tilstrækkeligt til at afdække perioden. Herunder at vurdere hvor lang perioden er, og om et bridge-letter er tilstrækkeligt. Et bridge-letter består af følgende dele[1]:

- Erklæringens start- og slutdato
- Væsentlige ændringer til det interne kontrolmiljø
- En udtalelse om, at serviceorganisationen ikke er bekendt med væsentlige ændringer ud over dem, der er nævnt i bridge-letteret
- En påmindelse om, at brugerorganisationen er ansvarlig for at udføre de komplementerende kontroller
- En forespørgsel til brugerorganisationen om at læse erklæringen
- En disclaimer om, at bridge-letteret ikke er en erstatning for selve erklæringen

5.7. De 14 ISO-kontrolområder

Mens der findes mange muligheder for valg af governance-framework for it-styring, så er der en stærk tendens til, at virksomheder og organisationer herhjemme orienterer sig efter ISO 27001/02:2013. Det beskrev vi i kapitel 2. Derfor benyttes de enkelte ISO-hovedområder i Anneks A som kontrolmål. Hvilke kontrolmål der efterleves og skal gennemgås af it-revisor, afhænger helt og holdent af den ønskede erklæringstype samt den reviderede organisationsopbygning og it-risici.

It-revision omfatter ofte kun en delmængde af de samlede 14 kontrolmål. Fordi de er så almene styringsværktøjer, vælger vi at give en kort introduktion til dem. I felten vil it-revisor anvende ovennævnte 4 metodikker og stikprøvetagning for at vurdere efterlevelsen af hver enkelt. I mange tilfælde lægges der ekstra vægt på kontrolmålene: Adgangsstyring, håndtering af ændringer og impactstyring. Revisionsplanen skræddersys i hver case efter de enkelte kontrolmål og det overordnede revisionsmål med at afgive erklæring. Her vil it-revisor delkonkludere og konkludere samlet på, om informationssikkerhedspolitikken og de enkelte kontroller matcher de forhold, som beskrives i SoA'en. SoA'en rummer listen over udvalgte foranstaltninger, som virksomheden finder passende for at imødegå de identificerede risici på it-fronten.

Uden yderligere introduktion kaster vi os ud i det.

---

1. What are Bridge (Gap) Letters in SOC Reports? (f. SSAE 16/18) (linfordco.com).

5. Informationssikkerhedspolitikker
Retningslinjer for styring af informationssikkerhed
Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Det første kontrolmål har til formål at sikre en overordnet informationssikkerhed, der matcher både kommercielle krav og relevante love. Det handler om en styring af it i form af klare politikker, retningslinjer og procedurer for de øvrige kontrolmål. På den måde omkapsler ISO's kontrolområde 5 alle de andre, og det er fundamentalt for at komme i gang med en proaktiv it-styring.

Der indgår en vejledning til, hvad en informationssikkerhedspolitik skal indeholde. Blandt andet en forretningsstrategi, et overblik over det nuværende og forventede trusselsmiljø, afgrænsning og målsætninger samt processer for afvigelser og undtagelser mm. Alle vedtagelser skal være ledelsesgodkendt. Derudover bør der listes en kontrolansvarlig for hver politik, som står for udvikling, gennemgang og evaluering.

Helt konkret vil it-revisor gå ind og efterspørge en informationssikkerhedspolitik og tjekke for risikoanalyse, årshjul og opsætning af et ISMS-system, hvori alle procedurerne registreres løbende. Der vil være fokus på den overordnede it-strategi og budgettering. Findes der klare retningslinjer for noget så essentielt som brug af e-mail og internet? Er der foretaget en realistisk vurdering af risici og tænkt over worst case-scenarier og nødplaner? Informationssikkerhedspolitikken danner grundlag for resten af it-revisionen, fordi den fungerer som referencepunkt. Det er her, den reviderede virksomhed selv udstikker de retningslinjer og procedurer, hvis design, implementering og effektive funktion i perioden it-revisor tjekker.

