INFO

Foreningen af Interne Revisorer

Nummer 68 | April 2018 | 23. årgang

Minitema

● Robotics

COSO ERM 2017

Det nye rammeværk for risikostyring

GDPR

Opskrift på revision af data-behandlere

10 tips to reduce the costs of internal controls in 2018

INFOs redaktion

Ansvarshavende redaktør
Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Europæiske Rejseforsikring
☎ 33 27 84 82 ✉ brs@europaeiske.dk

Øvrig redaktion
Seniorspecialist
Lea Kehlet Halsø
Nykredit
☎ 44 55 93 01 ✉ lea@nykredit.dk

Revisionschef
Michael Ravbjerg Lundgaard
DSB
☎ 24 68 06 01 ✉ mirl@dsb.dk

Revisionschef
Louise Claudi Nørregaard
PensionDanmark
☎ 33 74 80 13 ✉ lcn@pension.dk

Chefspecialist, CIA
Tobias Zorde
Nykredit
☎ 21 18 54 97 ✉ tzo@nykredit.dk

Revisor
Klaus Nordmann Østrup
Københavns Kommune
☎ 33 66 24 13 ✉ zx7z@ir.kk.dk

Næste nummer
INFO 69 udkommer i september 2018.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO
Artikler i INFO påskønnes med en vingave.

Forsidefoto
UnknownNet

Redaktionens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Seniorspecialist Glenn Thunø
Intern revision
Nykredit
Kalvebod Brygge 1-3
1780 København V

Synspunkter, der kommer til udtryk i medlemsbladet, behøver ikke nødvendigvis at svare til bestyrelsens opfattelse eller være udtryk for foreningens officielle standpunkt.

Indhold

Nyt fra bestyrelsen

Referater fra bestyrelsesmøder lægges på foreningens hjemmeside umiddelbart efter mødernes afholdelse.

Du kan her løbende holde dig opdateret på bestyrelsens arbejde på hjemmesiden under "Nyheder".

www.iia.dk

Leder

Pia Sønderlund Nielsen, Koncernrevisionschef, COR, Finansministeriet

Velkommen til dette nummer af INFO med et minitema om Robotics, fokus på GDPR, fokus på det nye COSO ERM 2017 samt 10 gode råd til at reducere omkostningerne til intern kontrol.

Robot Process Automation (RPA) – kært barn har mange navne. Vi lægger i vores robot-tema ud med introduktion fra Henrik Olsen til, hvad en robot egentlig er for noget. Henrik tager os igennem, hvad det er en robot kan, og hvilke overvejelser du kan gøre, før du starter din rejse ud i robotternes verden.

Her i Finansministeriet, hvor jeg arbejder, er vi også i fuld gang med at implementere robotter – dette særligt i Statens Administration, som er statens Shared Servicecenter for Løn og bogholderi, og som servicerer de fleste statslige institutioner med betaling af fakturaer og udbetaling af løn. Indtil videre er der en håndfuld robotter i brug og flere er stærkt undervejs. Der er stort potentiale i at få frigivet medarbejdernes tid til andre vigtige opgaver, som ikke kan automatiseres og som ikke er ensartede og standardiserede. Intern revision har en vigtig rolle i udviklingen og implementeringen af robotter og sikringen af det kontrolmiljø, som danner rammerne for robotternes virke.

Zeeshan Rajan fra PwC kommer i sin artikel ind på, hvordan interne revisionsfunktioner selv kan anvende robotter i deres arbejde – forestil dig kedelige rutineopgaver blive udført af en robot og så få frigivet tiden til andre revisionsområder, som understøtter ledelsens strategi. Jeg synes, det lyder spændende at arbejde med fremover. Vi hører gerne fra interne revisioner i foreningen, som tager robotter i anvendelse i udførelsen af revisionen. Det kunne være spændende at bruge hinandens erfaringer, da jeg tror, at der er et stort sammenfald i de områder, hvor intern revision med fordel kan anvende robotter.

I dette nummer kan du også læse Deloittes' Michael Baggers input til revision af GDPR-compliance hos databehandlere. Hans artikel sætter en god ramme for det arbejde, som vi står overfor og som lige om lidt er virkelighed – uanset hvilket form for assurance, du skal give til ledelsen. Det giver rigtig god mening at finde en model, hvor databehandlerens kunder ikke hver især skal stille op og kontrollere databehandlerens håndtering af deres oplysninger. Der er et stort behov for en assurance fra revisionens side – et arbejde som i den forstand måske ikke adskiller sig ret meget fra revisors normale funktion.

Du kan i dette nummer også stifte bekendtskab med det nye COSO ERM fra september 2017. Benjamin Vanggaard fra EY tager os kyndigt igennem betydningen af det nye rammeværk og påpeger forskellene fra den gamle kube fra 2004. Benjamin kæder det nye rammeværk behændigt sammen med INFO's tema i sidste nummer om at intern revision skal forblive relevant og arbejde hen imod at blive en 'trusted advisor' for virksomheden.

Til slut forkæler vi jer med 10 tips til at reducere omkostninger ved interne kontroller ved Hernan Huwyler fra Deloitte.

Så med dette nummer er vi alle klædt på til forår, robotter, nye rammeværker, GDPR ikrafttrædelse og en hel masse spændende intern revision. God læselyst og rigtig god sommer!

Nye certificeringer

CIA (Certified Internal Auditor)
Heino Hansen, Nordea
Nina Senstius, Saxo Bank

Et stort tillykke med certificeringen !!!!

Call for assistance with the new IIA strategy!

Dear IIA member,

The Danish Chapter of IIA has been working with a new strategy that will be launched in the beginning of 2018. The strategy has been defined with four streams and examples of objectives that will be the foundation for the Chapter towards 2020. However, since it is a member organization, the Board of Directors encourage every member in IIA to contribute with their input, ideas and actions to realize the full potential and output of the strategy.

Therefore, you will find a form at iia.dk, where every member is welcome to sign-up for contributing to the execution of the strategy. **Please note that the work will be organized by Skype or similar, as required.** Any contribution, is welcome!

Nyt fra redaktionen

Birgitte Rousing Svenningsen, Revisionschef, CIA, CISA, Europæiske Rejseforsikring

Vi har desværre i redaktionen måtte sige farvel til vores jyske redaktionsmedlem Monica Vestergaard Rasmussen. Monica har fået en ny stilling uden for branchen og har derfor forladt redaktionen. Jeg vil benytte lejligheden til at sige tak for indsatsen, inputtene og ikke mindst et godt humør. Fra redaktionen ønsker vi Monica held og lykke med de nye udfordringer.

På den anden side har vi også været så heldige at kunne sige velkommen til et nyt redaktionsmedlem – Klaus Nordmann Østrup. Klaus har de sidste syv år arbejdet som intern revisor hos Københavns Kommune. Herudover har Klaus en cand.merc.aud. baggrund, hvor hans afhandling vedrørende cand.merc.aud. dimittenders karrierevalg efterfølgende blev udgivet i bogform. Vi ser meget frem til samarbejdet med Klaus.

Foreningen anser redaktionsarbejdet som yderst vigtigt. INFO og videreformidling af trends inden for faget intern revision er yderst væsentligt for, at vi som interne revisorer fortsat kan være værdiskabende. Jeg har selv siddet i redaktionen i en række år og synes stadig, at det er sjovt at bidrage til arbejdet. Det giver mulighed for at præge bladets indhold og giver samtidig en mulighed for at holde sig opdateret med, hvad der sker i vores branche lige nu.

Vi kan lige nu godt bruge nogle flere redaktionsmedlemmer. Jo flere vi er, jo flere skuldre er der til at bære opgaverne. Jeg kan derfor kun opfordre til, at interesserede melder sig på banen. Er det dig, eller kender du en som måtte være interesseret, er du velkommen til at tage kontakt til mig på brs@europaeiske.dk.

Boganmeldelse

Controllerfunktionen. Forebyggelse og håndtering af divergerende rolleforventninger og rollestress
af Bent Warming-Rasmussen, Jesper Marquart, Jesper Raalskov og John Wiingaard. Udgivet på Karnovs forlag.

Bogen "Controllerfunktionen" går bagom den faglige dimension i jobbet som controller. Temaet for bogen belyser, hvordan en controller kan forebygge og håndtere konfliktende forventninger til rollen som controller.

Disse konfliktende forventninger beskrives i bogen som de stressfaktorer en controller er udsat for i jobbet. Ikke stress som i psykiske lidelser, men mere i form af, hvad der gør at controlleren ikke performer effektivt og efficient.

Bogen giver den enkelte controller en række redskaber og værktøjer at navigere efter i takt med et stigende behov for, at controllere både skal agere sparringspartner og kontrollant.

Derudover giver den selskabsledelsen i virksomhederne samt andre praktikere en beskrivelse af hvordan vi fastholder, udvikler og rekruttere de "rigtige" controller.

Controllerens dilemmaer giver sig udslag i forskellige former for rollestress, som i nogen grad kan sammenlignes med de modsætninger som kendes blandt eksterne og interne revisorer som både skal være kontrollanter og være værdiskabende sparringspartnere.

Revisorer vil sikkert også kunne genkende problematikkerne og finde inspiration i bogens redskaber og værktøjer.


IIA årsmøde 2018
Best Western
NYBORG STRAND
HOTEL OG KONFERENCECENTER
Afholdes i dagene
17.5-18.5.2018
Tilmeld dig på
www.iia.dk

COSO ERM 2017 – Integrating with Strategy and Performance: Slut med at kaste med terninger

Benjamin Vanggaard, Senior Consultant, EY Advisory

Overblik: COSO ERM 2017 rammeværk for risikostyring

- I september 2017 udgav COSO boarded en opdatering til ERM rammeværket fra 2004 med navnet "Enterprise Risk Management - Integrating with Strategy and Performance"
- Det opdaterede rammeværk lægger fokus på risikostyringens betydning for sammenhængen mellem virksomhedsstrategi og virksomhedens performance
- COSO ERM-kuben udgår og erstattes med fem komponenter og tyve principper
- Rammeværket sigter at lukke den relevans-kløft der er mellem brugere af ERM og producenter/udøvere – der betegnes som en rejse fra en risikostyret målfokusering til at foretage målfokuseret risikostyring (moving from a risk-centric approach to an objective centric approach)
- Flere meningsdannere indenfor ERM-området mener at rammeværktøjet ikke formår at lukke forventningskløften og at yderligere operationalisering er nødvendigt.

I denne artikel belyser jeg hvorfor det nye rammeværk er særligt relevant i en tid hvor forskellige interessenter (herunder IA) må se indad og definere sin relevans overfor en stadig mere forventningsfuld ledelse. Tiden hvor ERM var risiko-centreret, med fokus på risikoregistre og heatmaps, er forbi.

For at forblive relevant og indtræde i en trusted-advisor relation[1], må IA ERM-deltagerne bidrage med ledelses*relevant* viden fokuseret på forretningsmål. Ledelsen forventer at ERM i stigende grad gør brug af digitale enablers for at bidrage til en konvergerende risikostyring – på tværs af forsvarslinjerne. Ny teknologi stiller øgede krav til effektivitet og måden at arbejde på.

Et nyt rammeværk imødekommer udfordringerne med et ændret risikolandskab

Inden forskellen mellem COSO 2017 og 2004 oplistes vil jeg starte et andet sted. I et mødelokale hos EY på Frederiksberg.

Mandag d. 5. marts sidder et par kollegaer og jeg og gennemgår resultaterne af vores nordiske undersøgelse omkring emner som ERM, interne kontroller og digitale enablers: GRC, Data Analytics, Proces Mining og Robotics.

Vores gæster den dag, to repræsentanter for IA i en større dansk virksomhed – en virksomhed som med egne ord lever af at være dagslysingeniører – er mindst lige så interesserede i emnerne som vi selv er.

Figur 1: Den digitale revolution udfordrer måden vi arbejder på og nye risici (muligheder) opstår

De havde ikke engang deltaget i undersøgelsen. Mødet var sat til at vare 1 time. Det tog 2,5 time.

Emnerne er højaktuelle hvilket bl.a. understreges af at COSO i 2017 har udsendt en opdatering af deres rammeværk for Enterprise Risk Management.

Ny teknologi forandrer forretningsmodeller og skaber nye muligheder og risici. Man kan tale om en egentlig digital revolution som vist i **Figur 1** på foregående side. For at håndtere nye risici og de øgede krav til relevans har det været nødvendigt med en opdatering af rammeværket med særlig vægt på risikostyringens rolle med at koble strategi og målopfyldelse sammen.

Den digitale revolution betyder, at flere brancher oplever at adgangsbarriere nedbrydes og at konkurrencen derfor vil stige (f.eks. Blockchain i finanssektoren). I et forsøg på at undslippe det blodrøde farvand er der mere end nogensinde brug for en holistisk risikostyring, som ikke kun adresserer risici når virksomheden har valgt en strategi. Der er i større grad brug for at virksomheden *løbende* er tro mod sin vision, mission og kerneværdier – da selv den bedst eksekverede strategi kan fejle hvis ikke den udføres med hjertet på rette sted, med den rette kultur. Samtidig er det nødvendigt at virksomheder arbejder målstyret og tager de nødvendige risici. Det er ikke længere nok at arbejde med ERM som en defensiv disciplin for at beskytte værdi. ERM skal være en del af virksomhedens værdiskabende tiltag.

Der er brug for en målfokuseret risikostyring og ikke en risikostyret målfokusering

Tilbage til EY's nordiske undersøgelse om trends indenfor risikostyring med særlig fokus på ERM og interne kontroller.

Følgende kan uddrages af undersøgelsen:

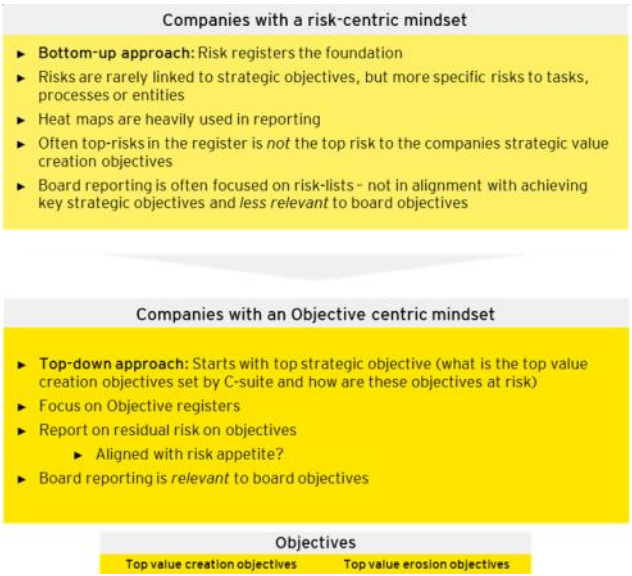
- IC funktionen har svært ved at se sine værdiskabende aktiviteter
- IC funktionen vurderer ikke at være koordineret med øvrige risikostyringsinitiativer/funktioner
- IC funktionen har (stadig) ikke fokus på at opbygge kompetencer indenfor strategi
- Det største kompetencebehov er indenfor de tekniske discipliner
- De fleste IC funktioner har svært ved at redegøre for et budget til at inkludere de teknologiske muligheder i deres arbejde.

