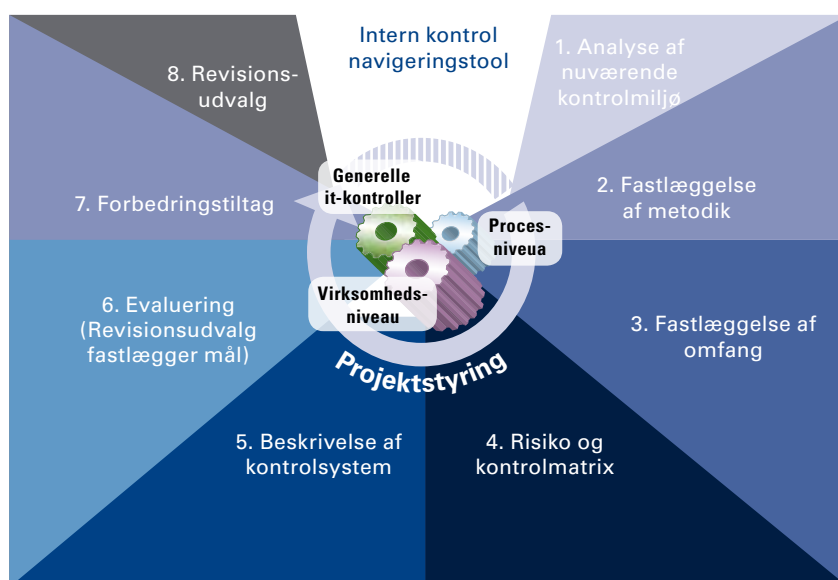
5.2 Organisering af opgaven med opbygning af et systematisk og integreret kontrolsystem

Det er vigtigt for implementeringen af et internt kontrolsystem, at opgaven fastsættes og organiseres hensigtsmæssigt fra start, og at målet er klart og præcist defineret, således at deltagerne og den øvrige organisation er klar over, hvad der kan forventes af dem.

Følgende faktorer er vigtige og kan være afgørende for en vellykket strukturering af et internt kontrolsystem:

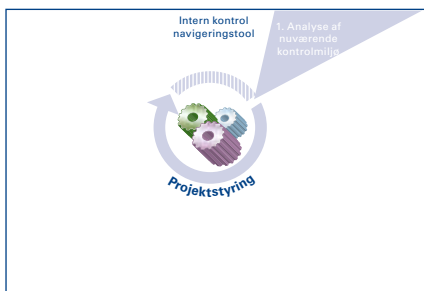
- Den ansvarlige skal være en del af virksomhedens daglige ledelse og rapportere direkte til den øvre ledelse
- Den ansvarlige skal besidde den rette erfaring og have en passende forståelse for regnskabsmæssige forhold, risikostyring og interne kontroller
- Der skal udarbejdes en detaljeret plan, som realiserede resultater løbende måles op mod
- Der skal være tilstrækkelige ressourcer til rådighed
- It-ansvarlige skal involveres fra start
- Kontrollerne skal implementeres efter en top/down, tilgang hvilket betyder, at kontroller der afdækker risici på koncern niveau implementeres først og derefter i virksomheden, alt afhængigt af virksomhedsstruktur

Ved opstart er det vigtigt, at der udarbejdes en plan for hele forløbet. At tænke opgaven til ende vil bidrage til at reducere de risici, der er forbundet med implementeringen. Nedenstående punkter kan med fordel inddrages i forløbet og danne grundlag for de overvejelser, virksomheden skal gøre sig ved struktureringen af det interne kontrolsystem. Punkterne kan ligeledes anvendes i de følgende år for at få justeret kontrolmiljøet, så det bliver en fast del af risikovurderingen i virksomheden.



Terminologi m.v. bør i videst muligt omfang standardiseres og være på plads inden arbejdet påbegyndes, primært med hensyn til at opnå ensartethed og kvalitet i dokumentationen. Det samme gælder for den proces, der efter endt implementering skal håndtere ændringer og opfølgning i kontrolsystemet. Det er vigtigt, at det i denne del af implementeringen overvejes, hvordan der efter

endt implementering følges op på igangværende aktiviteter. Dette skal ses i sammenhæng med revisionsudvalgets opgaver omkring overvågning.



5.3 Analyse af det nuværende kontrolmiljø

Med udgangspunkt i kravene er der følgende to vigtige forhold, som med fordel kan/skal afklares tidligt i forløbet:

1. Hvad ønskes beskrevet i årsrapporten? (årsregnskabsloven § 107 b)
2. Hvordan overvåger revisionsudvalget, at virksomhedens interne kontrolsystem og eventuelle interne revisions- og risikostyringssystemer fungerer effektivt? (revisorloven § 31).

Tidlig afklaring af ovenstående vil sætte ambitionsniveauet for det fremadrettede arbejde og samtidig give et overblik over hvilket ressourceforbrug, der skal anvendes, dels i tid, dels i interne/eksterne ressourcer.

5.3.1 Hvad ønskes beskrevet i årsrapporten

Beskrivelsen i årsrapporten af hovedelementerne af den interne kontrol i forbindelse med regnskabsafleggelsen bør indeholde tilstrækkelig og overordnet information, som gør det muligt at forstå, hvordan det interne kontrolsystem er struktureret. Beskrivelsen bør relateres til hovedområderne for intern kontrol knyttet til regnskabsafleggelsen. Dette kan omfatte kontrolmiljøet, risikovurderingen, kontrolaktiviteterne, information og kommunikation samt opfølgning.

Anvender virksomheden en etableret begrebsramme for intern kontrol, bør dette angives. Eksempel på dette kan være Committee of Sponsoring Organizations of the Treadway Commisions (COSO's) , jf. bilag 2.

Virksomheden kan med fordel anvende COSO som reference og til at fastsætte virksomhedens nuværende status inden for de områder, som kan benævnes som hovedelementerne af et internt kontrolsystem. Første trin i ombygningen vil i givet fald være at indsamle data for de fem hovedelementer:

Kontrolmiljøet

- Hvordan har virksomheden organiseret sig omkring intern kontrol?
- Hvilke procedurer/politikker og interne kontroller har bestyrelsen/direktionen vedtaget på væsentlige områder knyttet til regnskabsafleggelsen?

Virksomhedens risikovurderingsproces

- Hvem gennemfører risikovurderingsprocessen?
- Hvordan gennemføres risikovurderingsprocessen?

Informationssystemet

- Er der etableret en kommunikationspolitik mht intern kontrol og risiko styring?
- Hvordan er informationssystemerne indrettet?
- Hvordan informeres og kommunikeres om intern kontrol i virksomheden?

Kontrolaktiviteter

- Tager kontrolaktiviteterne udgangspunkt i risikovurderingen?
- Hvilke kontroller er etableret?
- Hvordan er kontrollerne dokumenteret?

Overvågning

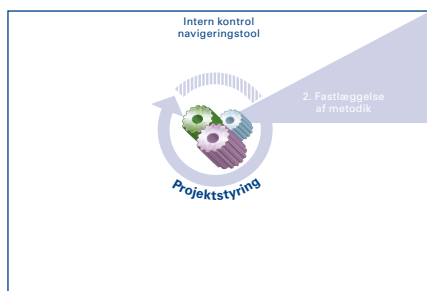
- Hvordan overvåges det interne kontrolsystem?
- Hvordan rapporteres der om kontrollernes gennemførelse og eventuelle svagheder?

5.3.2 Hvad skal der rapporteres til revisionsudvalget/bestyrelsen

Som andet punkt omkring struktureringen af det interne kontrolsystem kan virksomheden med fordel overveje, hvad der skal rapporteres til revisionsudvalget og/eller bestyrelsen. Uafhængigt af tidspunktet for revisionsudvalgets etablering eller beslutning omkring hvorledes intern kontrol skal overvåges, kan udvalget/virksomheden med fordel overveje følgende elementer:

- Hvad skal rapporteres?
- Hvor ofte skal der rapporteres?
- Hvornår skal der rapporteres?
- Hvem skal modtage rapporteringen?
- Hvordan kommunikerer tilbage i organisationen?

Ovenstående punkter kan have indflydelse på opbygningen af det interne kontrolmiljø, idet standarder for rapportering bør være en integreret del heraf. For at få en ensartet rapportering bør dette overvejes tidligt i processen, da det kan kræve mange ressourcer at ændre rapporteringsstrukturen. Dette er naturligvis afhængigt af virksomhedens kompleksitet og antallet af rapporterende enheder.

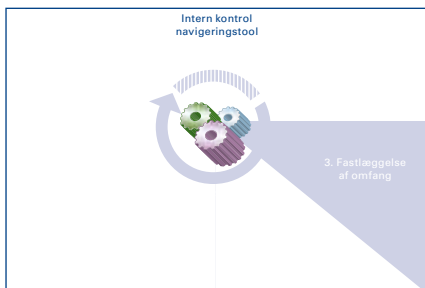


5.4 Fastlæggelse af metodik

Efter fastlæggelse af overblik/status over virksomhedens nuværende kontrolmiljø, herunder hvad der ønskes beskrevet i årsrapporten samt hvordan og hvad, der skal rapporteres til revisionsudvalget og bestyrelsen, er næste trin i systematiseringen af det interne kontrolmiljø at sikre en integration i virksomhedens normale driftsaktiviteter. På denne måde sikres, at systematiseringen af det interne kontrolmiljø ikke forbliver et enkeltstående projekt, men overgår til en fast del af virksomhedens aktiviteter. Metodikken kan omfatte følgende punkter:

1. Hvad beskrives i årsrapporten?
2. Rapportering til revisionsudvalget/ledelsen
3. Hvor ofte samt hvordan gennemføres risikovurderingsprocessen? (Se afsnit 5.5)
4. Hvilke områder skal styrkes (trin 1), kontrolmiljøet
5. Omfanget (Se afsnit 5.5)
6. Dokumentationsstandarder (Se afsnit 5.8)
7. Hvorledes udarbejdes og udfyldes kontrolmatrix? (Se afsnit 5.7)
8. Hvorledes evalueres kontrolmiljøet? (Se afsnit 5.9)
9. Hvorledes udarbejdes forbedringstiltag? (Se afsnit 5.9)
10. Godkendelsesprocedurer/governance struktur/tidsplan.

