A.5	**Politiques de sécurité de l'information**		
A.5.1	**Orientations de la direction en matière de sécurité de l'information**		**Observations**
A.5.1.1	Politiques de sécurité de l'information	1. Existe-t-il des politiques de sécurité ? 2. Ces politiques sont-ils approuvées par le management ? 3. Ces politiques sont-elles communiqués aux employés de la société ?	
A.5.1.2	Revue des politiques de sécurité de l'information	1. Les politiques de sécurité sont-elles passées en revue ? 2. Les revues sont-elles à un intervalle régulier ? 3. Des revues sont-elles établissent lors de changements ?	
A.6	**Organisation de la sécurité de l'information**		
A.6.1	**Organisation interne**		
A.6.1.1	Fonctions et responsabilités liées à la sécurité de l'information	Les responsabilités pour la protection des biens individuels et des processus de sécurité spécifiques sont-ils clairement identifiés, définis et communiqués aux parties concernés ?	

A.6.1.2	Séparation des tâches	Les fonctions et les domaines de responsabilité sont-ils séparés, afin de limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation ?	
A.6.1.3	Relation avec les autorités	1. Existe-t-il une procédure permettant de documenter quand, et par qui, des contacts avec les autorités compétentes (application de la loi, etc.) seront-ils effectués? 2. Existe-t-il un processus qui détaille comment et quand le contact est requis? 3. Existe-t-il un processus de partage systématique des contacts et des renseignements?	
A.6.1.4	Relation avec des groupes de travail spécialisés	Des personnes dans l'organisation investies dans la sécurité du SI ont-elles des relations appropriées avec des groupes d'intérêt, des forums spécialisés, professionnels, associations	

		dans la sécurité de l'information	
A.6.1.5	La sécurité de l'information dans la gestion de projet	Tous les projets font-ils l'objet d'une évaluation de la sécurité de l'information?	
A.6.2	**Appareils mobiles et télétravail**		
A.6.2.1	Politique en matière d'appareils mobiles	1. Existe-t-il une politique de sécurité mobile ? 2. La politique est-elle approuvée par la direction? 3. Cette politique (document) reporte-t-il les risques additionnels concernant l'usage des appareils mobiles (Vol, utilisation de Hotspot, etc.) ?	
A.6.2.2	Télétravail	1. Y a-t-il une politique pour le télétravail ? 2. La politique est-elle approuvée par la direction? 3. Existe-t-il un processus défini pour que les « télétravailleurs » puissent accéder à distance à l'organisation ? 4. Les télétravailleurs ont-ils les conseils et l'équipement	

		nécessaires pour protéger leurs biens?	
A.7	**La sécurité des ressources humaines**		
A.7.1	**Avant l'embauche**		
A.7.1.1	Sélection des candidats	1. La vérification des antécédents sont-elles effectuées sur tous les nouveaux candidats à l'emploi? 2. Ces contrôles sont-ils approuvés par l'autorité de gestion appropriée? 3. Les contrôles des antécédents sont-ils règlementaires, éthiques et pertinents ? 4. Le niveau de contrôle est-il en adéquation avec l'analyse de risque ?	

A.7.1.2	Termes et conditions d'embauche	1. Tous les employés, les parties prenantes et les utilisateurs tiers sont-ils priés de signer des accords de confidentialité et de non-divulgation? 2. Les contrats d'emploi / de services couvrent-ils spécifiquement la nécessité de protéger les informations commerciales?	
A.7.2	**Pendant la durée du contrat**		
A.7.2.1	Responsabilités de la direction	1. Les managers (de tous les niveaux) sont-ils engagés dans l'utilisation de la sécurité dans l'entreprise ? 2. Le management et la conduite des politiques conduit-il, encourage t-il les employés, les parties prenantes, les utilisateurs à appliquer les politiques et procédures de sécurité ?	
A.7.2.2	Sensibilisation, apprentissage et formation à la sécurité de l'information	Les employés, parties prenantes sont-ils inscrits à des formations de sensibilisation suivant leurs domaines de travail ?	

