EXEMPLE DE MODÈLE DE LISTE DE CONTRÔLE D'ÉVALUATION DES RISQUES DE CYBERSÉCURITÉ

CONTRÔLE ISO 27001	PHASES D'IMPLÉMENTATION	TÂCHES	EN CONFORMITÉ ?	REMARQUES
5	***Politiques de sécurité de l'information***			
5.1	**Orientations de la direction en matière de sécurité de l'information**			
5.1.1	Politiques de sécurité de l'information	Des politiques de sécurité existent ?	☐	
		Toutes les politiques sont approuvées par la direction ?	☐	
		Preuve de conformité ?	☐	
6	***Organisation de la sécurité de l'information***			
6.1	**Rôles et responsabilités en matière de sécurité de l'information**			
6.1.1	Rôles et responsabilités en matière de sécurité	Rôles et responsabilités définies ?	☐	
6.1.2	Répartition des tâches	La répartition des tâches est définie ?	☐	
6.1.3	Contact avec les autorités	L'organisme ou l'autorité de vérification est contactée pour la vérification de la conformité ?	☐	
6.1.4	Contact avec des groupes d'intérêt particuliers	Des contacts sont établis avec des groupes d'intérêt particuliers concernant la conformité.	☐	
6.1.5	Sécurité de l'information dans la gestion de projet	Preuve de la sécurité de l'information dans la gestion de projet ?	☐	
6.2	**Appareils mobiles et télétravail**			
6.2.1	Politique pour les appareils mobiles	Politique définie pour les appareils mobiles ?	☐	
6.2.2	Télétravail	Une politique pour le télétravail est définie ?	☐	
7	***Sécurité des ressources humaines***			
7.1	**Avant l'embauche**			
7.1.1	Filtrage	Une politique pour le filtrage des employés avant leur embauche est définie ?	☐	
7.1.2	Durée et conditions d'embauche	Une politique pour la durée et les conditions d'embauche est définie ?	☐	
7.2	**Pendant la durée du contrat**			
7.2.1	Responsabilités de gestion	Une politique sur les responsabilités de gestion est définie ?	☐	
7.2.2	Sensibilisation, éducation et formation à la sécurité de l'information	Une politique pour la sensibilisation, l'éducation et la formation à la sécurité de l'information est définie ?	☐	
7.2.3	Processus disciplinaire	Une politique pour les processus disciplinaires concernant la sécurité de l'information est définie ?	☐	

7.3	**Licenciement et changement d'emploi**			
7.3.1	Responsabilités liées au licenciement ou au changement d'emploi	Une politique pour le licenciement ou le changement d'emploi en matière de sécurité de l'information est définie ?	☐	
8	***Gestion des actifs***			
8.1	**Responsabilités relatives aux actifs**			
8.1.1	Inventaire des actifs	La liste des actifs est complète ?	☐	
8.1.2	Propriété des actifs	Propriété totale sur la liste des actifs.	☐	
8.1.3	Politique d'utilisation acceptable des actifs	Une politique sur l'« utilisation acceptable » des actifs est définie ?	☐	
8.1.4	Retour des actifs	Une politique de retour des actifs est définie ?	☐	
8.2	**Classification de l'information**			
8.2.1	Classification de l'information	Une politique pour la classification des informations est définie.	☐	
8.2.2	Étiquetage des informations	Une politique pour l'étiquetage des informations est définie ?	☐	
8.2.3	Gestion des actifs	Une politique pour la gestion des actifs est définie.	☐	
8.3	**Manipulation des supports**			
8.3.1	Gestion des supports amovibles est définie	Une politique sur la gestion des supports amovibles est définie.	☐	
8.3.2	Élimination des supports	Une politique pour l'élimination des supports est définie.	☐	
8.3.3.	Transfert des supports physiques	Une politique pour le transfert des supports physiques est définie.	☐	
9	***Contrôle d'accès***			
9.1	**Responsabilités relatives aux actifs**			
9.1.1	Politique de contrôle d'accès	Une politique pour le contrôle d'accès est définie ?	☐	
9.1.2	Accès aux réseaux et aux services réseau	Une politique pour l'accès aux réseaux et aux services réseau est définie ?	☐	
9.2	**Responsabilités relatives aux actifs**			
9.2.1	Enregistrement et désinscription des utilisateurs	Une politique pour l'enregistrement et la désinscription des ressources utilisateur est définie ?	☐	
9.2.2	Provisionnement de l'accès des utilisateurs	Une politique pour le provisionnement de l'accès des utilisateurs est définie ?	☐	
9.2.3	Gestion des droits d'accès privilégiés	Une politique pour la gestion des droits d'accès privilégiés est définie.	☐	

