

Avant-propos

Chapitre 1

Gérer la complexité des SI avec la matrice 2MSI

- 1. La multiplication, la convergence et l'interaction des technologies .. 7
- 2. Des organisations de plus en plus dépendantes de leur SI. 9
- 3. La segmentation des compétences et des ressources humaines. 11
- 4. Le bug et la faille sont dans les interstices 13
- 5. Du risque financier au risque pénal, la gestion des risques 17
- 6. Le management des SI se prête particulièrement à l'analyse systémique 19

Chapitre 2

Appliquer la méthode 2MSI

- 1. La matrice de monitoring des systèmes d'information 23
- 2. Les sept couches du système d'information 24
- 3. La ressource, sa gestion, sa préservation 26
- 4. Synopsis de la matrice en 21 briques. 28
- 5. Trois critères communs pour qualifier chaque brique du SI 31
- 6. Les repères sur l'écosystème méthodologique des SI 37

Chapitre 3

Auditer et évaluer un système d'information

- 1. Auditer, c'est décrire et qualifier 47
- 2. La matrice 2MSI structure la méthodologie de l'audit. 48
- 3. La matrice 2MSI organise les informations nécessaires à la réalisation de l'audit 51

2—Pilotage d'un système d'information

Méthode et bonnes pratiques

4. Du diagnostic aux préconisations opérationnelles 61
5. Les priorités d'action et le plan d'action 63
6. Retour d'expérience : l'audit SI de la Société nouvelle de transport . 64

Chapitre 4

Formuler une stratégie pour le SI

1. Une entreprise est un organisme vivant 73
2. Le modèle de l'alignement stratégique 74
3. Quelques exemples d'alignements stratégiques 78
4. Synthèse de la stratégie pour les systèmes d'information
de la Centrale d'achat des sociétés d'habitat - (CashSA) 84

Chapitre 5

Manager avec un schéma directeur du SI

1. La notion de schéma directeur 87
2. Formuler des axes directeurs pour chacune
des briques de la matrice 2MSI 91
3. Un SDSI en perpétuel renouvellement 94
4. Les critères 2MSI pour manager le SDSI 96
5. Le périmètre du SDSI : exemple d'application de la matrice 2MSI . . 98

Chapitre 6

Urbaniser le système d'information

1. La notion d'urbanisation 103
2. La démarche d'urbanisation 105
3. Les enjeux de l'urbanisation 108
4. Les dilemmes auxquels doit répondre le SI manager 111

- 5. Les réponses aux dilemmes : l'expérience de l'Agence publique territoires entreprenants. 113
- 6. Exemple appliqué : l'urbanisation fonctionnelle de la GRC et de l'e-administration de la ville d'Étaint-Lalampe 117

Chapitre 7

Définir et piloter une politique d'infogérance

- 1. L'infogérance, problématique des SI modernes 123
- 2. Les avantages et les inconvénients du choix de l'infogérance 127
- 3. Définir le périmètre d'une politique d'infogérance. 132
- 4. L'infogérance à la carte ou par grands domaines : quel modèle choisir ? 135
- 5. Formaliser contractuellement le périmètre de la prestation d'un infogérant 138
- 6. Gérer les infogérances en cascade 147
- 7. Définir les unités d'œuvre d'un contrat d'infogérance. 149
- 8. La protection du patrimoine informationnel 154
- 9. Le monitoring de la réversibilité avec la matrice 2MSI 156

Chapitre 8

Assurer la sécurité du SI et manager les risques

- 1. Prendre la mesure de l'enjeu sécurité et des risques 159
- 2. Manager la sécurité et les risques 164
- 3. Formaliser la politique de sécurité des SI (PSSI) 172
- 4. Former et éduquer les utilisateurs 175
- 5. Prendre en compte la spécificité de chaque métier. 176
- 6. S'assurer de l'application de la PSSI. 178
- 7. Le socle d'une PSSI globale. 179

4—Pilotage d'un système d'information

Méthode et bonnes pratiques

- 8. Le RGPD et la protection des données personnelles. 183
- 9. Organiser la résilience face à l'incident 188

