ISO Checklist

Gap Analyses

ISO 27001

Bedrijfsnaam

Geschreven door: Naam

Online ISO

Voldoen we aan?	J/N
4.0 Context van de organisatie	
4.1 Inzicht verkrijgen in de organisatie en haar context	
1. Heeft u het doel (de doelen) van het ISMS bepaald?	
2. Heeft u de interne en externe problemen bepaald die relevant zijn voor het doel van het ISMS?	
3. Heeft u bepaald hoe interne en externe problemen het vermogen van het ISMS kunnen beïnvloeden om de beoogde resultaten te bereiken?	
4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden	
4. Heeft u belanghebbende partijen bepaald?	
5. Bestaat de lijst met de vereisten van alle belanghebbende partijen?	
6. Is de scope gedocumenteerd met duidelijk gedefinieerde grenzen en toepasbaarheid?	
4.4 Managementsysteem voor informatiebeveiliging	
7. Heeft u een informatiebeveiligingsbeheersysteem opgezet, gedocumenteerd, geïmplementeerd, onderhouden en voortdurend verbeterd volgens ISO 27001-vereisten?	
5.0 Leiderschap	
5.1 Leiderschap en betrokkenheid	
8. Zijn de algemene ISMS-doelstellingen compatibel met de strategische richting?	
9. Zorgt het management ervoor dat de benodigde ISMS-bronnen indien nodig beschikbaar zijn?	
10. Zorgt het management ervoor dat ISMS de beoogde resultaten behaalt?	
5.2 Beleid	
11. Bestaat er een informatiebeveiligingsbeleid met opgenomen doelstellingen of een kader voor het stellen van doelstellingen?	
12. Is het informatiebeveiligingsbeleid gedocumenteerd en gecommuniceerd binnen het bedrijf en aan andere belanghebbenden partijen?	
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	
13. Zijn rollen, verantwoordelijkheden en autoriteiten voor informatiebeveiliging toegewezen en gecommuniceerd?	
6.0 PLANNING	
6.1 Maatregelen om risico's te beperken en kansen te benutten	
14. Are internal and external issues, as well as interested parties' requirements, considered while addressing risks and opportunities?	
6.1.2 Risicobeoordeling van informatiebeveiliging	
15. Is er een gedocumenteerd proces om informatiebeveiligingsrisico's te identificeren, inclusief de risicoacceptatiecriteria en criteria voor risicobeoordeling?	
6.1.3 Behandeling van informatiebeveiligingsrisico's	
16. Is het risicobehandelingsproces gedocumenteerd, inclusief de opties voor risicobehandeling en hoe u een toepasselijkheidsverklaring kunt opstellen?	
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken	
17. Zijn informatiebeveiligingsdoelstellingen vastgesteld bij relevante functies van de organisatie, gemeten waar praktisch en consistent met het informatiebeveiligingsbeleid?	

Voldoen we aan?	J/N
18. Bestaat er een plan of een groep plannen om de informatiebeveiligingsdoelstellingen te bereiken, inclusief de aangewezen verantwoordelijkheid, de evaluatiemethode en de middelen en het tijdschema voor het plan (de plannen)?	
7.0 Ondersteuning	
7.1 Middelen	
19. Zijn er voldoende middelen voorzien voor alle elementen van het ISMS?	
7.2 Competentie	
20. Wordt passende competentie beoordeeld en waar nodig opleiding gegeven aan personeel dat taken uitvoert die de informatiebeveiliging kunnen beïnvloeden? Worden er competentiegegevens bijgehouden?	
7.3 Bewustzijn	
21. Is het personeel op de hoogte van het informatiebeveiligingsbeleid, hun rol en de gevolgen van het niet naleven van de regels?	
22. Is er een communicatieproces met betrekking tot informatiebeveiliging, inclusief de verantwoordelijkheden en wat te communiceren, met wie en wanneer?	
7.5 Gedocumenteerde informatie	
23. Bevat de documentatie van het ISMS het informatiebeveiligingsbeleid, doelstellingen en doelen, de reikwijdte van het ISMS, de belangrijkste elementen en hun interactie, documenten en registraties van ISO 27001 en die welke door het bedrijf zijn geïdentificeerd?	
24. Is ervoor gezorgd dat het beheer van documenten en registraties bestaat, inclusief wie documenten beoordeelt en goedkeurt, en waar en hoe ze worden gepubliceerd, opgeslagen en beschermd?	
25. Wordt gedocumenteerde informatie van externe oorsprong gecontroleerd?	
8.0 Uitvoering	
8.1 Operationele planning en beheersing	
26. Beschikt de organisatie over de nodige gedocumenteerde informatie om er zeker van te zijn dat haar processen volgens plan worden uitgevoerd?	
27. Worden geplande wijzigingen gecontroleerd? Worden de gevolgen van ongeplande wijzigingen beoordeeld om zo nodig mitigerende maatregelen te identificeren?	
28. Worden uitbestede processen geïdentificeerd en gecontroleerd?	
8.2 Risicobeoordeling van informatiebeveiliging	
29. Zijn de risico's, hun eigenaren, waarschijnlijkheid, gevolgen en het risiconiveau geïdentificeerd? Zijn deze resultaten gedocumenteerd?	
8.3 Informatiebeveiligingsrisico's behandelen	
30. Bestaat er een risicobehandelplan, goedgekeurd door de risico-eigenaren?	
31. Is er een gedocumenteerde lijst met alle noodzakelijke controles, met de juiste motivering en implementatiestatus?	
9.0 Evaluatie van de prestaties	
9.1 Monitoren, meten, analyseren en evalueren	
32. Is er gedefinieerd wat gemeten moet worden, met welke methode, wie verantwoordelijk is, wie de resultaten zal analyseren en evalueren?	

