AARHUS UNIVERSITET

Gap-analyse

ST - ISO27001 Modenhed

Analyse af	ISO 27001:2013 Anneks A
Navn	ST - ISO27001 Modenhed
Ansvarlig	ST - AGRO / Erik Steen Kristensen
Udførende	Siscon
Ændret	02.05.2017
Ikke behandlet	0 af 114

Yderligere information og symbolforklaring findes på sidste side(r)

ISO 27001:2013 ANNEKS A

5. INFORMATIONSSIKKERHEDSPOLITIKKER

5. 1. RETNINGSLINJER FOR STYRING AF INFORMATIONSSIKKERHED

5. 1. 1. Politikker for informationssikkerhed ! (80%) → ! (60%)

Ledelsen skal fastlægge og godkende et sæt politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.

5. 1. 2. Gennemgang af politikker for informationssikkerhed ! (80%) → ! (60%)

Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.

6. ORGANISERING AF INFORMATIONSSIKKERHED

6. 1. INTERN ORGANISERING

6. 1. 1. Roller og ansvarsområder for informationssikkerhed ! (60%) → ! (60%)

Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.

6. 1. 2. Funktionsadskillelse ! (80%) → ! (60%)

Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.

6. 1. 3. Kontakt med myndigheder ! (80%) → ! (60%)

Der skal opretholdes passende kontakt med relevante myndigheder.

6. 1. 4. Kontakt med særlige interessegrupper ! (60%) → ! (60%)

Der skal opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.

6. 1. 5. Informationssikkerhed ved projektstyring ! (60%) → ! (60%)

Informationssikkerhed skal anvendes ved projektstyring, uanset projekttype.

6. 2. MOBILT UDSTYR OG FJERNARBEJDSPLADSER

6. 2. 1. Politik for mobilt udstyr ! (60%) → ! (60%)

Der skal vedtages en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.

6. 2. 2. Fjernarbejdspladser ! (60%) → ! (60%)

Der skal implementeres en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.

7. PERSONALESIKKERHED

7. 1. FØR ANSÆTTELSEN

7. 1. 1. Screening ! (60%) → ! (60%)

Efterprøvning af alle jobkandidaters baggrund skal udføres i overensstemmelse med relevante love, forskrifter og etiske regler og skal stå i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.

7. 1. 2. Ansættelsesvilkår og -betingelser ! (40%) → ! (60%)

Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informationssikkerhed.

7. 2. UNDER ANSÆTTELSEN

7. 2. 1. Ledelsesansvar ! (60%) → ! (60%)

Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.

7. 2. 2. Bevidsthed om, uddannelse og træning i informationssikkerhed ! (40%) → ! (60%)

Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter skal ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, i det omfang det er relevant for deres jobfunktion.

7. 2. 3. Sanktioner ! (60%) → ! (60%)

Der skal være etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.

7. 3. ANSÆTTELSESFORHOLDETS OPHØR ELLER ÆNDRING

7. 3. 1. Ansættelsesforholdets ophør eller ændring ! (60%) → ! (60%)

Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, skal defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.

8. STYRING AF AKTIVER

8. 1. ANSVAR FOR AKTIVER

8. 1. 1. Fortegnelse over aktiver ! (80%) → ! (60%)

Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.

8. 1. 2. Ejerskab af aktiver ! (60%) → ! (60%)

Der skal udpeges en ejer i organisationen for hvert aktiv.

8. 1. 3. Accepteret brug af aktiver ! (60%) → ! (60%)

Regler for accepteret brug af information og aktiver i relation til information- og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og implementeres.

8. 1. 4. Tilbagelevering af aktiver ! (60%) → ! (60%)

Alle medarbejdere og eksterne brugere skal aflevere alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.

8. 2. KLASSIFIKATION AF INFORMATION

8. 2. 1. Klassifikation af information ! (20%) → ! (60%)

Information skal klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.