A.7.2.3	Processus disciplinaire	1. Existe-t-il un processus disciplinaire formel qui permet à l'organisation de prendre des mesures contre les employés qui ont commis une violation de la sécurité de l'information? 2. Celles-ci sont elles communiqués aux parties intéressés ?	
A.7.3	**Rupture, terme ou modification du contrat de travail**		
A.7.3.1	Achèvement ou modification des responsabilités associées au contrat de travail	1. Existe-t-il une procédure documentée pour mettre fin ou modifier des fonctions professionnelles d'un employé? 2. Y a-t-il des fonctions dans la sécurité de l'information pouvant ne pas survivre si un employé est en rupture de contrat ? 3. L'organisation est-elle en mesure de faire respecter les obligations d'un employé en sécurité de l'information avant son départ ?	
A.8	**Gestion des actifs**		
A.8.1	**Responsabilités relatives aux actifs**		

A.8.1.1	Inventaire des actifs	1. Existe-t-il un inventaire de tous les actifs associés à l'information et moyens de traitement de l'information ? 2. Cet inventaire est-il mise à jour ?	
A.8.1.2	Propriété des actifs	Tous les biens informationnels ont-il un propriétaire clairement défini qui est conscient de ses responsabilités ?	
A.8.1.3	Utilisation correcte des actifs	1. Existe-t-il une politique d'utilisation pour chaque classe / type d'actif d'information? 2. Les utilisateurs sont-ils au courant de cette politique avant utilisation?	
A.8.1.4	Restitution des actifs	Y a-t-il un processus en place pour que les employés en fin de contrat retournent les actifs en leur possession ?	
A.8.2	**Classification de l'information**		

A.8.2.1	Classification des informations	1. Existe-t-il une politique régissant la classification de l'information? 2. Existe-t-il un processus par lequel toutes les informations peuvent être classées de manière appropriée?	
A.8.2.2	Marquage des informations	Existe-t-il un processus ou une procédure pour s'assurer que la classification de l'information est correctement marquée sur chaque actif?	
A.8.2.3	Manipulation des actifs	1. Existe-t-il une procédure pour traiter chaque classification d'information? 2. Les utilisateurs d'actifs informationnels ont-ils été informés de cette procédure?	
A.8.3	**Manipulation des supports**		
A.8.3.1	Gestion des supports amovibles	1. Existe-t-il une politique régissant les supports amovibles? 2. Existe-t-il un processus couvrant « comment les supports amovibles sont gérés »?	

		3. La politique et les processus (s) sont-ils communiqués à tous les employés utilisant des supports amovibles?	
A.8.3.2	Mise en rebut des supports	Existe-t-il une procédure formelle régissant la façon dont les supports amovibles sont détruits ?	
A.8.3.3	Manipulation des actifs	1. Existe-t-il une politique et un processus documentés détaillant la façon dont les médias physiques devraient être transportés? 2. Les médias sont ils protégés contre les accès non autorisés, les abus, la corruption?	
A.9	**Contrôle d'accès**		
A.9.1	**Exigences métier en matière de contrôle d'accès**		

A.9.1.1	Politique de contrôle d'accès	1. Existe-t-il une politique de contrôle d'accès documentée? 2. La politique est-elle basée sur les exigences du business? 3. La politique est-elle communiquée de façon appropriée?	
A.9.1.2	Accès aux réseaux et services réseau	Des contrôles sont-ils en place pour s'assurer que les utilisateurs ont seulement accès aux ressources du réseau qu'ils ont été spécialement autorisés à utiliser et qui sont nécessaires à leurs tâches?	
A.9.2	**Gestion de l'accès utilisateur**		
A.9.2.1	Enregistrement et désinscription des utilisateurs	Existe-t-il un processus d'enregistrement de l'accès des utilisateurs en place?	
A.9.2.2	Distribution des accès aux utilisateurs	Y a-t-il un processus formel de maîtrise de la gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs de tous	