Chapitre 9

Manager la connaissance, instrumenter le SI

- 1. Donner toute son importance à la question documentaire. 193
- 2. Inventorier et analyser le patrimoine documentaire 194
- 3. Instrumenter le patrimoine documentaire 198

Chapitre 10

Organiser la DSI

- 1. L'organisation des hommes est indispensable
au bon fonctionnement du SI 203
- 2. L'analyse des fonctions et processus 205
- 3. La grille de concordance organigramme/
gouvernance/processus/infogérants 207
- 4. Les points d'attention pour la construction
d'un organigramme de DSI 209

Chapitre 11

Manager les RH et conduire le changement

- 1. Utiliser la matrice 2MSI pour manager les RH. 213
- 2. Manager les compétences 214
- 3. Manager les objectifs 221
- 4. Manager la qualité 223
- 5. Manager la dynamique de changement 228

Chapitre 12

Accompagner et responsabiliser les utilisateurs

| | |
|--|-----|
| 1. Placer l'utilisateur au centre du SI | 235 |
| 2. L'identité numérique et la responsabilité personnelle | 236 |
| 3. La sécurité et les bonnes pratiques | 238 |
| 4. L'action et la responsabilité professionnelle en environnement dématérialisé | 243 |
| 5. Les utilisations professionnelle et personnelle | 247 |
| 6. La citoyenneté numérique, la déontologie | 250 |
| 7. Le droit à la déconnexion | 252 |

Annexe

| | |
|--|------------|
| Siglothèque - Sociolecte informatique | 255 |
|--|------------|

| | |
|-----------------|-----|
| Index | 259 |
|-----------------|-----|

Avant-propos

Chapitre 1

Prérequis

- 1. Introduction 11
- 2. Que suppose une bonne gouvernance ? 12
 - 2.1 La prise de décision 13
 - 2.2 La définition de la structure organisationnelle 14
 - 2.3 La mise en avant des avantages 17
 - 2.4 L'intérêt commun 18
- 3. Quels rôles pour quelles responsabilités ? 19
 - 3.1 L'identification des rôles 19
 - 3.2 La cohérence entre l'identification et l'attribution 20
 - 3.3 Le cadrage juridique 21
- 4. Que prévoir en termes de ressources ? 22
 - 4.1 La variété des ressources 23
 - 4.2 L'estimation des ressources nécessaires 24
- 5. Quel serait un contexte favorable ? 25

Chapitre 2

Finalités de la norme

- 1. Les principes constitutifs de la norme 27
 - 1.1 Les enjeux de la norme 28
 - 1.2 Les finalités de la norme 29
 - 1.3 La cible de la norme 30
 - 1.3.1 La cible : tout ou partie d'une personne morale 30
 - 1.3.2 La cible : une personne physique 32
 - 1.4 L'investissement induit 33

2 _____ Sécurité de l'information

et ISO 27001

| | | |
|-------|--|----|
| 2. | L'obtention d'une certification ISO 27001 | 34 |
| 2.1 | La synthèse du processus de certification d'une entité | 35 |
| 2.2 | Les motivations pour une certification | 35 |
| 2.3 | Les limites d'une certification | 36 |
| 3. | Le recueil de bonnes pratiques | 37 |
| 3.1 | Le concept d'état de l'art. | 38 |
| 3.2 | Le traitement d'un thème précis | 39 |
| 3.3 | Évaluation de la maturité sécurité. | 40 |
| 3.4 | Préparation à la certification | 41 |
| 4. | La formation de personnes. | 41 |
| 4.1 | Une bonne approche de la norme | 42 |
| 5. | Rappel des points clés. | 45 |
| 6. | Cas pratiques | 47 |
| 6.1 | Cas pratique 1 | 47 |
| 6.2 | Cas pratique 2 | 48 |
| 6.2.1 | Exercice 1 : certification d'une société. | 49 |
| 6.2.2 | Exercice 2 : certification d'un directeur financier | 52 |