8. 2. 2. Mærkning af information ! (20%) → ! (60%)

Der skal udarbejdes og implementeres et passende sæt af procedurer til mærkning af information i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.

8. 2. 3. Håndtering af aktiver ! (20%) → ! (60%)

Der skal udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.

8. 3. MEDIEHÅNDTERING

8. 3. 1. Styring af bærbare medier ! (40%) → ! (60%)

Der skal implementeres procedurer til styring af bærbare medier i overensstemmelse med det klassifikationssystem, som organisationen har vedtaget.

8. 3. 2. Bortskaffelse af medier ! (60%) → ! (60%)

Medier skal bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.

8. 3. 3. Fysiske medier under transport ! (40%) → ! (60%)

Medier, der indeholder information, skal beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport.

9. ADGANGSSTYRING

9. 1. FORRETNINGSMÆSSIGE KRAV TIL ADGANGSSTYRING

9. 1. 1. Politik for adgangsstyring ! (60%) → ! (60%)

En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.

9. 1. 2. Adgang til netværk og netværkstjenester ! (60%) → ! (60%)

Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.

9. 2. ADMINISTRATION AF BRUGERADGANG

9. 2. 1. Brugerregistrering og -afmelding ! (60%) → ! (60%)

Der skal implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder.

9. 2. 2. Tildeling af brugeradgang ! (80%) → ! (60%)

Der skal implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.

9. 2. 3. Styring af privilegerede adgangsrettigheder ! (80%) → ! (60%)

Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.

9. 2. 4. Styring af hemmelig autentifikationsinformation om brugere ! (80%) → ! (60%)

Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp afen formel administrationsproces.

9. 2. 5. Gennemgang af brugeradgangsrettigheder ! (40%) → ! (60%)

Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.

9. 2. 6. Inddragelse eller justering af adgangsrettigheder ! (80%) → ! (60%)

Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller skal tilpasses efter en ændring.

9. 3. BRUGERNES ANSVAR

9. 3. 1. Brug af hemmelig autentifikationsinformation ! (60%) → ! (60%)

Det skal være et krav, at brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.

9. 4. STYRING AF SYSTEM- OG APPLIKATIONSADGANG

9. 4. 1. Begrænset adgang til informationer ! (60%) → ! (60%)

Adgang til information og applikationssystemers funktioner skal begrænses i overensstemmelse med politikken for adgangsstyring.

9. 4. 2. Procedurer for sikker log-on ! (60%) → ! (60%)

Hvis det kræves i henhold til politikken for adgangsstyring, skal adgang til systemer og applikationer styres af en procedure for sikker log-on.

9. 4. 3. System for administration af adgangskoder ! (60%) → ! (60%)

Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder med god kvalitet.

9. 4. 4. Brug af privilegerede systemprogrammer ! (40%) → ! (60%)

Brugen af systemprogrammer, der kan omgå system- og applikationskontroller, skal begrænses og styres effektivt.

9. 4. 5. Styring af adgang til kildekoder til programmer ! (20%) → ! (60%)

Adgang til kildekoder til programmer skal begrænses.

10. KRYPTOGRAFI

10. 1. KRYPTOGRAFISKE KONTROLLER

10. 1. 1. Politik for anvendelse af kryptografi ○ → ! (60%)

Der skal udarbejdes og implementeres en politik for anvendelse af kryptografi til beskyttelse af information.

10. 1. 2. Administration af nøgler ○ → ! (60%)

Der skal udarbejdes og implementeres en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.

11. FYSISK SIKRING OG MILJØSIKRING

11. 1. SIKRE OMRÅDER

11. 1. 1. Fysisk perimetersikring ! (60%) → ! (60%)

Der skal defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.

11. 1. 2. Fysisk adgangskontrol ! (80%) → ! (60%)

Sikre områder skal være beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.

11. 1. 3. Sikring af kontorer, lokaler og faciliteter ! (60%) → ! (60%)

Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og etableres.