		les systèmes et de tous les services d'information ?	
A.9.2.3	Gestion des droits d'accès à privilèges	Les comptes d'accès privilégiés sont-ils gérés et contrôlés séparément?	
A.9.2.4	Gestion des information secrètes d'authentification des utilisateurs	Existe-t-il un processus de gestion formel pour contrôler l'attribution d'informations d'authentification secrètes?	
A.9.2.5	Revue des droits d'accès d'utilisateurs	1. Existe-t-il un processus permettant aux propriétaires d'actifs de réviser régulièrement leurs droits d'accès à leurs actifs? 2. Ce processus d'évaluation est-il vérifié?	
A.9.2.6	Suppression ou adaptation des droits d'accès	Existe-t-il un processus pour s'assurer que les droits d'accès des utilisateurs sont supprimés lors de la cessation d'emploi ou du contrat, ou sont-ils ajustés en fonction du changement de rôle dans l'organisation ?	

A.9.3	**Responsabilités des utilisateurs**		
A.9.3.1	Utilisation d'informations secrètes d'authentification	1. Existe-t-il un document regroupant comment les informations contenant l'authentification secrète doit être utilisé ? 2. Celle-ci est-elle communiqué à tous les utilisateurs ?	
A.9.4	**Contrôle de l'accès au système et aux applications**		
A.9.4.1	Restriction d'accès à l'information	L'accès à l'information et les fonctions d'application système sont-elles restreintes conformément à la politique de contrôle d'accès?	
A.9.4.2	Sécuriser les procédures de connexion	Lorsque la politique de contrôle d'accès l'exige, l'accès est-il contrôlé par une procédure de connexion sécurisée?	
A.9.4.3	Système de gestion des mots de passe	1. Les systèmes de mots de passe sont-ils interactifs? 2. Des mots de passe complexes sont-ils requis?	

A.9.4.4	Utilisation de programme utilitaire à privilèges	Les programmes utilitaires à privilégiés sont-ils restreints et surveillés?	
A.9.4.5	Contrôle d'accès au code source des programmes	L'accès au code source des programmes est-il protégé?	
A.10	**Cryptographie**		
A.10.1	**Mesures cryptographiques**		
A.10.1.1	Politique d'utilisation des mesures cryptographiques	Y a-t-il une politique pour les contrôles cryptographiques ?	
A.10.1.2	Gestion des clés	Y a-t-il une politique pour la gestion sur l'utilisation, la protection et la durée de vie des clés cryptographiques (cycle de vie) ?	
A.11	**Sécurité physique et environnementale**		
A.11.1	**Zones sécurisées**		

A.11.1.1	Périmètre de sécurité physique	1. Y a-t-il un périmètre de sécurité définit ? 2. Les informations sensible, critique sont-elles isolé et dans un endroit contrôlé ?	
A.11.1.2	Contrôle d'accès physique	Les zones contrôlés ont-elles des systèmes permettant de vérifier que seulement les personnes autorisées ont accès ?	
A.11.1.3	Sécurisation des bureaux, des salles et équipements	1. Les bureaux, salles et équipements ont t-ils été pensé avec de la sécurité ? 2. Y a-il des processus pour la maintient de la sécurité physique (bureaux propres, fermetures des bureaux) ?	
A.11.1.4	Protection contre les menaces extérieures et environnementales	Existe t-il des protections physiques contre les désastres naturels, les attaques malveillantes ou les accidents ?	
A.11.1.5	Travail dans les zones sécurisées	1. Existe t-il des zones de travails sécurisées ? 2. Des processus ont-ils été établi pour ces zones de travails ?	

		3. Ces processus sont-ils surveillés et améliorés ?	
A.11.1.6	Zone de livraison et de chargement	1. Y a-t-il des zones de livraisons/de chargement isolés afin d'éviter des accès non-autorisés ? 2. L'accès à ces zones de chargements sont-elles contrôlés ? 3. L'accès à partir des zones de chargement est-il isolé des installations de traitement de l'information?	
A.11.2	**Matériels**		
A.11.2.1	Emplacement et protection des matériels	1. Les dangers environnementaux sont-ils identifiés et pris en compte lorsque les emplacements des équipements sont sélectionnés? 2. Les risques liés aux accès / passants non autorisés sont-ils pris en compte lors de l'installation du matériel?	

