

# Sommaire

<b>Du même auteur</b> .....	<b>XI</b>
<b>Présentation de l'auteur</b> .....	<b>XV</b>
<b>Note de l'éditeur</b> .....	<b>XVII</b>
<b>Préface</b> .....	<b>XIX</b>
<b>Avant-propos</b> .....	<b>XXI</b>
<b>Introduction</b> .....	<b>XXIII</b>
<b>Rappel sur les éditions précédentes</b> .....	<b>XXV</b>

## Partie I

### Sécurité et information

<b>Clé n° 1 La sécurité, qu'est-ce que c'est ?</b> .....	<b>3</b>
1.1 La définition de la sécurité .....	3
1.2 Les composantes de la sécurité .....	5
1.3 Les acteurs de la sécurité .....	5
1.4 Monsieur Sécurité .....	7
<b>Clé n° 2 L'information, qu'est-ce que c'est ?</b> .....	<b>9</b>
2.1 La définition de l'information .....	9
2.2 La définition de la donnée .....	10
2.3 Le système d'information .....	11
2.4 Le traitement de l'information .....	11
2.5 Le traitement automatisé de l'information .....	12

<b>Clé n° 3 Structure des normes ISO/CEI 27000</b> .....	<b>13</b>
3.1 Structure normative .....	14
3.2 ISO/CEI 27000:2016 .....	16
3.3 ISO/CEI 27001:2013 .....	17
3.4 ISO/CEI 27002:2013 .....	19
3.5 ISO/CEI 27003:2010 .....	20
3.6 ISO/CEI 27004:2009 .....	22
3.7 ISO/CEI 27005:2011 .....	23
3.8 ISO/CEI FDIS 27011 .....	25
<b>Clé n° 4 Exigences de la norme ISO/CEI 27001:2013</b> .....	<b>27</b>
4.1 L'organisation de la norme .....	27
4.2 Le contexte de l'organisme (§ 4 de la norme) .....	28
4.3 Le <b>leadership</b> (§ 5 de la norme) .....	30
4.4 Planification (§ 6 de la norme).....	31
4.5 Support (§ 7 de la norme) .....	33
4.6 Fonctionnement (§ 8 de la norme) .....	36
4.7 Évaluation des performances .....	(§ 9 de la norme) 37
4.8 Amélioration (§ 10 de la norme).....	39
<b>Clé n° 5 La déclaration d'applicabilité</b> .....	<b>41</b>
5.1 Rôle de la Déclaration d'applicabilité (DdA) .....	41
5.2 Thèmes « sécurité » imposés .....	42
5.3 Les sous-thèmes sécurité imposés.....	43
5.4 Comment y répondre ? .....	44
<b>Clé n° 6 La gestion des actifs</b> .....	<b>47</b>
6.1 Qu'est-ce qu'un actif ? .....	47
6.2 Comment identifier un actif ? .....	48
6.3 Comment gérer un actif ?.....	50
<b>Clé n° 7 Les processus de gestion des risques</b> .....	<b>51</b>
7.1 Qu'est-ce qu'un risque ? .....	51
7.2 Comment identifier un risque ? .....	52
7.3 Typologie d'impacts sur les actifs – Notion de « DIC » .....	54
7.4 Analyser et évaluer les risques .....	58

7.5 Déterminer les risques acceptables.....	61
7.6 Traiter les risques.....	62
7.7 Approuver les risques résiduels.....	63
7.8 Le management des risques.....	63
<b>Clé n° 8 Les incidents de sécurité.....</b>	<b>65</b>
8.1 Un incident, qu'est-ce que c'est ? .....	65
8.2 Les facteurs déclenchant d'un incident.....	66
8.3 Les caractéristiques des incidents.....	67
8.4 Le traitement des incidents.....	69
8.5 Assurer la continuité de l'activité.....	73
<b>Clé n° 9 Les exigences d'un système de gestion.....</b>	<b>79</b>
9.1 Exigences d'un système de gestion.....	80
9.2 Le contexte de l'organisation (§ 4 de la norme).....	82
9.3 <i>Leadership</i> (§ 5 de la norme).....	84
9.4 Planification (§ 6 de la norme).....	85
9.5 Support (§ 7 de la norme).....	87
9.6 Fonctionnement (§ 8 de la norme).....	88
9.7 Évaluation (§ 9 de la norme).....	89
9.8 Amélioration (§ 10 de la norme).....	91
<b>Clé n° 10 Le processus de certification.....</b>	<b>93</b>
10.1 Accréditation et certification.....	93
10.2 Les acteurs, les instances.....	94
10.3 Les catégories de certifications.....	95
10.6 L'audit initial de certification.....	97
<b>Conclusion.....</b>	<b>99</b>

## Partie II

### Fiches techniques

<b>Fiche technique n° 1 : vocabulaire et définitions.....</b>	<b>103</b>
<b>Fiche technique n° 2 : sommaire de la norme ISO/CEI 27000:2016.....</b>	<b>113</b>
<b>Fiche technique n° 3 : sommaire de la norme ISO/CEI 27001:2013.....</b>	<b>117</b>