11. 1. 4. Beskyttelse mod eksterne og miljømæssige trusler ! (80%) → ! (60%)

Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker skal tilrettelægges og etableres.

11. 1. 5. Arbejde i sikre områder ! (40%) → ! (60%)

Procedurer for arbejde i sikre områder skal tilrettelægges og etableres.

Kommentarer

Justeret ned fra 3 til 2. Man stoler på bygningsservice, men stiller ikke selv krav til dem.

11. 1. 6. Områder til af- og pålæsning ! (40%) → ! (60%)

Adgangssteder som fx områder til af- og pålæsning og andre steder, hvor uautoriserede personer kan komme ind på området, skal styres og så vidt muligt adskilles fra informationsbehandlingsfaciliteter for at undgå uautoriseret adgang.

11. 2. UDSTYR

11. 2. 1. Placering og beskyttelse af udstyr ! (20%) → ! (60%)

Udstyr skal placeres og beskyttes, således at risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes.

11. 2. 2. Understøttende forsyninger (forsyningssikkerhed) ! (20%) → ! (60%)

Udstyr skal beskyttes mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger.

11. 2. 3. Sikring af kabler ○ → ! (60%)

Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, skal beskyttes mod indgreb, interferens og skader.

11. 2. 4. Vedligeholdelse af udstyr ! (60%) → ! (60%)

Udstyr skal vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet.

11. 2. 5. Fjernelse af aktiver ! (40%) → ! (60%)

Udstyr, information og software må ikke fjernes fra organisationen uden forudgående tilladelse.

11. 2. 6. Sikring af udstyr og aktiver uden for organisationen ! (40%) → ! (60%)

Der skal etableres sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen.

11. 2. 7. Sikker bortskaffelse eller genbrug af udstyr ! (60%) → ! (60%)

Alt udstyr med lagringsmedier skal verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.

Kommentarer

Har ikke styr på mindre ting som fx små eksterne diske, eller USB nøgler

11. 2. 8. Brugerudstyr uden opsyn ! (40%) → ! (60%)

Brugere skal sikre, at udstyr, som er uden opsyn, er passende beskyttet.

11. 2. 9. Politik for ryddeligt skrivebord og blank skærm ! (20%) → ! (60%)

Der skal udarbejdes en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.

12. DRIFTSSIKKERHED

12. 1. DRIFTSPROCEDURER OG ANSVARSOMRÅDER

12. 1. 1. Dokumenterede driftsprocedurer ! (60%) → ! (60%)

Driftsprocedurer skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem.

12. 1. 2. Ændringsstyring ! (40%) → ! (60%)

Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, skal styres.

12. 1. 3. Kapacitetsstyring ! (40%) → ! (60%)

Anvendelsen af ressourcer skal overvåges og tilpasses, og der skal foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.

Kommentarer

Scorer mellem 1-3, afhængig af hvad der er fokus på.

12. 1. 4. Adskillelse af udviklings-, test- og driftsmiljøer ! (60%) → ! (60%)

Udviklings-, test- og driftsmiljøer skal adskilles for at nedsætte risikoen for uautoriseret adgang til eller ændringer af driftsmiljøet.

12. 2. BESKYTTELSE MOD MALWARE

12. 2. 1. Kontroller mod malware ! (60%) → ! (60%)

Der skal implementeres kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.

12. 3. BACKUP

12. 3. 1. Backup af information ! (60%) → ! (60%)

Der skal tages backupkopier af information, software og systembilleder, og disse skal testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.

12. 4. LOGNING OG OVERVÅGNING

12. 4. 1. Hændelseslogning ! (40%) → ! (60%)

Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser skal udføres, opbevares og gennemgås regelmæssigt.

12. 4. 2. Beskyttelse af log-oplysninger ! (20%) → ! (60%)

Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang.