A.11.2.2	Services généraux	1. Existe t-il un système d'alimentation sans interruption ? 2. Ont-ils été testé et et le résultat montre t-il un délai approprié?	
A.11.2.3	Sécurité du câblage	1. Des évaluations des risques ont-elles été menées sur l'emplacement des câbles d'alimentation et de télécommunications? 2. Sont-ils situés à des endroits ou il sont protégés contre les interférences, les interceptions ou les dommages?	
A.11.2.4	Maintenance des matériels	Existe-t-il un calendrier de maintenance rigoureux?	
A.11.2.5	sorties des actifs	1. Existe-t-il un processus qui contrôle comment les actifs sont supprimés ? 2. Ce processus est-il appliqué? 3. Des contrôles sur place sont-ils effectués?	
A.11.2.6	Sécurité des matériels et des actifs hors des locaux	1. Existe-t-il une politique couvrant la sécurité des actifs hors site?	

		2. Cette politique est-elle largement communiquée?	
A.11.2.7	Mise en rebut ou recyclage sécurisé(e) des matériels	1. Existe-t-il une politique couvrant comment les actifs d'information peuvent être réutilisés? 2. Lorsque les données sont effacées, est-ce que cela est correctement vérifié avant la réutilisation / élimination?	
A.11.2.8	Matériels utilisateur laissés sans surveillance	1. L'organisation a-t-elle une politique sur la façon dont les équipements sans surveillance devraient être protégés? 2. Des systèmes techniques sont-ils en place pour sécuriser l'équipement qui a été laissé sans surveillance par inadvertance?	
A.11.2.9	Politique du bureau propre et de l'écran verrouillé	1. Existe-t-il une politique du bureau propre / écran ? 2. Est-ce bien appliqué?	
A.12	**Sécurité liée à l'exploitation**		
A.12.1	**Procédures et responsabilités liées à l'exploitation**		

	Procédure d'exploitations documentées	1. Les procédures d'exploitation sont-elles bien documentées? 2. Les procédures sont-elles mises à la disposition de tous les utilisateurs qui en ont besoin?	
A.12.1.2	Gestion des changements	Existe-t-il un processus de gestion du changement contrôlé?	
A.12.1.3	Dimensionnement	Existe-t-il un processus de gestion de la capacité?	
A.12.1.4	Séparation des environnements de développement, de test et d 'exploitation	L'organisation applique-t-elle une ségrégation des environnements de développement, de test et d'exploitation?	
A.12.2	**Protection contre les logiciels malveillants**		
A.12.2.1	Mesures contre les logiciels malveillants	1. Les processus de détection des logiciels malveillants sont-ils en place? 2. Les processus sont-ils destinés à empêcher la propagation de logiciels malveillants en place? 3. L'organisation a-t-elle un processus et une capacité à	

		récupérer d'une infection malveillante.	
A.12.3	**Sauvegarde**		
A.12.3.1	Sauvegarde des informations	1. Existe-t-il une politique de sauvegarde convenue? 2. La politique de sauvegarde de l'organisation est-elle conforme aux cadres juridiques pertinents? 3. Les sauvegardes sont-elles conformes à la politique? 4. Les tests de sauvegarde sont-ils effectués?	
A.12.4	**Journalisation et surveillance**		
A.12.4.1	Journalisation des évènements	Les journaux d'événements appropriés sont-ils maintenus et régulièrement examinés?	
A.12.4.2	Protection de l'information journalisée	Les installations de journalisation sont-elles protégées contre la falsification et l'accès non autorisé?	