Ovenstående understreger behovet for et rammeværk med en (forretnings-) målfokuseret risikostyring, ikke en risikostyret målfokusering. For at forblive relevant for virksomheden må ERM indsatsen være værdiunderstøttende. Omkostningsreducering og beskyttelse mod worst-case udfald er blevet hygiejnefaktorer. Dét var én af hovedfokusområderne i COSO 2004.

Uden et rammeværktøj der understøtter denne overbevisning, vil der være en fragmenteret forståelse af styringsdimensionen ift. strategiske mål, hvilket vil medføre manglende risiko koordinering på tværs af forsvarslinjerne.

Samtidig, når IT-miljøet og teknologiudvikling udfordrer bl.a. IA-funktionen er det nødvendigt at kompetencer på IT-området øges. IA skal i endnu større grad være i stand til at sætte sig ind i ny teknologi og kunne bruge teknologi. I EY henviser vi til *digitale enablers*, dvs. værktøjer som øger relevansen af deltagerne i risikofunktionen da værktøjerne – sammen med IA's forretningskendskab – bringer indsigt til ledelsesbordet. Ny relevant viden til beslutningstager.

Relevansen og den værdiskabende indsats sker når arbejdsopgaverne målrettes forretningsmål og giver indsigt til forretningen. Udfordringen er dog to-benet: På den ene side skal risikofunktionen reelt komme "med noget nyt" og forretningen skal imødekomme funktionens input. Det er en udfordring når fokus med COSO 2004 var en defensiv risikostyring, dvs. fokus på at beskytte værdi ved at nedbringe risici til et acceptabelt niveau og ikke at se mulighederne for at kombinere risici og performance.



Funktionerne omkring risikostyring har ofte dyb forretningsforståelse (eksempelvis IA), men mangler værktøjerne til at få initiativer implementeret.

Flere rammeværk understreger aktiviteter som "understand the business" som fundamentet for at være en trusted advisor. Når forståelsen er på plads må man ligesom håndværkeren kigge på værktøjsbæltet: Kunne ny input være GRC til en koordineret og værdiskabende risikoindsats? Kunne det være dataanalyse og Process Mining. Kunne det være robotter?

COSO 2017 lægger særlig vægt på kultur (bl.a. lysten og evnen til at tage ny teknologi til sig) og hvordan risikostyringen anvendes som limen mellem strategi og performance i virksomheden. Dette understreges bl.a. af *princip nr. 18: leverages information and Technology* (mere omkring komponenter og principper i næste afsnit).

Jeg vil slutteligt henvise til en artikel som meget sigende henviser til en svunden tid hvor dinosaurerne herskede. Hvis ikke IA og andre deltagere i ERM er i stand til at forstå og imødekomme nye muligheder i det nye risicilandskab så risikerer man at uddø – ligesom dinosaurerne[2].

På samme måde kan ovenstående rejse sammenfattes i den nye opdatering af COSO ERM rammeværket - Integrating with Strategy and Performance: En reel risikotransformation.

Introduktion til det nye COSO ERM 2017 rammeværk for risikostyring

Indtil nu har artiklen beskrevet behovet for en ændring i ERM-tilgangen. Nedenfor belyser jeg indholdet af COSO 2017 og i næste afsnit laver jeg sammenligningen til det gamle rammeværk, COSO 2004.

COSO 2017 tager udgangspunkt i virksomhedens strategi som det vigtigste værdigenerende element og strukturerer risici, der truer denne, i tre separate dimensioner - se **Tabel 1**.

Det *nye* bliver således at ERM bliver en holistisk og iterativ tilgang til risikostyring. Den er ikke længere kun fokuseret på styring af risici under udførslen af en allerede valgt strategi. Rammeværket understreger at konsekvenserne, og tilknyttede risici, er langt større ved valget af strategi og de tilknyttede antagelser.

Når strategien nedbrydes i forretningsmål bliver ERM midlet til at understøtte de værdiskabende aktiviteter så det ønskede afkast på den investerede kapital opnås, under hensyntagen til den valgte risikoprofil. I rammeværkets afsnit to – den forklarende del - gives der bud på rapportering af risici på forretningsmål - se **Figur 2** og **Figur 3** på næste side.

Tabel 1: Risici forbundet med virksomhedens strategi; Antagelser, valg og udførsel

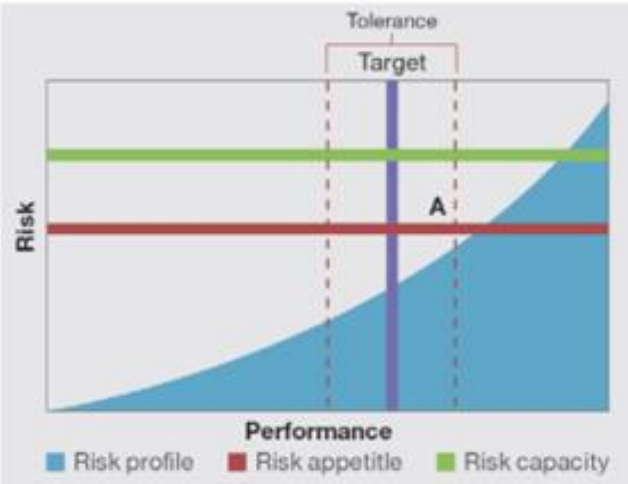
Strategivalg (possibility of strategy not aligning)	Manglende ensretning imellem strategien og mission, vision og kerneværdier. Selv en veleksekveret strategi som ikke er ensrettet med virksomhedens kerneværdier, vil potentielt nedbryde virksomhedens værdi igennem tab af konkurrenceevne.
Strategi antagelser (og implementering) (implications from the strategy chosen)	Den valgte strategis risikoprofil, via de underliggende antagelser, og følgevirkning/ konsekvenserne er ikke aligned med virksomhedens risikovillighed. Valg af strategi vil påvirke måden virksomheden opsætter forretningsmål og driver performance. Strategi har en risikoprofil baseret på antagelser – både interne antagelser om f.eks. kompetencer og eksterne antagelser såsom markedsudvikling og kundetrends. Det er derfor vigtigt at ledelsen forstår konsekvenserne af de valgte antagelser på den efterfølgende implementering og udførsel af strategien. Fx risikerer virksomheden ved eksekvering af den valgte strategi (ubevidst) at påtage sig en risiko, der overstiger virksomhedens risikoappetit.
Strategiudførsel (risk to executing the strategy)	Risici ved selve udførslen af strategien kan have så høj effekt, at selve grundlaget for strategien kan blive truet. Et eksempel på dette er ny (forstyrrende) teknologi som f.eks. blockchain, hvilket kan true grundlaget for bankvirksomhed som vi kender den i dag. Det kan også være ondsindede tiltag som f.eks. Cyber-kriminalitet som ikke længere kun er kendte tiltag som f.eks. phishing men også andre mere erroderende angreb som f.eks. Code Injections (ændringer i kildesystemer) og Ransomware (eksempelvis NetPetay hos Maersk Line, som kostede 1,3-1,9 mia. dkk og tvang værdikæden i knæ).

Af **Figur 2** fremgår det, at den accepterede risiko – varians omkring et target – defineres for hvert relevant forretningsmål. Med øget afkast følger en forøget risikoprofil, og virksomhedens optimale target bliver fastsat med hensyntagen til den definerede risikoappetit. **Figur 3** viser hvordan målene og den tilhørende risikoprofil gøres operationelle.

COSO 2017 nedbryder risici forbundet med virksomhedens strategi (den inderste farvede cirkel) i fem komponenter og tyve vejledende principper. Tre komponenter fokuserer på kernedriften og to fokuserer på støtteaktiviteter. Kultur står nævnt som et bærende element, hvilket er nyt ift. COSO 2004 - se **Figur 4** på næste side.

Det fremgår at rammeværket er skrevet ud fra et *forretningsperspektiv*: Hvordan virksomheden via sit interne værdisæt, med en målfokuseret risikostyring forbedrer virksomhedens driftsresultat. COSO 2017 lægger vægt på virksomhedskulturens betydning for medarbejderne risikovillighed og det strategiske mind-set.

Figur 2: Risiko tolerancen skal være afstemt med virksomhedens risikoprofil



Herudover bliver anvendelsen af ny teknologi til at understøtte risikostyringen afgørende (princip nummer 18). Derfor henviser jeg også i artiklen til digitale enablers. Ved yderligere analyse fremgår det også at rammeværket lægger fokus på data og nye teknologier, i stedet for (informations)systemer. Det interessante er beslutningsgrundlaget, ikke IT i sig selv.

Men hvordan står det så til med lysten til at bruge ny teknologi og at udvikle og tiltrække de rette kompetencer?

Resultaterne fra det nordiske survey viser, at der er et forventningskløft imellem hvad deltagerne i ERM (her den interne kontrolfunktion) lægger vægt på af kompetencer og de kompetencer som efterspørges af interessenterne. Det er bl.a. dataanalyse, at kunne drive forandringer, tekniske kompetencer og forståelse af forretningsstrategi - se **Figur 5** på næste side.

Det er interessant, for det er netop disse kompetencer man ville forvente at skulle gøre brug af når COSO 2017 skal implementeres (indsigt i forretningsmål/strategi, brug af teknologi, drive forandringer imod øget performance under hensyntagen til risici).

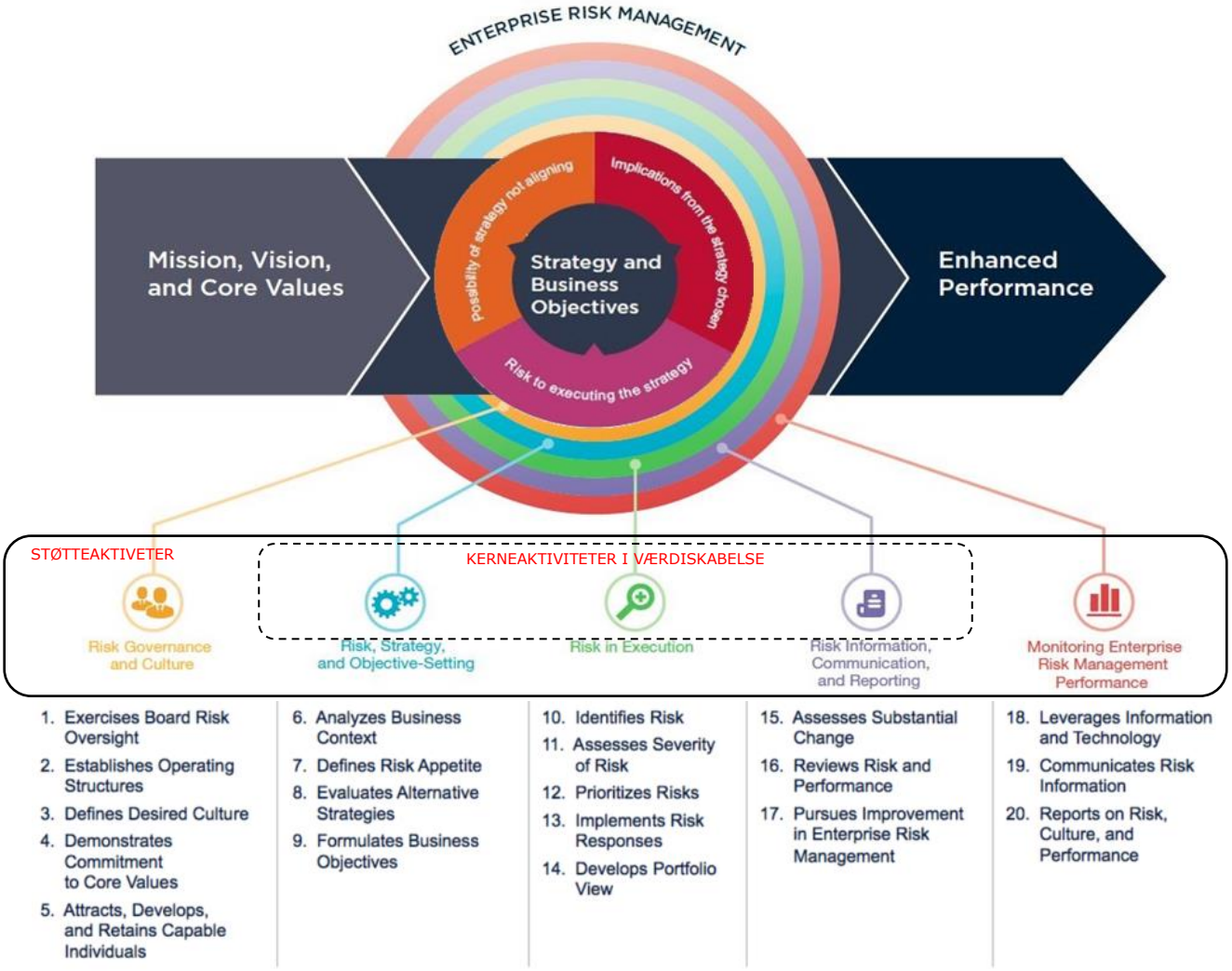
Resultaterne forelå inden det nye COSO 2017 rammeværk udkom. Jeg vil derfor udlede at der formegentlig over en længere periode i praksis har været brug for at kunne tænke som i det nye rammeværk – og kompetencerne, men at rammeværket (teorien) først nu ser ud til at indse dette.