12. 4. 3. Administrator- og operatørlog ! (20%) → ! (60%)

Aktiviteter udført af systemadministrator og systemoperatør skal logges, og loggen skal beskyttes og gennemgås regelmæssigt.

12. 4. 4. Tidssynkronisering ! (60%) → ! (60%)

Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne skal være synkroniseret til en enkelt referencetidskilde.

Kommentarer

Det er vigtigt i forhold til forsøg - så det ligger mellem 3 og 4.

12. 5. STYRING AF DRIFTSSOFTWARE

12. 5. 1. Softwareinstallation på driftssystemer ! (60%) → ! (60%)

Der skal implementeres procedurer til styring af softwareinstallationen på driftssystemer.

12. 6. SÅRBARHEDSSTYRING

12. 6. 1. Styring af tekniske sårbarheder ! (40%) → ! (60%)

Der skal løbende indhentes informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.

12. 6. 2. Begrænsninger på softwareinstallation ! (60%) → ! (60%)

Der skal fastlægges og implementeres regler om softwareinstallation, som foretages af brugerne.

12. 7. OVERVEJELSER I FORBINDELSE MED AUDIT AF INFORMATIONSSYSTEMER

12. 7. 1. Kontroller i forbindelse med audit af informationssystemer ! (20%) → ! (60%)

Auditkrav og -aktiviteter, der indebærer verifikation af driftssystemer, skal planlægges og aftales omhyggeligt for at minimere afbrydelser af forretningsprocesserne.

Kommentarer

Håndteres i praksis fra gang til gang - derfor altid Ad-hoc.

13. KOMMUNIKATIONSSIKKERHED

13. 1. STYRING AF NETVÆRKSSIKKERHED

13. 1. 1. Netværksstyring ○ → ! (60%)

Netværk skal styres og kontrolleres for at beskytte informationer i systemer og applikationer.

13. 1. 2. Sikring af netværkstjenester ○ → ! (60%)

Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester skal identificeres og indgå i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede.

13. 1. 3. Opdeling af netværk ○ → ! (60%)

Grupper af informationstjenester, brugere og informationssystemer skal opdeles i netværk.

13. 2. INFORMATIONSOVERFØRSEL

13. 2. 1. Politikker og procedurer for informationsoverførsel ! (40%) → ! (60%)

Der skal foreligge formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr.

13. 2. 2. Aftaler om informationsoverførsel ! (60%) → ! (60%)

Aftaler skal omhandle sikker overførsel af forretningsinformation mellem organisationen og eksterne parter.

13. 2. 3. Elektroniske meddelelser ! (40%) → ! (60%)

Informationer i elektroniske meddelelser skal beskyttes på passende måde.

13. 2. 4. Fortroligheds- og hemmeligholdelsesaftaler ! (60%) → ! (60%)

Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, skal identificeres, gennemgås regelmæssigt og dokumenteres.

14. ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE AF SYSTEMER

14. 1. SIKKERHEDSKRAV TIL INFORMATIONSSYSTEMER

14. 1. 1. Analyse og specifikation af informationssikkerhedskrav ! (20%) → ! (60%)

Informationssikkerhedsrelaterede krav skal være omfattet af kravene til nye informationssystemer eller forbedringer af eksisterende informationssystemer.

14. 1. 2. Sikring af applikationstjenester på offentlige netværk ! (20%) → ! (60%)

Informationer i forbindelse med applikationstjenester over offentlige netværk skal beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring.

Kommentarer

Justeret ned i forhold til det i svarede.
Snakken bar præg af, at der ikke var enighed omkring det - og dermed er vi på en score omkring 1.

14. 1. 3. Beskyttelse af handelsapplikationer og -tjenester ○ → ! (60%)

Informationer i forbindelse med handelsapplikationer og -tjenester skal beskyttes for at forhindre ufuldstændig transmission, fejlforsendelser, uautoriseret ændring af meddelelser, uautoriseret offentliggørelse, uautoriseret kopiering eller retransmission af meddelelser.

