الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

ISO/IEC 27002

Comparatif entre la version 2013 et la version 2005

Évolutions du document

Version	Date	Nature des modifications	Auteur
1.0	22/07/2014	Version initiale	ANSI

Critère de diffusion

Public	Interne	Diffusion restreinte	Hautement Confidentiel

Sommaire

1. Introduction

La norme ISO/IEC 27002 est un code de bonne pratique pour le management de la sécurité de l'information. C'est un document consultatif générique et non pas une spécification formelle comme la norme ISO/IEC 27001. Elle recommande des mesures de sécurité de l'information portant sur les objectifs de contrôle de sécurité de l'information résultant des risques pour la confidentialité, l'intégrité et la disponibilité des informations. Les organisations qui adoptent la norme ISO/IEC 27002 doivent évaluer leurs propres risques de sécurité de leurs informations, clarifier leurs objectifs de contrôle et appliquer des mesures appropriées (ou même d'autres formes de traitement des risques) en utilisant la norme à titre indicatif.

2. Relation avec l'ISO/IEC 27001

La norme ISO/IEC 27001 définit formellement les exigences requises pour un système de management de la sécurité de l'information (SMSI). Elle utilise la norme ISO/IEC 27002 pour indiquer les mesures appropriés de sécurité de l'information au sein du SMSI, mais comme l'ISO/IEC 27002 est simplement un code de bonne pratique/lignes directrices plutôt qu'une norme de certification, les organismes sont libres de choisir et de mettre en œuvre d'autres mesures, voire adopter d'une manière alternative un ensemble complet de mesures de sécurité de l'information comme ils l'entendent. ISO/IEC 27001 comprend un résumé (un peu plus que les titres de chapitre en fait) des mesures de la norme ISO/IEC 27002 à l'annexe A. Dans la pratique, la plupart des organismes qui adoptent la norme ISO/IEC 27001 adoptent également la norme ISO/IEC 27002.

3. Contenu de la norme ISO/IEC 27002 version 2013 par rapport à la version 2005

ISO/27002 : 2005	ISO/27002 : 2013
11 chapitres	14 chapitres
39 objectifs	35 objectifs
133 mesures	114 mesures

3.1. Les chapitres

Les 14 chapitres de la norme constituant les clauses de contrôle de sécurité précisent les objectifs de contrôle et les mesures de sécurité. Chaque chapitre est représenté par une structure standard : un ou plusieurs paragraphes de premier niveau, chacun indiquant un objectif de contrôle, et chaque objectif de contrôle est pris en charge à son tour par une ou des mesures plus indiquées, chaque mesure est suivie par des directives de mise en œuvre associées, et dans certains cas, par des notes explicatives supplémentaires.

a. Structure des chapitres

ISO/27002 :2005	ISO/27002 :2013
	5. Politiques de sécurité de l'information
5. Politique de sécurité	6. organisation de la sécurité de l'information
6. Organisation de la sécurité de l'information	7. Sécurité liée aux ressources humaines
	8. Gestion des actifs

7. Gestion des actifs 8. Sécurité liée aux ressources humaines 9. Sécurité physique et environnementale	9. Contrôle d'accès
	10. Cryptographie
	11. Sécurité physique et environnementale
10. Gestion de l'exploitation et des télécommunications	12. Sécurité liée à l'exploitation 13. Sécurité des télécommunications
11. Contrôle d'accès	
12. Acquisition, développement et maintenance des systèmes d'information	14. Acquisition, développement et maintenance des systèmes
	15. Relations avec les fournisseurs
13. Gestion des incidents liés à la sécurité de l'information	16. Gestion des incidents liés à la sécurité de l'information
14. Gestion de la continuité de l'activité	17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
15 Conformité	18. Conformité

