

**Avant-propos**

**Partie 1 : Sinistres et risques**

**Chapitre 1**

**Mieux connaître les sinistres**

- 1. Mieux connaître les sinistres ..... 15
  - 1.1 Définition d'un sinistre ..... 15
    - 1.1.1 Sinistre avec perte de données ..... 16
    - 1.1.2 Sinistre sans perte de données ..... 17
  - 1.2 Petits maux, grands effets ..... 18
  - 1.3 De l'importance de la disponibilité et de la résilience. .... 18
- 2. Taxonomie des sinistres ..... 19
  - 2.1 Sinistre chronique ..... 19
    - 2.1.1 Sinistre chronique accidentel ..... 19
    - 2.1.2 Sinistre chronique volontaire ..... 20
  - 2.2 Sinistre physique ..... 22
  - 2.3 Sinistre environnemental ..... 23
- 3. Caractéristiques des sinistres ..... 25
  - 3.1 Durée ..... 25
    - 3.1.1 Le facteur chance ..... 26
    - 3.1.2 La durée, votre pire ennemi. .... 26
  - 3.2 Amplitude ..... 27
  - 3.3 Ne jamais oublier les facteurs externes ..... 28

# 2 \_\_\_\_\_ Protection des données

Disponibilité et résilience des données

## Chapitre 2

### Conséquences d'un sinistre

1. Introduction . . . . .	31
2. Conséquences financières . . . . .	32
3. Conséquences sur l'intégrité . . . . .	33
4. Conséquences pénales . . . . .	34
5. Estimation des coûts liés à une indisponibilité de service ou une perte de données . . . . .	37
5.1 Le coût humain de production . . . . .	38
5.2 La perte de productivité . . . . .	38
5.3 Formule de calcul globale . . . . .	40

## Chapitre 3

### Métriques opérationnelles, risque et impact

1. Introduction . . . . .	41
2. Analyse des risques . . . . .	42
2.1 Le risque . . . . .	43
2.2 Cartographie des risques encourus . . . . .	44
3. Bilan d'impact sur l'activité . . . . .	45
3.1 Ciblage des activités essentielles . . . . .	45
3.2 Analyse d'impact sur les activités . . . . .	46
4. Gestion des risques . . . . .	47
4.1 L'évitement . . . . .	48
4.2 Le transfert . . . . .	49
4.3 L'atténuation . . . . .	50
4.4 L'acceptation . . . . .	50
5. Conciliation du risque avec l'investissement . . . . .	51

Partie 2 : Protection des données

Chapitre 4  
Sécurité informatique

- 1. Objectifs et exigences . . . . . 55
  - 1.1 Les facteurs critiques d'un SMSI . . . . . 56
  - 1.2 Les deux stratégies complémentaires de la sécurité informatique. . . . . 56
  - 1.3 Sécurité préventive . . . . . 57
  - 1.4 Sécurité curative . . . . . 60
  - 1.5 Sécurité informatique et conformité réglementaire. . . . . 62
    - 1.5.1 Modèles de conformité des données. . . . . 62
    - 1.5.2 Auditabilité et traçabilité des données. . . . . 63
  - 1.6 Cycle de vie de la donnée . . . . . 64
    - 1.6.1 Génération de la donnée . . . . . 65
    - 1.6.2 Exploitation de la donnée . . . . . 65
    - 1.6.3 Archivage de la donnée . . . . . 66
    - 1.6.4 Purge de la donnée. . . . . 66
- 2. Règlement général sur la protection des données (RGPD) . . . . . 67
  - 2.1 Objectifs du RGPD . . . . . 67
  - 2.2 Champ d'application matériel et définition . . . . . 68
  - 2.3 Implications majeures du RGPD . . . . . 69
    - 2.3.1 Droit à l'effacement. . . . . 69
    - 2.3.2 Sécurité du traitement . . . . . 71
    - 2.3.3 Principes généraux applicables aux transferts . . . . . 73
  - 2.4 Transfert des données vers les GAFAM . . . . . 74
- 3. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). . . . . 76
  - 3.1 Application extraterritoriale de la loi . . . . . 76
  - 3.2 Une loi inconciliable avec le RGPD . . . . . 77