Der er brug for et kompetenceløft indenfor flere tekniske discipliner og en større forståelse for de digitale mulighe-

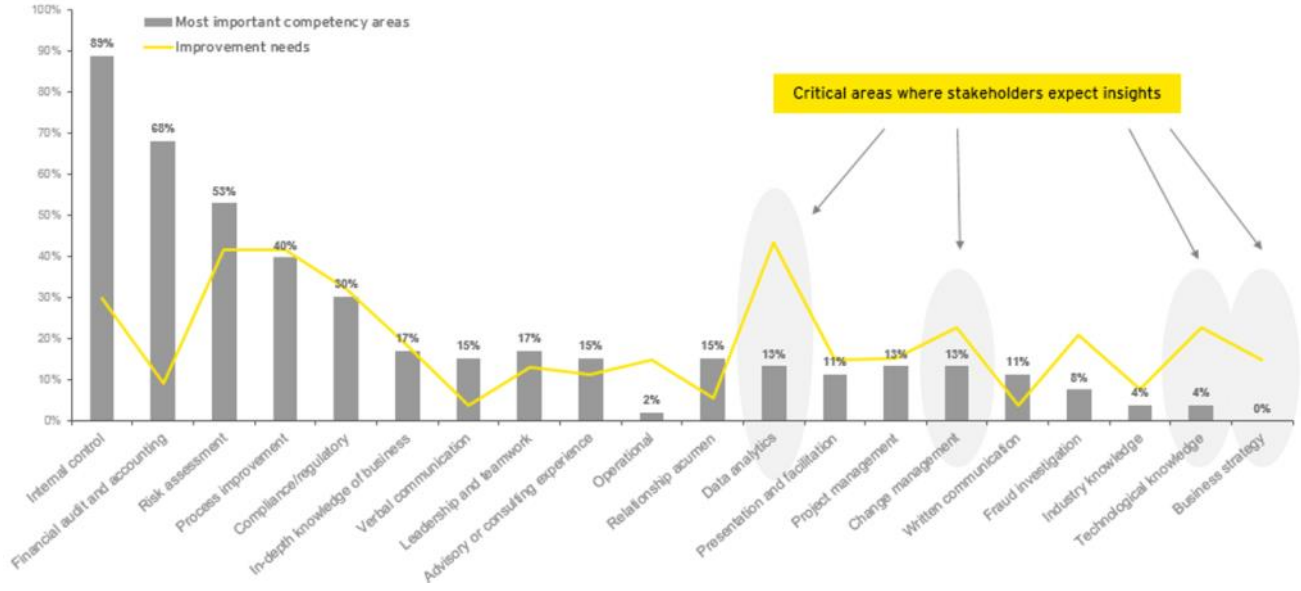
Figur 3: Eksempel på rapportering som viser den accepterede varians fra target

Business Objective	Target	Tolerance
Return on investment (ROI) for an asset manager	Target 5% annual return on its portfolio	3% to 7% annual return
On-line home delivery orders for a restuarant	Target delivery within 40 minutes	30– to 50-minute delivery time
Minimize missed calls from a call center	Target 2% of overall calls	1% to 5% of overall calls

Figur 4: ERM understøtter de værdiskabene aktiviteter ved at skabe sammenhæng mellem virksomhedens identiet og forbedret performance



Figur 5: Fire kompetencer er særlig efterspurgte af interessenter



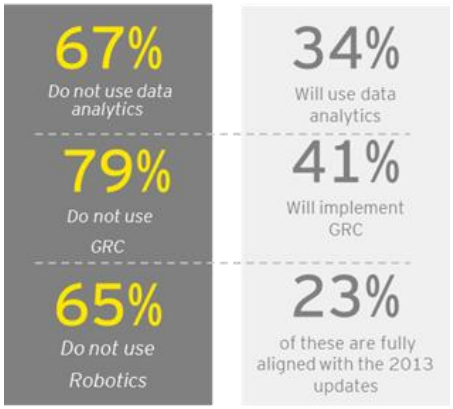
der. IIA's egen CIA certificering er netop blevet opdateret set i lyset af ovenstående.

Kompetencer og de rette værktøjer bliver nøglen til at være en forretningspartner – hvis vi ikke skal ende som revisor-dinosaurer (jf. tidligere).

Hvad kunne være inspiration til værktøjer og er virksomhederne i gang?

Tre overordnede tekniske værktøjer til at understøtte ERM er Data analyse, GRC og robotter (som f.eks. kan udføre reelle kontroller og køre rapportering).

Herudover er der også forskellige virksomheders konceptualisering/implementering af ERM, f.eks. EY NextGen ERM (fremgår kort senere med et inspirationseksempel).



Over halvdelen af respondenterne anvender ikke værktøjerne. Under halvdelen svarer at der ikke er umiddelbare planer om at gøre brug af værktøjerne. Ved nærmere gennemgang af svarene relateres tøven med nye værktøjer til manglende viden omkring værktøjerne eller er virksomheden endnu ikke har undersøgt business casen.

Det nye: Definitionen af ERM ændres og fokus rettes mod strategi, forretningsmål og præstationer

Tabel 2 på næste side sammenfatter min gennemgang af COSO 2004 og COSO 2017.

En af de værdiskabende kerneaktiviteter i ERM rammeværket er rapportering og kommunikation af (forretnings-)risici. Det nyere fokus på forretningsmål giver sammenhæng til beslutningstagen og tilsyn (oversight).

I **Figur 6** på side 14 er et udsnit fra en rapportering på forretningsmål fra EY's NextGen[3] ERM. Ligesom eksemplet fra COSO 2017, så er der defineret et target for forretningsmålet og en acceptabel varians (risiko omkring forventningen).

En rapportering som inddrager forretningen, hvor hovedfokus er på forretningsmål medfører en helt anden relevant og udviklende dialog – hvormed ERM bliver en iterativ proces, som løbende tilpasses strategien og hvor den strategiske udvikling løbende indvirker på risikostyringen.

Perspektivering

Det naturlige spørgsmål efter en analyse af det nye rammeværk bliver selvfølgelig – **er vi så i mål med ERM**? **Måske**.

Flere meningsdannere indenfor ERM har både gode ting og mindre gode ting at sige om rammeværket. Tim Leech (Risk Oversigt) er overordnet positiv omkring springet til en målfokuseret risikostyring. Han mener dog at udviklingen kommer alt for sent. Han har skrevet om "objective-centric" risikostyring i de sidste 20 år. Han mener at der mangler mere operationalisering af rammeværket.

Samtidig konkluderer provokatøren Alexei Sidorenko (Risk Academy) at der ikke er noget nyt i rammeværket – "here comes captain obvious". Han mener at ISO 31000 på flere måder er COSO overlegent. Jeg er dog ikke enig (dén analyse må vente til en anden gang).

Jeg tror det er sundt at lade sig inspirere – og provokere – af holdningsdannere indenfor sit felt. Det tvinger os alle til at kunne argumentere for ERM i vores organisation.

Nu er jeg konsulent, som bl.a. lever af at sælge implementeringsværktøjer i kølvandet af sådanne nye(ere) rammeværk – som f.eks. COSO 2017, så, **hvad mener du?**

Inspiration med IIA Danmark

D. 20 februar i år afholdte PwC et oplæg omkring interessenters forventninger til IA-funktionen. Det er et rigtig vigtigt sted at starte. Som opfølgning på dette og set i lyset af denne artikel påtænker EY at afholde et arrangement i samarbejde med IIA Danmark for interesserede der går mere i dybden omkring spørgsmålet hvordan. Mere information herom vil kunne følges på IIAs hjemmeside.

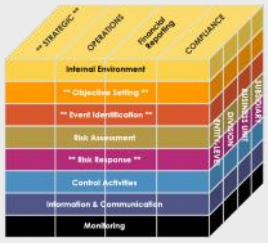
Noter

[1] Se bl.a. mini-temaet i sidste udgave af INFO #67: Stay Relevant!

[2] https://iaonline.theiia.org/blogs/chambers/2017/Pages/Seven-Signs-You-Might-Be-a-Jurassic-Auditor.aspx

[3] http://www.ey.com/Publication/vwLUAssets/ey-next-generation-enterprise-risk-management/$FILE/ey-next-generation-enterprise-risk-management.pdf

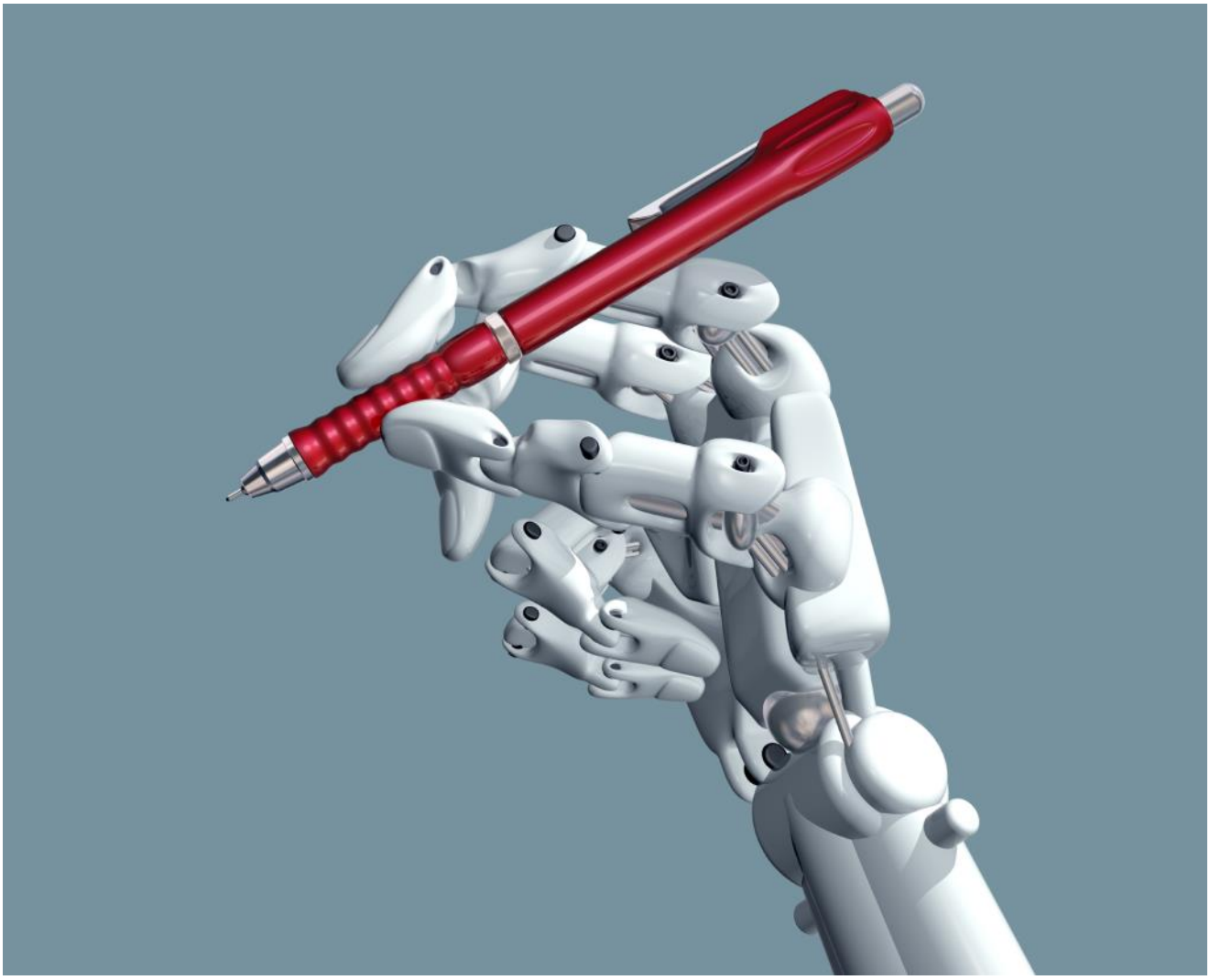
Tabel 2: ERM COSO 2004 og COSO 2017

	COSO 2004 **Enterprise Risk Management** **- Integrated Framework**	**COSO 2017** **Enterprise Risk Management** **- Integrating with Strategy and Performance**
Fokus	*Proces perspektiv*	*(Forretnings-) Målperspektiv*
Formål	Give vejledning til udvikling af ERM programmer (Fokus på *processen*)	Skabe sammenhæng mellem strategi, risici (styring) og præstationer/målopfyldelse (Fokus på understøttelse af de værdiunderstøttende aktiviteter)
Definition af Enterprise Risk Management	*Risikostyring med fokus på værdibeskyttelse ud fra virksomhedens risikoprofil* (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"	*Risikostyring som et aktivt værktøj til at skabe værdi, som ikke kan afgrænses til specifikke processer* "The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manager risk in creating, preserving and realizing value"
Aktiv/passiv værdifokus	*Passiv* Fokusere på at beskytte værdi og minimere risici til et acceptabelt niveau, med et begrænset fokus på forretningsmål og strategi	*Aktiv* ERM anvendes til at understøtte og beskytte de værdiskabende aktiviteter
Visualisering	Kubus med 3 dimensioner 	Værdikæde med 5 bånd 
Risici	Fokus på risici-svar (acceptér, reducér, dele eller undgå)	Arbejder med risikostyring ud fra et mulighedsperspektiv i hele værdikæden, imens værdi beskyttes
Kultur	Nævner ikke særskilt kultur	Lægger stor vægt på kultur som det første af fem komponenter og som en ny del af den nye definition af ERM
Anskuelse af rammeværk for intern kontrol	*Substituerende* (prøver at omfavne intern kontrol rammeværket)	*Komplimenterende* (adskiller ERM fra intern kontrol)
Bestanddele	**Otte komponenter:** 1. Internt miljø 2. Målsætning 3. Identificering af begivenheder 4. Risikovurdering 5. Risikoreaktion 6. Kontrolaktiviteter 7. Information og kommunikation 8. Overvågning	**Fem komponenter (og 20 principper):** 1. Styring og kultur 2. Strategi og (forretnings-) målsætning 3. Målstyring 4. Review og revision 5. Information, kommunikation og rapportering

Figur 6: Eksempel på rapportering af forretningsmål (EY NextGen ERM)

Goal	Target	Risk range		Priority	Key indicators
		Downside	Upside		
Organic growth	12% by 2020	8%	13%	**High**	▸ YOY revenue growth (existing products) ▸ Revenue growth from new product launches ▸ Revenues from new customer sales
Cash flow	5% EBITDA growth	4% EBITDA growth	7% EBITDA growth	**Low**	▸ Labor cost increase ▸ Gross margin % increase ▸ Non-labor SG&A % increase
Brand	#1 or #2 by market share	< #2 in 1+ core markets	#1 in all core markets	**Medium**	▸ Customer loyalty index ▸ % change in net promoter scores ▸ Net increase in social media subscribers
Operational excellence	1.5 asset turnover ratio	1.3 ATR	1.7 ATR	**Medium**	▸ Defect rate % ▸ Production asset downtime ▸ Critical IT systems availability
Talent transformation	#1 employer in industry	< #2 employer	#1 employer	**High**	▸ Employee engagement scores ▸ Labor mix (traditional, virtual, bots) ▸ Turnover rate ▸ Training hours per FTE
Digital and IT transformation	20% process automation by 2020	< 10% process automation	> 25% process automation	**High**	▸ Processes using robotics or AI ▸ % data on cloud ▸ Legacy IT system requirements

Minitema: Robotics



Verden ændrer sig med stadig stigende hastighed. Robotic Process Automation (RPA) og det mere udviklede Artificial Intelligence er virksomhedernes nye tiltag i udviklingen af digital teknologi. Der er tale om digital medarbejder. En softwarerobot, som kan automatisere processer i virksomhederne, en billig og lynhurtig medarbejder af højeste kvalitet. Henrik beskriver i dette nummer, hvad RPA er og hvordan det bruges i virksomhederne i dag og vil blive brugt i fremtiden. Som Intern revision er vi også nødt til løbende at tilpasse os denne udvikling, derfor har vi bedt Zeeshan Rajan fra PwC om at give sit bud på hvordan vi revisorer skal revidere denne nye digitale teknologi og hvordan vi selv kan bruge den i vores arbejde. Endvidere har fået lov til at bringe en artikel fra Internal Auditor bladet om "Audit In An Age Of Intelligent Machines".