b. Changements

- Le chapitre « **Acquisition, développement et maintenance des systèmes d'information** » est scindé en deux pour mieux mettre en évidence le sujet de la **cryptographie**
- Le chapitre « **Gestion de l'exploitation et des télécommunications** » est divisé en trois (« **Sécurité de l'exploitation** », « **Sécurité des télécommunications** », « **Relations avec les fournisseurs** ») pour mieux clarifier les périmètres de responsabilités d'acteurs bien distincts.
- Le chapitre 5. a changé de sens : Politiques de sécurité de l'information et non plus « Politique »
    - Inclut la politique de sécurité de l'information de l'ancien chapitre 5,
    - Demande la déclinaison de la politique de sécurité de l'information en politiques par thème
- Le chapitre 14 (Gestion de la continuité de l'activité), qui a changé de sens, est remplacé par le chapitre 17 (Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité)
    - Titre du chapitre : objectif 1 de l'ancien chapitre (14.1),
    - Changement total de l'esprit du chapitre : attention portée sur la continuité de la sécurité et non plus sur la continuité de l'activité,
    - Ajout d'un objectif (Redondances) pour assurer la disponibilité des moyens de traitement de l'information,
    - Renvoi vers les normes ISO 22301, 22313 et 27031
- Le chapitre 13 (Gestion des incidents liés à la sécurité de l'information) est remplacé par le chapitre 16 (même titre)
    - La gestion des incidents n'est plus dans la norme ISO 27001 :2013 (ISO 27001 :2005 : 3.6, 4.2.2, 4.2.3, 4.3.3)
    - Fusion de deux objectifs en un seul,
    - Deux mesures ont été ajoutées :
        - Traitement des incidents conformément aux procédures (était dans l'ISO 27001:2005 4.2.2 h)),
        - Appréciation des événements liés à la sécurité et leur classification en incidents (n'était pas dans l'ISO 27001:2005)

- L'objectif 12.3 (Cryptographie) est mis à part dans un chapitre spécifique (10)
    - Modification de l'objectif
        - On ne parle plus de l'utilisation des moyens cryptographique pour protéger l'information
        - On garantit l'utilisation correcte et efficace de la cryptographie
    - Politique de gestion des clés
        - Dans la version 2005 : politique pour favoriser l'utilisation des techniques cryptographiques,
        - Dans la version 2013 : politique sur l'utilisation, la protection et la durée de vie des clés
    - Ajout de l'objectif « authentification » dans les directives de mise en œuvre de la mesure « 10.1.1 Politique sur l'utilisation des contrôles cryptographiques »
    - Gestion des clés
        - Suppression de l'explication de la différence entre algorithme « symétrique » et « asymétrique »

3.2. Les objectifs de contrôle de sécurité

Ces objectifs sont formulés de manière plus synthétique, ce qui offre une plus grande souplesse dans l'implémentation.

Exemple

ISO/27002 :2005	ISO/27002 :2013
6.1 Organisation interne **Objectif:** gérer la sécurité de l'information au sein de l'organisme. Un cadre de gestion devrait être créé pour initier et contrôler la mise en œuvre de la sécurité de l'information au sein de l'organisation. La direction doit approuver la politique de sécurité de l'information, attribuer des rôles de sécurité et coordonner et examiner la mise en œuvre de la sécurité dans toute l'organisation. Si nécessaire, une source spécialisée en conseil de sécurité de l'information doit être établie et mise à disposition au sein de l'organisme. Des contacts avec des spécialistes ou des groupes de sécurité externes, y compris les autorités compétentes, doivent être développés pour suivre les tendances dans le secteur, surveiller les normes et les méthodes d'évaluation et fournir des points de liaison appropriés lors de la manipulation des incidents liés à la sécurité de l'information.	**6.1 Organisation interne** **Objectif :** Etablir un cadre de gestion pour initier et contrôler la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisme.