# 4 --- Protection des données

Disponibilité et résilience des données

4.	Gestion des risques liés à la confidentialité . . . . .	78
4.1	Traitement des données sensibles . . . . .	78
4.2	Contre-mesures à la divulgation des données. . . . .	79
4.2.1	Anonymisation de la donnée . . . . .	80
4.2.2	Pseudonymisation de la donnée . . . . .	82
4.3	Sécurité cryptographique des données . . . . .	83
4.3.1	Chiffrement de la donnée en transit . . . . .	84
4.3.2	Chiffrement de bout en bout de la donnée . . . . .	86
4.3.3	Méthodes cryptographiques . . . . .	87
4.4	Adoption d'une stratégie de souveraineté numérique . . . . .	90
4.4.1	Des enjeux et objectifs versatiles . . . . .	91
4.4.2	Souveraineté numérique et données à caractère personnel . . . . .	91

## Chapitre 5

### Technologies de protection de données

1.	Introduction . . . . .	97
1.1	Un peu d'histoire . . . . .	97
1.2	Une période sombre pour les données. . . . .	98
1.3	Voguent les données. . . . .	99
1.4	Des nouvelles exigences et nouvelles technologies. . . . .	100
1.5	Les familles SPiT et APiT . . . . .	101
1.5.1	APiT (Any Point-in-Time) . . . . .	101
1.5.2	SPiT (Single Point-in-Time) . . . . .	103
1.5.3	La nature des données : un facteur important. . . . .	105
1.5.4	Granularité des données par technologie. . . . .	106
2.	Sauvegarde . . . . .	108
2.1	Un retour en arrière . . . . .	108
2.2	Les trois principes élémentaires. . . . .	108
2.2.1	Automatisation . . . . .	109
2.2.2	Mémorisation . . . . .	109
2.2.3	Isolation . . . . .	110

3.	Réplication	112
3.1	Modes de réplication	113
3.1.1	Réplication synchrone	113
3.1.2	Réplication asynchrone	114
3.2	Techniques de réplication	116
3.2.1	Réplication basée sur le stockage	117
3.2.2	Réplication basée sur l'hôte	118
3.2.3	Réplication basée sur l'hyperviseur	119
3.2.4	Réplication basée sur l'application/base de données	120
3.3	Réplication par le réseau	121
3.3.1	Débit et bande passante de la réplication par le réseau	121
3.3.2	Les trois facteurs limitants	122
3.4	Exemple de réplication intersites	126
3.4.1	Estimation du volume de données à répliquer	127
3.4.2	Qualité de service de la ligne	129
3.4.3	Mesure de la latence intersites avec netperf	130
3.4.4	Mesure de la latence intersites avec ping	132
3.4.5	Incidence de la latence sur le débit effectif	133
3.5	Comparatif des différentes techniques de réplication	135
3.6	Choix de la réplication FC ou IP	137
4.	Protection continue des données (CDP)	138
4.1	Une technologie en avance sur son temps	138
4.2	Fonctionnement et architecture de la CDP	138
4.2.1	Architecture CDP In-Band	139
4.2.2	Architecture CDP Side-Band	140
4.2.3	Architecture CDP Out-of-Band	141
4.3	Protection des données structurées avec la CDP	142
4.4	Avantages de la CDP	143
5.	Cliché instantané (snapshot)	144
5.1	Fournisseur matériel de clichés instantanés	147
5.2	Fournisseur logiciel de clichés instantanés	148
5.3	Clichés instantanés avec une machine virtuelle	148

