Management de la sécurité de l’information

Implémentation ISO 27001

Mise en place d’un SMSI et audit de certification

2e édition
# Table des matières

Avant-propos ................................................................................................................... 1

Partie I – Les systèmes de management de la sécurité de l’information

Chapitre 1 – Les systèmes de management ................................................................. 5
  Qu’est-ce qu’un système de management ? .............................................................. 5
  Principaux systèmes de management ...................................................................... 6
  Propriétés des systèmes de management .................................................................. 7
    Large spectre de métiers et de compétences ......................................................... 7
    Un projet fédérateur et mobilisateur ...................................................................... 8
    Importance de l’écrit ............................................................................................... 8
    Auditabilité ............................................................................................................ 9
  Apports des systèmes de management .................................................................... 9
    Premier apport : l’adoption de bonnes pratiques ............................................... 9
    Second apport : l’augmentation de la fiabilité ....................................................... 10
    Troisième apport : la confiance ............................................................................ 10
  Le modèle PDCA ..................................................................................................... 11
  Sécurité de l’information ....................................................................................... 13
  Historique des normes .......................................................................................... 15

Chapitre 2 – La norme ISO 27001 .............................................................................. 17
  Premier constat ....................................................................................................... 17
  Objectifs généraux .................................................................................................. 17
  Structure de la norme ............................................................................................. 19
  Phase Plan du SMSI .............................................................................................. 21
    Étape 1 : définir le périmètre et la politique ......................................................... 21
    Étape 2 : apprécier les risques ............................................................................ 23
    Étape 3 : traiter le risque et identifier le risque résiduel .................................... 26
    Étape 4 : sélectionner les mesures de sécurité ................................................... 30
Management de la sécurité de l’information

Phase Do du SMSI ......................................................... 32
Plan de traitement des risques ......................................... 32
Déployer les mesures de sécurité ...................................... 33
Générer des indicateurs ................................................... 34
Former et sensibiliser le personnel .................................... 34
Gérer le SMSI au quotidien .............................................. 36
Détection et réaction rapide aux incidents ......................... 36
Phase Check du SMSI ..................................................... 37
Les audits internes .......................................................... 38
Le contrôle interne ......................................................... 39
Les revues ................................................................. 40
Phase Act du SMSI ........................................................ 41
Actions correctives ......................................................... 42
Actions préventives ........................................................ 42
Actions d’amélioration .................................................... 42

Chapitre 3 – La norme ISO 27002 ......................................... 45
Deux approches de la sécurité .......................................... 45
Les formalisateurs .......................................................... 45
Les techniciens ............................................................. 46
Une complémentarité nécessaire ...................................... 47
Présentation de la norme ................................................. 48
Structure générale .......................................................... 48
Chapitres de l’ISO 27002 .................................................. 50
Utilisation de la norme .................................................... 54

Chapitre 4 – Comparaison et usages des deux normes .......... 55
Quelques comparaisons ................................................... 55
Sur la forme ................................................................ 55
Sur le fond ................................................................... 56
Interaction entre les normes .............................................. 57
L’ISO 27001 a-t-elle besoin de l’ISO 27002 ? ................. 58
L’ISO 27002 a-t-elle besoin de l’ISO 27001 ? .................. 58
Deux normes complémentaires ....................................... 59
Usages de l’ISO 27001 ..................................................... 59
Adopter de bonnes pratiques ........................................... 59
Diminuer le coût lié aux audits ........................................ 61
# Table des matières