Une approche multidisciplinaire de la sécurité de l'information doit être encouragée.	
7.1 Responsabilités relatives aux actifs **Objectif:** atteindre et maintenir une protection adéquate des actifs de l'organisation. Tous les actifs doivent être pris en compte et avoir un propriétaire désigné. Les propriétaires doivent être identifiés pour tous les actifs et la responsabilité pour le maintien de contrôles appropriés doit être attribuée. La mise en œuvre des contrôles spécifiques peut être déléguée, le cas échéant, par le propriétaire, mais le propriétaire reste responsable de la protection adéquate des actifs.	**8.1 Responsabilités relatives aux actifs** **Objectif:** identifier les actifs de l'organisation et définir les responsabilités de protection appropriées.
12.1 Exigences de sécurité applicables aux systèmes d'information **Objectif :** S'assurer que la sécurité est une partie intégrante des systèmes d'information. Les systèmes d'information comprennent les systèmes d'exploitation, l'infrastructure, les applications métier, les progiciels, les services et les applications développés par les utilisateurs. La conception et la mise en œuvre du système d'information supportant le processus d'entreprise peut être crucial pour la sécurité. Les exigences de sécurité doivent être identifiées et convenues avant l'élaboration et / ou la mise en œuvre des systèmes d'information. Toutes les exigences de sécurité doivent être identifiés lors de la phase d'expression des besoins d'un projet et justifiées, convenues et documentées dans le cadre de la conception générale du système d'information.	**14.1 Exigences de sécurité applicables aux systèmes d'information** **Objectif :** S'assurer que la sécurité de l'information fait partie intégrante des systèmes d'information sur l'ensemble du cycle de vie. Cela inclut également les exigences pour les systèmes d'information qui fournissent des services sur les réseaux publics.
15.3 Prises en compte de l'audit du système d'information **Objectif :** Optimiser l'efficacité et réduire le plus possible l'interférence avec le/du processus d'audit du système d'information. Il devrait y avoir des contrôles pour protéger les systèmes opérationnels et les outils d'audit lors des audits des systèmes d'information.	**12.7 Prises en compte de l'audit du système d'information** **Objectif :** minimiser l'impact des activités d'audit sur les systèmes opérationnels

La protection est également nécessaire pour préserver l'intégrité et prévenir la mauvaise utilisation des outils d'audit.	

3.3. Les mesures de sécurité

Chacun des objectifs de contrôle de sécurité est pris en charge par au moins une mesure, soit un total de 114 (contre 133 pour la version 2005). Cependant, le chiffre global est quelque peu trompeur, car les directives de mise en œuvre recommandent de nombreuses mesures réelles.

La mesure relative à la « Messagerie électronique 13.2.3 », par exemple, est soutenue par la protection des messages contre les accès non autorisés, la disponibilité et la fiabilité du service, les considérations légales et réglementaires (par exemple les exigences pour l'utilisation de signatures électroniques), l'obtention de l'autorisation avant l'utilisation de services publiques externes tels que la messagerie instantanée, les réseaux sociaux ou le partage de fichiers, et l'implémentation de niveaux élevés d'authentification pour le contrôle d'accès à partir des réseaux publiques.

La formulation tout au long de la norme indique clairement ou implique que cette liste de mesures n'est pas un ensemble exhaustif. Un organisme peut avoir des objectifs de contrôle de sécurité de l'information légèrement différents ou complètement nouveaux, nécessitant d'autres mesures à la place de ou en plus de celles qui sont énoncées dans la norme.

4. Résumé des changements

ISO/27002 :2005	ISO/27002 :2013
5. SECURITY POLICY 5.1 INFORMATION SECURITY POLICY 5.1.1 Information security policy document 5.1.2 Review of the information security policy	5. INFORMATION SECURITY POLICIES (titre modifié) 5.1 Management direction for information security (titre modifié) 5.1.1 Policies for information security (titre modifié) 5.1.2 Review of the Policies for information security (titre modifié)
6. ORGANIZATION OF INFORMATION SECURITY 6.1 INTERNAL ORGANIZATION 6.1.1 Management commitment to information security (supprimé) 6.1.2 Information security co-ordination (supprimé) 6.1.3 Allocation of information security responsibilities 10.1.3 Segregation of duties (déplacé) 6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 11.7 MOBILE COMPUTING AND TELEWORKING (déplacé) 11.7.1 Mobile computing and communications 11.7.2 Teleworking	6. ORGANIZATION OF INFORMATION SECURITY 6.1 INTERNAL ORGANIZATION 6.1.1 Information security roles and responsibilities (titre modifié) 6.1.2 Segregation of duties (déplacé) 6.1.3 Contact with authorities 6.1.4 Contact with special interest groups 6.1.5 Information security in project management (nouveau) 6.2 MOBILE DEVICES AND TELEWORKING (déplacé et titre modifié) 6.2.1 Mobile device policy (titre modifié) 6.2.2 Teleworking
8. HUMAN RESOURCE SECURITY 8.1 PRIOR TO EMPLOYMENT 8.1.1 Roles and responsibilities (supprimé)	7. HUMAN RESOURCE SECURITY 7.1 PRIOR TO EMPLOYMENT