6. Organisering af informationssikkerhed
6.1 Intern organisering
Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften at informationssikkerhed i organisationen.

Det er vigtigt, at der er et solidt ledelsesgrundlag for at implementere de nødvendige politikker og procedurer for den ønskede informationssikkerhed. Dette kontrolmål har til formål at strukturere roller og ansvarsområder og måden, virksomheden organiserer it-arbejdet på. Ansvar

dækker både internt og eksternt. Dvs. at hvis virksomheden har outsourcet væsentlige dele af sin it-drift, så skal der være en klar håndtering af leverandøren og leverandørens it-systemer.

Alle beføjelser skal gerne dokumenteres, så it-revisor hurtigt kan finde frem til den kontrolansvarlige. Det er også her, funktionsadskillelse kommer ind i billedet. Modstridende funktioner bør adskilles, så risikoen for magtmisbrug, fejl og uautoriseret anvendelse mindskes mest muligt. En anden kontrol er vedligeholdelse af kontakt med myndigheder. Det kan være alt fra offentlige myndigheder som politi, Datastyrelsen eller Arbejdstilsynet til leverandører som forsyningsselskaber og alarmcentraler.

6.2 Mobilt udstyr og fjernarbejdspladser
Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.

Kontrolmålet om organisering udstikker retningslinjer over for både medarbejdernes brug af mobilt udstyr og beskyttelse af forretningsinformation ved privat brug. Fjernarbejdspladser rummer en række både fysiske og fortrolighedsmæssige risici, som der bør foreligge klare politikker for. It-revisor reviderer på formaliserede aftaler med leverandører, forretningsbeskrivelser for udvikling og drift af it-systemet samt procedurer for eksempelvis adgang til mobilt udstyr hjemmefra. Der er særligt fokus på funktionsadskillelse mellem udvikling, test og drift af it-funktioner.

7. Medarbejdersikkerhed
7.1 Før ansættelsen
Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.

Kontrolmål 7.1 handler om at uddanne og indføre medarbejderne, så de kan tage ansvar for it-styringen i deres tildelte funktion. Det er vel at mærke et ledelses- og et HR-ansvar – både før, under og efter ansættelsen. Ved nye ansættelser bør der køres en passende screeningsproces af vedkommendes profil og fortid. Særligt hvis ansættelsen går ud på at udfylde en sikkerhedsrolle. I selve kontrakten bør organisationens informationssikkerhedspolitik indgå og fastslå en forpligtelse til at holde data fortrolige, intakte og (u)tilgængelige. Medarbejderne skal kende til deres juridiske ansvar og de risici, der er, når de betjener for eksempel it-software, mobilt udstyr og fysiske servere.

7.2 Under ansættelsen
Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.

Under ansættelsen kan et såkaldt it-bevidstgørelsesprogram på løbende basis indføre medarbejderne i de procedurer, der beskytter organisationens data. Basale kontroller som opdatering af passwords, malwareopdagelse og håndtering af personfølsomme printede dokumenter gennemgås, så risiko for fejl fra medarbejdernes side minimeres. Organisationen kan vælge at indføre sanktioner, hvis en medarbejder (eller leverandør) forårsager et it-sikkerhedsnedbrud.

7.3 Ansættelsesforholdets ophør eller ændring
Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.

Ved ansættelsens ophør skal det kommunikeres klart og tydeligt, hvilke forpligtelser der gælder. En medarbejder må eksempelvis ikke røbe forretningsstrategi eller udformning af CIS-kontroller eller applikationskontroller til beskyttelse mod angreb og datatab til udenforstående parter.

8. Styring af aktiver
8.1 Ansvar for aktiver
Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Alle informationsaktiver – dvs. aktiver, der indeholder data, samt selve dataen – skal beskyttes. Det kræver først og fremmest en klar fortegnelse over samtlige aktiver, som driftssystemer, fildrev, teknologi, servere, mailsystemer, økonomisystemer, informationer mm. i organisationen. Hvert aktiv bør have en ejer, som er ansvarlig for at sikre adgangsbegrænsninger og klassifikationer samt sikker bortskaffelse, når tid er.