God læselyst!

Hvad er Robotic Process Automation (RPA) egentligt?

Henrik Olsen, Blogger

Indledning

Robotic Process Automation er et meget varmt emne i øjeblikket. Denne artikel har til sit formål at fortælle hvad RPA egentlig er for noget og hvordan det bruges i virksomhederne i dag og i fremtiden.

Definition af RPA

Robotic Process Automation er også kaldet RPA. Men du har måske også hørt det omtalt som et af følgende ord:

- Kontorrobotter
- Robotics
- Softwarerobotter.

Det er dog præcist det samme og ordene dækker over det samme tema, der i bund og grund handler om at automatiserer arbejdsopgaver ved hjælp af RPA.

Det kan sammenlignes med en robot ved et samlebånd. Den pakker f. eks. 10 æg i en æggebakke og lukker låget efterfølgende. Dette var tidligere en manuel og en repeterende opgave, som blev fortaget mange gange i løbet af dagen. Derfor grundlæggende perfekt kandidat for en robot.

På samme måde er det med RPA eller netop begrebet "Software Robotter". Her kunne eksemplet være modtagelsen af en kundeordre på mail. Kundeordren er en PDF fil, som medarbejderen skal indtaste ind i virksomhedens ordresystem. RPA vil kunne gå ind og gøre præcist det samme som medarbejderen. Den vil kunne gå ind i mailsystemet og "læse" PDF filen. Efterfølgende laver den indtastningen i ordresystemet og flytter til sidste mailen over i folderen "oprettet". Dette gør robotten hurtigere og med en højere kvalitet.

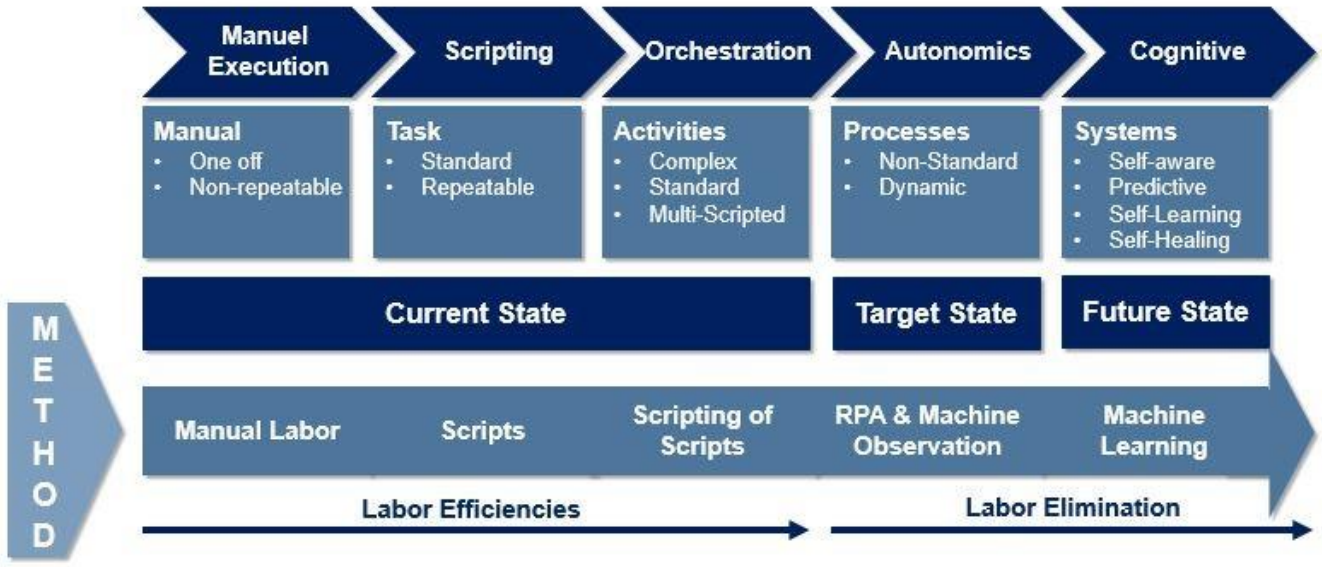
RPA er derfor et af flere værktøjer, som virksomheden kan bruge til at automatisere og effektivisere sine administrative opgaver.

Ifølge en rapport fra McKinsey & Company og Innovationsfonden fra den 27. april 2017, så kan automatisering og kunstig intelligens være i stand til at erstatte op til 40 procent af danskernes arbejdstimer (gælder kun for arbejdstimer på kontoret).

I rapporten fra McKinsey & Company skriver global partner Bjarne Corydon følgende[1]:

"Automatiseringen kommer til at have en enorm betydning for de danske samfund og danskerne i de næste årtier, og vi skal hilse den velkommen, da den kan skabe vækst, nye industrier og jobs, og bedre velfærd. Men det er vigtigt, at vi allerede nu begynder at forberede os på

Figur 1: Udviklingen i automatiseringen



de store omvæltninger, der ligger forude, herunder hvordan vi sikrer en effektiv omstilling af arbejdsstyrken og tilpasning af uddannelsessystemet."

Selvom Bjarne Corydon mener at automatiseringen kommer til at have en enorm betydning i fremtiden, så har automatisering været her i mange år. Vi har blot kaldt det noget andet.

I **Figur 1** på foregående side vises lidt om den evolution som automatiseringen har været igennem.

For efterhånden over 15 år siden gik man fra det rent manuelle arbejde og over til at bruge ting som scripts og makroer. For en 5-7 år siden var vi nået til det punkt, hvor tingene blev mere avanceret og også kompliceret. Så kom der scripting af scripts og ting som VBA (Visual Basic for Applications) til f. eks. Excel eller Access.

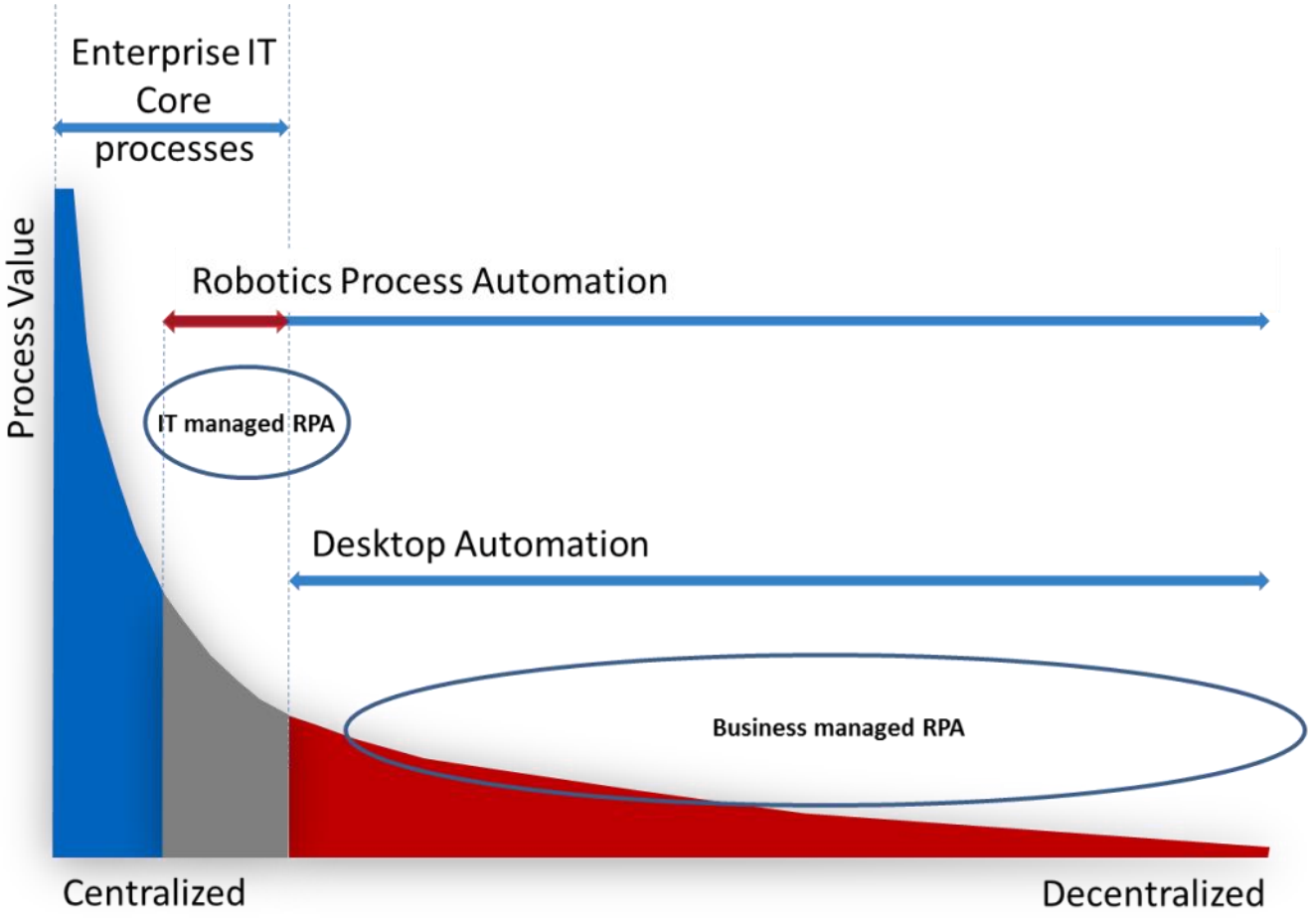
Alt dette var for at blive mere effektiv og kunne håndtere større mængder af data med de samme medarbejdere. Med RPA, så er fokus flyttet. Det er nu også et spørgsmål om at reducere brugen af medarbejdere ved hjælp af RPA. Opgaven er forsat den samme – nu er der blot kommet IT-værktøjer, som er bedre gearet til at være Enterprise systemer således at IT-afdelingerne vil acceptere og drive dem, som enhver anden central forretningsapplikation.

Derfor kan RPA fint sidestilles med at køre et script eller en makro. Selvom den RPA software vi ser nu, bliver mere sofistikerede og avanceret, så skal det forsat sættes op til at køre en proces – nu blot i et mere kontrolleret miljø og med en governance omkring løsningen. Det skal også være en proces, som starter med struktureret data, da RPA i sin centrale form ikke kan gøre ustrukturerede data til strukturerede data. Derfor har det betydning for hvilke processer man kan og bør starte med.

Hvad kan RPA så hjælpe med og hvad er fordelene?

RPA er en teknologisk revolution inden for effektivisering af virksomhedens repeterbare administrative opgaver, og

Figur 2: "The Long Tail" modellen som viser at du skal overveje meget hvor du starter din RPA rejse.



det er noget som sker lige nu. Frigivelse af medarbejderens tid til andre vigtige opgaver der ikke kan automatiseres er i fokus.

RPA er softwarerobotter der efterligner en medarbejders administrative opgaveløsning, f.eks. opgaver inden for økonomi, regnskab, HR eller lønområdet, på tværs af systemer og dokumenter, uden at ændre på de underliggende systemer og dokumenter.

Kendetegn for RPA-egnede processer:

- Manuelle repeterbare administrative opgaver med mange gentagelser
- Desuden også gerne opgaver med et højt tidsforbrug (åbne/lukke docs/systemer – PDF, Excel, mails, felter i ældre IT-systemer, Word osv.).

Selvom en proces har menneskelige beslutningsprocesser, kan robotten forsat bruges og være gavnlig. Den kan gennemføre standardopgaverne og lade brugeren beslutte når det er relevant.

Desuden kan robotter forebygge fejl og ensarte kvaliteten. I oplever sikkert, at hvis man skal gennemføre samme proces 50 gange, så "går man lidt kold i opgaven". Det gør en robot ikke – den forsætter med samme hastighed og kvalitet. Eneste krav er at datakvaliteten er i orden fra starten af.