# 6 Protection des données

Disponibilité et résilience des données

5.4	Méthodes de clichés instantanés . . . . .	149
5.4.1	Copie sur écriture (COW - Copy-on-Write) . . . . .	149
5.4.2	Redirection sur écriture (ROW - Redirect-on-Write) . . . . .	156
5.4.3	Clone ou COFA (Copy on First Access) . . . . .	164
5.5	Comparatif entre les méthodes de clichés instantanés . . . . .	174
5.5.1	Lecture/écriture de bloc de données . . . . .	174
5.5.2	Différences entre cliché instantané et clone . . . . .	176
5.6	Recommandations sur l'utilisation des clichés instantanés . . . . .	182
5.6.1	Estimation de l'espace nécessaire . . . . .	182
5.6.2	Calcul avec de multiples clichés instantanés . . . . .	183
5.6.3	Cas spécifique d'accroissement d'un cliché instantané . . . . .	186
6.	Choix des technologies en réponse aux sinistres . . . . .	187
6.1	Niveau de protection . . . . .	188
6.2	Sauvegarde . . . . .	189
6.3	Cliché instantané . . . . .	191
6.4	Clone . . . . .	193
6.5	Réplication . . . . .	195
6.6	CDP . . . . .	196
7.	Déduplication des données . . . . .	198
7.1	Une méthodologie révolutionnaire . . . . .	198
7.2	Les principes de la déduplication . . . . .	198
7.2.1	La déduplication par segments de données à longueur variable . . . . .	199
7.2.2	La déduplication par blocs de données à longueur fixe . . . . .	204
7.2.3	Comparaison entre segments de données à longueur variable et blocs fixes . . . . .	206
7.3	Efficacité de la déduplication avec les sauvegardes . . . . .	208
7.4	Calcul du coefficient de réduction . . . . .	209
7.4.1	Les facteurs à prendre en compte . . . . .	211
7.4.2	Les deux ennemis : la compression et le chiffrement . . . . .	211
7.4.3	Estimation du taux de réduction . . . . .	212
7.4.4	Calcul du volume de stockage nécessaire . . . . .	213
7.4.5	Conséquences d'un mauvais dimensionnement . . . . .	215

- 7.4.6 Diminution du volume de données dédupliquées . . . . . 225
- 7.5 Déduplication et réplication : le duo gagnant . . . . . 226
  - 7.5.1 Vérification des segments de données à répliquer . . . . . 227
  - 7.5.2 Communication des segments de données manquants 228
  - 7.5.3 Transmission des segments de données manquants . . . 229
  - 7.5.4 Mise à jour des métadonnées . . . . . 230
- 7.6 Bande passante et réplication des données dédupliquées . . . . . 231
  - 7.6.1 Pourquoi les données ne sont-elles pas compressées ? . 232
  - 7.6.2 Comment calculer le volume initial à répliquer ? . . . . . 233
- 7.7 Mise en place de la réplication initiale . . . . . 235
  - 7.7.1 Première méthode de seeding . . . . . 235
  - 7.7.2 Deuxième méthode de seeding . . . . . 236
- 7.8 Méthodes de déduplication . . . . . 237
  - 7.8.1 Déduplication de données à la source . . . . . 237
  - 7.8.2 Déduplication de données à la cible . . . . . 238
  - 7.8.3 Avantages et inconvénients par méthode . . . . . 239
- 7.9 Conclusion et recommandations importantes . . . . . 239
  - 7.9.1 Sécurisation des données dédupliquées . . . . . 240
  - 7.9.2 Intégrité des données dédupliquées . . . . . 240
  - 7.9.3 Conformité des données dédupliquées . . . . . 241

**Chapitre 6**

**Métriques techniques et niveaux de service**

- 1. Les métriques techniques fondamentales . . . . . 243
  - 1.1 Perte de données maximale admissible . . . . . 243
  - 1.2 Délai maximal d'interruption admissible . . . . . 246
- 2. Autres paramètres techniques . . . . . 248
  - 2.1 L'intervalle de fonctionnement en mode dégradé . . . . . 248
  - 2.2 Fenêtre de sauvegarde . . . . . 263
    - 2.2.1 Multiples fenêtres de sauvegarde . . . . . 263
    - 2.2.2 Fenêtre de sauvegarde nulle . . . . . 264
    - 2.2.3 Débit et fenêtre de sauvegarde . . . . . 265