It-revisor vil fokusere på, om der er klare regler for brug og styring af aktiver. Og selvfølgelig at reglerne efterleves i dagligdagen. Bliver udstyr tilbageleveret efter endt ansættelse? Er der en klar og præcis klassifikation af, hvad der er vigtige data eller følsom information? Er systemet gennemført i hele organisationen? En god klassifikation angiver værdien af et aktiv i forhold til organisationens generelle opretholdelse af CIA-principperne.

8.2 Klassifikation af information
Kontrolmål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.

Klassifikation og risikoanalyse hænger tæt sammen, fordi klassifikation handler om, hvor kritisk en potentiel offentliggørelse af fortrolig information vil være. Kritisk data bør markeres, så det er synligt for alle organisationens medarbejdere.

8.3 Mediehåndtering
Kontrolmål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

Flytbare mediedrev er særligt følsomme, hvoraf der skal være klare retningslinjer for, hvordan de krypteres, samt hvem der kan flytte dem og overføre information.

9. Adgangsstyring
9.1 Forretningsmæssige krav til adgangsstyring
Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter

Klare procedurer for adgangsstyring er centrale for at opretholde en god it-skik. Der skal være regler for både fysisk og logisk adgang og begrænsning af samme. Ikke alle medarbejdere bør eksempelvis have adgang til fildrev D med organisations bogførings- og salgsposteringer, ligesom ikke alle skal kunne tilgå ISMS-systemet eller medarbejderhistorik. Organisationens forretningsmæssige krav ligger til grund for adgangsstyringen, og dem skal alle (ansatte, leverandører og samarbejdspartnere) være bekendt med.

9.2 Administration af brugeradgang
Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.

Kontrolmålet om adgangsstyring skal sikre, at uvedkommende har begrænset eller ingen adgang til information og informationsbehandlingsfaciliteter. Derfor skal der være sikkerhedskrav til forretningsapplikationer og formel autorisation af brugeradgange til netværk og netværkstjenester. Generelt bør brugere ikke have adgang til informationssystemer, som de ikke betjener i forbindelse med deres arbejde.

9.3 Brugernes ansvar
Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.

Fornuftig adgangsstyring kræver en grundig proces for administration og godkendelse af brugere. Flere adgangsrettigheder kan med fordel samles i brugerprofiler, og nogle rettigheder kan (og bør) kun tildeles periodisk.

9.4 Styring af system- og applikationsadgang
Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.

Alle brugere skal behandle passwords fortroligt og vælge stærke kodeord. Der skal være en klar adskillelse mellem systemprogrammer og den applikationssoftware, som værner om dem. It-revisor vil undersøge, om der er en klar forretningsgang for autorisation af brugere til it-systemerne. Helt lavpraktisk kræver det gode kontroller som krav om komplekse passwords der bedre kan modstå for eksempel ordbogsangreb og en periodisk revurdering af adgangsrettigheder.

10. Kryptografi
10.1 Kryptografiske kontroller
Kontrolmål: At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og eller integritet.

Et andet ISO-kontrolmål omfatter udarbejdelsen af en kryptografipolitik med det formål at beskytte informationer bedst muligt. Det forudsætter klare krav til beskyttelsesniveauet og viden om aktuelle risici som virus, hackerangreb og sårbarheder ved transportering af mobilt udstyr. Administration af nøgler er en vigtig kontrol i denne sammenhæng. Kryptografi kan også imødekomme andre risici, som f.eks. utilsigtet brugeradgang.

It-revisor vil kigge ind i livscyklusforløbet for en kryptografinøgle og spørge, hvem der er ansvarlig for at iværksætte og destruere den. Aktivering ved modtagelse og indbyggede beskyttelsesmekanismer er et vigtigt fokusområde. Kryptografi er et af de mest anvendte kontrolområder i ISO 27001 og dermed også i it-revisors gennemgang. Dette skyldes, at det er en effektfuld generel it-kontrol, som bakker op om samtlige andre kontrolmål.