A.12.4.3	Journaux administrateur et opérateur	Les journaux sysadmin / sysop sont-ils maintenus, protégés et régulièrement examinés?	
A.12.4.4	Synchronisation des horloges	Toutes les horloges de l'organisation sont-elles synchronisées ?	
A.12.5	**Maîtrise des logiciels en exploitation**		
A.12.5.1	Installation de logiciels sur des systèmes en exploitation	Existe-t-il un processus en place pour contrôler l'installation de logiciels sur des systèmes opérationnels ?	
A.12.6	**Gestion des vulnérabilités techniques**		
A.12.6.1	Gestion des vulnérabilités techniques	1. L'organisation a-t-elle accès à des informations mises à jour et en temps opportun sur les vulnérabilités techniques ? 2.Existe-t-il un processus pour évaluer et réagir à toutes les nouvelles vulnérabilités à mesure qu'elles sont découvertes ?	
A.12.6.2	Restriction liées à l'installation de logiciels	Existe-t-il des processus pour restreindre la façon dont les utilisateurs installent le logiciel ?	

A.12.7	**Considérations sur l'audit du système d'information**		
A.12.7.1	Mesures relatives à l'audit des systèmes d'information	1. Le SI sont-ils soumis à vérification ? 2. L'audit ne perturbe t-il pas l'entreprise ?	
A.13	**Sécurité des communications**		
A.13.1	**Management de la sécurité des réseaux**		
A.13.1.1	Contrôle des réseaux	Existe-t-il un processus de gestion du réseau en place ?	
A.13.1.2	Sécurité des services de réseau	1. L'organisation met-elle en œuvre une approche de gestion des risques qui identifie tous les services de réseau et les accords de service ? 2. La sécurité est-elle obligatoire dans les accords et les contrats avec les fournisseurs de services (en interne et sous-traités). 3. Les SLA liés à la sécurité sont-ils mandatés ?	
A.13.1.3	Cloisonnement des réseaux	La topologie du réseau impose-t-elle une ségrégation des réseaux pour différentes tâches ?	
A.13.2	**Transfert de l'information**		

A.13.2.1	Politiques et procédures de transfert de l’information	1. Les politiques organisationnelles régissent-elles la façon dont les informations sont transférées ? 2. Les procédures permettant de transférer les données sont-elles mises à la disposition de tous les employés ? 3. Des contrôles techniques pertinents sont-ils en place pour empêcher les transferts de données non autorisés ?	
A.13.2.2	Accords en matière de transfert d’information	Les contrats conclus avec des parties externes et les accords au sein de l'organisation détaillent-ils les conditions requises pour sécuriser les informations commerciales en cours de transfert?	
A.13.2.3	Messagerie électronique	Les politiques de sécurité couvrent-elles l'utilisation du transfert d'informations lors de l'utilisation de systèmes de messagerie électronique ?	

A.13.2.4	Engagement de confidentialité ou de non-divulgation	1. Les employés, les entrepreneurs et les agents signent-ils des accords de confidentialité ou de non-divulgation ? 2. Ces engagements sont-ils soumis à un examen régulier ? 3. Les enregistrements des engagements sont-ils maintenus ?	
A.14	**Acquisition, développement et maintenance des systèmes d'information**		
A.14.1	**Exigences de sécurité applicables aux systèmes d'information**		
A.14.1.1	Analyse et spécification des exigences de sécurité de l'information	1. Les exigences de sécurité de l'information sont-elles spécifiées lorsque de nouveaux systèmes sont introduits? 2. Lorsque les systèmes sont améliorés ou mise à jour, les exigences de sécurité sont-elles spécifiées et abordées?	
A.14.1.2	Sécurisation des services d'application sur les réseaux publics	Les applications qui envoient des informations sur des réseaux publics protègent-elles de manière appropriée les informations contre les activités frauduleuses, les conflits contractuels, les	

		divulgateurs non autorisés et les modifications non autorisées?	
A.14.1.3	Protection des transactions liées aux services d'application	Des contrôles sont-ils en place pour empêcher une transmission incomplète, une mauvaise transposition, une altération de message non autorisée, une divulgation non autorisée, une duplication de message non autorisée ou des attaques de répétition?	
A.14.2	**Sécurité des processus de développement et d'assistance technique**		
A.14.2.1	Politique de développement sécurisé	1. L'organisation développe-t-elle un logiciel ou un système? 2. Si l'item ci-dessus est affirmatif existe-t-il des politiques exigeant la mise en œuvre et l'évaluation des contrôles de sécurité?	
A.14.2.2	Procédures de contrôle des changements de système	Existe-t-il un processus formel de contrôle des changements?	