14. 2. SIKKERHED I UDVIKLINGS- OG HJÆLPEPROCESSER

14. 2. 1. Sikker udviklingspolitik ! (20%) → ! (60%)

Der skal fastlægges og anvendes regler for udvikling af software og systemer i organisationen.

14. 2. 2. Procedurer for styring af systemændringer ! (20%) → ! (60%)

Ændringer af systemer inden for udviklingslivscyklussen skal styres ved hjælp af formelle procedurer for ændringsstyring.

14. 2. 3. Teknisk gennemgang af applikationer efter ændringer af driftsplatforme ! (40%) → ! (60%)

Ved ændring af driftsplatforme skal forretningskritiske applikationer gennemgås og testes for at sikre, at ændringen ikke indvirker negativt på organisationens drift eller sikkerhed.

14. 2. 4. Begrænsning af ændringer af softwarepakker ! (20%) → ! (60%)

Ændringer af softwarepakker skal vanskeliggøres, begrænses til nødvendige ændringer, og alle ændringer skal styres effektivt.

14. 2. 5. Principper for udvikling af sikre systemer ○ → ! (60%)

Principper for udvikling af sikre systemer skal fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med alle implementeringer af informationssystemer.

14. 2. 6. Sikkert udviklingsmiljø ○ → ! (60%)

Organisationer skal etablere sikre udviklingsmiljøer for systemudvikling og -integration, som dækker hele systemudviklingens livscyklus.

14. 2. 7. Outsourcet udvikling ○ → ! (60%)

Organisationen skal føre tilsyn med og overvåge systemudviklingsaktiviteter, der er outsourcet.

14. 2. 8. Systemsikkerhedstest ! (20%) → ! (60%)

Test af sikkerhedsfunktionalitet skal udføres ved udvikling.

14. 2. 9. Systemgodkendelsestest ! (20%) → ! (60%)

Der skal etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.

14. 3. TESTDATA

14. 3. 1. Sikring af testdata ○ → ! (60%)

Testdata skal udvælges omhyggeligt og skal beskyttes og styres.

15. LEVERANDØRFORHOLD

15. 1. INFORMATIONSSIKKERHED I LEVERANDØRFORHOLD

15. 1. 1. Informationssikkerhedspolitik for leverandørforhold ! (40%) → ! (60%)

Informationssikkerhedskravene til at minimere risiciene forbundet med leverandørers adgang til organisationens aktiver skal aftales med leverandøren og skal dokumenteres.

15. 1. 2. Håndtering af sikkerhed i leverandøraftaler ! (40%) → ! (60%)

Alle relevante informationssikkerhedskrav skal fastlægges og aftales med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens information.

Kommentarer

Er justeret lidt ned.

De fleste bruger eksterne leverandører - fx Google, DropBox e.lign.

Disse leverandører er også omfattet, og sjældent så godt styret.

15. 1. 3. Forsyningskæde for informations- og kommunikationsteknologi (IKT) ! (20%) → ! (60%)

Aftaler med leverandører skal indeholde krav til håndtering af informationssikkerhedsrisici forbundet med forsyningskæden for informations- og kommunikationsteknologi tjenester og -produkter.

15. 2. STYRING AF LEVERANDØRYDELSER

15. 2. 1. Overvågning og gennemgang af leverandørydelser ! (40%) → ! (60%)

Organisationer skal regelmæssigt overvåge, gennemgå og auditere leverandørydelser.

15. 2. 2. Styring af ændringer af leverandørydelser ! (40%) → ! (60%)

Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, -procedurer og -kontroller, skal styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, -systemer og -processer er, og til en revurdering af risici.