# 8 --- Protection des données

Disponibilité et résilience des données

2.3	Fréquence de sauvegarde . . . . .	265
2.3.1	Erreur d'ajustement de la fréquence de sauvegarde . . . . .	266
2.3.2	Ajustement de la fréquence de sauvegarde . . . . .	268
2.3.3	Autre stratégie avec une fenêtre de sauvegarde nulle . . . . .	270
2.4	Rétention des données . . . . .	271
2.4.1	Cartographie des données . . . . .	271
2.4.2	Localisation et type de support de stockage . . . . .	274
2.4.3	Perception de la rétention des données . . . . .	276
2.4.4	Calcul de la rétention des données . . . . .	279
2.4.5	Politique de rétention des données . . . . .	281
3.	Entre promesse et réalité . . . . .	293
3.1	Entente de niveau de service . . . . .	294
3.1.1	Conseils et principes de rédaction . . . . .	294
3.1.2	Tout est question d'équilibre . . . . .	295
3.1.3	Exemple de SLA . . . . .	296
3.2	Objectifs de niveau de service . . . . .	297
3.3	Indicateurs de niveau de service . . . . .	299

## Chapitre 7

### Infrastructure de sauvegarde

1.	De multiples objectifs . . . . .	301
1.1	Stockage primaire et stockage secondaire . . . . .	302
1.1.1	Le stockage primaire au cœur de l'hébergement des données . . . . .	302
1.1.2	Le stockage secondaire au service de la protection des données . . . . .	302
1.2	Composants élémentaires . . . . .	303
1.2.1	Serveur maître . . . . .	304
1.2.2	Catalogue de sauvegarde . . . . .	304
1.2.3	Nœud de stockage . . . . .	310
1.2.4	Client . . . . .	310
1.2.5	Dispositif de stockage secondaire . . . . .	311



1.3	Les agents de sauvegarde	311
1.4	Flux de sauvegarde	312
1.5	Mécanismes de sauvegarde	314
2.	Introduction aux performances	315
2.1	Les goulots d'étranglement	315
2.2	Performances théoriques et pratiques	316
2.2.1	Limitations liées à l'architecture interne	318
2.2.2	Limitations liées à la topologie des fichiers	320
2.2.3	Limitations liées à l'activité du serveur	321
3.	Architectures de sauvegarde	321
3.1	Sauvegarde réseau	322
3.2	Sauvegarde hors réseau	324
3.3	Sauvegarde NDMP	326
3.4	Sauvegarde hors hôte	328
3.5	Sauvegarde sans agent	330
3.5.1	Architecture SAN sans agent	331
3.5.2	Architecture virtuelle sans agent	334
3.5.3	Architecture réseau sans agent	336
4.	Types de sauvegarde	339
4.1	Sauvegardes totales et incrémentales	340
4.2	Sauvegardes totales et différentielles	342
4.3	Sauvegarde synthétique	344
4.3.1	Précautions à prendre	346
4.3.2	Quelques cas d'usage	347
4.4	Sauvegardes en mode bloc	347
4.5	Sauvegardes instantanées	348
5.	Modes de sauvegarde	349
5.1	Sauvegarde à froid	349
5.2	Sauvegarde à chaud	350