Ved gennemgang af ovenstående punkter sikres, at alle aspekter i opbygningen samt integrationen af det interne kontrolmiljø inddrages som en fast del af virksomhedens planlægningsaktiviteter. Dette sætter rammerne for kontrolsystemet og vil samtidig være anvendeligt i kommunikationen såvel internt som eksternt.



5.5 Fastlæggelse af omfang og identifikation af risici

Ved fastlæggelsen af omfanget skal det afklares, hvilke risici og kontroller, der skal omfattes af risikostyringssystemet. Omfanget påvirker kompleksiteten samt ressource- og omkostningsforbruget. Virksomheden bør derfor kun i begrænset omfang medtage forhold, der ikke relaterer sig til regnskabsafslæggelsen.

Formålet med at fastlægge omfanget er at identificere de processer, der er forbundet med væsentlige risici ud fra en risikobaseret top-down tilgang.

De væsentlige risici omfatter risici, der kan svække eller true koncernens eksistens samt risikoen for at overse vigtige forretningsmæssige muligheder.

Risikobaseret betyder, at virksomheden skal gennemgå de regnskabsposter og processer, hvor der er risiko for væsentlige fejl i regnskabsafslæggelsen. Erfaringen viser, at ikke-rutinemæssige processer samt skøn og estimater ofte er forbundet med den højeste risiko.

Top-down tilgangen indebærer, at virksomheden først skal identificere de eksisterende kontroller på koncernniveau, der håndterer risikoen for væsentlige fejl. Hvis sådanne kontroller ikke eksisterer eller ikke afdækker alle væsentlige risici, skal kompenserende og/eller yderligere kontroller identificeres på et lavere niveau. Er en given proces afhængig af it-applikationer (systemer) og/eller automatiserede applikationskontroller, skal de generelle it-kontroller for sådanne systemer også omfattes af risikostyringssystemet.

Ved fastlæggelsen af omfanget skal der tages udgangspunkt i koncernregnskabet. Regnskabsposter og processer, som for koncernregnskabet er væsentlige og risikofyldte, kan ligge i moderselskabet og/eller i dattervirksomhederne. Da væsentlighed på koncernniveau generelt er større end på selskabsniveau, kan der være regnskabsposter og processer i de enkelte dattervirksomheder, som ikke er væsentlige på koncernniveau. Af denne årsag er det vigtigt at fastlægge omfanget på koncernniveau.

Nedenstående tre figurer illustrerer de trin, som virksomhederne skal igennem ved identifikation af væsentlige områder forbundet med risiko:

Skema for risikovurderingsprocessen

Væsentlighedsniveau 0 < 5 Lav > 5 < 15 Moderat > 15 Høj	Analyse af effekt			Effekt			Udsagn					
	år	Sidste år	% af samlede aktiver eller samlede driftsindtægter	Væsentlighed	Risiko for fejl i regnskabet	Samlet effekt i regnskabet	Fuldstrændighed	Tilstedeværelse	Nøjagtighed	Værdiansættelse	Rettigheder og forpligtelser	Præsentation og oplysning
	2008	2007		H, M, L	H, M, L	1-6						
Resultatopgørelse												
Omsætning	100	105	100,0 %	Høj	Høj	6	√	√	√			
Personaleomkostninger	24	20	24,0 %	Høj	Moderat	5	√	√	√			√
Total – Aktiver	200	200	200,0 %									
Varebeholdning	50	50	25,0 %	Høj	Høj	6		√		√		√
Debitorer	4	6	2,0 %	Lav	Lav	2		√		√	√	√
Total – Passiver	200	200	200,0 %									
Lån	12	12	6,0 %	Moderat	Moderat	4	√		√		√	√
Andre forpligtigelser	45	36	22,5 %	Høj	Lav	4	√				√	√
Noter												
Brandskadeforsikring af materielle anlægsaktiver	5	3		Moderat	Lav	3	√	√	√			√

Ovenstående figur er et eksempel på, hvordan der på koncernniveau kan identificeres regnskabsposter, som er væsentlige og risikofyldte. Ved væsentlige skal forstås, en fejl i regnskabsafleggelsen der er så stor, at det vil påvirke regnskabslæserens beslutningstagen. I eksemplet er angivet tre niveauer for hhv. væsentlighed og risiko; høj (H), moderat (M) eller lav (L). For at give overblik samt fokusere på hvilke poster, der har højest risiko, kan et point-system med fordel anvendes. Ud fra de tre kategorier H, M og L kan de enkelte poster gives følgende værdier: H=3, M=2 og L=1. Hvis den samlede score (væsentlighed + risiko for fejl i regnskabet) tilsammen udgør 4 eller mere, er det i eksemplet vurderet, at regnskabsposten er væsentlig og risikofyldt og derfor indbefattet i det fremadrettede arbejde.

Efter at de væsentlige og risikofyldte regnskabsposter er identificeret, vurderes det, hvilket regnskabsudsagn posterne relateres til.

De væsentlige og risikofyldte regnskabsposter på koncernniveau er nu identificeret, men bør efterfølgende nedbrydes, således at det identificeres hvilke enheder i koncernen, der har en betydelig del af den væsentlige og risikofyldte regnskabspost.

Som det fremgår af nedenstående figur, er de tre væsentligste regnskabsposter fra figuren på foregående side fremhævet sammen med de enheder, der bidrager væsentligt til posterne. Ved at opretholde dette fokus vil virksomhederne opnå dels en fokuseret indsats, dels en ressourcemæssig besparelse i og med, at ikke alle enheder inddrages. Beregningsgrundlaget for fastsættelsen kan være en 80/20 regel, kombineret med en vurdering af størrelsen af den enkeltstående enhed.

Enheder der skal inddrages

Opdelt pr. område	År	Sidste år	% af samlede aktiver eller samlede driftsindtægter	Samlet effekt i regnskabet	Enhed				Andel af total	
					Danmark	Sverige	Norge	Tyskland	Total	Andel i %
	2008	2007		1 – 6						
Resultatopgørelse										
Omsætning	100	105	100 %	6	40	10	30	20	100	100 %
Personaleomkostninger	24	20	24 %	5	2	8	6	8	22	92 %
Total – Aktiver	200	200	200 %							
Varebeholdning	50	50	25 %	6	46	2	2	2	46	92 %
Debitorer	4	6	2 %	2	1	1	1	1	0	0 %
Total – Passiver	200	200	200 %							
Lån	12	12	6 %	4	3	3	3	3	12	100 %
Andre forpligtigelser	45	36	23 %	4	40	2	2	2	40	89 %
Noter										
Brandskadeforsikring af materielle anlægsaktiver				3						

Tredje og sidste trin i fastlæggelsen af omfang er, at identificere de forretningsprocesser (herunder it-applikationer) der skal være omfattet. Ud fra de identificerede risikoforbundne regnskabsposter på koncernniveau opstilles de relaterede forretningsprocesser, som understøtter regnskabsposten. I eksemplet i figuren på næste side, ses hvilke processer der er identificeret som værende understøttende for regnskabsposten. Resultatet af denne vurdering anvendes til at målrette de kontroller, som skal opsættes, for at imødekomme risiciene forbundet med regnskabsaflæggelsen.

Processer der skal inddrages

Opdelt pr. proces	Samlet effekt i regnskabet	Koncern-niveau	Processer					Månedsafslutning og finansiel rapportering
			Kontroller	Salg	Indkøb	HR	Produktion	
	1 – 6							
Resultatopgørelse								
Omsætning	6	nej	x					x
Personaleomkostninger	5	delvis		x	x			x
Total – Aktiver								
Varebeholdning	6			x			x	x
Debitorer	2							
Total – Passiver								
Lån	4							
Andre forpligtigelser	4	delvis	x		x	x		x
Andet								
Brandskadeforsikring af materielle anlægsaktiver	3	ja						

5.6 Fastlæggelse af hensigtsmæssige kontroller

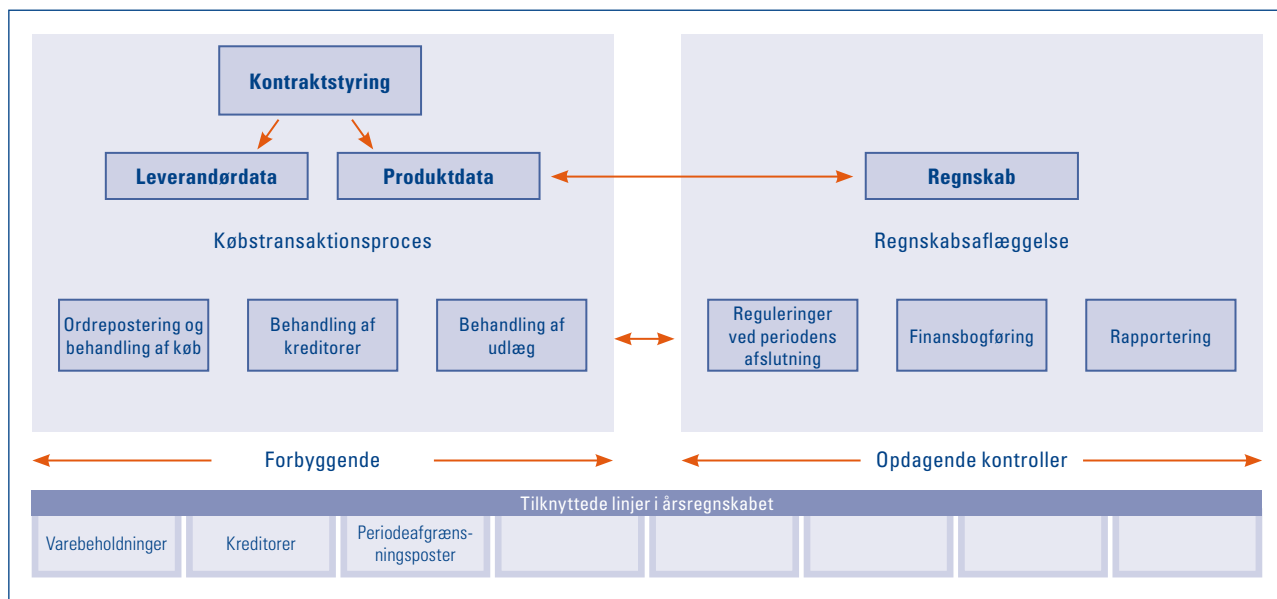
Interne kontroller findes i enhver virksomhed, men graden af formalisering, dokumentation og effektivt varierer fra virksomhed til virksomhed. Derfor kan der være behov for at analysere eksisterende informations-, dokumentations- og kontrolsystemer med henblik på at fastlægge hensigtsmæssige kontroller.