<b>Fiche technique n° 4 : sommaire de la norme ISO/CEI 27002:2013</b> .....	<b>119</b>
<b>Fiche technique n° 5 : sommaire de la norme ISO/CEI 27005:2011</b> .....	<b>123</b>
<b>Fiche technique n° 6 : définition du domaine d'application</b> .....	<b>127</b>
<b>Fiche technique n° 7 : thèmes de la déclaration d'applicabilité</b> .....	<b>129</b>
<b>Fiche technique n° 8 : exemples de catégories d'actifs</b> .....	<b>131</b>
<b>Fiche technique n° 9 : exemple d'inventaire des actifs</b> .....	<b>133</b>
<b>Fiche technique n° 10 : types de menaces</b> .....	<b>135</b>
<b>Fiche technique n° 11 : sources de menaces humaines</b> .....	<b>137</b>
<b>Fiche technique n° 12 : vulnérabilités et menaces</b> .....	<b>139</b>
<b>Fiche technique n° 13 : la disponibilité</b> .....	<b>143</b>
<b>Fiche technique n° 14 : les niveaux de gravité</b> .....	<b>145</b>
<b>Fiche technique n° 15 : probabilité des risques</b> .....	<b>147</b>
<b>Fiche technique n° 16 : criticité et acceptabilité des risques</b> .....	<b>149</b>
<b>Fiche technique n° 17 : la criticité des risques</b> .....	<b>151</b>
<b>Fiche technique n° 18 : activités de traitement des risques</b> .....	<b>153</b>
<b>Fiche technique n° 19 : exemple de tableau/plan de traitement des risques</b> .....	<b>155</b>
<b>Fiche technique n° 20 : le processus de gestion du risque en matière de sécurité de l'information</b> .....	<b>157</b>
<b>Fiche technique n° 21 : management du risque</b> .....	<b>159</b>
<b>Fiche technique n° 22 : exemple de pondération de probabilité d'un danger</b> .....	<b>161</b>
<b>Fiche technique n° 23 : exemple de pondération de la fréquence d'exposition à un danger</b> .....	<b>163</b>
<b>Fiche technique n° 24 : la gestion des incidents</b> .....	<b>165</b>
<b>Fiche technique n° 25 : le plan de reprise (continuité)</b> .....	<b>167</b>
<b>Fiche technique n° 26 : le processus</b> .....	<b>169</b>
<b>Fiche technique n° 27 : le manuel de management de la sécurité de l'information</b> .....	<b>173</b>

<b>Fiche technique n° 28 : description de la fonction de Monsieur Sécurité – <i>Risk manager</i></b> .....	<b>175</b>
<b>Fiche technique n° 29 : l'amélioration continue</b> .....	<b>177</b>
<b>Fiche technique n° 30 : la gestion de l'amélioration</b> .....	<b>179</b>
<b>Fiche technique n° 31 : quelques méthodes pour les risques</b> .....	<b>181</b>
<b>Fiche technique n° 32 : dix règles d'or pour la sécurité informatique</b> .....	<b>183</b>
<b>Normes et standards</b> .....	<b>185</b>
<b>Sites Internet</b> .....	<b>189</b>

# Introduction

La notion de sécurité est un terme très vaste qui, en fonction du contexte ou des interlocuteurs concernés, recouvre des éléments bien différents.

Les hommes sont placés dans un environnement. Des interactions existent entre les individus que nous sommes et la nature (la terre, l'eau et l'air) qui nous entoure. Ces relations sont généralement régies par un certain équilibre. Mais l'équilibre peut être amené à basculer dans un sens ou dans l'autre. Parfois, il peut être rompu brutalement, on parle alors de cataclysme naturel (tremblement de terre, inondation, éruption volcanique, *tsunami*, tornade, cyclone, etc.). Parfois, le phénomène est plus lent (tectonique des plaques, réchauffement climatique, etc.).

L'équilibre peut aussi être mis en péril à la suite de l'activité humaine. Soit sournoisement (pollution, appauvrissement des sols, épuisement de ressources naturelles), soit brutalement : on parle alors d'accident (explosion, incendie, transport/circulation, etc.).

Dans nos civilisations développées technologiquement, les sources de dangers réels ou potentiels sont accentuées du fait de l'utilisation de moyens (machines faites par la main de l'homme) qui, par exemple, augmentent la vitesse ou impactent un plus grand nombre de personnes. Le moindre accident, qu'il soit le résultat de phénomènes naturels ou le résultat de l'intervention humaine, peut entraîner des conséquences importantes. À tel point que s'est même développé un principe dit « de précaution » qui peut aller jusqu'à refuser des actions par peur des conséquences.

De plus en plus, nous exprimons un besoin de sécurité qui rassure et donne la force d'agir. Sinon, c'est l'immobilisme et le refus d'avancer qui conduit à la mort.

Dans le domaine des technologies de l'information, nous sommes dans le domaine de l'immatériel et du virtuel. Les objets manipulés étant invisibles, les dangers sont plus difficiles à appréhender. Par contre, les conséquences sont bien réelles et souvent plus lourdes de conséquences que dans le monde réel. Les mesures de précaution à imaginer et à mettre en œuvre nécessitent un niveau d'abstraction important.

Pour répondre à ces besoins de « confiance », des méthodes et des normes sont apparues, gage de maturité. La démarche méthodologique proposée dans cet ouvrage contribue à cet objectif d'amélioration de la sécurité de l'information.

Le présent ouvrage comporte deux parties :

- ▶ La première partie développe les éléments clés qui permettent de :
  - ▼ comprendre les mécanismes de la norme internationale ISO/CEI 27001 dans sa version 2013 ;
  - ▼ de mettre en place dans votre organisation les réponses aux exigences de la norme et de son Annexe A (normative) ;
  - ▼ d'aller jusqu'à la certification, si tel est votre projet.
- ▶ La deuxième partie comporte 32 fiches techniques qui accompagnent la démarche méthodologique et qui sont autant d'outils pratiques pour une mise en œuvre efficace.