Chapitre 3

La norme ISO 27001

| | | |
|-----|--|----|
| 1. | Contextualisation de la norme | 55 |
| 2. | Rappel historique sur sa construction. | 57 |
| 3. | Domaine adressé. | 58 |
| 4. | Usage actuel de la norme | 60 |
| 4.1 | Obtenir la certification ISO 27001 | 61 |
| 4.2 | Un point de passage vers d'autres certifications | 63 |
| 4.3 | Répondre aux exigences des donneurs d'ordre | 65 |
| 4.4 | Obtenir un avantage concurrentiel | 66 |
| 4.5 | Une reconnaissance internationale | 67 |
| 5. | Philosophie de la norme | 67 |

| | | |
|-------|--|-----|
| 6. | Contenu de la norme | 69 |
| 6.1 | Clause 4 : contexte de l'organisation. | 70 |
| 6.1.1 | Compréhension de l'organisation et de son contexte | 70 |
| 6.1.2 | Compréhension des besoins et des attentes des parties intéressées. | 71 |
| 6.1.3 | Détermination du domaine d'application du système de management de la sécurité de l'information | 73 |
| 6.1.4 | Système de management de la sécurité de l'information | 77 |
| 6.2 | Clause 5 : leadership. | 77 |
| 6.2.1 | Leadership et engagement de la direction. | 77 |
| 6.2.2 | Politique | 80 |
| 6.2.3 | Rôles, responsabilités et autorités au sein de l'organisation. | 81 |
| 6.3 | Clause 6 : planification. | 85 |
| 6.3.1 | Généralités | 86 |
| 6.3.2 | Appréciation des risques | 86 |
| 6.3.3 | Traitement des risques. | 87 |
| 6.4 | Clause 7 : support. | 89 |
| 6.4.1 | Gestion des ressources | 90 |
| 6.4.2 | Gestion des compétences. | 92 |
| 6.4.3 | Sensibilisation. | 93 |
| 6.4.4 | Communication | 93 |
| 6.4.5 | Gestion documentaire | 94 |
| 6.5 | Clause 8 : fonctionnement. | 95 |
| 6.5.1 | Planification et contrôle opérationnel. | 95 |
| 6.5.2 | Appréciation des risques | 95 |
| 6.6 | Clause 9 : évaluation des performances | 97 |
| 6.6.1 | Surveillance, mesures, analyse et évaluation | 97 |
| 6.6.2 | Audit interne. | 98 |
| 6.6.3 | Revue de direction | 99 |
| 6.7 | Clause 10 : amélioration. | 100 |
| 6.7.1 | Gestion des non-conformités. | 100 |
| 6.7.2 | Amélioration continue. | 101 |

4 _____ Sécurité de l'information

et ISO 27001

| | | |
|-----|------------------------------|-----|
| 6.8 | Annexe A. | 101 |
| 7. | Rappel des points clés. | 102 |

Chapitre 4

Les politiques et mesures de sécurité

| | | |
|-------|---|-----|
| 1. | Introduction | 105 |
| 2. | Politique de gouvernance et politique de sécurité | 107 |
| 3. | Bonnes pratiques de définition d'une politique de gouvernance. | 108 |
| 3.1 | Préciser les objectifs | 108 |
| 3.2 | État des lieux et plan projet | 109 |
| 3.3 | Négocier les objectifs, les moyens et le calendrier | 112 |
| 3.4 | Points clés de la gouvernance. | 113 |
| 3.5 | Organisation de la gouvernance : comitologie | 114 |
| 3.5.1 | Comité stratégique | 115 |
| 3.5.2 | Comité opérationnel | 116 |
| 3.6 | Sensibilisation et formation. | 118 |
| 3.7 | Audit interne. | 118 |
| 3.8 | Fonctionnement et évaluation des performances | 118 |
| 3.9 | Communication | 119 |
| 3.10 | Amélioration continue | 119 |
| 4. | Bonnes pratiques de rédaction d'une politique de sécurité | 119 |
| 4.1 | De la bonne définition des règles (mesures) | 121 |
| 4.2 | De la bonne formulation des règles (mesures) | 125 |
| 5. | Points clés d'une politique de sécurité : les pratiques ISO 27002 | 126 |
| 5.1 | Chapitre 5 : politiques de sécurité de l'information. | 126 |
| 5.2 | Chapitre 6 : organisation de la sécurité de l'information. | 127 |
| 5.3 | Chapitre 7 : sécurité des ressources humaines | 128 |
| 5.4 | Chapitre 8 : gestion des actifs | 128 |
| 5.5 | Chapitre 9 : contrôle d'accès | 129 |
| 5.6 | Chapitre 10 : cryptographie. | 131 |
| 5.7 | Chapitre 11 : sécurité physique et environnementale | 132 |