For at opbygge et stærkt kontrolmiljø er det vigtigt at tage højde for, at kontroller og deres egenskaber er forskellige. Nedenstående figur illustrerer, hvordan kontroller og deres styrke er i forhold til hinanden.

Kontrol	Manuel	Automatisk
Forebyggende	Middel	Stærk
Opdagende	Svag	Middel

Automatiske kontroller er normalt forebyggende og som følge heraf stærke, hvorimod manuelle kontroller som regel er opdagende og derved svage kontroller. Det er derfor ikke ligegyldigt, hvordan kontroller udføres og implementeres i en organisation. Jo flere automatiske kontroller en virksomhed har, desto stærkere er kontrolmiljøet.

For at skabe et effektivt kontrolmiljø bør det identificeres, hvor kontroller skal implementeres. Dette bør gøres ud fra en "vugge til grav" vurdering af processen og skal rette fokus mod, hvad kontrollen skal afdække, samt hvilken styrke kontrollen skal have.



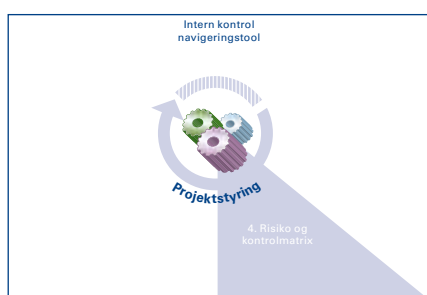
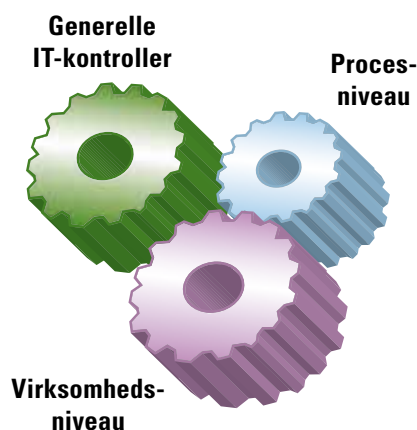
Ovenstående eksempel illustrerer et "process flow", hvor forbyggende kontroller er i selve processen, hvorimod opdagende kontroller ligger uden for processen.

Virksomheden bør foretage en gennemgående analyse af det eksisterende kontrolsystem og etablere målsætninger på følgende tre niveauer:

Indarbejdelse af risikostyring i virksomheden er grundlæggende en proces bestående af planlægning, handling, overvågning og læring

- *Kontroller på virksomhedsniveau*, som består af kontroller, der kan påvirke forskellige dele af organisationen og dermed også flere processer i virksomheden. Som eksempel kan nævnes udarbejdelse af politikker og procedurer og retningslinjer for håndhævelse heraf, eksempelvis en regnskabsmanual, uddelegering af bemyndigelse til de rette personer, etablering af udvalg samt ledelsesmæssig overvågning af kontroller på procesniveau.
- *Kontroller på procesniveau*, der dækker risikoen for væsentlige fejl forbundet med regnskabsafklæggelsen, fra det tidspunkt hvor transaktioner initieres og registreres til de præsenteres og oplyses i den finansielle rapportering. Manuelle kontroller kan eksempelvis være afstemninger af bankkonti til ekstern dokumentation. Automatiske kontroller er typisk indbygget i it-applikationer, og kan omfatte kontrol af, at fakturering til en kunde ikke overstiger et fastsat kreditmaksimum samt automatisk matchning af foretagne registreringer. Det er også muligt at foretage en kombination af automatiske og manuelle kontroller, eksempelvis når en automatisk genereret fejlmeddelelse under en lønkørsel udløser en manuel gennemgang og opfølgning på fejl. Som udgangspunkt er automatiske kontroller at foretrække, da de ofte er mere pålidelige og omkostningsbesparende i forhold til manuelle kontroller.
- *Generelle it-kontroller*, der sikrer, at der bl.a. er hensigtsmæssig funktionsadskillelse i de it-applikationer, som anvendes, således at funktionsadskillelsen understøtter den organisatoriske funktionsadskillelse, samt at der foretages kontrollerede ændringer til it-systemer. Dette sikrer, at automatiske kontroller kontinuerligt fungerer efter hensigten.

Et velfungerende internt kontrolsystem indebærer, at de tre niveauer indbyrdes hænger sammen.



5.7 Risiko- og kontrolmatrix

Virksomheden kan med fordel udarbejde en generisk risiko- og kontrolmatrix, der er en skematisk opdeling af væsentlige risici forbundet med regnskabsaf-læggelsen.

Formålet med en generisk risiko- og kontrolmatrix er, at virksomheden definerer de kontroller, der vil være de mest hensigtsmæssige, uafhængigt af hvilke kontroller der allerede måtte være implementeret. Ud fra metoden i risikovurderingsprocessen er fokus og omfang fastlagt på koncernniveau, hvorfor den generiske risiko- og kontrolmatrix ligeledes vil have fokus på kontroller, der afdækker koncern risici. Deraf navnet generisk risiko- og kontrolmatrix.

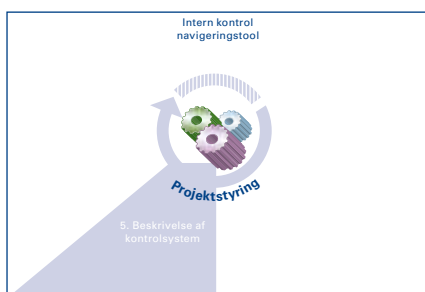
En generisk *risiko- og kontrolmatrix* vil eksempelvis gøre det muligt at identificere, hvorvidt der er etableret tilstrækkelige kontroller for en given risiko. Med udgangspunkt i kontrolmatrixen kan det identificeres, hvorvidt flere kontroller afdækker samme risiko, eller en enkelt kontrol afdækker et større antal risici (optimering af kontroller). Dog skal man være opmærksom på, at kontroller relateret til en regnskabspost ikke nødvendigvis dækker alle relevante regnskabsudsagn, og det kan derfor være nødvendigt at etablere mere end én kontrol for at afdække risikoen for fejl i én regnskabspost.

Det kan være hensigtsmæssigt at samarbejde med virksomhedens eksterne revisor ved udarbejdelsen af kontrolmatrixen, således at der så vidt muligt bliver overensstemmelse mellem denne og de af ekstern revisor identificerede risici i revisionsplanlægningen

Generisk risiko- og kontrolmatrix

Kontrol mål	Risiko	Kontrolaktivitet	Ønskeligt bevis	Revisionsmål	COSO-komponent
K1 Tilgodehavender afspejler den korrekte værdiansættelse baseret på sandsynligheden for indsamling, erfaringer og virksomhedens retningslinjer	K1.1 Tilgodehavender er ikke korrekt værdiansat	K1.1.1 Debitor forfaldsli- ster samt for- faldne beløb gennemgås regelmæssigt og handlingsplan udarbejdes	Forfaldsli- ster med markeringer omkring udestå- ende samt tilhø- rende rykkeproce- dure er gennem- gået. Hensættelse til tab på debitor- er er gennemgået og godkendt	Fuldstændighed Tilstedeværelse Nøjagtighed	Kontrolaktivitet
		K1.1.2 Finanssystemet er opsat således, at forfaldne udestå- ende er korrekt beregnet	Udskrift fra regn- skabssystem hvor forfaldsli- ster efterregnes	Fuldstændighed Nøjagtighed	Kontrolaktivitet

Ovenstående figur illustrerer en generisk risiko- og kontrolmatrix og tager sit udgangspunkt i de fra risikovurderingsprocessens identificerede områder, som skal understøttes af hensigtsmæssige kontroller. De to første kolonner afdækker mål og risiko med opsatte kontroller. Derudover indeholder matrixen en beskrivelse af de kontroller, som vil være mest hensigtsmæssige at have implementeret i virksomheden eller i de enheder, som er omfattet af opgavens omfang. Dernæst er det angivet som en hjælp til de involverede enheder, hvilken dokumentation der skal være, for at en kontrol er implementeret rigtigt.



5.8 Beskrivelse af kontrolsystem

Efter at den generiske kontrolmatrix er udarbejdet, bør den fremsendes til de enheder, der bidrager til fastsatte risici ud fra risikovurderingsprocessen. Baseret på den generiske kontrolmatrix bør de enkelte enheder udfylde nedenstående dokumentationsmatrix.

Dokumentationsmatrix

Dokumentation	Bevis for given kontrol	Frekvens af kontrol	Kontrollejer	Ansvarlig for at gennemføre kontrollen
K.1.1.1 Reference til Standard Operating Procedure (SOP), eller en kort beskrivelse af forretningsgangen	K.1.1.1 Hvad er beviset for at kontrollen udføres?	K.1.1.1 Hvor ofte udføres kontrollen? Å = Årligt M = Månedlig U = Ugentligt D = Dagligt K = Kontinuerligt	K.1.1.1 Hvem er ansvarlig for kontrollen?	K. 1.1.1 Hvem udfører kontrollen?