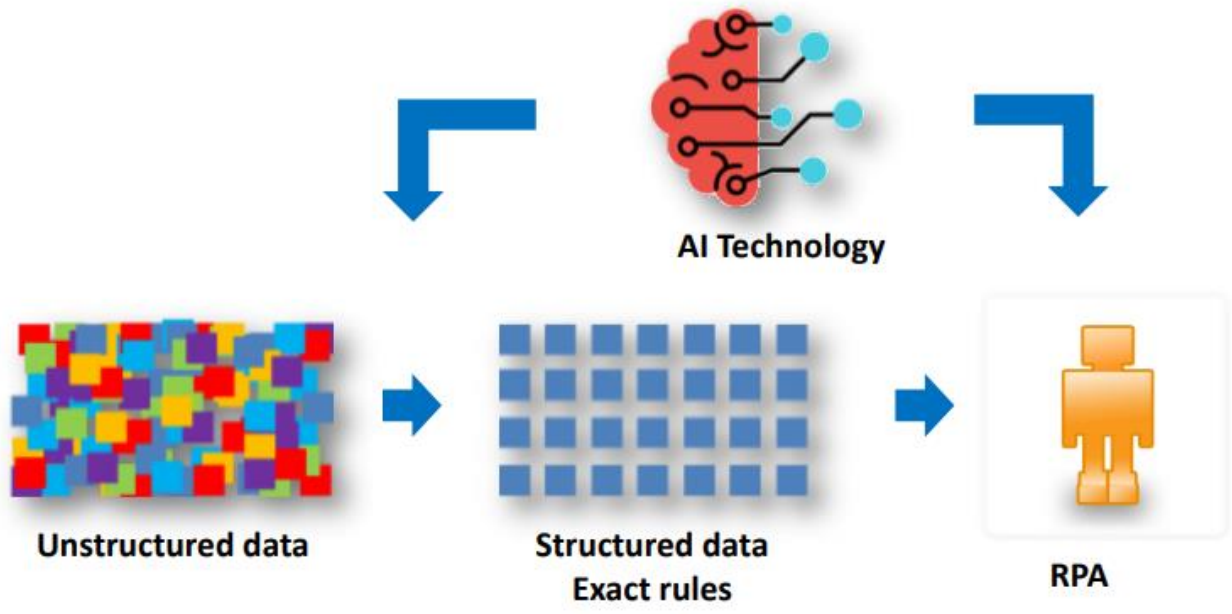
Robotter kan kopiere menneskelige arbejdsgange og uden besvær bevæge sig fra Excel til et ERP-system og afslutte med at sende en bekræftelsesmail til relevante konsulenter. Ofte kræver det ikke mere end 2-4 uger for en erfaren udvikler at implementere og aktivere en procesautomatisering. Det vil sige, at man som virksomhed straks får mulighed for at høste fordelene ved investeringen.

I alle virksomheder er der medarbejdere, som varetager regnskab og lønadministration, HR opgaver, ordremodtagelser og mange andre ting, som sker på samme måde dag efter dag. Disse er selvsagt tilbagevendende opgaver, som består af gentagne processer. Det er disse processer, som RPA ofte er perfekte til at automatiserer.

Ved brug af modellen "The Long Tail" - se **Figur 2** på foregående side - er det vist, hvilke processer du bør starte med at kigge på. Det som erfaringerne viser er, at det er de decentrale processer, som har en mindre samlede procesværdi, der er bedst egnede til at starte med.

Grunden er at du ofte får en hurtigere start og får lavet et antal robotter, som kan vise værdien, samt også give dig erfaringen med at drive robotter. Vælger du fra starten af en mere kompleks proces, så vil du støde ind i flere udfordringer. Det kunne være adgangen til flere programmer, flere stakeholders eller blot en kompleks proces.

Figur 3: AI teknologier kan hjælpe med at lave struktur i ustruktureret data.



Så anbefalingen er klart at starte i det små og simple for hurtigere at kunne fejre nogle successer og skabe erfaring.

Hvad er næste skridt for RPA?

De næste skridt for RPA er at benytte sig af nogle af de nye teknologier (ref. **Figur 1**). Det er det såkaldte kognitive område og teknologier som kunstig intelligens (AI) og Machine Learning er det næste som kommer i spil med RPA. Det betyder at RPA nu kan trænes til at genkende nye situationer med Machine Learning eller bruge AI til at forstå ting som at læse indkommende mail og sende dem videre eller svare på dem.

RPA robotterne er forsat "dumme", men de får nu hjælp af teknologien til at kunne løse flere processer. Det er netop dette **Figur 3** på foregående side forsøger at vise. Der kommer noget ustruktureret data ind via f. eks. e-mail og AI hjælper så med at gøre disse data struktureret, således at RPA kan tage over og starte sin automatiske proces.

Teknologien er derfor medvirkende til at RPA kan håndtere opgaver, som indeholder stor variation i den data som skal behandles, som et dokument eller e-mail med fri tekst har.

Dermed er det nok sikkert at sige, at RPA er kommet for at blive og at vi kommer til at se meget mere til det i de næste år fremover. Der vil derfor ikke være mange virksomheder, som ikke vil have en eller anden form for RPA som en naturlig del af deres IT-landskab inden for de næste 2-3 år.

Noter

[1] https://innovationsfonden.dk/da/presse/kunstig-intelligens-flytter-ind-paa-de-danske-arbejdspladser

Robotic Process Automation giver en række nye muligheder og forpligtelser til intern revision

Zeeshan Rajan, Senior Manager, PwC

Indledning

Virksomheder konkurrerer om at få frigjort den værdi, som den næste generation af digitale teknologier rummer, herunder den digitale arbejdskraft, som rækker langt ud over brugen af makroer i et regneark. Robotic Process Automation (RPA) udgør én form for digital arbejdskraft der involverer anvendelsen af softwarerobotter til automatisering af processer.

Softwarerobotterne er lette at konfigurere, kræver begrænset IT-ekspertise og kan hurtigt komme i spil og sætte gang i automatisering af manuelle opgaver. De kan udføre aktiviteter som fx at kopiere og indsætte data mellem applikationer, afstemme og foretage krydshenvisning af data mellem forskellige systemer og træffe overordnede beslutninger i bestemte dele af forretningsprocessen. RPA benyttes også i mere dynamiske miljøer, herunder til aktiviteter der involverer direkte kontakt med kunder og medarbejdere, fx behandling af forsikringskrav fra kunder eller oprettelse af nye medarbejdere med de rette IT-adgange.

RPA's bidrag til virksomhedens drift og konkurrencemæssige positionering er væsentlig på flere områder: Økonomisk værdi, fordele i forhold til arbejdskraft, kvalitetsforbedringer, fleksibel udførelse, hastighed og smidighed.

> **PwC estimerer, at 45 % af alle arbejdsopgaver kan automatiseres ved hjælp af robotteknologi.**

Derudover udgør RPA-projekter, der dokumenterer værdien af automatisering og gør medarbejderne fortrolige med den digitale arbejdskraft, ofte et springbræt til endnu mere omfattende initiativer, der inkluderer maskinel indlæring (Machine Learning) eller andre former for kunstig intelligens.

I forhold til intern revision bringer RPA både en række nye muligheder og forpligtelser med sig. Den interne revision har således mulighed for at blive en betroet rådgiver og samarbejdspartner med lederne af andre funktioner og forretningsområder om at forbedre kontrolmiljøet, efterhånden som forretningsprocesserne re-designes og automatiseres ved hjælp af RPA. Der vil inden for intern revision være behov for nye testmetoder i forbindelse med de nye automatiserede processer.

Interne revisorer har også et ansvar for at forstå de risici, som RPA bringer med sig, og sikre, at virksomhedens kontroller er fornuftigt udformet og fungerer effektivt for at imødegå disse risici. Og her findes måske i virkeligheden den største mulighed: Test af kontroller og andre opfølgnings opgaver kan automatiseres via RPA, hvilket øger kapaciteten i den interne revision og frigør revisorer til at fokusere på mere værdiskabende aktiviteter.

Efterhånden som RPA's momentum øges, kan interne revisorer holde trit ved at hjælpe virksomheden med at forstå og styre RPA-risiciene og ved at tage RPA til sig i deres egen funktion.

Få hjælp til at forstå og styre RPA-risici

Automatisering kan uden tvivl øge compliance og mindske risici. I modsætning til mennesker, som kan springe trin over i processer, eller som er inkonsekvente i den måde, de udfører en transaktion på, udfører en softwarerobot opgaven i henhold til en standardiseret metode, der er fordomsfri og uden afvigelser, hvilket sikrer en høj grad af nøjagtighed. Men RPA kan også føre til risici, hvis der ikke er implementeret passende kontroller samt overvågning heraf. Eksempelvis vil eventuelle fejl – fordi RPA-handlinger udføres konsekvent – blive et systemisk og udbredt problem på tværs af den pågældende forretningsgang og det pågældende datasæt. Eller hvis der er foretaget en ændring i en forretningsgang, men robotten ikke er blevet modificeret for at imødegå ændringen, kan det resultere i fejl eller unøjagtigheder. Derudover er der også en risiko for, at nogen skaffer sig uretmæssig adgang til robotten. Derved kan den ændres eller anvendes til at udføre uautoriserede handlinger.

Revisionschefer og deres teams skal forstå, hvordan virksomheden bruger RPA, og hvordan RPA påvirker virksomhedens risikoprofil, ved at betragte eksponering bredt og på tværs af flere risikokategorier - se **Figur 1** på næste side.

Hvis man helt fra begyndelsen etablerer governance for RPA i relation til kontroller, kan det være med til effektivt at mindske potentielle risici. Ved at forankre governance, risikostyring og kontroller i virksomhedens mobilisering

og implementering af RPA, kan virksomhederne opdage forhold, før de bliver til egentlige problemer. At komme godt fra start er langt mere effektivt – også fra et omkostningsmæssigt synspunkt – end hvis man senere prøver at samle op på politikker og kontroller.

Ved at involvere den interne revision tidligt i RPA-processen sikres nuancerede drøftelser, vurdering af risici og enighed om de overordnede rammer for governance og krav til procesdesign.

Automatisering af kontroller, test af kontroller og andre interne opgaver

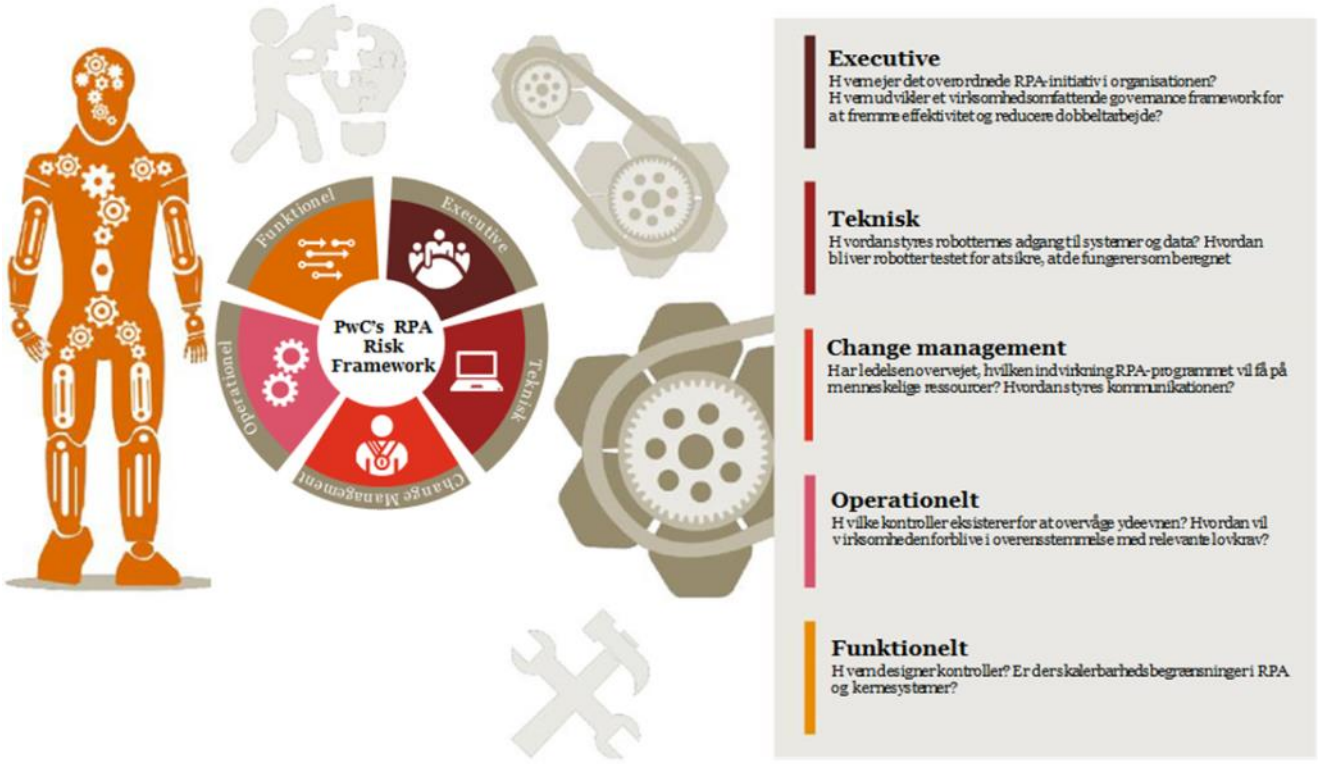
Kontroller kræver i sagens natur en ensartet aktivitet og et dokumentationsniveau, der gentages igen og igen – karakteristika, der gør dem til ideelle kandidater til automatisering. Ud over at hjælpe virksomheden med at forstå RPA-risici er den interne revision i den perfekte position til at identificere og anbefale kontroller, der er velegnede til automatisering.

Automatisering af kontroller har en positiv afsmittende virkning på den interne revision. Testmetoder skal ændres for processer, der netop er blevet automatiseret, men testen af den automatiserede kontrol vil efter al sandsynlighed til gengæld også være langt mere effektiv.

Mange revisionschefer er på udkig efter mere effektive metoder til at opfylde basale compliance-krav for interne kontroller. I tilfælde hvor automatisering af kontroller ikke er mulig eller på plads, kan automatisering af test af kontroller måske være en mulighed. I en stor organisation kan anvendelse af RPA til automatiseret test af generelle kontroller potentielt frigive tusindvis af revisortimer, som i stedet kan benyttes til andre højt prioriterede revisioner.

Ved hjælp af automatiserede tests kan den interne revision teste alle datapopulationer frem for at foretage stikprøver, og ledelsen kan have større tillid til, at kontrollerne er udformet og fungerer effektivt.

Figur 1: Fem risikokategorier i forbindelse med implementering af RPA



Ud over automatiseret test af kontroller, rummer RPA et betydeligt potentiale for at ændre den måde, hvorpå den interne revision arbejdes. Nogle af de opgaver, der kan automatiseres ved hjælp af RPA, omfatter bl.a.:

- At identificere åbne poster, sende mails til ansvarlige parter, foretage opfølgning, når deadlines ikke overholdes, og dokumentere status for udbedring
- At registrere fremgang i forhold til den årlige revisionsplan eller at registrere og overvåge key risk indicators (KRI'er)
- At automatisere rapportering og aktiviteter relateret til udarbejdelse af dashboards, herunder udfyldelse af revisionsudvalget og ledelsens rapport-templates eller den interne revisions scorecards
- At vurdere datakvaliteten i systemerne, fx i stamdata, og kontrollere fuldstændigheden i forhold til felter, dubletter og validering.

For at få fuld udnyttelse af fordelene ved RPA skal implementeringen håndteres med samme disciplin og omtanke som alle andre teknologibaserede projekter. Den interne revision bør udnytte virksomhedens digitale initiativ som en teknologisk platform for omkostningsbesparelser og øget risikoafdækningen.