Voldoen we aan?	J/N
33. Worden de meetresultaten gedocumenteerd, geanalyseerd en geëvalueerd door verantwoordelijke personen?	
9.2 Interne audit	
34. Bestaat er een auditprogramma dat de timing, verantwoordelijkheden, rapportage, auditcriteria en reikwijdte definieert?	
35. Worden interne audits uitgevoerd volgens een auditprogramma, resultaten gerapporteerd via een intern auditrapport en relevante corrigerende maatregelen naar voren gebracht?	
36. Wordt de directiebeoordeling regelmatig uitgevoerd en worden de resultaten gedocumenteerd in de notulen van de vergadering?	
37. Heeft het management beslist over alle cruciale kwesties die belangrijk zijn voor het succes van het ISMS?	
10.0 Verbetering	
10.1 Continue verbetering	
38. Wordt het ISMS voortdurend aangepast om zijn geschiktheid, toereikendheid en effectiviteit te behouden?	
10.2 Afwijkingen en corrigerende maatregelen	
39. Reageert de organisatie op elke afwijking?	
40. Overweegt de organisatie de oorzaak van de afwijking te elimineren en zo nodig corrigerende maatregelen te nemen?	
41. Worden alle afwijkingen geregistreerd, samen met corrigerende maatregelen?	

Voldoen we aan?	J/N
Bijlage A.	
A.5 Organisatorische Maatregelen	
42. Zijn er gepubliceerde, door het management goedgekeurde beleidsmaatregelen ter ondersteuning van informatiebeveiliging?	
43. Wordt het informatiebeveiligingsbeleid herzien en bijgewerkt?	
44. Zijn alle verantwoordelijkheden voor informatiebeveiliging gedefinieerd?	
45. Zijn taken en verantwoordelijkheden goed gescheiden, gezien situaties van belangenverstrengeling?	
46. Zijn er contacten met relevante autoriteiten gedefinieerd?	
47. Zijn er contacten met belangenverenigingen of beroepsverenigingen gedefinieerd?	
48. Worden projecten uitgevoerd volgens de aspecten van informatiebeveiliging?	
49. Zijn er regels gedefinieerd voor een veilige omgang met mobiele apparaten?	
50. Zijn er regels die bepalen hoe de informatie van de organisatie wordt beschermd met het oog op telewerklocaties?	
51. Bestaat er een inventaris van bedrijfsmiddelen?	
52. Heeft elk actief bedrijfsmiddel in de inventaris een aangewezen eigenaar?	
53. Zijn er regels voor het omgaan met informatie en bedrijfsmiddelen gedefinieerd?	
54. Worden bedrijfsmiddelen terugbetaald door werknemers en aannemers wanneer hun dienstverband wordt beëindigd?	
55. Zijn er procedures die bepalen hoe gerubriceerde informatie moet worden gelabeld en verwerkt?	
56. Zijn er procedures die bepalen hoe met bedrijfsmiddelen moet worden omgegaan?	
57. Zijn er procedures die bepalen hoe met verwijderbare media moet worden omgegaan in overeenstemming met de classificatieregels?	
58. Zijn er formele procedures voor het verwijderen van de media?	
59. Zijn de media die gevoelige informatie bevatten tijdens transport beschermd?	
60. Is er een toegangscontrolebeleid?	
61. Hebben de gebruikers alleen toegang tot de middelen die ze mogen?	
62. Worden toegangsrechten verleend via een formeel registratieproces?	
63. Is er een formeel toegangscontrolesysteem bij het inloggen op informatiesystemen?	
64. Worden speciale toegangsrechten met bijzondere aandacht beheerd?	
65. Worden wachtwoorden en andere geheime authenticatiegegevens op een veilige manier verstrekt?	
66. Controleren eigenaren van bedrijfsmiddelen periodiek alle bevoorrechte toegangsrechten?	
67. Worden de toegangsrechten bijgewerkt wanneer er een verandering is in de gebruikerssituatie?	
68. Zijn er regels voor gebruikers om wachtwoorden en andere authenticatie-informatie te beschermen?	
69. Is de toegang tot informatie in systemen beperkt volgens het toegangscontrolebeleid?	
70. Is een veilige aanmelding vereist op systemen volgens het toegangscontrolebeleid?	