8.1.2 Screening 8.1.3 Terms and conditions of employment 8.2 DURING EMPLOYMENT 8.2.1 Management responsibilities 8.2.3 Information security awareness, education and training 8.2.3 Disciplinary process 8.3 TERMINATION OR CHANGE OF EMPLOYMENT 8.3.1 Termination responsibilities	7.1.1 Screening 7.1.2 Terms and conditions of employment 7.2 DURING EMPLOYMENT 7.2.1 Management responsibilities 7.2.3 Information security awareness, education and training 7.2.3 Disciplinary process 7.3 TERMINATION AND CHANGE OF EMPLOYMENT (titre modifié) 7.3.1 Termination or change of employment responsibilities (titre modifié)
7. ASSET MANAGEMENT 7.1 RESPONSIBILITY FOR ASSETS 7.1.1 Inventory of assets 7.1.2 Ownership of assets 7.1.3 Acceptable use of assets 8.3.2 Return of assets (déplacé) 7.2 INFORMATION CLASSIFICATION 7.2.1 Classification guidelines 7.2.2 Information labeling and handling 10.7 MEDIA HANDLING (déplacé) 10.7.1 Management of removable media 10.7.2 Disposal of media 10.7.3 Information handling procedures 10.7.4 Security of system documentation (supprimé)	8. ASSET MANAGEMENT 8.1 RESPONSIBILITY FOR ASSETS 8.1.1 Inventory of assets 8.1.2 Ownership of assets 8.1.3 Acceptable use of assets 8.1.4 Return of assets (déplacé) 8.2 INFORMATION CLASSIFICATION 8.2.1 Classification of information (titre modifié) 8.2.2 Labeling of information (titre modifié) 8.2.3 Handling of assets (nouveau) 8.3 MEDIA HANDLING (déplacé) 8.3.1 Management of removable media 8.3.2 Disposal of media 8.3.3 Physical media transfer (titre modifié)
11. ACCESS CONTROL 11.1 BUISINESS REQUIREMENT FOR ACCESS CONTROL 11.1.1 Access control policy 11.2 USER ACCESS MANAGEMENT 11.2.1 User registration 11.2.2 Privilege management 11.2.3 User password management (déplacé) 11.2.4 Review of user access rights 8.3.3 Removal of access rights (déplacé) 11.3 USER RESPONSIBILITIES 11.3.1 Password use (supprimé) 11.5 OPERATING SYSTEM ACCESS CONTROL 11.6.1 Information access restriction (déplacé) 11.5.1 Secure log-on procedures 11.5.2 User identification and authentication (supprimé) 11.5.3 Password management system 11.5.4 Use of system utilities 12.4.3 Access control to program source code (déplacé) 11.5.5 Session time-out (supprimé) 11.5.6 Limitation of connection time (supprimé) 11.6 APPLICATION AND INFORMATION ACCESS CONTROL (supprimé) 11.6.2 Sensitive system isolation (supprimé)	9. ACCESS CONTROL 9.1 BUISINESS REQUIREMENTS OF ACCESS CONTROL (titre modifié) 9.1.1 Access control policy 9.1.2 Access to networks and network services (nouveau) 9.2 USER ACCESS MANAGEMENT 9.2.1 User registration and de-registration (titre modifié) 9.2.2 User access provisioning (nouveau) 9.2.3 Management of privileged access rights (titre modifié 9.2.4 User password management (déplacé) 9.2.5 Review of user access rights 9.2.6 Removal or adjustment of access rights (déplacé et titre modifié) 9.3 USER RESPONSIBILITIES 9.3.1 Use of secret authentication information (nouveau) 9.4 SYSTEM AND APPLICATION ACCESS CONTROL (titre modifié) 9.4.1 Information access control (déplacé et titre modifié) 9.4.2 Secure log-on procedures 9.4.3 Password management system 9.4.4 Use of privileged utility programs (titre modifié) 9.4.5 Access control to program source code (déplacé)
12.3 CRYPTOGRAPHIC CONTROLS (déplacé) 12.3.1 Policy on the use of cryptographic controls 12.3.2 Key management	10. CRYPTOGRAPHY (nouveau) 10.1 CRYPTOGRAPHIC CONTROLS 10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management
9. PHYSICAL AND ENVIRONMENTAL SECURITY	11. PHYSICAL AND ENVIRONMENTAL SECURITY