Det er PwC's erfaring, at en vellykket udrulning af RPA kræver overvejelser i forhold til indførelse af et fuldstændigt regelsæt: En strategi for udvælgelse af de rigtige processer samt prioritering af disse; governance; udvikling, test og anvendelse; og den rette infrastruktur, support og driftsmodel til håndtering af den nye arbejdsstyrke af robotter. En formel strategi og plan vil resultere i, at der vises den omhu i forbindelse med automatiseringsinitiativet, der er nødvendig for at gøre det til et bæredygtigt, transformerende projekt. Veltilrettelagt og god undervisning kan hurtigt udruste slutbrugerne i den interne revision med de nødvendige kvalifikationer til at implementere en langsigtet, holdbar digital arbejdsstyrke i den nye driftsmodel.

Hvorfor vente?

Revisionscheferne er under fortsat pres i forhold til at øge den interne revisions bidrag til forretningen og optimere omkostningerne. RPA har potentiale til at levere betydelige produktivitets- og omkostningsforbedringer såvel som risikoafdækning. Det er blevet tid til, at den interne revision tager proaktivt del i organisationens RPA-initiativer og udarbejder en strategi og et roadmap over sin egen anvendelse af RPA. I takt med at den næste bølge af nye teknologier skaber disruption i alle brancher, vil det fremsynede revisionsudvalg undersøge mulighederne i RPA, og revisionschefer, der skrider til handling nu, kan komme foran - se **Figur 2** for spørgsmål som revisionschefen bør overveje.

Figur 2: Spørgsmål som revisionschefen bør overveje

Audit In An Age Of Intelligent Machines

Article by Tim McCollum. Tim McCollum is Internal Auditor's associate managing editor.

This article was reprinted with permission from the December 2017 issue of Internal Auditor, published by The Institute of Internal Auditors, Inc., www.theiia.org.

Already in use at many organizations, artificial intelligence is poised to transform the way business operates.

While monitoring transactions, an alert bank data analyst noticed unusual payments from a computer manufacturer to a casino. Because casinos are heavily computerized, one would expect the payments to go to the computer company. The analyst alerted an investigative agent, who rapidly scoured websites, proprietary data stores, and dark web sources to find detailed information about the two parties. The data revealed that the computer manufacturer was facing a criminal indictment and a civil law suit. Meanwhile, the casino had lost its gambling license due to money laundering and had set up shop in another country. Further investigation revealed the computer manufacturer was using the casino to launder money before the company's legal issues drove it out of business.

The bank's data analyst was a machine learning algorithm. The investigative agent was an artificial intelligence (AI) agent.

AI is all around. It's monitoring financial transactions. It's diagnosing illnesses, often more accurately than doctors. It's carrying out stock trades, screening job applicants, recommending products and services, and telling people what to watch on TV. It's in their phones and soon it will be driving their cars.

And it's coming to organizations, maybe sooner than people realize. Research firm International Data Corp. says worldwide spending on cognitive and AI systems will be $12 billion this year. It predicts spending will top $57 billion by 2021.

"If you think AI is not coming your way, it's probably coming sooner than you think it is," says Yulia Gurman, director of internal audit and corporate security for the Packaging Corporation of America in Lake Forest, Ill. Fresh off of attending a chief audit executive roundtable about AI, Gurman says AI wouldn't have been on the agenda a year ago. Like most of her peers present, she hasn't had to address AI within her organization yet. Now it's on her risk assessment radar. "Internal auditors should be alerting the board about what's coming their way," she says.

The Learning Algorithm

Intelligent technology has already found a place on everyday devices. That personal assistant on the kitchen counter or on the phone is an AI. Alexa, Cortana, and Siri can find all sorts of information for people, and they can talk to other machines such as alarm systems, climate control, and cleaning robots.

Yet, most people don't realize they are interacting with AI. Nearly two-thirds of respondents to a recent survey by software company Pegasystems say they have not or aren't sure they have interacted with AI.

"Internal auditors should be alerting the board about what's coming their way."
Yulia Gurman

But questions about the technologies they use — such as personal assistants, email spam filters, predictive search terms, recommended news on Facebook, and online shopping recommendations — reveal that 84 percent are interacting with AI, according to the What Consumers Really Think About AI report.

What makes AI possible is today's massive availability of data and computing power, as well as significant advances in the quality of the machine learning algorithms that make AI applications possible, says Pedro Domingos, a professor of computer science at the University of Washington in Seattle and author of *The Master Algorithm*. When AI researchers like Domingos talk about the technology, they often are referring to machine learning. Unlike other computer applications that must be written step-by-step by people, machine learning algorithms are designed to program themselves.

"The technology is never going to accuse somebody of a crime or a regulatory violation."
David McLaughlin

The algorithm does this by analyzing huge amounts of data, learning about that data, and building a predictive model based on what it's learned. For example, the algorithm can build a model to predict the risk that a person will default on his or her credit card based on various factors about the individual, as well as historical factors that lead to default.

Driven by Data

Using AI to make predictions takes huge amounts of data. But data isn't just the fuel for AI, it's also the killer application. In recent years, organizations have been trying to harness the power of big data. The problem is there's too much data for people and existing data mining tools to analyze quickly.

That is among the reasons why data-driven businesses are turning to AI. Five industries — banking, retail, discrete manufacturing, health care, and process manufacturing — will each spend more than $1 billion on AI this year and are forecast to account for nearly 55 percent of worldwide AI spending by 2021, according to IDC's latest Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide. What these industries have in common is lots of good data, says David Schubmehl, research director, Cognitive/AI Systems, at IDC. "If you don't have the data, you can't build an AI application," he explains. "Owning the right kind of data is what makes these uses possible."

Retail and financial services are leading the way with AI. In retail, Amazon's AI-based product recommendation solutions have pushed other traditional and online retailers like Macy's and Wal-Mart Stores Inc. to follow suit. But it's not just the retailers themselves that are driving product recommendations, Schubmehl says. Image recognition AI apps can enable people to take a picture of a product they saw on Facebook or Pinterest and search for that product — or something similar and less expensive. "It's a huge opportunity in the marketplace," he says.

Meanwhile, banks and financial service firms are using AI for customer care and recommendation systems for financial advice and products. Fraud investigation is a big focus. "The idea of using machine learning and deep learning to connect the dots is something that is very helpful to organizations that have traditionally relied on experienced investigators to have that 'aha moment,'" Schubmehl says.

That's what happened with the casino and the computer manufacturer. "The way AI works in that scenario is to say, 'Something is different. Let's bring it back to the central brain and analyze whether this is risky or not risky,'" says David McLaughlin, CEO and founder of AI software company QuantaVerse, based in Wayne, Pa. "The technology is never going to accuse somebody of a crime or a regulatory violation. What it's going to do is allow the people who need to make that determination focus in the right areas."

Currently, IDC says automated customer service agents and health-care diagnostic and treatment systems are the applications where organizations are investing the most. Some of the AI uses expected to rise the most over the next few years are intelligent processing automation, expert shopping advisors, and public safety and emergency response.

Regardless of the use, Schubmehl says it's the business units that are pushing organizations to adopt AI to advance their business and deal with potential disrupters. Because of the computing power needed, most industries are turning to cloud vendors, some of whom may also be able to help build machine learning algorithms.

Is AI Something to Fear?

Despite its potential, there is much fear about the risks that AI poses to both businesses and society at large. Some worry that machines will become too smart or get out of control.

There have been some well-publicized problems. Microsoft developed an AI chatbot, Clippy, that after interacting with people, started using insulting and racist language and had to be shut down. More recently, Facebook shut down an experimental AI system after its chatbots started communicating with each other in their own language, in violation of their programming. In the financial sector, two recent stock market "flash crashes" were attributed to AI applications with unintended consequences.

Respondents to the World Economic Forum's (WEF's) 2017 Global Risks Perception Survey rated AI highest in potential negative consequences among 12 emerging technologies. Specifically, AI ranked highest among technologies in economic, geopolitical, and technological risk, and ranked third in societal risk, according to the WEF's Global Risks Report 2017.

Employment

One of the biggest concerns is whether AI might eliminate many jobs and what that might mean to people both economically and personally. Take truck driving, the world's most common profession. More than 3 million people in the U.S. earn their living driving trucks and vans. Consulting firm McKinsey predicts that one-third of commercial trucks will be replaced by self-driving vehicles by 2025.

According to the Pew Research Center's recent U.S.-based Automation in Everyday Life survey, 72 percent of respondents are worried about robots doing human jobs. But only 30 percent think their own job could be replaced (see "The Jobs Question" at the bottom of this page). That may be wishful thinking. "However long it takes, there's not going to be any vertical industry where there's not the opportunity to automate humans out of a job," says John C. Havens, executive director of the IEEE Global AI Ethics Initiative. He says that will be the case as long as businesses are measured primarily by their ability to meet financial targets. "The bigger question is not AI. It's economics."

Ethics

With organizations racing to develop AI, there is concern that human values will be lost along the way. Havens and the IEEE AI Ethics Initiative are advocating for putting applied ethics at the front end of AI development work. Consider the emotional factors of children or elderly persons who come to think of a companion robot in the same way they would a person or animal. And who would be accountable in an accident involving a self-driving car — the vehicle or the person riding in it?

THE JOBS QUESTION

By now, internal auditors may be asking themselves, "Is AI going to take my job?" After all, an Oxford University study rated accountants and auditors among the professionals most vulnerable to automation. Of course, internal auditors aren't accountants. But are their jobs safe?

Actually, AI may be an opportunity, says IDC's David Schubmehl. He says many of the manual processes internal auditors review are going to be automated. Auditors will need to check how machine learning algorithms are derived and validate the data on which they are based. And, they'll need to help senior executives understand AI-related risks. "There's going to be tremendous growth in AI-based auditing, looking at risk and bias, looking at data," Schubmehl explains. "Auditors will help identify and certify that machine learning and AI applications are being fair."

Using AI to automate business processes will create new risks for auditors to address, says Deloitte & Touche LLP's Will Bible. He likens it to when organizations began to deploy enterprise resource planning systems, which shifted some auditors' focus from reviewing documents to auditing system controls. "I don't foresee an end to the audit profession because of AI," he says. "But as digital transformation occurs, I see the audit profession re-evaluating the risks that are relevant to the audit."

Internal audit could use AI to analyze an entire data set to identify cases that require the most scrutiny.

"The phrase we use is 'ethics is the new green,'" Havens explains, likening AI ethics to the corporate responsibility world. "When you address these very human aspects of emotion and agency early on — much earlier than they are addressed now — then you build systems that are more aligned to people's values. You avoid negative unintended consequences and you identify more positive opportunities for innovation."

Privacy and Security

Using AI to gather data poses privacy risks for both individuals and businesses. All those personal assistant requests, product recommendations, and customer service interactions are gathering data on people — data that organizations eventually could use to build a comprehensive model about their customers. Organizations using personalization agents must walk a fine line. "You want to personalize something to the point where you can get the purchase offer," Schubmehl says, "but you don't want to personalize it so much that they say, 'This is really creepy and knows stuff about me that I don't want it to know.'"

All that data creates a compliance obligation for organizations, as well. And it is also valuable to cyber attackers.

Output

Although AI has potential to help organizations make decisions more quickly, organizations need to determine whether they can trust the AI model's recommendations and predictions. That all depends on the reliability of the data, Domingos says. If the data isn't reliable or it's biased, then the model won't be reliable either. Moreover, machine learning algorithms can overinterpret data or interpret it incorrectly. "They can show patterns," he points out. "But there are other patterns that would do equally well at explaining what you are seeing."

Control

If machine learning algorithms become too smart, can they be controlled? Domingos says there are ways to control machine learning algorithms, most notably by raising or lowering their ability to fit the data such as through limiting the amount of computation, using statistical significance tests, and penalizing the complexity of the model.

He says one big misconception about AI is that algorithms are smarter than they actually are. "Machine learning systems are not very smart when they are making important decisions," he says. Because they lack common sense, they can make mistakes that people can't make. And it's difficult to know from looking at the model where the potential for error is. His solution is making algorithms more transparent and making them smarter. "The risk is not from malevolence. It's from incompetence," he says. "To reduce the risk from AI, what we need to do is make the computer smarter. The big risk is dumb computers doing dumb things."

Knowledge

Domingos says concerns about AI's competence apply as well to the people who are charged with putting it to use in businesses. He sees a large knowledge gap between academic researchers working on developing AI and the business employees building machine learning algorithms, who may not understand what it is they are doing. And he says, "Part of the problem is their bosses don't understand it either."

Governance

That concern for governance is one area the WEF's Global Risk Report questions — specifically, whether AI can be governed or regulated. Components of AI fall under various standards bodies: industrial robots by ISO standards, domestic robotics by product certification regulations, and in some cases the data used for machine learning by data governance and privacy regulations. On their own, those pieces may not be a big risk, but collectively they could be a problem. "It would be difficult to regulate such things before they happen," the report notes, "and any unforeseeable consequences or control issues may be beyond governance once they occur."

"You don't want to personalize it so much that they say, 'This is really creepy and knows stuff about me that I don't want it to know."
David Schubmehl

AI in IA

Questions of risk, governance, and control are where internal auditors come into the picture. There are similarities between deploying AI and implementing other software and technology, with similar risks, notes Will Bible, audit and assurance partner with Deloitte & Touche LLP in Parsippany, N.J. "The important thing to remember is that AI is still computer software, no matter what we call it," he says. One area where internal auditors could be useful, Bible says, is assessing controls around the AI algorithms — specifically whether people are making sure the machine is operating correctly.

If internal auditors are just getting started with AI, their external audit peers at the Big 4 firms are already putting it to work as an audit tool. Bible and his Deloitte colleagues are using optical character recognition technology called Argus to digitize documents and convert them to a readable form for analysis. This enables auditors to use data extraction routines to locate data from a large population of documents that is relevant to the audit.

For auditors, AI speeds the process of getting to a decision point and improves the quality of the work because it makes fewer mistakes in data extraction. "You can imagine a day when you push a button and you're given the things you need to follow up on," Bible says. "There's still that interrogation and investigation, but you get to that faster, which makes it a better experience for audit clients."