11. Fysisk sikring og miljøsikring
11.1 Sikre områder
Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Et vigtigt skridt i den rigtige retning mod god it-styring er at sikre, at kun udvalgte medarbejdere har adgang til for eksempel lager, serverrum og driftscenter. Ellers øges risikoen for beskadigelse og forstyrrelse af organisationens data og databehandling betydeligt. Konkrete tiltag er adgangskontroller til områder med en sikkerhedsprofil og UPS-sikring af kritisk udstyr. Kabler til el og kommunikation skal adskilles for at undgå interferens, ligesom kommunikationstjenester bør beskyttes mod potentiel aflytning fra tredjeparters side.

Fysisk perimetersikring kan opnås med forskellige midler, som f.eks. indbrudsalarmer eller afskærmning omkring en bygning eller et lokale. Indsatsen er selvsagt målrettet områder, hvor fortrolig information behandles og lagres, som maskinstuer eller datacentre. Hemmelig PIN-kode, tofaktoridentifikation og adgangskort er alle gode værktøjer til at sikre og dokumentere efterlevelsen af dette kontrolmål.

11.2 Udstyr
Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.

Miljømæssige trusler omfatter skade forårsaget af brand, oversvømmelse, eksplosion eller lignende menneske- og naturskabte trusler. For at sikre et trygt arbejdsmiljø kan organisationen rådføre sig med eksperter og investere i udstyr, der modvirker driftsafbrydelse, kompromittering eller tab. Software med licens og følsomme data skal fjernes eller overskrives for kassation eller salg. Derudover er det en god ide at indføre en såkaldt "ryddeligt skrivebord og blank skærm"-politik. Dvs. at alle papirer med forretningsinformationer låses inde i et skab, computeren er per default logget ud, og der er tilkoblet skærmlås eller tastaturlås.

12. Driftssikkerhed
12.1 Driftsprocedurer og ansvarsområder
Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsudstyr.

Målet her er simpelt: At sikre en korrekt og sikker drift af informationsbehandlingsfaciliteterne. Organisationen bør kunne fremvise klare og dokumenterede procedurer for driftsinstrukser til både installation og konfiguration af systemer, automatiserede og manuelle forretningsgange og håndtering af fejl eller usædvanligheder. Også her spiller funktionsadskillelse en central rolle i at skabe klare linjer for overgangen mellem udviklingsfase og implementeringsfase ved en given software.

Ændringsstyring (change management) er den nok mest centrale kontrol under driftssikkerhed. Kontrollen omfatter blandt andet en formel godkendelsesprocedure for foreslåede ændringer og registrering af samme. Al relevant personale skal informeres rettidigt om de nye systemændringer. Ændringsstyring er et område, hvor it-revisor benytter stikprøver for at teste godkendelse af ændringer i den it-understøttede drift har fungeret effektivt i revisionsperioden. Det kan være alt fra mailsystemer over login til bogføringssystemet til oprettelse af nye ordrer.

12.2 Beskyttelse mod malware

Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

En virksomhed bør have regler for ledelsesrapportering, når fejl opdages i driftssystemet. Desuden kan en række opdagende og forebyggende applikationskontroller installeres for at modvirke malware. Malware- og reparationssoftware skal løbende opdateres, og der tages backup af vigtig information med jævne mellemrum.

12.3 Backup

Kontrolmål: At beskytte mod tab af data.

Backup skal testes over revisionsperioden for at sikre, at der altid vil kunne reetableres data, hvis nødvendigt. Det er særligt vigtigt for den fortsatte drift, hvis der skulle ske nedbrud. Det er vigtigt, at der bliver fulgt op på, at backups køreres succesfuldt, samt at der følges op på fejl.

12.4 Logning og overvågning

Kontrolmål: At registrere hændelser og tilvejebringe bevis.