9.1 SECURE AREAS 9.1.1 Physical security perimeter 9.1.2 Physical entry controls 9.1.3 Securing offices, rooms and facilities 9.1.4 Protecting against external and environmental threats 9.1.5 Working in secure areas 9.1.6 Public access, delivery and loading areas 9.2 EQUIPMENT SECURITY 9.2.1 Equipment siting and protection 9.2.2 Supporting utilities 9.2.3 Cabling security 9.2.4 Equipment maintenance 9.2.7 Removal of property (déplacé) 9.2.5 Security of equipment off-premises 9.2.6 Secure disposal or re-use of equipment 11.3.2 Unattended user equipment (déplacé) 11.3.3 Clear desk and clear screen policy (déplacé)	11.1 SECURE AREAS 11.1.1 Physical security perimeter 11.1.2 Physical entry controls 11.1.3 Securing offices, rooms and facilities 11.1.4 Protecting against external and environmental threats 11.1.5 Working in secure areas 11.1.6 Delivery, and loading areas (titre modifié) 11.2 EQUIPMENT (titre modifié) 11.2.1 Equipment siting and protection 11.2.2 Supporting utilities 11.2.3 Cabling security 11.2.4 Equipment maintenance 11.2.5 Removal of assets (déplacé et titre modifié) 11.2.6 Security of equipment and assets off-premises (titre modifié) 11.2.7 Secure disposal or re-use of equipment 11.2.8 Unattended user equipment (déplacé) 11.2.9 Clear desk and clear screen policy (déplacé)
10. OPERATIONS SECURITY 10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 10.1.1 Documented operating procedures 10.1.2 Change management 10.3.1 Capacity management (déplacé) 10.1.4 Separation of development, test, and operational facilities 10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 10.4.1 Controls against malicious code 10.4.2 Controls against mobile code (combiné) 10.5 BACKUP 10.5.1 Information backup 10.10 MONITORING 10.10.1 Audit logging 10.10.2 Monitoring system use (combiné) 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging (supprimé) 10.10.6 Clock synchronization 12.4.1 Control of operational software (déplacé) 12.6 TECHNICAL VULNERABILITY MANAGEMENT (déplacé) 12.6.1 Control of technical vulnerabilities 15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS (déplacé) 15.3.1 Information systems audit controls 15.3.2 Protection of information systems audit tools (combiné)	12. OPERATIONS SECURITY 12.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 12.1.1 Documented operating procedures 12.1.2 Change management 12.1.3 Capacity management (déplacé) 12.1.4 Separation of development, testing and operational environments (titre modifié) 12.2 PROTECTION FROM MALWARE (titre modifié) 12.2.1 Controls against malware (titre modifié) 12.3 BACKUP 12.3.1 Information backup 12.4 LOGGING AND MONITORING (titre modifié) 12.4.1 Event logging (titre modifié) 12.4.2 Protection of log information 12.4.3 Administrator and operator logs 12.4.4 Clock synchronization 12.5 CONTROL OF OPERATIONAL SOFTWARE 12.5.1 Installation of soft-ware on operational systems (nouveau) 12.6 TECHNICAL VULNERABILITY MANAGEMENT 12.6.1 Management of technical vulnerabilities (titre modifié) 12.6.2 Restrictions on software installation 12.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS (déplacé) 12.7.1 Information systems audit controls
11.4 NETWORK ACCESS CONTROL (déplacé) 11.4.1 Policy on use of network services 11.4.2 User authentication for external connections (supprimé) 11.4.3 Equipment identification in networks (supprimé) 11.4.4 Remote diagnostic and configuration port protection (supprimé) 11.4.5 Segregation in networks 11.4.6 Network connection control (supprimé) 11.4.7 Network routing control (supprimé) 10.8 EXCHANGE OF INFORMATION (déplacé)	13. Communications security 13.1 NETWORK SECURITY MANAGEMENT 13.1.1 Network controls 13.1.2 Security of network services 13.1.3 Segregation in net works 13.2 INFORMATION TRANSFER (titre modifié)