Ovenstående dokumentationsmatrix udfyldes af alle de enheder, der er defineret i risikovurderingsprocessen. Enhederne skal besvare, hvordan de håndterer de i den generiske kontrolmatrix definerede kontroller. Dokumentationen er en forretningsgangsbeskrivelse af hvordan kontrol udføres, derudover dokumentation (bevis) på hvorledes kontrollen er udført, hvor ofte kontrollen udføres, hvem ejeren af kontrollen er samt hvem der udfører kontrollen.

Det anbefales, at alle templates (generisk kontrolmatrix, dokumentationsmatrix, forretningsbeskrivelser, forbedringstiltag osv.) som enhederne skal anvende, er udarbejdet fælles for alle, så der efterfølgende kan dannes et samlet overblik.

Dokumentationsopgaven vil uden tvivl blive den opgave, som mange virksomheder vil opfatte som den mest ressourcekrævende. Men det er en vigtig og central del i at have et veldokumenteret kontrolmiljø.

Forretningsgangsbeskrivelser bør besvare følgende grundlæggende spørgsmål (hvem, hvad, hvornår, hvor, hvorfor, hvordan, hvor ofte?). Dokumentationen af kontroller skal beskrive, hvorledes fejl rettes, når de opdages som følge af udførelsen af en kontrol.

Eksempel på kontrolbeskrivesskema

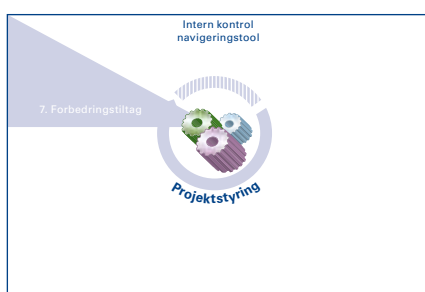
Generel information	
Firmanavn	XXX A/S
Kontrolnavn	K.1.1.1
Proces	Forfaldne debitorer
Kontrolmål	Tilgodehavender afspejler den korrekte værdiansættelse baseret på sandsynligheden for indsamling, erfaringer og virksomhedens retningslinjer
Risiko	Tilgodehavender er ikke korrekt værdiansat.
Kontrolprocedure	Debitor forfaldslistes samt forfaldne beløb gennemgås regelmæssigt og handlingsplan udarbejdes.
Kontrolejer	Regnskabsansvarlig

Kontrol information	
Beskrivelse af kontrol	<p>En gang pr. kvartal udskriver debitorbogholder en debitor forfaldsliste, hvor en gennemgang af alle forfaldne debitorer foretages. Gennemgangen tager sit udgangspunkt i de retningslinjer, som er udarbejdet (se politik deb2009).</p> <p>Debitorer 30><60 dage, skal have første rykker.</p> <p>Debitorer 60><90 dage, skal have anden rykker, der hensættes 25 %.</p> <p>Debitorer 90><120 dage, kunden kontaktes af salgsansvarlig, der hensættes 50 %.</p> <p>Debitorer >120 dage, engagement med kunden tages op til overvejelse og der hensættes 100 %.</p> <p>Møde mellem CFO og salgsdirektør afholdes, hvor handlingsplan udarbejdes. Ansvaret for det videre forløb overgår til salgsdirektøren.</p> <p>Debitorbogholderens gennemgang afleveres til den regnskabsansvarlige for godkendelse, inden politikken for forfaldne debitorer udføres.</p>
Beskrivelse af handling hvis kontrollen ikke opfyldes	Hvis dele af de fastlagte politikker ikke efterleves (kontrolleres af group controller) udarbejdes en afvigelsesrapport (se politik afv2009), som sendes til regnskabschefen. Group controller iværksætter en handlingsplan, således at kontrollen efterleves og afventer CFO tilbagemelding. Hvis kontrollen gentagne gange ikke udføres, vil group controller rapportere afvigelsen til revisionsudvalget.
Frekvens	Kvartalsvis

En beskrivelse giver i sig selv ikke sikkerhed for, at kontrol er korrekt udformet og fungerer som beskrevet. Virksomheden bør derfor foretage en gennemgang af det eksisterende interne kontrolsystem, f.eks. ved at følge de enkelte transaktioner fra initiering til de indgår i den finansielle rapportering.

Endvidere kan det være relevant at vurdere kontrolsystemets effektivitet, dvs. hvorvidt kontrolsystemet fungerer som tiltænkt over en fastlagt periode.

Efter at enhederne (og koncernen) har udfyldt dokumentationsmatrixen samt beskrevet de forretningsgange, der understøtter kontrollerne, kan det vise sig, at de opsatte kontroller fra den generiske kontrolmatrix ikke bliver opfyldt eller ikke er implementeret i den pågældende enhed. Den generiske kontrolmatrix er de kontroller, virksomheden ønsker at implementere, hvorimod dokumentationsmatrixen er hvad enhederne har implementeret. Den forskel, der måtte være, kan udløse, at der efterfølgende skal foretages ændringer i kontrollerne eller, at der skal implementeres nye. Disse ændringer eller forbedringstiltag skal ligeledes planlægges og godkendes inden de implementeres.



5.9 Forbedringstiltag

Virksomheden bør beskrive hvilke tiltag, der skal gennemføres, når mangler identificeres. F.eks. hvorledes forbedringer bør implementeres, og hvorledes implementeringsprocessen bør overvåges. Erfaringer viser, at mangler vedrørende it-forhold bør gives høj prioritet, idet de kan have en betydelig indvirkning på andre dele af det interne kontrolsystem, samt at udbedring af mangler ofte er meget ressourcekrævende.

Beskrivelsen af forbedringstiltag kan følge strukturen illustreret i figuren nedenfor, hvor manglen og effekt heraf samt foreslåede forbedringstiltag anføres i tabelform. Figuren giver overblik over forbedringstiltagene og en ensartet metode til godkendelse af tiltagene. Denne struktur giver ligeledes mulighed for at få en ensartet rapportering fra alle enheder i en koncern og derigennem prioritere, hvilke områder der skal tages hånd om først.

Forbedringstiltag/planlægningsværktøj

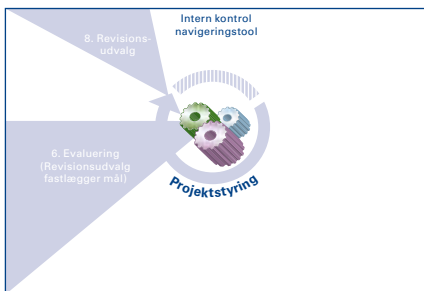
Kontrollens modenhed 1-6	Hvis modenhed er 1-2, beskriv handlingsplan for kontrol	Deadline for implementering af tiltag	Ansvar for gennemførelse af tiltag
K.1.1.1 Er kontrollen implementeret og hvor stærk er den. 1 = ikke implementeret 6= implementeret og testet	K.1.1.1 Beskriv hvordan kontrol kan styrkes og hvilke tiltag der skal gennemføres	K.1.1.1 Hvornår vil tiltaget være implementeret	K.1.1.1 Hvem er ansvarlig for gennemførelse af tiltaget

Af figuren ovenfor ses, at det for hver enkelt kontrol fra den generiske kontrolmatrix skal vurderes, hvilken modenhed den pågældende kontrol har. Dette kan gøres ud fra en skala fra 1 - 6.

- 1: Kontrollen eksisterer ikke
- 2: Kontrollen er ikke implementeret, men forbedringstiltag igangsat
- 3: Kontrollen er under implementering, men ikke dokumenteret

- 4: Kontrollen er implementeret, men ikke dokumenteret
- 5: Kontrol implementeret og dokumenteret
- 6: Kontrol implementeret, dokumenteret og testet.

Beskrivelsen af forbedringstiltag giver et overblik og en ensartet metode til godkendelse af tiltagene. Et vigtigt punkt er ikke alene modenheden af kontrollen, men også hvilken handlingsplan en ny eller forbedret kontrol skal efterleve. Værktøjet kan anvendes som grundlag for rapportering til revisionsudvalget, da det kan give en status over implementering. Opdeles den generiske risiko- og kontrolmatrix efter processer og ligeledes efter enheder, kan værktøjet benyttes som et prioriteringsredskab som virksomheden kan styre sine ressourcer efter.



5.10 Overvågning af virksomhedens interne kontrol- og risikostyringssystemer

Årsregnskabsloven stiller ikke krav om, at der i årsrapporten skal rapporteres omkring effektiviteten af virksomhedernes interne kontrolsystem.

Revisionsudvalget har til opgave, at overvåge om virksomhedens interne kontrolsystem, eventuelle interne revision og risikostyringssystemer fungerer effektivt. Revisionsudvalget skal ikke overvåge alle kontroller i virksomheden, men kun de der af revisionsudvalget vurderes som værende betydelige som følge af, at de relaterer sig til væsentlige transaktionsstrømme eller risici.

Det er vigtigt, at revisionsudvalget indledningsvis får defineret, hvad de vurderer som værende væsentlige transaktionsstrømme eller risici, således at overvågningen kan tilrettelægges på det grundlag.

Har virksomheden et systematiseret og veldokumenteret kontrolsystem, kan der foretages en mere effektiv og målrettet overvågning, da det er beskrevet, hvilke risici virksomheden er udsat for, og hvilke kontroller virksomheden har til at afdække disse risici.

Effektiv overvågning er en del af et velfungerende internt kontrolsystem. For at sikre en effektiv overvågning bør ledelsen have en passende forståelse af virksomhedens risici og interne kontroller. Endvidere bør der fastlægges en proces, som sikrer, at overvågning af kontroller udføres baseret på et væsentlighedsniveau.

For at kunne håndtere overvågningen af de interne kontroller i større virksomheder, kan opgaven delegeres til eksempelvis lokale ledelser, kontrollere eller interne revisorer. Resultatet heraf bør rapporteres til den øverste ledelse.

Overvågning af implementering og strukturering af kontrolsystemet

Overvågningen af det interne kontrolsystem kan deles op i to dele:

- Overvågning af implementering
- Løbende overvågning af om implementerede kontroller fungerer effektivt og afdækker de risici som virksomheden er eksponeret ovenfor

Implementeringen kan med udgangspunkt i den proces som er beskrevet i afsnit 5.1 til 5.9 overvåges ved, at det vurderes hvor langt virksomheden er i det skitserede forløb.