16. STYRING AF INFORMATIONSSIKKERHEDSBRUD

16. 1. STYRING AF INFORMATIONSSIKKERHEDSBRUD OG FORBEDRINGER

16. 1. 1. Ansvar og procedurer ! (60%) → ! (60%)

Ledelsesansvar og procedurer skal fastlægges for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.

16. 1. 2. Rapportering af informationssikkerhedshændelser ! (60%) → ! (60%)

Informationssikkerhedshændelser skal rapporteres ad passende ledelseskanaler så hurtigt som muligt.

16. 1. 3. Rapportering af informationssikkerhedssvagheder ! (60%) → ! (60%)

Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester har pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i informationssystemer og -tjenester.

16. 1. 4. Vurdering af og beslutning om informationssikkerhedshændelser ! (60%) → ! (60%)

Informationssikkerhedshændelser skal vurderes, og det skal besluttes, om de skal klassificeres som informationssikkerhedsbrud.

16. 1. 5. Håndtering af informationssikkerhedsbrud ! (40%) → ! (60%)

Informationssikkerhedsbrud skal håndteres i overensstemmelse med de dokumenterede procedurer.

16. 1. 6. Erfaring fra informationssikkerhedsbrud ! (60%) → ! (60%)

Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, skal anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.

16. 1. 7. Indsamling af beviser ! (20%) → ! (60%)

Organisationen skal definere og anvende procedurer til identifikation, indsamling, anskaffelse og opbevaring af informationer, som kan tjene som bevis.

17. INFORMATIONSSIKKERHEDSASPEKTER VED NØD-, BEREDSKABS- OG REETABLERINGSSTYRING

17. 1. INFORMATIONSSIKKERHEDSKONTINUITET

17. 1. 1. Planlægning af informationssikkerhedskontinuitet ! (20%) → ! (60%)

Organisationen skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.

17. 1. 2. Implementering af informationssikkerhedskontinuitet ! (20%) → ! (60%)

Organisationen skal fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.

17. 1. 3. Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten ! (20%) → ! (60%)

Organisationen skal verificere de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.

17. 2. REDUNDANS

17. 2. 1. Tilgængelighed af informationsbehandlingsfaciliteter ! (40%) → ! (60%)

Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.

18. OVERENSSTEMMELSE

18. 1. OVERENSSTEMMELSE MED LOV- OG KONTRAKTKRAV

18. 1. 1. Identifikation af gældende lovgivning og kontraktkrav ! (60%) → ! (60%)

Alle relevante lov-, myndigheds- og kontraktkrav samt organisationens metode til overholdelse af disse krav skal være klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen.

18. 1. 2. Immaterielle rettigheder ! (60%) → ! (60%)

Der skal implementeres passende procedurer til at sikre, at der er overensstemmelse med lov-, myndigheds- og kontraktkrav i relation til immaterielle rettigheder og anvendelse af beskyttede softwareprodukter.

18. 1. 3. Beskyttelse af registreringer ! (20%) → ! (60%)

Registreringer skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse i overensstemmelse med lov-, myndigheds- og kontraktkrav samt forretningsmæssige krav.

18. 1. 4. Privatlivets fred og beskyttelse af personoplysninger ! (60%) → ! (60%)

Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter.

18. 1. 5. Regulering af kryptografi ! (20%) → ! (60%)

Kryptografi skal anvendes i overensstemmelse med alle relevante aftaler, love og forskrifter.

18. 2. GENNEMGANG AF INFORMATIONSSIKKERHED

18. 2. 1. Uafhængig gennemgang af informationssikkerhed ! (20%) → ! (60%)

Organisationens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) skal

gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.

18. 2. 2. Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

! (20%) → ! (60%)

Lederne skal regelmæssigt undersøge, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.

18. 2. 3. Undersøgelse af teknisk overensstemmelse

! (40%) → ! (60%)

Informationssystemer skal undersøges regelmæssigt for, om de er i overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder.

INFO

? Ikke behandlet
✖ Nej
! Delvis
✔ Ja
○ Irrelevant