- 5.8 Chapitre 12 : sécurité liée à l’exploitation. 132
- 5.9 Chapitre 13 : sécurité des communications 133
- 5.10 Chapitre 14 : acquisition, développement, maintenance. 134
- 5.11 Chapitre 15 : relation avec les fournisseurs 134
- 5.12 Chapitre 16 : gestion des incidents 135
- 5.13 Chapitre 17 : aspects de la sécurité
dans la gestion de la continuité de l’activité. 136
- 5.14 Chapitre 18 : conformité 137
- 6. Du caractère virtuel d’une politique de sécurité. 138
- 7. Rappel des points clés. 139
- 8. Cas pratique : quelques conseils en matière de politique. 141

Chapitre 5

La démarche d'analyse des risques

- 1. Rappels des principaux concepts de sécurité 147
 - 1.1 Sécurité de l'information 147
 - 1.2 Besoins de sécurité 149
 - 1.2.1 Sources du besoin de sécurité. 150
 - 1.2.2 Critères de sécurité 151
 - 1.2.3 Échelle de criticité. 153
 - 1.3 Protection des éléments sensibles 154
 - 1.3.1 Enjeux de sécurité. 154
 - 1.3.2 Objectifs de sécurité. 158
 - 1.4 Risques de sécurité 159
 - 1.4.1 Évaluation de l'imprévu 159
 - 1.4.2 Définition 160
 - 1.4.3 Approche pour la valorisation du risque 160
 - 1.4.4 Finalité du risque 161

6 _____ Sécurité de l'information

et ISO 27001

| | | |
|-------|--|-----|
| 2. | Vers une identification des risques | 163 |
| 2.1 | Notions sous-jacentes aux risques. | 163 |
| 2.1.1 | Vulnérabilité | 163 |
| 2.1.2 | Source de menace | 164 |
| 2.1.3 | Menace | 164 |
| 2.1.4 | Objet | 164 |
| 2.1.5 | Scénario de menace | 165 |
| 2.2 | Des scénarios aux risques. | 166 |
| 2.2.1 | Regroupement des scénarios de menace | 166 |
| 2.2.2 | Évaluation de la menace pesant sur les besoins de sécurité. | 166 |
| 2.2.3 | Identification des risques stratégiques | 167 |
| 2.2.4 | Préparation à l'identification des risques opérationnels | 169 |
| 3. | Poursuite du travail d'analyse sur les risques | 177 |
| 3.1 | Du général au particulier | 177 |
| 3.1.1 | Description du contexte. | 178 |
| 3.1.2 | Recueil de l'information stratégique | 178 |
| 3.1.3 | Prise en compte de la menace | 181 |
| 3.1.4 | Prise en compte des risques stratégiques. | 183 |
| 3.1.5 | Prise en compte des risques opérationnels | 184 |
| 3.2 | Confrontation à l'existant | 186 |
| 3.2.1 | Validation des scénarios de menace | 186 |
| 3.2.2 | Validation des risques. | 187 |
| 3.3 | Synthèse | 187 |
| 4. | Cas pratique | 189 |
| 4.1 | Énoncé du cas | 189 |
| 4.2 | Réponse possible. | 190 |

Chapitre 6
La gestion des risques

- 1. Introduction 193
- 2. Gouvernance du risque. 194
 - 2.1 Identification des risques à traiter. 194
 - 2.2 Organisation pour la prise de décisions. 195
 - 2.3 Gérer les évolutions 196
 - 2.4 Niveau de risque exprimé. 196
- 3. Traitement des risques 197
 - 3.1 Interprétation des éléments de l'analyse. 197
 - 3.1.1 Couverture des risques. 197
 - 3.1.2 Seuil et critères d'acceptation du risque 197
 - 3.2 L'organisation du traitement 198
 - 3.3 Options de traitement 199
 - 3.4 Mesures de sécurité 200
 - 3.5 Risques résiduels 201
- 4. Amélioration de la gestion des risques 201
 - 4.1 Appréciation du niveau courant de risques. 202
 - 4.2 Appréciation du niveau courant de sécurité 203
 - 4.3 Amélioration du niveau de sécurité. 205
- 5. Rappel des points clés. 205
- 6. Cas pratique 207
 - 6.1 Énoncé du cas 207
 - 6.2 Pistes de réponse possible. 208
 - 6.2.1 RISQUE 1 208
 - 6.2.2 RISQUE 2 209
 - 6.2.3 RISQUE 3 211