I forbindelse med implementering af specifikke kontroller, kan for eksempel forbedringstiltag/planlægningsværktøjet anvendes som udgangspunkt for overvågningen af hvorledes implementeringen af kontrollerne forløber.

Forbedringstiltag/planlægningsværktøj

Kontrollens modenhed 1-6	Hvis modenhed er 1-2, beskriv handlingsplan for kontrol	Deadline for implementering af tiltag	Ansvar for gennemførelse af tiltag
K.1.1.1 Er kontrollen implementeret og hvor stærk er den. 1 = ikke implementeret 6 = implementeret og testet	K.1.1.1 Beskriv hvordan kontrol kan styrkes og hvilke tiltag der skal gennemføres	K.1.1.1 Hvornår vil tiltaget være implementeret	K.1.1.1 Hvem er ansvarlig for gennemførelse af tiltaget

Som det fremgår af ovenstående matrix, anvendes en modenhedsskala (kontrollens modenhed 1-6), hvor 1 indikerer, at kontrollen ikke eksisterer, og 6 at kontrollen er implementeret, dokumenteret og testet.

Med udgangspunkt i ovenstående kan der udarbejdes en samlet rapportering/ vurdering af den igangværende implementering. I nedenstående figur er det illustreret, hvorledes der kan rapporteres til ledelsen samt revisionsudvalget.

Figuren nedenfor viser antallet af kontroller for forretningsenhed 1 og 2 samt virksomheden som helhed, herunder hvilken modenhed kontrollerne har. I denne forbindelse er det vigtigt, at få defineret hvad en acceptabel status er, jf. nedenstående farvekodning.

Enhed 1			Enhed 2			Virksomhed		
	Antal kontroller	Værdi		Antal kontroller	Værdi		Antal kontroller	Værdi
Modenhed 1	5	5	Modenhed 1	1	1	Modenhed 1	6	6
Modenhed 2	8	16	Modenhed 2	1	2	Modenhed 2	9	18
Modenhed 3	15	45	Modenhed 3	1	3	Modenhed 3	16	48
Modenhed 4	20	80	Modenhed 4	20	80	Modenhed 4	40	160
Modenhed 5	8	40	Modenhed 5	20	100	Modenhed 5	28	140
Modenhed 6	12	72	Modenhed 6	20	120	Modenhed 6	32	192
I alt	68	258	I alt	63	306	I alt	131	564
Gennemsnit		3,8			4,9			4,3

Tolerancegrænser	
0.00 - 2.50	Rød
2.51 - 4.99	Gul
5.00 - 6.00	Grøn

Hvis den samlede rapportering for enheden ligger under gennemsnittet (enhed 1), kan ledelsen eller revisionsudvalget anmode om, at der prioriteres ressourcer til denne enhed.

Ved at anvende trafiklys kan der skabes et hurtigt overblik over implementeringsforløbet og fokus kan rettes mod enheder/processer, som kræver større bevågenhed. Udover ovenstående rapportering kan andre relevante dokumenter vedlægges som bilag.

Når de interne kontroller er implementerede, bør fokus ændres til hvorvidt kontrollerne udføres og fungerer effektivt.

For at foretage en objektiv vurdering af effektiviteten af de interne kontroller kræves det, at der er et sæt af kriterier, som danner grundlag for vurderingen.

Bestyrelsen/revisionsudvalget bør løbende modtage rapportering om overvågning af interne kontroller

Disse kriterier fastlægges almindeligvis af ledelsen på baggrund af en vurdering af væsentlighed og risici, herunder hvilken tolerancetærskel som accepteres. Dvs. en virksomhed kan have effektive kontroller, selv om ikke alle risici bliver afdækket.

Baseret herpå skal det vurderes, om udformningen af kontrollerne afdækker væsentlige risici inden for en acceptabel tolerancetærskel, samt at de implementerede kontroller fungerer over tid. F.eks. kan det være tilstrækkeligt, at nogle kontroller udføres årligt, mens andre udføres dagligt.

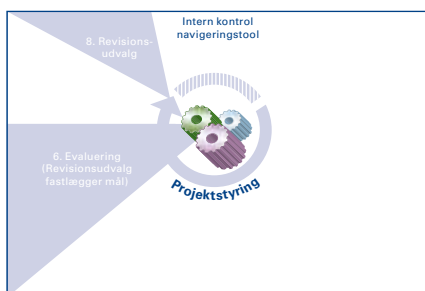
Nedenfor er skitseret et simpelt værktøj, som kan give et overblik over kontrollens effektivitet. Forudsætningen for værktøjet er, at en kontrol kan være udført eller ikke udført. Hvis den er udført, kan den antage værdien 1 og hvis den ikke er, værdien 0. Defineres der herudover intervaller for hvornår et kontrolmiljø fungerer effektivt (grøn), fungerer delvist effektivt (gul) eller ikke fungerer effektivt (rødt), kan der gives et overskueligt billede af status på virksomhedens interne kontroller. Det bør i tillæg til dette rapporteres, hvilke kontrolnedbrud der har været og hvorfor inden for en given tidshorisont. Yderligere bør det rapporteres, hvilke forbedringer der kunne være aktuelle, f.eks fokus fra manuelle til automatiske kontroller eller at have forbyggende frem for opdagende kontroller.

Virksomheden			Virksomheden				
	Kontroller	Fungerer	Værdi		Kontroller	Fungerer	Værdi
Proces 1	10	9	0,90	Enhed 1	3	3	1,00
Proces 2	10	10	1,00	Enhed 2	5	4	0,80
Proces 3	10	8	0,80	Enhed 3	8	5	0,63
Proces 4	10	6	0,60	Enhed 4	15	10	0,67
proces 5	10	9	0,90	Enhed 5	20	18	0,90
Proces 6	10	7	0,70	Enhed 6	9	9	1,00
I alt	60	49	0,82		60	49	0,82

Tolerancegrænser	
0.00 - 0.74	Rød
0.74 - 0.89	Gul
0.90 - 1.00	Grøn

Rapporteringen bør fokusere på om der er konstateret væsentlige kontrolnedbrud eller svagheder, herunder hvilken betydning de faktisk har haft, kunne have haft eller kan få for virksomheden, og hvilke tiltag der er iværksat for at afhjælpe dem.

Bliver ledelsen opmærksom på væsentlige interne kontrolnedbrud eller svagheder, skal den fastlægge/undersøge, hvor nedbruddet eller svagheden er opstået og revurdere effektiviteten af ledelsens løbende processer for udarbejdelse, drift og overvågning af det interne kontrolsystem.



5.11 Intern revision

I henhold til revisorloven skal revisionsudvalget overvåge, om virksomhedernes eventuelle interne revision og risikostyringssystemer fungerer effektivt.

Intern revisions formål kan variere fra virksomhed til virksomhed, men almindeligvis består intern revisions opgaver i at overvåge virksomhedens interne kontrolsystem på vegne af bestyrelsen/revisionsudvalget.

Behovet for en intern revision varierer alt efter virksomhedens individuelle forhold, herunder kompleksiteten og omfanget af virksomhedens aktiviteter, antallet af medarbejdere og virksomhedens kultur.

Ved vurderingen af behovet for en intern revision skal bestyrelsen overveje, om der er andre måder at opnå tilstrækkelig og objektiv sikkerhed for det interne kontrolsystems effektivitet.

Behovet for intern revision kan opstå som følge af, at eventuelle udviklingstendenser og aktuelle forhold i virksomhedens interne miljø, markeder eller andre aspekter af det eksterne miljø, kan have forøget eller forventes at forøge virksomhedens risici. Eksempler på sådanne udviklingstendenser:

- Omstrukturering af organisationen
- Ændringer i rapporteringsprocesser og de underliggende informationssystemer
- Konstatning af negative udviklingstendenser ved overvågningen af interne kontrolsystemer
- Stigende forekomst af uforudsete eller uacceptable resultater
- Indtræden på nye væsentlige markeder eller markeder med høj risiko
- Ændringer i arbejdsstyrkens aflønning
- Organisationens kultur.

Hvis virksomheden har en intern revision, er det sædvanligt, at bestyrelsen og/eller revisionsudvalget en gang om året gennemgår dennes arbejdsområde, bemyndigelse og ressourcer. Det anbefales, at bestyrelsen og/eller revisionsudvalget herunder overvejer følgende:

- Hvor effektivt hjælper den interne revisionsfunktion direktionen og bestyrelsen med at opnå virksomhedens målsætninger?
- Er den interne revisionsfunktion respekteret i hele virksomheden?
- Tilføjer den interne revisionsfunktion virksomheden værdi, og måles denne værdi?
- Hvor ofte rapporterer den interne revisionsfunktion til revisionsudvalget eller hele bestyrelsen?
- Hvor godt tilpasser den interne revisionsfunktion sig til ændringer i virksomheden?

Kapitel 6

Praktiske problemstillinger

Ved implementering af den nye lovgivning er der mange forhold, der skal tages højde for. Nedenfor er skitseret nogle af de praktiske problemstillinger, som er erfaret fra implementeringer af interne kontrol- og risikostyrings-systemer i bl.a. USA og UK:

- Målet med implementeringen er ikke klart defineret før projektet i gang-sættes.

Det anbefales, at udgangspunkt for projektet er hvad der forventes skrevet i årsrapporten.

Det anbefales, at virksomhedens eksterne revisor involveres tidligt i proces-sen, således at allerede foretagne risikovurderinger vedrørende regnskabs-aflæggelsen så vidt muligt genbruges.

- Manglende involvering fra den øverste ledelse, da projektet opfattes som et projekt for økonomi-/regnskabsfunktionen.

Det anbefales, at hele organisationen så vidt muligt orienteres om projektet, og den øverste ledelse tager aktivt del i implementeringen.

- Ressourcebehovet undervurderes og der er ikke den nødvendige tid til at gennemføre opgaven.