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fournir la confiance aux clients</td>
<td>63</td>
</tr>
<tr>
<td>Autres motivations</td>
<td>63</td>
</tr>
<tr>
<td>Usages de l’ISO 27002</td>
<td>65</td>
</tr>
<tr>
<td>Tableaux de bord</td>
<td>65</td>
</tr>
<tr>
<td>Consolidation de tableaux de bord</td>
<td>66</td>
</tr>
<tr>
<td>Consolidation d’audits</td>
<td>67</td>
</tr>
<tr>
<td>Politiques de sécurité</td>
<td>68</td>
</tr>
<tr>
<td>Exigences de sécurité</td>
<td>69</td>
</tr>
<tr>
<td>Chapitre 5 – La série des normes ISO 27000</td>
<td>71</td>
</tr>
<tr>
<td>Présentation de la série des normes</td>
<td>71</td>
</tr>
<tr>
<td>Les normes formulant des exigences</td>
<td>72</td>
</tr>
<tr>
<td>ISO 27001, la référence</td>
<td>72</td>
</tr>
<tr>
<td>ISO 27006, pour les organismes de certification</td>
<td>72</td>
</tr>
<tr>
<td>Les guides de bonnes pratiques</td>
<td>74</td>
</tr>
<tr>
<td>ISO 27000 ou le vocabulaire des SMSI</td>
<td>75</td>
</tr>
<tr>
<td>ISO 27002 : la liste des mesures de sécurité</td>
<td>76</td>
</tr>
<tr>
<td>ISO 27003 au sujet de la démarche projet</td>
<td>76</td>
</tr>
<tr>
<td>ISO 27004 ou la gestion des indicateurs</td>
<td>77</td>
</tr>
<tr>
<td>ISO 27005 et l’appréciation des risques</td>
<td>78</td>
</tr>
<tr>
<td>ISO 27007, sur l’audit des SMSI</td>
<td>79</td>
</tr>
<tr>
<td>ISO 27008 ou le contrôle des mesures de sécurité</td>
<td>79</td>
</tr>
<tr>
<td>Les autres normes</td>
<td>81</td>
</tr>
<tr>
<td>Les normes sectorielles</td>
<td>81</td>
</tr>
<tr>
<td>Les autres normes en projet</td>
<td>81</td>
</tr>
<tr>
<td>Partie II – Implémente un SMSI</td>
<td></td>
</tr>
<tr>
<td>Chapitre 6 – Le projet de mise en place du SMSI</td>
<td>85</td>
</tr>
<tr>
<td>Nature du projet</td>
<td>85</td>
</tr>
<tr>
<td>Chef de projet</td>
<td>86</td>
</tr>
<tr>
<td>Projet de mise en place du SMSI</td>
<td>87</td>
</tr>
<tr>
<td>Approche séquentielle</td>
<td>87</td>
</tr>
<tr>
<td>Approche projet</td>
<td>89</td>
</tr>
<tr>
<td>Principales erreurs à éviter</td>
<td>95</td>
</tr>
<tr>
<td>Coût et suivi du projet</td>
<td>97</td>
</tr>
<tr>
<td>Éléments du projet de SMSI</td>
<td>99</td>
</tr>
</tbody>
</table>
Table des matières

Chapitre 10 – Audit interne et suivi des actions .................................................. 141
Audit interne ........................................................................................................... 141
Exigence normative ............................................................................................. 141
L’état d’esprit de l’audit interne ............................................................................ 142
Programmation des audits internes ..................................................................... 143
Déroulement des audits internes ......................................................................... 145
Comment mettre en place l’audit interne ? ...................................................... 147
Dans une PME ....................................................................................................... 147
Dans les grandes structures sans audit interne .................................................. 148
Dans les grandes structures avec audit interne .................................................... 149
Guide d’audit ........................................................................................................ 150
Suivi des actions .................................................................................................. 151
Éléments du sous-projet d’audit et de suivi d’actions ......................................... 153