8 _____ Sécurité de l'information

et ISO 27001

Chapitre 7

La planification et le run

| | |
|---|-----|
| 1. Introduction | 213 |
| 2. Objectifs et causalités des actions | 215 |
| 2.1 Actions de gouvernance | 215 |
| 2.2 Actions de mise en conformité réglementaire et contractuelle | 216 |
| 2.3 Action de réduction des risques | 217 |
| 2.4 Actions d'amélioration continue | 219 |
| 3. Formalisation des actions | 220 |
| 4. Un énoncé clair et précis de l'action attendue | 223 |
| 5. Structuration du plan d'action | 225 |
| 6. Pilotage du plan d'action | 227 |
| 7. Mise en œuvre, exploitation et amélioration du système de gouvernance | 227 |
| 8. Rappel des points clés | 229 |
| 9. Cas pratique | 229 |

Chapitre 8

Les modalités de surveillance et de suivi

| | |
|---|-----|
| 1. Introduction | 235 |
| 2. La surveillance : un élément essentiel de l'amélioration | 235 |
| 3. Contrôle et suivi : que surveiller ? | 237 |
| 3.1 Définir des indicateurs à bon escient | 237 |
| 3.2 En faire assez | 238 |
| 3.3 Ne pas en faire trop | 239 |
| 4. De manière progressive et adaptée | 240 |

- 5. Définition des éléments de contrôle et de suivi : les indicateurs. . . 241
 - 5.1 Élaboration d'un indicateur 242
- 6. Quelques indicateurs de gouvernance. 246
- 7. Quelques indicateurs d'efficacité des mesures de sécurité. 247
- 8. Exploitation des indicateurs. 248
- 9. Communication, acceptation par les équipes. 248
- 10. Définition des éléments de contrôle et de suivi : les tableaux de bord 249
- 11. Rappel des points clés. 252
- 12. Cas pratique 253

Chapitre 9
L'évaluation

- 1. Introduction 257
- 2. Pourquoi faire des audits ? 259
 - 2.1 Audit de conformité réglementaire 259
 - 2.2 Audit de contrôle d'un sous-traitant 260
- 3. Référentiels d'audit. 261
- 4. Audit de certification 263
 - 4.1 Référentiels d'audit. 263
 - 4.2 Choix d'un organisme auditeur/organisme de certification . . 265
 - 4.2.1 La relation donneur d'ordre/organisme de certification 268
 - 4.2.2 La relation auditeur/audité 269
- 5. Profil type d'un auditeur 272
 - 5.1 De la certification de personnes. 272
 - 5.2 Des compétences requises de l'équipe d'audit 273
 - 5.2.1 Expérience 273
 - 5.2.2 Bagage technique et mise à jour des connaissances . . . 274
 - 5.2.3 Communication écrite et orale 275

10 _____ Sécurité de l'information

et ISO 27001

| | |
|--|-----|
| 6. Modalités d'audit | 276 |
| 6.1 Réunion de lancement | 277 |
| 6.2 Revue documentaire. | 277 |
| 6.3 Audit sur site. | 278 |
| 6.4 Réunion de clôture, constats, négociation | 280 |
| 7. Plan de remédiation et mise à jour du plan d'action | 283 |
| 8. L'audit, une étape indispensable à l'amélioration. | 283 |
| 9. Rappel des points clés. | 284 |
| 10. Cas pratique | 285 |
| 10.1 Les non-conformités inadmissibles | 285 |
| 10.2 Les marronniers des auditeurs | 286 |
| 10.3 Quelques exemples de non-conformités discutables | 288 |
| | |
| Index | 291 |