10.8.1 Information exchange policies and procedures 10.8.2 Exchange agreements 10.8.3 Physical media in transit (supprimé) 10.8.4 Electronic messaging 10.8.5 Business information systems (supprimé)	13.2.1 Information transfer policies and procedures (titre modifié) 13.2.2 Agreements on information transfer (titre modifié) 13.2.3 Electronic messaging 13.2.4 Confidentiality or non- disclosure agreements (nouveau)
12. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 12.1.1 Security requirements analysis and specification 12.2 CORRECT PROCESSING IN APPLICATIONS (supprimé) 12.2.1 Input data validation 12.2.2 Control of internal processing 12.2.3 Message integrity 12.2.4 Output data validation 12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 12.5.1 Change control procedures 12.5.2 Technical review of applications after operating system changes 12.5.3 Restrictions on changes to software packages 12.5.4 Information leakage (supprimé) 12.5.5 Outsourced software development 12.4.2 Protection of system test data	14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE (titre modifié) 14.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 14.1.1 Information security requirements analysis and Specification (titre modifié) 14.1.2 Securing application services on public networks (nouveau) 14.1.3 Protecting application services transactions (nouveau) 14.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 14.2.1 Secure development policy (nouveau) 14.2.2 System change control procedures (titre modifié) 14.2.3 Technical review of applications after operating platform changes 14.2.4 Restrictions on changes to software packages 14.2.5 Secure system engineering principles (nouveau) 14.2.6 Secure development environment 14.2.7 Outsourced development 14.2.8 System security testing (nouveau) 14.2.9 System acceptance testing (nouveau) 14.3 Test data (nouveau) 14.3.1 Protection of test data (titre modifié)
6.2 EXTERNAL PARTIES (déplacé) 6.2.1 Identification of risks related to external parties 6.2.2 Addressing security when dealing with customers 6.2.3 Addressing security in third party agreements 10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT (déplacé) 10.2.1 Service delivery (supprimé) 10.2.2 Monitoring and review of third party services 10.2.3 Managing changes to third party services	15. SUPPLIER RELATIONSHIPS (titre modifié) 15.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS 15.1.1 Information security policy for supplier relationships 15.1.2 Addressing security within supplier agreements 15.1.3 Information and communication technology supply chain (nouveau) 15.2 SUPPLIER SERVICE DELIVERY MANAGEMENT (titre modifié) 15.2.1 Monitoring and review of supplier services (titre modifié) 15.2.2 Managing changes to supplier services (titre modifié)
13. INFORMATION SECURITY INCIDENT MANAGEMENT 13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 13.2.1 Responsibilities and procedures 13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES (supprimé) 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses 13.2.2 Learning from information security incidents 13.2.3 Collection of evidence	16. INFORMATION SECURITY INCIDENT MANAGEMENT 16.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 16.1.1 Responsibilities and Procedures 16.1.2 Reporting information security events 16.1.3 Reporting information security weaknesses 16.1.4 Assessment of and decision on information security events (nouveau) 16.1.5 Response to information security incidents (nouveau) 16.1.6 Learning from information security incidents 16.1.7 Collection of evidence
14. BUSINESS CONTINUITY MANAGEMENT	17. Information security aspects of business

14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 14.1.1 Including information security in the business continuity management process (supprimé) 14.1.2 Business continuity and risk assessment (supprimé) 14.1.3 Developing and implementing continuity plans including information security (supprimé) 14.1.4 Business continuity planning framework (supprimé) 14.1.5 Testing, maintaining and re-assessing business continuity plans	continuity management 17.1 INFORMATION SECURITY CONTINUITY 17.1.1 Planning information security continuity (nouveau) 17.1.2 Implementing information security continuity (nouveau) 17.1.3 Verify, review and evaluate information security continuity (titre modifié) 17.2 REDUNDANCIES (nouveau) 17.2.1 Availability of information processing facilities
15. COMPLIANCE 15.1 COMPLIANCE WITH LEGAL REQUIREMENTS 15.1.1 Identification of applicable legislation 15.1.2 Intellectual property rights (IPR) 15.1.3 Protection of organizational records 15.1.4 Data protection and privacy of personal information 15.1.5 Prevention of misuse of information processing facilities (supprimé) 15.1.6 Regulation of cryptographic controls 6.1.8 Independent review of information security (déplacé) 15.2.1 Compliance with security policies and standards 15.2.2 Technical compliance checking	18. COMPLIANCE 18.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS (titre modifié) 18.1.1 Identification of applicable legislation and contractual requirements (titre modifié) 18.1.2 Intellectual property Rights 18.1.3 Protection of records 18.1.4 Privacy and protection of personally identifiable information (titre modifié) 18.1.5 Regulation of cryptographic controls 18.2 INFORMATION SECURITY REVIEWS (Nouveau) 18.2.1 Independent review of information security 18.2.2 Compliance with security policies and standards 18.2.3 Technical compliance review