Chapitre 11 – Appréciation des risques ................................................................. 155
Processus de gestion du risque ........................................................................... 155
Différentes méthodes ........................................................................................... 156
La norme ISO 27005 .............................................................................................. 157
Pourquoi cette norme ? ....................................................................................... 157
Structure de la norme ......................................................................................... 158
Conclusion sur l’ISO 27005 .................................................................................. 162
Différentes approches .......................................................................................... 163
Une appréciation des risques existe déjà ........................................................... 163
Démarche « canonique » ...................................................................................... 164
Démarche « pragmatique » .................................................................................. 164
Difficultés courantes de l’appréciation des risques ............................................. 167
Commencer l’appréciation ................................................................................... 167
Inventaire des actifs .............................................................................................. 167
Valoriser les actifs ............................................................................................... 170
Estimer le risque ................................................................................................... 172
Mesures de sécurité ............................................................................................. 173
Établir des niveaux de risque ............................................................................. 173
Définir les risques acceptables .......................................................................... 175
Étude de cas d’appréciation de risques .............................................................. 176
Oubli d’un risque .................................................................................................. 178
Éléments du sous-projet de gestion des risques ................................................. 178
<table>
<thead>
<tr>
<th>Chapitre 15 – Le principe de la certification</th>
<th>217</th>
</tr>
</thead>
<tbody>
<tr>
<td>La certification</td>
<td>217</td>
</tr>
<tr>
<td>Obtenir le certificat ISO 27001</td>
<td>217</td>
</tr>
<tr>
<td>Conserver le certificat</td>
<td>219</td>
</tr>
<tr>
<td>Les organismes de certification</td>
<td>221</td>
</tr>
<tr>
<td>Cadre réglementaire</td>
<td>221</td>
</tr>
<tr>
<td>Relations contractuelles avec l'audité</td>
<td>226</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapitre 16 – Les audits</th>
<th>229</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principes de base</td>
<td>229</td>
</tr>
<tr>
<td>Deux façons de considérer les audits</td>
<td>229</td>
</tr>
<tr>
<td>Principes de l'audit</td>
<td>230</td>
</tr>
<tr>
<td>Différents types d'audits</td>
<td>231</td>
</tr>
<tr>
<td>Programme d'audits</td>
<td>232</td>
</tr>
<tr>
<td>Déroulement d'un audit</td>
<td>234</td>
</tr>
<tr>
<td>1. Premier contact</td>
<td>234</td>
</tr>
<tr>
<td>2. Revue de documentation</td>
<td>235</td>
</tr>
<tr>
<td>3. Plan d'audit</td>
<td>235</td>
</tr>
<tr>
<td>4. Réunion d'ouverture</td>
<td>238</td>
</tr>
<tr>
<td>5. Activités d'audit</td>
<td>238</td>
</tr>
<tr>
<td>6. Réunion de clôture</td>
<td>239</td>
</tr>
<tr>
<td>7. Après l'audit</td>
<td>239</td>
</tr>
<tr>
<td>La notion de non-conformité</td>
<td>241</td>
</tr>
<tr>
<td>Différents types de non-conformités</td>
<td>241</td>
</tr>
<tr>
<td>Critères de qualification</td>
<td>242</td>
</tr>
<tr>
<td>Séquence de gestion d'une non-conformité</td>
<td>243</td>
</tr>
<tr>
<td>Procédure de contestation</td>
<td>247</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapitre 17 – Se préparer à l'audit de certification</th>
<th>249</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avant l'audit de certification</td>
<td>249</td>
</tr>
<tr>
<td>Audit à blanc</td>
<td>249</td>
</tr>
<tr>
<td>Informer</td>
<td>250</td>
</tr>
<tr>
<td>Préparer les documents</td>
<td>252</td>
</tr>
<tr>
<td>Prévoir les questions d'intendance</td>
<td>255</td>
</tr>
</tbody>
</table>
Management de la sécurité de l’information

Pendant l’audit ........................................ 257
   Revue de documentation .................................. 257
   Réunion d’ouverture ...................................... 258
   Activités d’audit ......................................... 258
   Réunion de clôture ......................................... 260
Après l’audit .................................................. 261
   Quelques conseils ........................................ 262
   Facteurs anxiogènes pour l’audité .......................... 262
   Éléments susceptibles d’indisposer l’auditeur .............. 263
   Erreurs à éviter ........................................... 264
   Points sur lesquels il faut rester ferme ...................... 265

Chapitre 18 – La vraie valeur de la certification ................ 267
   Quelle est la valeur réelle de la certification ? ........... 267
      Absurdité de la question ................................ 268
      Pertinence de la question ................................ 268
Les différents profils de certifications .......................... 268
   Cas n° 1 : les sociétés cherchant la conformité avant tout ..... 269
   Cas n° 2 : les sociétés maîtrisant déjà la sécurité ............. 269
   Cas n° 3 : les sociétés découvrant la sécurité avec l’ISO 27001 ....... 269
Les questions à se poser ....................................... 270
   Le périmètre de la certification ............................ 270
   La politique du SMSI ....................................... 272
   Les signes positifs ......................................... 273
Comment distinguer les SMSI des cas n° 1 et des cas n° 2 ? ...... 274
   Reconnaître les cas n° 1 ................................... 274
   Distinguer les cas n° 2 .................................... 275
   La difficulté de vérifier .................................... 275
Conclusion ....................................................... 276
Index ............................................................. 277