Kontrolmålet om driftssikkerhed er vigtigt, fordi mindre eller større forstyrrelser i driften kan være utrolig omkostningsfulde. Tabte arbejdstimer

og data koster dyrt – især for en it-tung virksomhed. Derfor reviderer it-revisor både på tekniske svagheder og manglende politikker, som hvis man ikke har en driftshåndbog eller en logning af driftsafviklingen. Klare forretningsgange for hasterettelser eller nødstilfælde hjælper virksomheden med at tackle tekniske sårbarheder hurtigt og effektivt.

12.5 Styring af driftssoftware
Kontrolmål: At sikre integriteten af driftssystemer

For at undgå for mange afbrydelser i driften grundet opdateringer er det vigtigt at fastlægge servicevinduer, hvor disse ikke forstyrrer den daglige drift. Procedure for styringen heraf skal derfor udarbejdes og implementeres.

12.6 Sårbarhedsstyring
Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.

Virksomheden skal løbende holde sig informeret om mulige sårbarheder i systemerne. Det sker ofte via benyttelse af en tredjepart, der har særlig viden inden for sårbarhedsscanninger og penetrationstests. Udarbejdes disse rapporter, er det op til virksomheden at reagere og tilpasse efter disse resultater. Alt sammen i tråd med en risikovurdering.

12.7 Overvejelser i forbindelse med audit af informationssystemer
Kontrolmål: At minimere virkningen af auditaktiviteter på driftssystemer.

Dette kontrolmål ser vi oftest taget ud af erklæringen. Kontrolmålet fokuserer på den risiko, der er, hvis revisor eller andre auditører får adgang til og kan påvirke driften direkte. Ser virksomheden dog en risiko her, skal det dokumenteres og håndteres.

13. Kommunikationssikkerhed
13.1 Styring af netværkssikkerhed
Kontrolmål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Netværkssikkerhed har til formål at beskytte alle informationer, der florerer på virksomhedens netværk – online som offline. Det er bedst at adskille den driftsansvarlige fra selve computerdriften, så den teknisk ansvarlige får lov at fokusere på foranstaltninger som begrænsning af

systemforbindelser og autentifikation, kryptering og net-tilslutningskontroller.

I nye som gamle netværkstjenester bør indgå en baseline for sikkerhedsmekanismer og styringskrav, og overholdelsen af disse skal løbende efterses af it-ansvarlige. Netværkstjenester omfatter alt fra servicenet til firewalls og IDS-systemer. En god måde at beskytte data på er at opdele store netværk i separate domæner beskyttet af gateways, som kan tilgås af afdelinger som HR, økonomi og jura. Alle identificerede forbedringsmuligheder bør registreres og lægges ind i en serviceforbedringsplan.

13.2 Informationsoverførsel
Kontrolmål: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

It-revisor er særligt opmærksom på politikker og procedurer for informationsoverførsel. Sensitivt data skal beskyttes mod afkodning, kopiering, ændring og flytning, når det kommunikeres elektronisk. I forbindelse med revision vil virksomheden skulle fremvise dokumentation på, at der er klare aftaler for informationsoverførsel og informationsbrug samt aftalte ansvarsforhold ifm. datatab.

14. Anskaffelse, udvikling og vedligeholdelse af systemer
14.1 Sikkerhedskrav til informationssystemer
Kontrolmål: At sikre, at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.

Kontrollerne under dette kontrolmål sikrer, at informationssikkerhed integreres i informationssystemerne gennem hele livscyklussen. Informationssikkerhed skabes via flere indsatser som politiker og forskrifter, brug af sårbarhedstærskler og gode dokumenterede kontroller og afstemninger i selve systemet. I forbindelse med forretningsprocesser kan blandt andet transaktionslogning og -overvågning og uafviselighedskrav benyttes.

Særligt fokus er på applikationstjenester som Wi-Fi eller cloudløsninger, der kører via offentlige netværk. Fortrolig omgang med data på dem kræver godkendelsesprocedurer og et klart konfidensniveau, når en medarbejder kommunikerer med andre online. I forbindelse med udbuds- og kontraktprocesser skal nøgledokumenters integritet og tilgængelighed beskyttes. Det samme gælder alle anvendte handelsapplikationer- og tjenester.