Det anbefales, at der etableres en projektorganisation, og nødvendige ressourcer indsættes.

Det anbefales, at der fastlægges en klar prioritering af opgaverne og kommunikation heraf.

- Identifikation af for mange og for generelle risici og kontroller.

Der anbefales en top-down risikobaseret tilgang til virksomhedens risiko-styringssystem. Herved undgås unødigt bureaukrati, for mange kontroller og fordybelse i irrelevante detaljer.

Det anbefales, at det samlede dokumentationsbehov, herunder metoder, værktøjer og templates, er fastlagt inden implementeringen igangsættes.

Kapitel 7

Afslutning

Ændringerne til årsregnskabsloven hvorefter virksomheder skal beskrive hovedelementerne i deres interne kontrol- og risikostyringssystemer i forbindelse med regnskabsafslæggelsesprocessen, forventes at afstedkomme øget arbejde med at dokumentere og strukturere processer og kontroller i danske børsnoterede virksomheder.

En beskrivelse af hovedelementerne kan umiddelbart forekomme enkel, ikke mindst i visse mindre virksomheder, men i større og mere komplekse koncerner vil redegørelsen og arbejdet med at dokumentere redegørelsen i sagens natur blive mere omfattende. Som illustration er der i bilag 1 udarbejdet et forslag til rapportering i årsrapporten. Forslaget er alene til illustration.



Bilag 1

Eksempel på rapportering i årsrapporten

Bestyrelsen og direktionen har det overordnede ansvar for koncernens risikostyring og interne kontrol i forbindelse med regnskabsaflæggelsesprocessen, herunder overholdelsen af relevant lovgivning og anden regulering i relation til regnskabsaflæggelsen (compliance).

Bestyrelsen finder, at "Tone-at-the-Top" er afgørende for god risikostyring og intern kontrol i forbindelse med regnskabsaflæggelsesprocessen. Bestyrelsen og direktionens holdning til god risikostyring og intern kontrol i forbindelse med regnskabsaflæggelsen indskærpes derfor til stadighed.

Koncernens risikostyring og interne kontroller i forbindelse med regnskabsaflæggelsesprocessen, inklusiv bl.a. it og skat, er designet med henblik på effektivt at styre, snarere end at eliminere, risikoen for fejl og mangler i forbindelse med regnskabsaflæggelsen.

Koncernens risikostyrings- og interne kontrolsystemer i forbindelse med regnskabsaflæggelsesprocessen kan alene skabe rimelig, men ikke absolut sikkerhed for, at uretmæssig brug af aktiver, tab og/eller væsentlige fejl og mangler i forbindelse med regnskabsaflæggelsen undgås.

Bestyrelsen/revisionskomitéen og direktionen vurderer løbende væsentlige risici og interne kontroller i forbindelse med koncernens aktiviteter og deres eventuelle indflydelse på regnskabsaflæggelsesprocessen.

Bestyrelsen har lagt det internationalt anerkendte COSO-framework til grund for sit arbejde med risikostyring og interne kontroller i forbindelse med regnskabsaflæggelsesprocessen.

Kontrolmiljø

Bestyrelsen vurderer mindst årligt koncernens organisationsstruktur og bemanningen på væsentlige områder, herunder inden for områder i forbindelse med regnskabsaflæggelsesprocessen inklusiv bl.a. it og skat.

Bestyrelsen og direktionen fastlægger og godkender overordnede politikker, procedurer og kontroller på væsentlige områder i forbindelse med regnskabsaflæggelsesprocessen. Grundlaget herfor er en klar organisationsstruktur, klare rapporteringslinjer, autorisations- og attestationsprocedurer samt personadskillelse ("the four-eye principle").

Bestyrelsen/revisionskomitéen vurderer årligt behovet for etablering af intern revision. Bestyrelsen har nedsat en intern revision, der refererer til bestyrelsen, og som i overensstemmelse med en vedtaget turnusplan stikprøvevis

reviderer forretningsgange og interne kontroller (operationel revision) på væsentlige og risikofyldte områder i forbindelse med regnskabsaflæggelsen.

Bestyrelsen har vedtaget politikker, manualer, procedurer m.v. inden for væsentlige områder i forbindelse med regnskabsaflæggelsen, herunder Code of Conduct, Code of Ethics, en regnskabs- og rapporteringsmanual (inklusiv minimumskrav til forretningsgange, interne kontroller, personadskillelse, afstemninger, godkendelse, autorisation, attestation, regnskabspraksis, intern og ekstern rapportering m.v.), en treasury- og finanspolitik (Treasury Manual) inklusiv godkendelse af modparter samt fastlæggelse af "lines" og "limits" for finanstransaktioner og modparter, en skattepolitik, en it-strategi, en it-sikkerhedspolitik samt en "whistle-blowing"-politik.

De vedtagne politikker, manualer og procedurer er tilgængelige på koncernens intranet, og overholdelsen heraf indskræpes løbende. Der foretages løbende stikprøvevis overvågning og kontrol af overholdelsen.

Direktionen overvåger løbende overholdelsen af relevant lovgivning og andre forskrifter og bestemmelser i forbindelse med regnskabsaflæggelsen (compliance) og rapporterer løbende herom til bestyrelsen/revisionskomitéen.

Risikovurdering

Bestyrelsen/revisionskomitéen og direktionen foretager mindst årligt en overordnet risikovurdering af risici i forbindelse med regnskabsaflæggelsesprocessen.

Bestyrelsen vedtager på det grundlag en koncern Risk Management-politik, der bl.a. indeholder en beskrivelse af de væsentligste risici i forbindelse med regnskabsaflæggelsesprocessen samt tiltag med henblik på at styre henholdsvis eliminere og/eller reducere risiciene.

Bestyrelsen og direktionen tager som led i risikovurderingen årligt stilling til risikoen for besvigelser og til de foranstaltninger, der skal tages med henblik på at reducere og/eller eliminere disse risici. Herunder vurderer bestyrelsen den daglige ledelses mulighed for at tilsidesætte kontroller og for at udøve upassende indflydelse på regnskabsaflæggelsen.

Ved væsentlige akquisitioner gennemføres en overordnet risikoanalyse for den nytilkøbte virksomhed, ligesom de væsentligste forretningsgange og interne kontroller i forbindelse med regnskabsaflæggelsen i de nytilkøbte virksomheder overordnet gennemgås som led i due diligence og/eller umiddelbart efter overtagelsen.

Beslutninger om tiltag med henblik på reduktion og/eller eliminering af risici baseres på en vurdering af væsentlighed og cost/benefit-analyser.

De væsentligste risici i forbindelse med regnskabsaflæggelsen fremgår af ledelsesberetningen og noterne til regnskabet, hvortil der henvises.

Kontrolaktiviteter

Kontrolaktiviteterne tager udgangspunkt i risikovurderingen. Målet med koncernens kontrolaktiviteter er at sikre, at de af direktionen udstukne mål, politikker, manualer, procedurer m.v. opfyldes, samt rettidigt at forebygge, opdage og rette eventuelle fejl, afvigelser og mangler m.v.

Kontrolaktiviteterne omfatter manuelle og fysiske kontroller samt generelle it-kontroller og automatiske applikationskontroller i de anvendte it-systemer m.v.

Der er minimumskrav til forsvarlig sikring af aktiver samt til afstemninger og regnskabsanalytisk gennemgang, herunder løbende vurdering af performance og opfyldelsen af vedtagne mål (Key Performance Indikatorer m.v.).

Direktionen har etableret en formel koncernrapporteringsproces, der omfatter budgetrapportering og månedlig rapportering inkl. afvigelsesrapporter med månedlig/kvartalsvis ajourføring af skøn for året. Rapporteringen omfatter, ud over resultatopgørelse, balance og pengestrømsopgørelse, tillige noter og supplerende oplysninger.

Der indhentes løbende oplysninger til brug for opfyldelsen af eventuelle notekrav samt andre oplysningskrav.

Bestyrelsen indhenter årligt en ledelseserklæring i hver enkelt rapporterende enhed i koncernen i relation til overholdelsen af de vedtagne koncernpolitikker og interne kontrolforskrifter.

Information og kommunikation

Bestyrelsen har vedtaget en informations- og kommunikationspolitik, der bl.a. overordnet fastlægger kravene til regnskabsafleggelsen og til den eksterne finansielle rapportering i overensstemmelse med lovgivningen og forskrifterne herfor.

Et af målene med den af bestyrelsen vedtagne informations- og kommunikationspolitik er, at sikre at gældende oplysningsforpligtelser overholdes, samt at de afgivne oplysninger er dækkende, fuldstændige og præcise.

Bestyrelsen lægger vægt på, at der – inden for de rammer, der gælder for børsnoterede virksomheder – er en åben kommunikation i virksomheden samt på, at den enkelte kender sin rolle i den interne kontrol i virksomheden.

Koncernens væsentligste risici og interne kontroller i forbindelse med regnskabsafleggesprocessen, bestyrelsens holdning hertil og de iværksatte tiltag i forbindelse hermed kommunikeres løbende internt i koncernen.

Bestyrelsen og direktionen lægger vægt på, at den enkelte medarbejder til stadighed, rettidigt har relevante informationer til rådighed til at kunne udføre opgaverne.

Informationssystemerne indrettes med henblik på, at der under hensyntagen til den for børsnoterede virksomheder foreskrevne fortrolighed løbende på relevant niveau identificeres, opsamles og kommunikeres relevant information, rapporter m.v., som gør det muligt for den enkelte effektivt og pålideligt at udføre opgaverne og at udføre kontroller. Målet hermed er, at virksomheden til stadighed kan rapportere troværdigt og kontrollere med henblik på effektivt at styre virksomheden operationelt, finansielt og i overensstemmelse med gældende lovgivning og forskrifter.

Informationssystemet med tilhørende manuelle og systemmæssige kontroller skal gøre det muligt at udføre og dokumentere kontroller effektivt og hensigtsmæssigt. Endvidere skal informationssystemet muliggøre, at der rettidigt

kommunikeres effektivt og pålideligt op og ned i organisationen samt, hvor relevant, med kunder, leverandører, myndigheder, aktionærer, investorer, finansmarkederne og pressen m.v.