# 10 \_\_\_\_\_ Protection des données

Disponibilité et résilience des données

5.3	Sauvegarde par cliché instantané. . . . .	352
5.3.1	Composants du service VSS . . . . .	353
5.3.2	Processus de cliché instantané en environnement physique	355
5.3.3	Processus de cliché instantané en environnement virtuel . . . . .	358
5.3.4	Cohérence d'une sauvegarde par cliché instantané . . . . .	358
5.3.5	Cliché instantané sans mise en cohérence. . . . .	359
5.3.6	Cliché instantané avec mise en cohérence. . . . .	361
5.4	Techniques de parallélisation . . . . .	361
5.4.1	Parallélisation des tâches de sauvegarde. . . . .	361
5.4.2	Parallélisation des flux de sauvegarde . . . . .	363
6.	Supports de stockage secondaire . . . . .	364
6.1	Stockage sur bande magnétique . . . . .	364
6.1.1	Le consortium LTO . . . . .	365
6.1.2	Principales caractéristiques techniques . . . . .	365
6.1.3	Feuille de route de la technologie LTO . . . . .	368
6.1.4	Fonctionnalité LTO-7 type M . . . . .	371
6.1.5	Fonctionnalité WORM . . . . .	372
6.1.6	Fonctionnalité de chiffrement matériel AES-256-GCM . . . . .	373
6.1.7	Fonctionnalité LTFS . . . . .	374
6.1.8	Cartouche de nettoyage . . . . .	376
6.1.9	Dispositifs de stockage sur bande magnétique . . . . .	378
6.1.10	Dimensionnement d'un dispositif de stockage sur bande magnétique. . . . .	379
6.1.11	Comparatif des dispositifs de stockage sur bande magnétique. . . . .	381
6.1.12	Fonctionnement d'une robotique de bandes . . . . .	382
6.1.13	Partition et partage d'une robotique de bandes. . . . .	383
6.1.14	Pilotage d'un dispositif de stockage sur bande magnétique. . . . .	384
6.1.15	Mise hors ligne des cartouches . . . . .	386
6.1.16	Isolation totale des données (Air Gap). . . . .	387

6.2	Stockage sur disque . . . . .	389
6.2.1	Comparatif entre les technologies SAS et SATA. . . . .	390
6.2.2	Dimensionnement d'un dispositif de stockage sur disque. . . . .	392
6.2.3	Dispositif de type dépôt de sauvegarde . . . . .	395
6.2.4	Système de robotique virtuelle . . . . .	395
6.2.5	Robotique de cartouches virtuelles. . . . .	396
6.2.6	Comparatif entre les trois dispositifs . . . . .	396
6.3	Comparatif des sauvegardes D2T et D2D . . . . .	397
6.3.1	Performances . . . . .	397
6.3.2	Stockage . . . . .	399
6.3.3	Coûts . . . . .	401
6.4	Niveaux de stockage. . . . .	405
6.5	Informatique en nuage. . . . .	407
6.5.1	Les cinq concepts clés . . . . .	409
6.5.2	Un changement de paradigme pour la protection des données. . . . .	410
6.5.3	Modèles techniques. . . . .	410
6.5.4	Modèle de responsabilité partagée . . . . .	411
6.5.5	Sauvegarde vers le nuage. . . . .	414
6.5.6	Sauvegarde dans le nuage . . . . .	415
6.5.7	Considérations importantes . . . . .	416
6.6	Stockage objet et Erasure Coding . . . . .	417
6.6.1	Caractéristiques du stockage objet. . . . .	417
6.6.2	Algorithme d'Erasure Coding . . . . .	418
6.6.3	Approche Scale-Up et Scale-Out . . . . .	418
6.6.4	Dimensionnement d'une solution de stockage objet . .	420
6.6.5	Fonctionnalité de stockage immuable . . . . .	422

### Chapitre 8

#### Protection contre le sinistre

1. Seven Tiers of Disaster Recovery . . . . .	423
2. Objectifs de la classification . . . . .	423
3. De l'importance de l'externalisation des données . . . . .	424
4. Niveaux de continuité d'activité . . . . .	424
4.1 Segment inférieur : sauvegarde et restauration . . . . .	425
4.2 Segment intermédiaire : récupération rapide des données . . . . .	426
4.3 Segment supérieur : disponibilité continue des données . . . . .	426
5. Description des niveaux de continuité d'activité . . . . .	427
5.1 Tier 1 : Data Backup but no « Hot Site » . . . . .	427
5.2 Tier 2 : Data Backup and « Hot Site » . . . . .	429
5.3 Tier 3 : Electronic Vaulting . . . . .	430
5.4 Tier 4 : Point-In-Time Copies . . . . .	432
5.5 Tier 5 : Software Replication - Transaction Integrity . . . . .	434
5.6 Tier 6 : Storage Mirroring (with or without Automation) . . . . .	435
5.7 Tier 7 : Site Mirroring with high Automation and Integration . . . . .	436
6. Choisir entre un PCA et un PRA . . . . .	437