14.2 Sikkerhed i udviklings- og hjælpeprocesser
Kontrolmål: At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.

Den reviderede virksomhed skal gerne kunne fremvise dokumentation for en sikker udviklingspolitik – både på papiret og i praksis. Denne omfatter metoder til softwareudvikling som koderetningslinjer for programmeringssprog, sikkerhedskrav i designfasen, sikre arkiver mm. Både det tidlige udformningsstadie og senere videreudvikling skal følge formelle procedurer for ændringsstyring, som kan kombineres med driften (kontrolområde 12).

Et sikkert udviklingsmiljø tager hensyn til følsomme data. Hvis systemudviklingen outsources, skal virksomheden være opmærksom på: Licensejerskab, kodeejerskab og immaterielle rettigheder, kontrakrav til udførsel, godkendelsestest af kvaliteten og bevis på overholdte sikkerhedstærskler anvendt til at sikre acceptable minimumsniveauer for privatlivssikring. Grundlæggende skal organisationen gøre alt for at sikre, at leverandører lever op til alt det ovenstående.

14.3 Testdata
Kontrolmål: At sikre beskyttelse af data, som anvendes til test.

Ved brug af testdata skal der foreligge en procedure for, hvordan testdata udvælges og generes. Herunder at det bliver beskyttet på tilstrækkelig vis, samt at det bliver styret tilstrækkeligt, jf. proceduren.

15. Leverandørforhold
15.1 Informationssikkerhed i leverandørforhold
Kontrolmål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Når en organisations serviceleverandører har adgang til aktiver, er der en de facto-risiko for kompromittering af fortrolighed, integritet og tilgængelighed. Derfor er det specielt vigtigt at beskytte adgang til aktiverne med informationssikkerhedskontroller. Serviceleverandører spænder bredt, lige fra it-ydelser over logistikinstallationer til finansielle tjenester som økonomisystemer.

Al adgang bør overvåges og styres nøje, ligesom der skal stilles krav om, at leverandører beskytter organisationens informationer. Informationssikkerhedskravene skal formaliseres med leverandøren i form af

kontrakt, samarbejdsaftale eller lignende. Betingelserne bør omfatte en beskrivelse og klassifikation af den tilgængelige information, at begge parter implementerer kontroller for overvågning, rapportering og audit samt en liste over medarbejdere med adgang og klare arbejdsgange i tilfælde af sikkerhedsnedbrud.

15.2 Styring af leverandørydelser
Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

Bemærk, at leverandørs overholdelse tit er essentiel for at efterleve lov og myndighedskrav. Det gælder især i forsyningskæden for IKT-tjenester (informations- og kommunikationsteknologi). Derfor bør virksomheden iværksætte ekstra sikkerhedsforanstaltninger for at validere de leverede IKT-produkter. Ansvaret for at håndtere forholdet med serviceleverandør bør uddelegeres til enten en udvalgt kontrolansvarlig eller et helt servicelederteam.

16. Styring af informationssikkerhedsnedbrud
16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Formålet er at sikre en ensartet og effektiv styring i tilfælde af informationssikkerhedsnedbrud og -hændelser. Det kræver ledelsesansvar og planlægning om, hvordan sikkerhedshændelser- og svagheder kommunikeres. Generelt bør organisationen have klare procedurer for registrering, klassifikation, opdatering, eskalering, løsning og lukning af problemer, som kan opstå, jf. risikoprofilen.

Problemerne skal altid håndteres på koordineret vis af de mest kompetente medarbejdere, som kan være med til at reducere konsekvensen af informationssikkerhedsbruddet. Konkrete metoder omfatter rapporteringsskemaer, passende kontakt med myndigheder, serviceleverandører og interessenter, notering af samtlige detaljer, kommunikation med kontaktpunkt mm.