Overvågning

Ethvert risikostyrings- og internt kontrolsystem skal løbende overvåges, kontrolleres og kvalitetssikres for at sikre, at det er effektivt.

Overvågningen sker ved løbende og/eller periodiske vurderinger og kontroller på alle niveauer i koncernen. Omfanget og hyppigheden af de periodiske vurderinger afhænger primært af risikovurderingen herfor og effektiviteten af de løbende kontroller.

Eventuelle svagheder, kontrolsvigt, overskridelser af udstukne politikker, rammer m.v. eller andre væsentlige afvigelser rapporteres op i organisationen i overensstemmelse med koncernens politikker og instruktionerne herfor. Svagheder, mangler og/eller overskridelser rapporteres til direktionen. Væsentlige forhold rapporteres tillige til revisionskomitéen/bestyrelsen.

Bestyrelsen/revisionskomitéen modtager løbende rapporter fra direktionen henholdsvis fra intern revision om overholdelsen af de udstukne retningslinjer m.v. samt om konstaterede svagheder, mangler og/eller overtrædelser af vedtagne politikker, forretningsgange og interne kontroller.

De generalforsamlingsvalgte revisorer rapporterer i revisionsprotokollatet til bestyrelsen væsentlige svagheder i koncernens interne kontrolsystemer i forbindelse med regnskabsafslæggelsesprocessen. Mindre væsentlige forhold rapporteres i Management Letters til direktionen.

Bestyrelsen/revisionskomitéen overvåger, at direktionen reagerer effektivt på eventuelle svagheder og/eller mangler, samt at aftalte tiltag i relation til styrkelse af risikostyring og interne kontroller i relation til regnskabsafslæggelsesprocessen implementeres som planlagt. Direktionen følger op på implementeringen af konstaterede svagheder i dattervirksomheder samt på forhold, der er omtalt i Management Letters m.v.

Bilag 2

COSO-Framework

Definition af intern kontrol og risikostyring

I 1992 udviklede "the Committee of Sponsoring Organizations of the Treadway Commission (COSO)" en model for evaluering af interne kontroller. COSO-modellen er i dag generelt accepteret som begrebsramme for interne kontroller og er udbredt som værende en standard for en virksomheds vurdering af deres interne kontrol og risikostyringssystem.

COSO Enterprise Risk Management (ERM) – Integrated Framework definerer *risikostyring* som følger:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

COSO definerer *intern kontrol* som følger:

"Internal control is a process effected by an entity's board of directors, management, and other personnel, and it is designed to provide reasonable assurance that organizational objectives can be met."

Som det fremgår, er målet med risikostyring og intern kontrol som udgangspunkt det samme, idet begge medvirker til, at virksomheden opnår sine mål.

COSO anvendes globalt, og mange vil kender begrebsrammen. COSO kan derfor anvendes i kommunikation til omverdenen om det interne kontrolsystem.

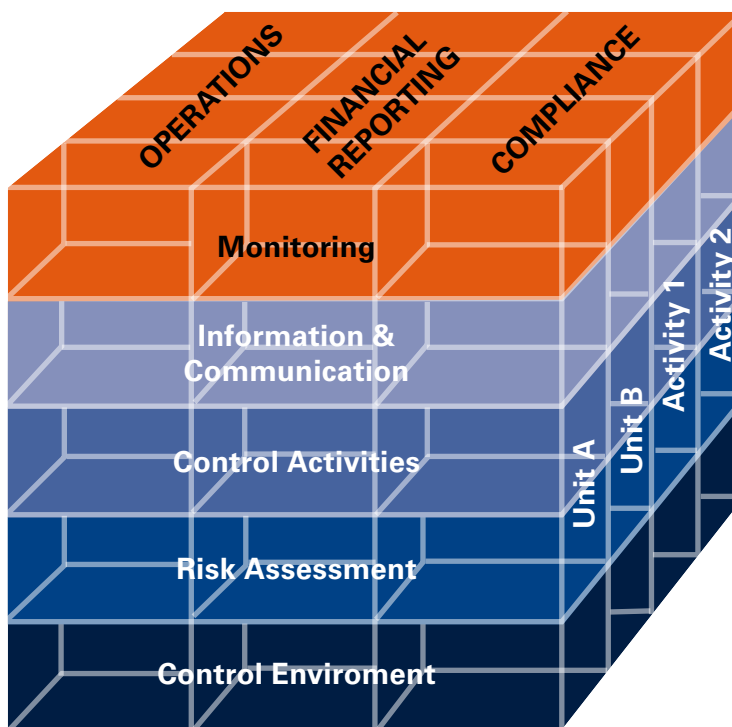
Det skal understreges, at årsregnskabsloven ikke kræver, at COSO anvendes som begrebsramme.

Komponenterne i et internt kontrolsystem

Et internt kontrolsystem omfatter politikker, processer, opgaver, adfærd, og andre aspekter i et virksomhed som tilsammen:

- Bidrager til en *effektiv drift*, fordi det er i stand til at reagere hensigtsmæssigt på væsentlige forretningsmæssige, operationelle, finansielle, compliance-relaterede og andre risici, der truer opnåelsen af virksomhedens mål, herunder at sikre aktiver mod forkert anvendelse, tab og besvigelser samt sikre, at forpligtelser identificeres og styres.
- Medvirker til at sikre kvaliteten af den interne og eksterne rapportering. Det kræver, at organisationen har de nødvendige registreringer og processer for at sikre rettidig, relevant og pålidelig intern og ekstern information.
- Medvirker til at sikre overholdelse af gældende love og regler samt interne politikker vedrørende udøvelse af virksomhedens aktiviteter.

Illustrativt er ovenstående vist i COSO-figuren vedrørende intern kontrol:



Et internt kontrolsystem bør i henhold til COSO generelt omfatte:

- **Kontrolmiljø (Control Environment)**

Kontrolmiljøet angiver organisationens retningslinjer og har indflydelse på, hvor opmærksomme medarbejderne er på kontrol. Det danner grundlag for alle andre dele af den interne kontrol, idet det skaber disciplin og struktur. Kontrolmiljøfaktorerne omfatter integritet, etiske værdier og kompetencer blandt virksomhedens medarbejdere, direktionens filosofi og bestyrelsesstil, hvordan direktionen uddelegerer bemyndigelser og ansvar og organiserer og udvikler medarbejderne samt bestyrelsens opmærksomhed og vejledning.²

- **Risikovurdering (Risk Assessment)**

Alle virksomheder udsættes for en række forskellige risici fra interne og eksterne kilder, som skal håndteres. Forudsætningen for risikovurderingen er, at der etableres mål, som er forbundet til forretningsmæssige planer og har en intern sammenhæng i virksomheden.

Risikovurderingen består af identifikation og analyse af relevante risici, der truer opnåelsen af virksomhedens mål og danner grundlag for, hvordan disse risici skal styres. Da økonomiske, branchemæssige, lovgivningsmæssige og driftsmæssige forhold til stadighed ændrer sig, er det nødvendigt at have mekanismer, der kan identificere og håndtere de særlige risici, der opstår i forbindelse med ændringer.²

² Internal control – integrated framework, udgivet i USA af the Committee of Sponsoring Organizations of the Treadway Commission (COSO) i 1992.

- **Kontrolaktiviteter (Control Activities)**

Kontrolaktiviteter er de politikker og procedurer, som er med til at sikre, at ledelsens beslutninger føres ud i livet. De medvirker til at sikre, at de nødvendige skridt tages til at imødegå risici, der truer opnåelsen af virksomhedens mål. Kontrolaktiviteter findes overalt i organisationen, på alle niveauer og alle funktioner. Kontrolaktiviteter omfatter godkendelse, autorisationer, verifikation, afstemning, sikring af aktiver og funktionsadskillelse.²

- **Informations- og kommunikationsprocesser (Information & Communication)**

Relevante informationer skal identificeres, opsamles og kommunikeres i en form og inden for en tidsramme, som giver medarbejderne mulighed for at udføre deres opgaver. Informationssystemer genererer rapportering, som indeholder driftsmæssige, finansielle og compliance-relaterede oplysninger, som gør det muligt at drive og kontrollere virksomheden. Det drejer sig ikke alene om internt genererede data, men også om oplysninger om eksterne begivenheder, aktiviteter og forhold, som er nødvendige for velinformeret beslutningstagning og ekstern rapportering.

Medarbejderne skal have klar besked fra den øverste ledelse om, at kontrolopgaven skal tages alvorligt. Alle i organisationen skal kende deres rolle i det interne kontrolsystem samt hvordan forretningsgange og kontrolaktiviteter relaterer sig til andres funktioners opgaver. De skal have mulighed for at kommunikere væsentlige oplysninger opad i systemet. Det er også vigtigt, at der er effektiv kommunikation med eksterne, f.eks. kunder, leverandører, myndigheder og aktionærer.²