A.14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation	Existe-t-il un processus pour s'assurer qu'un examen technique est effectué lorsque les plates-formes d'exploitation sont modifiées?	
A.14.2.4	Restrictions relatives aux changements apportés aux progiciels	Existe-t-il une politique qui exige quand et comment les paquets de logiciels peuvent être changer ou modifiés?	
A.14.2.5	Principes d'ingénierie de la sécurité des systèmes	L'organisation a-t-elle des principes documentés sur la manière dont les systèmes doivent être conçus pour assurer la sécurité?	
A.14.2.6	Environnement de développement sécurisé	1. un environnement de développement sécurisé at-il été établi? 2. Tous les projets utilisent-ils l'environnement de développement sécurisé de manière appropriée pendant le cycle de développement du système?	
A.14.2.7	Développement externalisé	1. Lorsque le développement a été externalisé, est-ce supervisé? 2. Le code développé à l'externe est-il sujet à une	

		évaluation de sécurité avant le déploiement?	
A.14.2.8	Test de la sécurité du système	Lorsque des systèmes ou des applications sont développés, les tests de sécurité sont-ils testés dans le cadre du processus de développement?	
A.14.2.9	Test de conformité du système	Existe-t-il un processus établi pour accepter de nouveaux systèmes / applications, ou mises à niveau, dans l'utilisation de la production?	
A.14.3	**Données de test**		
A.14.3.1	Protection des données de test	1. Existe-t-il un processus de séparation des données de test? 2. Les données de test sont-elles convenablement protégées?	
A.15	**Relations avec les fournisseurs**		
A.15.1	**Sécurité de l'information dans les relations avec les fournisseurs**		

A.15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs	1. La sécurité de l'information est-elle incluse dans les contrats établis avec les fournisseurs ? 2. Existe-t-il une approche de gestion des risques à l'échelle de l'organisation pour les relations avec les fournisseurs?	
A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs	1. Les fournisseurs ont-ils des exigences de sécurité documentées? 2. L'accès des fournisseurs à l'information et à l'infrastructure est-il contrôlé et surveillé?	
A.15.1.3	Chaîne d'approvisionnement des produits et des services informatiques	Les accords de fournisseur incluent-ils des exigences pour répondre à la sécurité de l'information dans la chaîne d'approvisionnement des services et des produits?	
A.15.2	**Gestion de la prestation du service**		
A.15.2.1	Surveillance et revue des services des fournisseurs	Les fournisseurs sont-ils soumis à un examen et une vérification réguliers?	

A.15.2.2	Gestion des changements apportés dans les services des fournisseurs	Les changements apportés à la prestation de services sont-ils assujettis à un processus de gestion qui comprend l'évaluation de la sécurité et des risques?	
A.16	**Gestion des incidents liés à la sécurité de l'information**		
A.16.1	**Gestion des incidents liés à la sécurité de l'information et améliorations**		
A.16.1.1	Responsabilités et procédures	Les responsabilités de gestion sont-elles clairement identifiées et documentées dans les processus de gestion des incidents?	
A.16.1.2	Signalement des évènements liés à la sécurité de l'information	1. Existe-t-il un processus de «timely reporting » opportun des événements de sécurité de l'information? 2. Existe-t-il un processus pour examiner et agir sur les événements signalés sur la sécurité de l'information?	
A.16.1.3	Signalement des failles liées à la sécurité de l'information	1.Existe-t-il un processus pour signaler les faiblesses identifiées en matière de sécurité de l'information? 2.Ce processus est-il largement communiqué?	