Informationssikkerhedsnedbrud skal forstås bredt som ineffektiv sikkerhedsstyring eller menneskelige fejl i den mildere ende og brud på adgangskontroller eller overtrædelse af politikker og retningslinjer i den mere alvorlige ende. Klare arbejdsgange kan forebygge hændelser,

men det kræver en konstant opdatering af den problem-management ansvarlige og en videregivelse af ændringer til den change-management ansvarlige. Et informationssikkerhedsnedbrud bør altid evalueres, hvoraf det er oplagt for it-revisor at undersøge, om der i kølvandet på et nedbrud eller en hændelse er blevet forbedret eller iværksat nye generelle it-kontroller eller applikationskontroller.

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

17.1 Informationssikkerhedskontinuitet

Kontrolmål: Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Selv i krise- eller katastrofesituationer skal organisationen sørge for informationssikkerhedskontinuitet. Det kræver, at en it-beredskabsplan integreres i enten nød-, beredskabs- og reetableringssyringen eller krisehåndteringen. I fravær af disse må ledelsen antage, at informationssikkerhedskravene er de samme som under normale driftsforhold. Organisationen bør fordele ledelsesansvar i krisesituationer og have uddannet beredskabspersonale, som er bemyndiget og kompetent til at varetage informationssikkerhed i force majeuretilfælde.

It-revisor kan ved gennemgang efterspørge en plan for retablering baseret på forudgående sårbarhedsanalyse og væsentlighed for de enkelte delsystemer. Eller varslingslister og en etableret kontaktliste til eksterne serviceleverandører af hardware, software og telekommunikation. Organisationen kan med fordel anvende kompenserende kontroller for de generelle it-kontroller, som ikke kan opretholdes ved eksempelvis et strømnedbrud, beskadigelse eller anden manglende funktion af normalt driftssoftware.

17.2 Redundans

Kontrolmål: At sikre tilgængeligheden af informationsbehandlingsfaciliteter.

For at virksomheden kan efterleve de gældende tilgængelighedskrav og risici, er det vigtigt at der er etableret tilstrækkeligt redundans i informationsbehandlingsfaciliteter.

18. Overensstemmelse
18.1 Overensstemmelse med lov- og kontraktkrav
Kontrolmål: At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav.

Helt basalt kræver dette kontrolmål en bevidsthed om gældende regler, som skal overholdes i informationssikkerhedssystemerne og brugen af dem. Ansvaret ligger på ledelsesniveau og ikke hos dem, der eksekverer i den daglige it-drift. Kontrolmålet er ofte ikke med i erklæringerne, da revisor i disse kontroller hurtigt vil stå på mål for en lang række forskellige lovgivninger. Det er svært at indhente tilstrækkeligt revisionsbevis på lige netop det, hvorfor området oftest udgår.

18.2 Gennemgang af informationssikkerhed
Kontrolmål: At sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.

Passende procedurer bør sikre overensstemmelse med regler i relation til immaterielle rettigheder (opfindelsesret), som gælder juridisk ved brug af bestemt software og informationsprodukter. Det tilladte antal af licensbrugere må selvsagt aldrig overskrides, ligesom tjenester ikke kan deles uden for organisationen. Registreringer inden for regnskab, data, transaktion eller lignende skal opbevares og beskyttes mod tab, ødelæggelse, forfalskning eller anden form for utilsigtet manipulation. Det kræver backupprocedurer for både fysiske lagringsmedier som papir eller mikrofiche samt elektroniske lagringsmedier, som skal sikres mod tab af data ved teknologiske ændringer.

Vigtigt er, at samtlige organisationens kontrolmål, kontroller, procedurer og politikker gennemgås for potentielle forbedringer uafhængigt og med jævne mellemrum for at sikre både efterlevelse og optimering af den samlede it-styring.

5.8. Tidsramme og interaktion med kunden

I dette afsnit gennemgår vi kort den indledende vurdering af revisionsbehov og møde samt interaktion med kunden. Kunden er i denne sammenhæng den reviderede organisation og ikke finansiel revisor, selvom sidstnævnte ret beset er kunden i den regnskabsunderstøttende it-revision. I dette afsnit vil vi ydermere berøre tidsrammen for udførelse af it-revisionen.