## Partie 3 : Disponibilité et résilience des données

### Chapitre 9

#### Restauration des données

1. L'opération de la dernière chance . . . . .	443
2. Mécanisme de restauration . . . . .	444
3. Sauvegarder, c'est bien, mais restaurer, c'est mieux . . . . .	445
4. Questions indispensables pour restaurer sereinement ses données . . . . .	446
4.1 En quoi le facteur humain influence-t-il la restauration des données ? . . . . .	446

- 4.2 Pourquoi ne faut-il pas sauvegarder toutes les données ? . . . . 449
- 4.3 Quel support de stockage doit-on utiliser  
pour restaurer rapidement des données ? . . . . . 450
- 4.4 Les copies de sauvegarde sont-elles en sécurité ? . . . . . 451
- 4.5 De combien de copies de sauvegarde  
convient-il de disposer ? . . . . . 452
- 4.6 À quelle fréquence doit-on sauvegarder les données ? . . . . . 452
- 4.7 Quelle durée de conservation doit-on avoir  
pour les copies de sauvegarde ? . . . . . 454
- 4.8 Quel est le coût associé à la sauvegarde des données ? . . . . . 455
- 4.9 Quel est le délai de restauration de mes données ? . . . . . 457
- 5. Stratégies de restauration . . . . . 459
  - 5.1 Restauration de la dernière version . . . . . 460
  - 5.2 Restauration d'une version spécifique . . . . . 461
  - 5.3 Restauration à un instant dans le temps . . . . . 462
  - 5.4 Restauration croisée . . . . . 465
- 6. Comportement lors de la restauration . . . . . 466
  - 6.1 Scénarios de restauration de données . . . . . 466

**Chapitre 10**  
**Bonnes pratiques de l'industrie**

- 1. Introduction . . . . . 469
- 2. Supervision de l'infrastructure . . . . . 469
  - 2.1 Diminuer les risques encourus . . . . . 470
  - 2.2 Critères principaux de la supervision . . . . . 471
- 3. Édition de rapports . . . . . 473
  - 3.1 Édition de rapports statistiques . . . . . 473
  - 3.2 Édition de rapports de tendance . . . . . 474
- 4. Gestion des incidents . . . . . 474

# 14 \_\_\_\_\_ Protection des données

Disponibilité et résilience des données

5.	Stratégie Disk-to-Disk-to-X	476
5.1	Stratégie D2D2T	477
5.2	Stratégie D2D2D	478
5.3	Stratégie D2D2C	478
6.	Obsolescence des supports de stockage secondaire	479
7.	Règle de sauvegarde 3-2-1	481
7.1	Règles relatives aux différentes copies	481
7.2	Règle de sauvegarde 3-2-1-1	483
8.	Réalisation de tests réguliers	484
8.1	Définition du périmètre et des objectifs	485
8.2	Planification	487
8.3	Fréquence	488

## Chapitre 11

### Disponibilité et résilience des données

1.	Obstacles en termes de communication dans l'entreprise	489
1.1	Introduction	489
1.2	Iceberg de l'ignorance	490
2.	Élaboration d'une politique de protection des données	491
2.1	En route vers une bonne gouvernance	491
2.2	Étapes de mise en œuvre	492
2.2.1	Cartographie	492
2.2.2	Périmètre et besoins	493
2.2.3	Risques et conséquences	494
2.2.4	Stratégie de continuité d'activité	495
2.2.5	Implémentation et appropriation	495
	Mot de la fin	497
	Index	501

**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