QuantaVerse's McLaughlin says internal auditors could take AI even farther by applying it to areas such as fraud investigation and compliance work. For example, rather than relying on auditors or compliance personnel to catch potential anti-bribery violations, internal audit could use AI to analyze an entire data set of expense reports to identify cases of anomalous behavior that require the most scrutiny. "Now internal audit has the five cases that really need a human to understand and investigate," McLaughlin says. "That dramatically changes the effectiveness of an internal audit department to protect the organization."

The key there is making sure a person is still in the loop, Bible says. "The nature of AI systems is you are throwing them into situations they probably have not seen yet," he notes. A person involved in the process can evaluate the output and correct the machine when it is wrong.

Building Intelligence

Bible and McLaughlin both advise internal audit departments to start with a small project, before expanding their use of AI tools. That goes for the organization, as well. Organizations first will need to take stock of their data assets and get them organized, a task where internal auditors can provide assistance.

"Part of the problem is their bosses don't understand [AI] either."
Pedro Domingos

For audit executives such as Gurman, the objective is to get up to speed as fast as possible on AI and all its related risks, so they can educate the audit committee and the board. "There is a lot of unknown," she concedes. "What risks are we bringing into the organization by being more efficient and using robots instead of human beings? Use of new technologies brings new risks."

To learn more about internal audit's role in AI,
DOWNLOAD The IIA's Artificial Intelligence: Considerations for the Profession of Internal Auditing.

Revision af GDPR compliance hos databehandlere

Michael Bagger, Director, Deloitte

Indledning

Den 25. maj 2018 udløber implementeringsperioden for den nye europæiske databeskyttelsesforordning (General Data Protection Regulation, GDPR). I forordningen sættes der fokus på sikring af individets rettigheder og data, og dermed øges kravene til virksomhedernes opbevaring og behandling af persondata.

Selvom en stor del af indholdet i forordningen, herunder hvordan data skal beskyttes, ikke er ændret, set i forhold til allerede gældende lovgivning, så drives debatten af få enkeltelementer fra lovteksten, som er med til at sætte scenen for virksomhedernes arbejde med at etablere foranstaltninger, der sikrer overholdelse af loven. Ord som bødestørrelser, Data Protection Officer (DPO) og henholdsvis dataansvarlig og databehandler, er flyttet ind i virksomhederne som aldrig før, og behovet for at synliggøre compliance over for kunder, samarbejdspartnere og investorer har aldrig været større.

Som følge heraf, er der stigende efterspørgsel efter blåstempling af interne procedurer og retningslinjer, og revision af området er i vækst. Efterspørgsel på assurance af de klassiske interne kontroller må for tiden se sig slået af efterspørgslen på GDPR-assurance.

Databeskyttelsesforordningen

Den nuværende persondatalov trådte i kraft i år 2000, efter flere år med implementering af databeskyttelsesdirektivet. Den 4. maj 2016 blev databeskyttelsesforordningen offentliggjort, og allerede fra d. 24 maj samme år trådte den i kraft. Samtidig blev en implementeringsperiode på de efterfølgende to år fastlagt. I den periode kunne virksomhederne tilpasse deres interne retningslinjer for håndtering af persondata, således at de understøtter overholdelse af den nye lovgivning. Ved udløb af implementeringsperioden pr. 25 maj 2018, ophæves samtidig den eksisterende persondatalov.

Overordnet set er mange af grundprincipperne i forordningen, i al væsentlighed, uændrede i forhold til den gældende persondatalov. Dog tilføres der også en række nye bestemmelser, samtidig med, at eksisterende bestemmelser i flere tilfælde indskærpes og præciseres.

Af de væsentligste områder, hvor der sker ændringer eller tilføjelser kan nævnes:

- Krav til konsekvensanalyser ved behandling af særlige typer af data
- Krav til risikoanalyse af sikkerheden omkring beskyttelse af data
- Større dokumentationskrav i form af procedurer og beskrivelser af systemer
- Datasikkerhed og fortrolighed skal fremadrettet tænkes ind i systemer og processer fra starten
- Skærpede krav til databehandleraftaler
- I visse tilfælde krav om etablering af en Databeskyttelsesrådgiver (DPO)
- Skærpet notifikationspligt ifm. datalæk
- Væsentligt skærpede sanktioner.

Behov for assurance

Tredjepartserklæringer er i vid udstrækning blevet anvendt for at synliggøre compliance i forhold til den gældende persondatalov, og de vil komme til at spille en endnu større rolle fremadrettet. Dels stilles der i databehandleraftalerne krav om, at databehandleren skal gøre en revisionserklæring tilgængelig, med mindre man ønsker on-site revision udført af de dataansvarlige, og dels vil en revisionserklæring fremadrettet blive en endnu større konkurrenceparameter i kampen om potentielle kunders data.

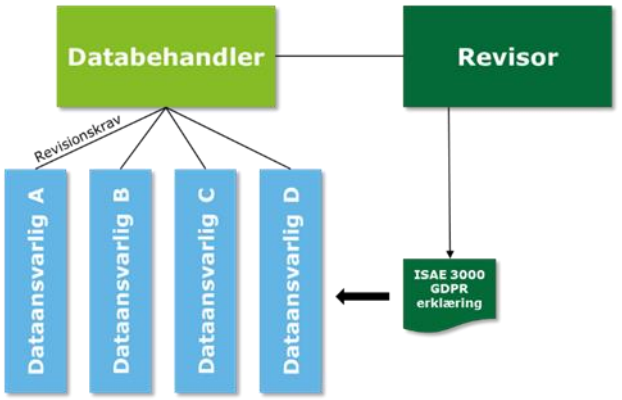
Set fra databehandlerens synsvinkel vil revision i form af en GDPR-erklæring, udført af et af de anerkendte revisionshuse, altid være at foretrække, frem for selv at skulle imødegå de dataansvarliges krav om egen revision. Det er utvivlsomt den mest effektive form for assurance, der kan gives for alle involverede parter, og man vil med en revisionserklæring kunne dække det fælles behov, som ligger hos størstedelen af de dataansvarlige.

Årsagen hertil skal findes i det faktum, at databehandlere oftest stræber efter en revision, der rammer så bredt som muligt, og dermed imødegår assurancebehovet fra den bredest mulige vifte af kunder. Og på denne front adskiller GDPR-erklæringen sig ikke fra andre typer af revisionserklæringer, hvor der arbejdes med begreberne generelle og specifikke erklæringer, afhængig af modtageren.

Dataansvarlige vil formentlig stile mod et fast sæt af grundprincipper for behandling og beskyttelse af data i

sine data-behandleraftaler, og derfor giver det mening for databehandleren med en revision efter de fælles principper, og dermed gå efter en generel erklæring.

Figur 1: Koncept for effektiv assurance via afgivelse af en samlet revisionserklæring



Som alternativ til revisionserklæringen kan databehandleren tillade den dataansvarlige selv at foretage revision, og via en mere målrettet revision give den dataansvarlige den fornødne assurance. Ressourcemæssigt er der nogenlunde samme træk på både den dataansvarlige og databehandleren for hver revision, så ineffektiviteten i ressourceforbruget ved individuelle revisioner er til at få øje på.

Revisionserklæringer

For virksomheder (både private og offentlige), som har outsourcet drift af systemer, der indeholder persondata, eller selve behandlingen af personoplysninger til en leverandør, vil det derfor ofte være relevant at indhente en revisorerklæring fra denne leverandør for derved at kunne dokumentere og påvise overholdelse af kravene i forordningen.

Udarbejdelse af en sådan revisionserklæring kan ske efter ISAE (International Standard on Assurance Engagements) 3000 standarden, (Andre erklærings-opgaver med sikkerhed end revision eller review af historiske finansielle oplysninger). Men hvor erklæringer, som følger den nuværende persondatalov, er mere begrænsede i den information og gennemsigtighed, der leveres til læseren, så er en GDPR-erklæring opbygget, så den tilbyder samme grad af detalje, som ligger i ISAE 3402 standarden. Herved stilles der også andre krav til databehandlerens input til rapporteringen, i form af både udtalelse og beskrivelse af system og kontroller.

Opstillet giver det følgende sammenligning af erklæringerne - se **Tabel 1**.

ISAE 3000-standarden er kendt og finder anvendelse i det meste af verden uden for USA, og den vil derfor være det oplagte valg. Hvis man i virke af databehandler alle-

Tabel 1: Indholdsmæssig sammenligning af GDPR-erklæringen med ISAE 3000 og ISAE 3402.

	ISAE 3000	ISAE 3000 - Persondata	ISAE 3402
Beskrivelse af leverandørens system	Valgfrit	Obligatorisk	Obligatorisk
Leverandørens udtalelse	Valgfrit	Obligatorisk	Obligatorisk
Beskrivelse af kontrolmål	Valgfrit	Obligatorisk	Obligatorisk
Beskrivelse af kontrolaktiviteter	Valgfrit	Obligatorisk	Obligatorisk
Beskrivelse af testhandlinger	Obligatorisk	Obligatorisk	Obligatorisk
Beskrivelse af resultat af de enkelte testhandlinger	Valgfrit	Obligatorisk	Obligatorisk
Samlet konklusion i revisors erklæring	Obligatorisk	Obligatorisk	Obligatorisk
Grad af sikkerhed	Begrænset eller høj	Begrænset eller høj	Høj

rede får udarbejdet en ISAE 3402-erklæring omhandlende eksempelvis generelle it-kontroller og driftssikkerhed, vil der være en del kontroller, der kan "genbruges" i en ISAE 3000-erklæring om overholdelse af GDPR.

Et alternativ til ISAE 3000-erklæringen kan være at kigge mod en amerikansk standard for tredjeparts-erklæringer - SOC (System and Organization Controls) 2-erklæring. SOC 2-erklæringen er i modsætning til en ISAE-erklæring en amerikansk standard udstedt af AICPA (American Institute of Certified Public Accounts), hvor revisor kan erklære sig om udvalgte Trust Service Principles og de underliggende kontrollers design, implementering og effektivitet. SOC 2-standarden vinder stigende indpas særligt i udlandet og rummer mulighed for at indeholde rapportering af både Security, Availability, Confidentiality, Processing Integrity og netop Privacy. Derved kan der rapporteres om både generelle it-kontroller og persondata i samme rapport.

Rammeværket fra FSR

Foreningen af Statsautoriserede Revisorers Cyber-sikkerhedsudvalg har udarbejdet et rammeværk om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger, som finder anvendelse ved udarbejdelse af GDPR-erklæringer. Rammeværket tager direkte udgangspunkt i forordningen, og FSR har på baggrund af de enkelte artikler, defineret eksempler på kontrolmål og tilhørende kontrolaktiviteter. Ved at implementere kontroller, som imødegår de definerede kontrolmål, kan virksomhederne understøtte deres arbejde med overholdelse af forordningen, artikel for artikel.

Som nævnt kan man ikke afgrænse sig fra lovgivningen, men omfanget af interne kontroller, som er påkrævet for at understøtte GDPR-compliancefunktionen, varierer afhængig af databehandlerens rolle over for dataansvarlig. I FSR's rammeværk skelnes i udgangssituationen mellem følgende grader af involvering (i stigende rækkefølge) for en databehandler:

Housing-ansvar
Et datacenter, som kun leverer hardware, fysisk sikring af udstyr, strøm og internetforbindelse.

Driftsansvar
En serviceleverandør, som varetager driften af eksempelvis servere og databaser.

Applikationsansvar
En serviceleverandør, som enten driver eller udvikler den dataansvarliges applikation(er).

Procesansvar
En serviceleverandør, som har det fulde ansvar for en eller flere af den dataansvarliges processer, eksempelvis en outsourcet lønproces.

Det vil sige, at en databehandler, som udelukkende har et housing-ansvar, i udgangssituationen vil have langt færre kontroller med i erklæringen, da ansvaret i databehandleraftalerne med deres kunder tilsvarende vil være begrænset. Eksempelvis vil det næppe være relevant for en housing-leverandør at etablere kontroller vedrørende berigtigelse eller sletning af data – det vil være den dataansvarliges ansvar.

Der følger for virksomhederne derfor en øvelse i, at afgrænse sig i forhold til de af virksomhedens ydelser, hvor der behandles persondata. Dermed ikke sagt at man kan afgrænse sig fra lovgivningen, men man kan afgrænse sig i forhold til områder, for hvilke der nødvendigvis skal gives assurance over for tredjepart.

Mængden af arbejde, som skal udføres både af revisor, men også af virksomheden selv, for at kunne levere en GDPR-erklæring til de dataansvarlige, afhænger direkte af det omfang erklæringen får i forhold til de services databehandleren leverer. Derfor er essensen at få styr på de relevante områder, typisk baseret på de indgåede databehandleraftaler.

Interne kontroller og dokumentation

Selve revisionsarbejdet udføres som test af interne kontroller, hvor revisor gennemgår kontrollernes design, implementering og operationelle effektivitet, med henblik på at vurdere, hvorvidt kontrollerne imødegår de definerede kontrolmål. På den baggrund udformer revisor erklæringens påtegning, på lige fod med andre typer af revisionserklæringer.

For at imødegå revisionskravet, vil virksomhedens interne GDPR-kontroller skulle dokumenteres på lige fod med eksempelvis generelle it-kontroller, kontroller der udføres ifm. månedsafslutning og lignende. Virksomheden kan således ved fremvisning af erklæringen dokumentere udførte kontroller.

Størstedelen af den påkrævede dokumentation ligger i virksomhedens skrevne procedurer for behandling og håndtering af persondata, og forberedelsesarbejdet vil i høj grad ligge i den formelle stillingtagen til, hvorledes behandling af persondata er etableret og sikret, og hvorledes kravene i forordningen er imødegået, herunder muligheden for berigtigelse, sletning etc. Med forordningen kommer der dog også mere fokus på løbende stillingtagen til, hvorvidt virksomhedens procedurer fortsat er

gældende. Tidligere har der været tendens til, at datapolitikker er blevet oprettet, og efterfølgende arkiveret som et statisk dokument.

For at opretholde et kontrolmiljø, som understøtter virksomhedens arbejde med overholdelse af GDPR-lovgivningen, så er der behov for en mere aktiv tilgang, og implementering af løbende kontroller, som sikrer, at virksomheden kontinuerligt kan overholde sine forpligtelser. Eksempelvis hvis der indgås aftale med en ny underleverandør, hvis der implementeres et nyt CRM-system, eller hvis medarbejdere får mulighed for hjemmearbejdspladser etc. I alle tilfælde bør virksomheden genoverveje de opsatte procedurer og kontroller, og forholde sig til, om disse stadig kan opretholdes under de nye og ændrede forhold.