Voldoen we aan?	J/N
71. Helpen de door de organisatie gebruikte wachtwoordbeheersystemen gebruikers om hun authenticatiegegevens veilig te beheren?	
72. Wordt het gebruik van hulpprogramma's gecontroleerd en beperkt tot specifieke werknemers?	
73. Is de toegang tot de broncode beperkt tot bevoegde personen?	
74. Is er een beleid om de risico's met betrekking tot leveranciers en partners te behandelen?	
75. Zijn relevante beveiligingseisen opgenomen in de overeenkomsten met leveranciers en partners?	
76. Bevatten de overeenkomsten met leveranciers en leveranciers beveiligingseisen?	
77. Worden leveranciers regelmatig gecontroleerd?	
78. Worden er bij wijzigingen in overeenkomsten en contracten met leveranciers en partners rekening gehouden met risico's en bestaande processen?	
79. Worden incidenten goed beheerd?	
80. Worden informatiebeveiligingsgebeurtenissen correct gerapporteerd?	
81. Rapporteren werknemers en contractanten over zwakke punten in de beveiliging?	
82. Worden beveiligingsgebeurtenissen correct beoordeeld en geclassificeerd?	
83. Zijn procedures voor het reageren op incidenten gedocumenteerd?	
84. Worden beveiligingsincidenten goed geanalyseerd?	
85. Bestaan er procedures die bepalen hoe bewijsmateriaal moet worden verzameld?	
86. Zijn er eisen gesteld aan de continuïteit van informatiebeveiliging?	
87. Bestaan er procedures die de continuïteit van de informatiebeveiliging tijdens een crisis of een ramp waarborgen?	
88. Wordt het uitoefenen en testen van continuïteit uitgevoerd?	
89. Heeft IT-infrastructuur redundantie (bijv .: secundaire locatie) opgenomen in de planning en exploitatie?	
90. Zijn wetgevende, regelgevende, contractuele en andere beveiligingseisen bekend?	
91. Bestaan er procedures om intellectuele eigendomsrechten te beschermen?	
92. Zijn registraties goed beschermd?	
93. Is persoonlijk identificeerbare informatie goed beschermd?	
94. Worden cryptografische controles correct gebruikt?	
95. Wordt informatiebeveiliging regelmatig beoordeeld door een onafhankelijke auditor?	
96. Controleren de managers regelmatig of het beveiligingsbeleid en de beveiligingsprocedures naar behoren worden uitgevoerd op hun verantwoordelijkheidsgebied?	
97. Worden informatiesystemen regelmatig herzien om te controleren of ze voldoen aan het informatiebeveiligingsbeleid en de -normen?	
A.6 Mensen	
98 Voert de organisatie achtergrondcontroles uit op kandidaten voor werk of voor aannemers?	
99. Zijn er overeenkomsten met werknemers en contractanten waarin de verantwoordelijkheden voor informatiebeveiliging worden gespecificeerd?	