- **Overvågning af det interne kontrolsystems effektivitet (Monotoring)**

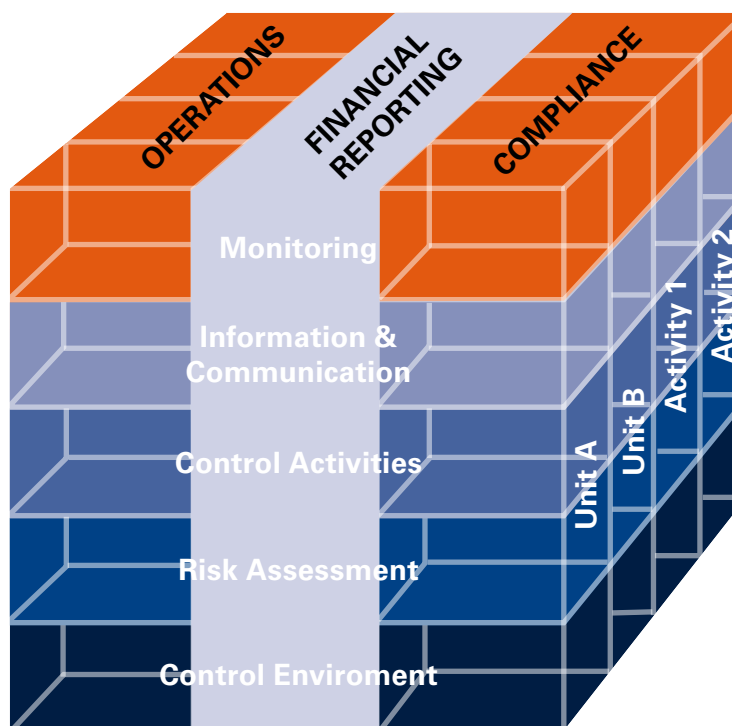
Interne kontrolsystemer skal overvåges – en proces som vurderer kvaliteten af systemets funktion over tid. Dette sker gennem løbende overvågningsaktiviteter, separate evalueringer eller en kombination heraf. I overvågningen indgår almindelige ledelses- og tilsynsaktiviteter samt andre handlinger, som medarbejderne udfører i forbindelse med deres arbejde. Omfanget og hyppigheden af separate evalueringer afhænger primært af en vurdering af risici og effektiviteten af de løbende overvågningsprocedurer. Mangler i den interne kontrol skal rapporteres opad i systemet, og alvorlige forhold skal rapporteres direkte til den øverste ledelse.³

Som illustreret på næste side udgør regnskabsprocessen kun en delmængde af det samlede interne kontrolsystem. I helheden indgår også kontrolaktiviteter relateret til drift (operation) og overholdelse (compliance) af lovgivning m.v.

Krav i årsregnskabsloven foreskriver, at virksomhederne beskriver det midterste spor (regnskabsaflæggelsesprocessen). anbefalingerne vedrørende god selskabsledelse omfatter principielt alle tre spor.

² Internal control – integrated framework, udgivet i USA af the Committee of Sponsoring Organizations of the Treadway Commission (COSO) i 1992.

³ Internal control – integrated framework, udgivet i USA af the Committee of Sponsoring Organizations of the Treadway Commission (COSO) i 1992.



For at kunne implementere et velfungerende internt kontrolsystem er det vigtig, at forstå de enkelte kontrollers formål og den sammenhæng de indgår i

Virksomheder kan med fordel anvende elementerne i COSO-modellen til at beskrive virksomhedens risikostyringsproces og de interne kontroller, der er etableret i relation til regnskabsafslæggelsesprocessen.

Bilag 3

Vurdering af interne kontrol- og risikostyringssystemer

Risikostyring er udgangspunktet i ethvert internt kontrolsystem.

For at vurdere virksomhedens interne kontrol- og risikostyringssystemer, kan virksomheden med fordel stille sig følgende spørgsmål:

Retningslinjer og politikker

- Har virksomheden en risikostyringspolitik der er klart defineret? Er den godkendt af bestyrelsen og udmeldt i organisationen og tilgængelig for organisationen og integreret i det daglige arbejde?
- Er der klart definerede roller og ansvar vedrørende identifikation, styring/ kontrol og rapportering af risici?

Adfærd

- Er der uafhængig overvågning af væsentlige interne kontroller og risikostyringsprocesser?
- Har de ansvarlige for risikostyring den nødvendige uddannelse?
- Efterlever medarbejderne virksomhedens risikoprofil?
- Forsøger organisationen at lære af en risikobegivenhed?

Roller og ansvarsområder

- Udføres kontroller af dem, der er ansvarlige for virksomhedens mål?
- Er ansvaret for rapporteringen klart defineret?
- Er der indskrevet ansvarsområder i alle relevante medarbejders jobbeskrivelser?

Konvertering af strategi til forretningsmæssige måls

- Afspejler de forretningsmæssige mål strategien?
- Bliver de forretningsmæssige mål kommunikeret klart ud i organisationen?

Målsætninger og kritiske succesfaktorer

- Har bestyrelsen et klart billede af mål og kritiske succesfaktorer?

Risikovillighed

- Er organisationens risikovillighed klart defineret?
- Er de enkelte forretningsområders mål justeret i forhold til de risici, de er udsat for?
- Er der udarbejdet handlingsplaner for at give organisationen en mere ønskværdig risikoprofil?

Risici, der truer performance

- Er der fastlagt risikostyringspolitikker, herunder kontroller for virksomhedens risici?
- Er risikovurderingsprocessen en integreret del af organisationens processer?
- Hjælper risikooplysningerne direktionen til at identificere ophobninger af risici og indbyrdes afhængigheder?

De mest hyppigt forekommende *svagheder* i risikostyringssystemer er:

- Politik for risikostyring – politikken er ikke nedskrevet og derfor åben for misforståelser og fejlagtig fortolkning
- Adfærd – der er faktorer, som får medarbejderne til at handle uhenigtsmæssigt
- Roller og ansvarsområder – ansvarsområderne er ikke klart definerede og meldt klart ud i hele organisationen
- Konvertering af strategi til forretningsmæssige mål – strategiske mål omsættes ikke direkte til forretningsmæssige mål
- Mål og kritiske succesfaktorer – bestyrelsen får ikke de rette informationer, de får for få (underinformation) eller for mange (overinformation)
- Risikovillighed – manglende forståelse for organisationens risikovillighed.

Indarbejdelse af risikostyring i virksomheden er grundlæggende en proces bestående af planlægning, handling, overvågning og læring

Vigtigheden i at etablere en begrebsramme for det interne kontrolsystem kan ikke understreges nok. Det gør det muligt for ledelsen at fastlægge, og herigennem styre hvordan kontrollernes enkelte bestanddele skal hænger sammen, og i hvilken sammenhæng de skal indgå.

Esbjerg

Havnegade 33
Postboks 371
6701 Esbjerg
Telefon 79 11 52 00
esbjerg@kpmg.dk

Faaborg

Bygmestervej 6
Postboks 31
5600 Faaborg
Telefon 62 61 84 37
faaborg@kpmg.dk

Frederikssund

Torvet 6
3600 Frederikssund
Telefon 47 31 77 77
frederikssund@kpmg.dk

Give

Torvegade 51
Postboks 18
7323 Give
Telefon 79 71 53 00
give@kpmg.dk

Haderslev

Jomfrustien 6
6100 Haderslev
Telefon 73 52 57 00
haderslev@kpmg.dk

Herning

Industrivej Nord 9
Postboks 360
7400 Herning
Telefon 96 27 61 00
herning@kpmg.dk

Hillerød

Søndre Jernbanevej 18D
3400 Hillerød
Telefon 38 18 30 00
hilleroed@kpmg.dk

Holstebro

Vestergade 16
7500 Holstebro
Telefon 97 42 14 44
holstebro@kpmg.dk

Horsens

Holmboes Allé 1, 6. etage
Postboks 79
8700 Horsens
Telefon 79 29 56 00
horsens@kpmg.dk

Juelsminde

Ringvejen 20
7130 Juelsminde
Telefon 79 29 56 00
horsens@kpmg.dk

Kolding

Kolding Åpark 1, 3. sal
Postboks 205
6000 Kolding
Telefon 76 34 49 00
kolding@kpmg.dk

København

Borups Allé 177
Postboks 250
2000 Frederiksberg
Telefon 38 18 30 00
kpmg@kpmg.dk

Nyborg

Baggersgade 9
5800 Nyborg
Telefon 65 31 42 42
nyborg@kpmg.dk

Næstved

Slagelsevej 67
4700 Næstved
Telefon 38 18 30 00
naestved@kpmg.dk

Odense

Englandsgade 25
Postboks 200
5100 Odense
Telefon 65 58 40 00
odense@kpmg.dk

Randers

Niels Brocks Gade 12
Postboks 236
8900 Randers C
Telefon 87 12 54 00
randers@kpmg.dk

Ringkøbing

Havnepladsen 3
Postboks 99
6950 Ringkøbing
Telefon 96 75 55 00
ringkoebing@kpmg.dk

Roskilde

Maglekildevej 7
4000 Roskilde
Telefon: 46 36 43 48
Telefax 72 29 30 30
roskilde@kpmg.dk

Svendborg

Mølmarksvej 198
Postboks 209
5700 Svendborg
Telefon 65 58 40 00
svendborg@kpmg.dk

Sønderborg

Sundsmarkvej 12
6400 Sønderborg
Telefon 73 42 64 00
soenderborg@kpmg.dk

Vejle

Brummersvej 2
Postboks 70
7100 Vejle
Telefon 76 43 48 00
vejle@kpmg.dk

Aabenraa

Skibbrogade 27
Postboks 94
6200 Aabenraa
Telefon 73 32 58 00
aabenraa@kpmg.dk

Aalborg

Vestre Havnepromenade 1A
Postboks 710
9100 Aalborg
Telefon 99 30 50 00
aalborg@kpmg.dk

Århus

Værkmestergade 25
Postboks 330
8100 Århus C
Telefon 86 76 46 00
aarhus@kpmg.dk

Net Source

Stationsparken 31-33
2600 Glostrup
Telefon 43 48 00 00
netsource@kpmg.dk

kpmg.dk

KPMG er et globalt netværk af firmaer, der leverer ydelser inden for revision, skat og rådgivning. KPMG er repræsenteret i 144 lande og har på verdensplan mere end 137.000 medarbejdere. De selvstændige medlemsfirmaer i KPMG-netværket er tilknyttet KPMG International, der er et schweizisk indregistreret kooperativ. KPMG International yder ikke professionelle services m.v. til kunder. I Danmark er vi omkring 1.600 medarbejdere.

© 2009 KPMG Statsautoriseret Revisionspartnerselskab, a Danish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International.

Denne publikation indeholder alene en generel gennemgang af et emne, som KPMG efter aftale kan yde nærmere rådgivning om. Selvom fejl og mangler i publikationen er forsøgt undgået, kan KPMG ikke påtage sig noget ansvar for dispositioner, som foretages uden vores forudgående rådgivning.

B08044

ISBN 87-91262-88-7