Hvis virksomheden allerede arbejder med kendte kontrolrammer, eksempelvis ISO 27001 eller COSO, så kan det være hjælp til at adoptere GDPR-arbejdet, idet kulturen omkring udførsel og dokumentation af kontroller er tilsvarende, og det mindset der ligger bag, hvor hele tilgangen er risikobaseret, i høj grad kan relateres til de kontroller, som fremgår af rammeværket fra FSR.

Afslutning

Der ligger en forventning hos de dataansvarlige virksomheder om, at de leverandører, der agerer databehandler overholder forordningen, når implementeringsperioden udløber i maj. Og hvis man ikke allerede er i gang med tilpasning til den nye virkelighed, så er det nok ved at være sidste udkald.

Der er ingen tvivl om, at paratheden til at arbejde med GDPR-compliance afhænger af mange faktorer, herunder modenheden af virksomhedens generelle kontrolmiljø. Og compliance opnås ikke udelukkende ved at implementere et system eller ansætte en DPO, og compliance er ikke en målstreg, der skal krydses, eller et flueben der skal sættes. Det er et fundament for virksomheden, som foruden de omtalte procedurer, kontroller og teknologi, der kan underlægges revision, i høj grad også omfatter mennesker, ledelse og kultur.

Et solidt overblik over data, der behandles, hvor de opbevares, og hvordan de transporteres, bør være første step på vejen mod at etablere interne processer og kontroller, som understøtter arbejdet med overholdelse af databeskyttelsesforordningen. Og i erklæringsøjemed vil de fleste virksomheders modenhed i udgangssituationen ikke være på et ønsket niveau - endnu. Men efterhånden som indholdet og kravene i forordningen bliver afmystificeret og nærmer sig noget konkret, så bliver målet også mere klart.

Den klassiske revisorens rolle har historisk set været at agere uafhængig kontrollant, og selvom emnet nu hedder GDPR, så har revisorens funktionen ikke ændret sig. Revisor afgiver uafhængig, gennemsigtig og detaljeret information til de dataansvarlige om, hvorvidt databehandlere beskytter og behandler data som foreskrevet af lovgivningen. Og den information vil for de fleste være værdifuld når der skal vælges samarbejdspartnere, til hvem man som dataansvarlig ofte overdrager betydelige mængder af virksomhedens vigtige data.

IIA PRISEN

Prisopgave om intern revision

Foreningen af Interne Revisorer uddeler 2 præmier til hovedopgaver på cand. merc. aud. studiet

1. præmie: 25.000 kr.
2. præmie: 15.000 kr.

Prisens formål er at fremme kendskabet til og forskningen inden for intern revision.

Hovedopgaven skal omfatte et emne og en problemformulering, som er relevant for forståelsen af intern revisions arbejde og betydning for de virksomheder, som har eller overvejer at etablere(t) en intern revisionsfunktion. For at komme i betragtning skal hovedopgaven have opnået karakteren 10 eller 12 og være afsluttet i perioden 1. august 2017 til 31. juli 2018.

Ansøgningen indsendes elektronisk til foreningens formand på ksh@nykredit.dk. Ansøgningen skal indeholde

1) kontaktinformationer
2) problemformulering, indledning og konklusion
3) hovedopgaven

Ansøgningsfristen er 31. juli 2018. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

Prisoverrækkelsen vil ske i løbet af efteråret 2018. Bedømmelsesudvalget består af medlemmer af bestyrelsen for Foreningen af Interne Revisorer og repræsentanter for læreanstalterne.

Den/de studerende bestemmer selv emnet for hovedopgaven, og der findes forslag til emner, som kan anvendes til inspiration, på foreningens hjemmeside www.iia.dk.

Foreningen af Interne Revisorer
The Institute of Internal Auditors - Denmark

10 tips to reduce the costs of internal controls in 2018

Hernan Huwyler, MBA, CPA
Sr. Manager, Risk Advisory,
Deloitte

In recent years, compliance and cybersecurity risks dominated both Board and Internal Audit agendas. After constantly evolving initiatives to address these risks, control structures resulted in a vast array of multi-layered controls increasing expenses and cluttering workflows. Transaction costs increased due to additional approval, reconciliation, and securing of data as well as testing activities. Also, with so many moving pieces, the internal control framework became inflexible to support changes in many organizations.

The right time to consider the efficiency and costs of controlling would be during the planning of the audit program for 2018. This article provides 10 practical suggestions intended to assist management in streamlining internal controls.

1. **Use the RACI model for formulating clear policies**: The RACI (Responsible/Accountable/Consulted/ Informed) model was initially developed by reengineering and project management specialists to define the responsibilities for the performance of specific activities across people and departments. Internal Audit can use this powerful model to facilitate the design of easy-to-follow policies and controls. In the RACI model, each sequential activity in a business process is mapped into a matrix to coordinate how managers and employees interact. Internal Audit could use the RACI approach to identify and remediate duplicated tasks, missing controls and lack of accountability. The model will help to avoid disputes about roles and control responsibilities which inevitably create inefficiencies.

2. **Base policies on control principles**: Heavily detailed policies not only lead to micromanagement, they are also susceptible of circumvention through the creation of unnecessary exceptions. Policies focusing on simple control objectives are easier to follow, and it is easier to audit compliance with such policies. Having intricate and fully documented sets of controls in policies will not better reduce risks involved in processes. On the contrary, they will reduce accountability and create possibilities of circumventing controls and complicate training. Controls based on principles produce policies which are economical and easier to comply with. They also simplify alignment of incentives with control performance and compilation of checklists for control self-assessments. Internal Audit could assess the efficiency and relevance of policies to suggest improvements to the business, including improve the template design and simplify the control narratives.

3. **Shorten approval chains**: Layers of approval accumulate over time as archeological evidence of power disputes in the management functions. Single and independent approvals should only be given when

transactions are trigged, and when exceptions occur. For instance, once a purchase order is approved and successfully fulfilled, it makes no business sense to ask for additional approval in the related vendor invoice or payment. Focusing approvals on collusion risks and exceptions can simplify the delegation of authority while reducing the processing time of transactions. Internal Audit can use data analytics, file interrogation techniques and interviews with business owners to identify delays and inefficiencies in the approval chains.

4. **Increase control thresholds**: Validation limits can be increased for transactions with lower fraud risks or higher control costs. For example, it makes no sense to create a dispute with a supplier when the amount to reclaim is lower than the costs of processing, booking and managing such dispute. Compensatory controls and detective monitoring can also help to increase control thresholds. Internal Audit can use stratification techniques to compare the control costs with risk exposure through transactional thresholds.

5. **Limit payment channels**: Companies using bank transfers (and sometimes even checks) from multiple accounts increase the controlling costs and create new fraud risks. Controls can be optimized by consolidating payment channels and diverting low-risk procurement to purchase cards. Internal Audit can analyze the number of transactions and their accumulated value for the different payment channels to assess the associated costs and risks.

6. **Rationalize the chart of account**: Poorly designed or inconsistent charts of account makes it harder to reconcile and control balances and to limit the ability to provide performance insights. Ensuring data integrity and consistency when charts of accounts are complex requires unnecessary controls in manipulating data for financial, management, tax, and operational reporting purposes. Hierarchies, roll-outs and consolidations should be easily traceable for controlling and prevent classification errors in bookings. Internal Audit can interview stakeholders in respect of how they perceive the chart of accounts and how it addresses the decision-making needs of the business.

7. **Group transactions**: Grouping the processing, booking, and approval of similar transactions can reduce the number of necessary controls. There are many strategies to reduce the number of control events by grouping transactions, for example by using framework contracts for supplies, blanket purchase orders and by limiting urgent procurement or payments. Internal Audit can ask the business owners to consider alternatives for reducing the number of events to control.

8. **Integrate assurance**: The lack of coordination between assurance functions results in overlapping policies and role definitions. Ad hoc remediation plans after fraud or findings detected by different types of audits end up in redundant controls, documents, and tools for addressing the same risk. Integrated assurance make it easier to address the root cause of deficiencies to avoid disconnected remediation plans. Close collaboration across the risk, control, and compliance functions will result in controls aligned with business risks. Assurance maps work well in integrating the lines of defense. Internal Audit can involve other assurance functions to develop a common framework with the support of the Board and their committees.

9. **Maximize ERP functionalities**: Poorly managed implementations do not make all the automated controls available in modern ERPs. Basic controls such as preventing double payments or payments without delivery slips are default settings in all ERPs, but complex functionalities may not be implemented during system roll-outs. Underutilized functionalities usually involve validating input data, setting recurring entries, operationalizing closing activities, parking documents for latter approval, managing credit limits, accessing incompatibilities, monitoring controls, documenting and validating master data changes, and preventing the splitting of vendor invoices. When reporting functionalities do not address information needs, both the finance department and the business create complex Excel spreadsheets to convert, reconcile, and control transactional data. Working with manual spreadsheets rather than directly using reports from ERPs can potentially leave controls susceptible of human errors when using outdated information and cost inefficiencies. Internal Audit can work with business owners and stakeholders to assess how all the ERP functionalities are implemented.

10. **Consider new business solutions**: Nowadays, there are plenty of solutions allowing automated policy enforcement. These paperless solutions reduce processing costs by automating time-consuming and error-prone manual processes, including their controls. Applications in this respect involve checking period-end reporting, performing automated reconciliations, processing travel and expense reports, e-invoicing, scanning documents, procurement portals, managing client credit, recording employee time and attendance,

and detecting fraud. For instance, solutions for workflows can manage pending actions, reminders, rejections, and alerts, and also keeping the period-end closing documents on a cloud platform improves communication. Analytics deserve a special mention here. Controls can be automated by real-time warnings and exception reports, based on analytics combining them with the thorough understanding of internal auditors. Internal Audit can be part of the consultation to identify and implement solutions to automate controls.

The responsibility for design and operation of a risk and internal control framework rests with the management, for instance, the CFO in terms of addressing accounting fraud and misreporting financial risks. In many instances, the management is still highly reliant on manual and complex controls. This is a tangible issue for Internal Audit since manual controls are difficult to test and increase the number of compliance findings. Internal auditors should impact on the control environment not only by assessing its adequacy and operation, but also by facilitating managers to enable stronger and cost-justifiable controls. Internal Audit can have frank discussions with top management about their aspirations, "gold standards", and available investments in the controlling areas. In the end, controls exist to generate a sustainable flow of income, to save money by reducing fraud and deviations from plans, and to address customer needs.

Nye medlemmer

Nye medlemmer i IIA fra 4.12.2017 – 5.4.2018

A.P. Møller Maersk
Wayne Allen Pfeister

Coop Danmark
Lars Nielsen

Danske Bank
Louise Vind Larsen
Henrik Nygaard
Kristina Birk Thomsen
Claus Fredenslund Mortensen

Nordea
Jelena Rakova

Nordjyske Bank
Marianne Jensen

Novo Nordisk
Carlos Pérez Horcas

Saxo Bank
Noel Martin Hoffmann Vang

Skandinaviska Enskilda Banken
Karoline Lefevre

Sparekassen Kronjylland
Mai-Britt Soo

Sparekassen Thy
Gritt Fisker

Uddannelsesaktiviteter

Er du opdateret på IIAs kursusudbud? Som altid findes datoer og emner for gå-hjem møder, kurser og konferencer på foreningens hjemmeside www.iia.dk under rubrikken "Uddannelse", hvor tilmelding til arrangementerne også foretages.

Nedenfor er fremhævet kommende planlagte kurser og møder, men listen bliver hele tiden opdateret, så det er bestemt værd at foretage et besøg på foreningens hjemmeside.

Kurser og gå-hjem møder

Kursus for pengeinstitut– og realkreditrevisorer, 19.4.2018. Afholdes på Quality Hotel Høje Taastrup.
CIA forberedelseskursus del 2. Afholdes på Tivoli Hotel, København.
IIA Årsmøde 2018, 17.5.2018-18.5.2018. Afholdes på Hotel Nyborg Strand.
Kursus for Forsikringsrevisorer, 30.5.2018. Afholdes på Forsikringsakademiet, Rungsted.

"Bagsmækken"

Foreningens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Vicerevisionschef Kim Stormly Hansen
Intern revision
Nykredit
Kalvebod Brygge 1-3
1780 København V

CVR nr. 73954215

Indmeldelse i foreningen

Indmeldelse i foreningen foretages på www.iia.dk eller til:

Chefsekretær Dorte Dreiøe
Nykredit
☎ 44 55 93 07 ✉ ddh@nykredit.dk

Jobannoncer

Jobannoncer for medlemmer kan bringes på foreningens hjemmeside og/eller i INFO.
Annoncer bringes kun i INFO, såfremt der er plads hertil.
Annonceudkast sendes til redaktionens adresse, jf. side 1, eller til glt@nykredit.dk.

Certificeringer

Nærmere oplysninger om certificeringer kan fås på IIA´s internationale hjemmeside www.globaliia.org eller ved kontakt til:

Heino Hansen, Internal Audit Manager, CIA, Nordea
☎ 31 18 38 01 ✉ heino.hansen@nordea.com

Peer Højlund, Chefspecialist, Nykredit
☎ 44 55 93 14 ✉ phc@nykredit.dk

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

Formand
Vicerevisionschef
Kim Stormly Hansen
Nykredit
☎ 44 55 93 17 ✉ ksh@nykredit.dk

Næstformand
Senior Vice President
Jesper Siddique Olsen
Danske Bank
☎ 45 12 76 58 ✉ jol@danskebank.dk

Kasserer
Koncernrevisionschef , CIA
Morten Bendtsen
PFA Pension
☎ 39 17 60 12 ✉ mob@pfa.dk

Sekretær
Senior Audit Manager, CIA, Afdelingsdirektør
Anette Kauffmann Laursen
Nordea
☎ 55 47 33 19 ✉ anette.laursen@nordea.com

Bestyrelsesmedlemmer
Regional Chief Auditor, CIA, CISA
Neil Jensen
RSA Scandinavia
☎ 40 42 64 26 ✉ njz@codan.dk

Koncernrevisionschef, COR
Pia Sønderlund Nielsen
Finansministeriet
☎ 25 26 27 72 ✉ pnn@fm.dk

Koncernrevisionschef
Poul-Erik Winther
Alm. Brand
☎ 45 47 78 97 ✉ abrpwe@almbrand.dk

Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Europæiske Rejseforsikring
☎ 33 27 84 82 ✉ brs@europaeiske.dk

Partner, CIA, CISA, CGEIT
Johan Bogentoft
PwC
☎ 29 27 62 96 ✉ Joa@pwc.dk