Voldoen we aan?	J/N
100. Eist het management actief van alle werknemers en contractanten dat zij zich houden aan de regels voor informatiebeveiliging?	
101. Volgen werknemers en aannemers trainingen om hun beveiligingstaken beter uit te voeren, en bestaan er bewustmakingsprogramma's?	
102. Heeft de organisatie een formeel disciplinair proces?	
103. Bestaan er overeenkomsten over informatiebeveiligingsverantwoordelijkheden die ook na beëindiging van het dienstverband geldig blijven?	
A.7 Fysieke Maatregelen	
104. Bestaan er beveiligde gebieden die gevoelige informatie beschermen?	
105. Is de toegang tot beveiligde gebieden beschermd?	
106. Zijn beveiligde gebieden op een beschermde manier gelegen?	
107. Zijn de alarmen, brandbeveiliging en andere systemen geïnstalleerd?	
108. Zijn werkprocedures voor beveiligde gebieden gedefinieerd?	
109. Zijn aflever- en laadruimtes beveiligd?	
110. Is de apparatuur goed beschermd?	
111. Heeft de apparatuur bescherming tegen energievariaties?	
112. Zijn de voedings- en telecommunicatiekabels voldoende beschermd?	
113. Wordt de apparatuur regelmatig onderhouden?	
114. Wordt de verwijdering van informatie en apparatuur naar buiten het bedrijfsterrein gecontroleerd?	
115. Zijn de bedrijfsmiddelen van de organisatie goed beschermd als ze zich niet op het terrein van de organisatie bevinden?	
116. Wordt informatie correct verwijderd van media of apparatuur die zal worden verwijderd?	
117. Zijn er regels om apparatuur te beschermen wanneer deze niet fysiek in het bezit is van de gebruikers?	
118. Is er beleid voor gebruikers over wat ze moeten doen als ze niet aanwezig zijn op hun werkstations?	
A.8 Technische Maatregelen	
119. Bestaat er een beleid om encryptie en andere cryptografische controles te reguleren?	
120. Zijn de cryptografische sleutels goed beschermd?	
121. Zijn de operationele procedures voor IT-processen gedocumenteerd?	
122. Worden wijzigingen die van invloed kunnen zijn op de informatiebeveiliging strikt gecontroleerd?	
123. Worden middelen bewaakt en plannen gemaakt om ervoor te zorgen dat ze in staat zijn om aan de eisen van gebruikers te voldoen?	
124. Zijn de ontwikkel-, test- en productieomgevingen gescheiden?	
125. Zijn antivirussoftware en andere software voor bescherming tegen malware geïnstalleerd en correct gebruikt?	
126. Is een back-upbeleid correct gedefinieerd en uitgevoerd?	
127. Worden relevante gebeurtenissen uit IT-systemen geregistreerd en periodiek geverifieerd?	
128. Zijn logs goed beschermd?	
129. Zijn beheerderslogboeken goed beschermd?	
130. Zijn klokken op alle IT-systemen gesynchroniseerd?	
131. Wordt de installatie van software strikt gecontroleerd?	
132. Worden de informatie en correctie van kwetsbaarheden goed beheerd?	

Voldoen we aan?	J/N
133. Zijn er regels om de beperkingen van software-installatie door gebruikers te definiëren?	
134. Zijn audits van productiesystemen goed gepland en uitgevoerd?	
135. Zijn beveiligingsvereisten voor netwerkdiensten gedefinieerd en opgenomen in overeenkomsten?	
136. Zijn de netwerken gescheiden gezien de risico's en de classificatie van bedrijfsmiddelen?	
137. Is de informatieoverdracht goed beschermd?	
138. Overwegen overeenkomsten met derden de bescherming tijdens informatieoverdracht?	
139. Zijn de berichten die via de netwerken worden uitgewisseld, goed beveiligd?	
140. Geeft de organisatie een lijst van alle vertrouwelijkheidsclausules die in overeenkomsten met derden moeten worden opgenomen?	
141. Zijn er beveiligingsvereisten gedefinieerd voor nieuwe informatiesystemen of voor wijzigingen daarin?	
142. Wordt applicatie-informatie die via openbare netwerken wordt overgedragen, op passende wijze beschermd?	
143. Wordt transactie-informatie die via de openbare netwerken wordt overgedragen, op passende wijze beschermd?	
144. Zijn er regels gedefinieerd voor de veilige ontwikkeling van software en systemen?	
145. Worden wijzigingen aan nieuwe of bestaande systemen goed gecontroleerd?	
146. Worden kritieke applicaties correct getest na wijzigingen in besturingssystemen?	
147. Worden alleen noodzakelijke wijzigingen aangebracht in informatiesystemen?	
148. Worden de principes voor het ontwerpen van veilige systemen toegepast op het ontwikkelingsproces van het organisatiesysteem?	
149. Is de ontwikkelomgeving goed beveiligd?	
150. Wordt de uitbestede ontwikkeling van systemen bewaakt?	
151. Worden de implementatie van beveiligingsvereisten getest tijdens systeemontwikkeling?	
152. Zijn er criteria voor het accepteren van de systemen gedefinieerd?	
153. Zijn testgegevens zorgvuldig geselecteerd en beschermd?	