		3. Existe-t-il un processus pour examiner et addresser les rapports en temps opportun?	
A.16.1.4	Appréciation des évènements liés à la sécurité de l'information et prise de décision	Existe-t-il un processus pour s'assurer que les événements de sécurité de l'information sont correctement évalués et classés?	
A.16.1.5	Réponse aux incidents liés à la sécurité de l'information	Existe-t-il un processus de réponse aux incidents qui reflète la classification et la sévérité des incidents de sécurité de l'information?	
A.16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information	Existe-t-il un processus ou framework qui permet à l'organisation d'apprendre des incidents de sécurité de l'information et de réduire l'impact / la probabilité des événements futurs?	
A.16.1.7	Collecte de preuves	1. Existe-t-il une politique pour le Forensic 2. Dans le cas d'un incident de sécurité de l'information, les données pertinentes	

		sont-elles collectées de manière à l'utiliser comme preuve?	
A.17	**Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité**		
A.17.1	**Continuité de la sécurité de l'information**		
A.17.1.1	Organisation de la continuité de la sécurité de l'information	La sécurité d'information est-elle incluse dans les plans de continuité de l'organisation?	
A.17.1.2	Mise en oeuvre de la continuité de la sécurité de l'information	La fonction de sécurité de l'information de l'organisation at-elle documenté, mis en œuvre et maintenu des processus pour maintenir la continuité du service lors d'une situation défavorable?	
A.17.1.3	Vérifier, revoir et évaluer la continuité de la sécurité de l'information	Les plans de continuité sont-ils validés et vérifiés à intervalles réguliers?	
A.17.2	**Redondances**		
A.17.2.1	Disponibilité des moyens de traitement de l'information	Les installations de traitement de l'information ont-elles une redondance	

		suffisante pour répondre aux exigences de disponibilité des organisations?	
A.18	**Conformité**		
A.18.1	**Conformité aux obligations légales et réglementaires**		
A.18.1.1	Identification de la législation et des exigences contractuelles applicables	1. L'organisation at-elle identifié et documenté toutes les exigences législatives, réglementaires ou contractuelles pertinentes liées à la sécurité? 2. La conformité est-elle documentée?	
A.18.1.2	Droits de propriété intellectuelle	1. Est-ce que l'organisation tient un registre de tous les droits de propriété intellectuelle et l'utilisation de produits logiciels exclusifs? 2. L'organisation surveille-t-elle l'utilisation de logiciels sans licence?	
A.18.1.3	Protection des enregistrements	Les dossiers sont-ils protégés contre les pertes, les destructions, les falsifications et l'accès ou la publication non autorisés	

		conformément aux exigences législatives, réglementaires, contractuelles et commerciales?	
A.18.1.4	Protection de la vie privée et protection des données à caractères personnelles	1. Les données personnelles sont-elles identifiées et classées de manière appropriée? 2. Les données personnelles sont-elles protégées conformément à la législation pertinente?	
A.18.1.5	Réglementation relative aux mesures cryptographiques	Les contrôles cryptographiques sont-ils protégés conformément à tous les accords, lois et règlements pertinents?	
A.18.2	**Revue de la sécurité de l'information**		
A.18.2.1	Revue indépendante de la sécurité de l'information	1. L'approche des organisations pour gérer la sécurité de l'information est-elle soumise à un examen indépendant régulier? 2. La mise en œuvre des contrôles de sécurité est-elle soumise à un examen indépendant régulier?	

A.18.2.2	Conformité avec les politiques et les normes de sécurité	1. L'organisation demande-t-elle aux gestionnaires d'examiner régulièrement le respect de la politique et des procédures dans leur domaine de responsabilité? 2. Les comptes-rendus sont-ils conservés?	
A.18.2.3	Vérification de la conformité technique	L'organisation effectue-t-elle régulièrement des examens techniques de conformité de ses systèmes d'information?	