9.2.4	Gestion des identifiants d'authentification des utilisateurs	Une politique sur la gestion des identifiants d'authentification des utilisateurs est définie.	☐	
9.2.5	Examen des droits d'accès des utilisateurs	Une politique pour l'examen des droits d'accès des utilisateurs est définie ?	☐	
9.2.6	Suppression ou l'ajustement des droits d'accès	Une politique pour la suppression ou l'ajustement des droits d'accès est définie ?	☐	
9.3	**Responsabilités des utilisateurs**			
9.3.1	Utilisation d'informations d'authentification secrètes	Une politique pour l'utilisation d'informations d'authentification secrètes est définie ?	☐	
9.4	**Contrôle d'accès aux systèmes et aux applications**			
9.4.1	Restrictions d'accès à l'information	Une politique pour les restrictions d'accès à l'information est définie ?	☐	
9.4.2	Procédures de connexion sécurisées	Une politique pour les procédures de connexion sécurisées est définie ?	☐	
9.4.3	Système de gestion des mots de passe	Une politique pour les systèmes de gestion des mots de passe est définie ?	☐	
9.4.4	Utilisation de programmes utilitaires privilégiés	Une politique pour l'utilisation de programmes utilitaires privilégiés est définie ?	☐	
9.4.5	Contrôle d'accès au code source du programme	Une politique pour le contrôle d'accès au code source du programme est définie.	☐	
10	***Cryptographie***			
10.1	**Mesures cryptographiques**			
10.1.1	Politique pour l'utilisation de contrôles cryptographiques	Une politique pour l'utilisation de contrôles cryptographiques est définie ?	☐	
10.1.2	Gestion des clés	Une politique pour la gestion des clés est définie ?	☐	
11	***Sécurité physique et environnementale***			
11.1	**Zones sécurisées**			
11.1.1	Périmètre de sécurité physique	Une politique pour le périmètre de sécurité physique est définie ?	☐	
11.1.2	Contrôles d'accès physique	Une politique pour les contrôles d'accès physique est définie ?	☐	
11.1.3	Sécurisation des bureaux, des salles et des installations	Une politique pour la sécurisation des bureaux, des salles et des installations est définie ?	☐	
11.1.4	Protection contre les menaces externes et environnementales	Une politique pour la protection contre les menaces externes et environnementales est définie ?	☐	
11.1.5	Travail dans des zones sécurisées	Une politique pour travailler dans des zones sécurisées est définie ?	☐	
11.1.6	Zones de livraison et de chargement	Une politique pour les zones de livraison et de chargement est définie ?	☐	

11.2	**Équipement**			
11.2.1	Implantation et la protection des équipements	Une politique pour l'implantation et la protection des équipements est définie ?	☐	
11.2.2	Prise en charge des services publics	Une politique pour la prise en charge des services publics est définie ?	☐	
11.2.3	Sécurité du câblage	Une politique pour la sécurité du câblage est définie ?	☐	
11.2.4	Maintenance de l'équipement	Une politique pour la maintenance de l'équipement est définie ?	☐	
11.2.5	Élimination des actifs	Une politique pour l'élimination des actifs est définie ?	☐	
11.2.6	Sécurité de l'équipement et des actifs hors des locaux	Une politique pour la sécurité de l'équipement et des actifs hors des locaux est définie ?	☐	
11.2.7	Élimination ou réutilisation sécurisées de l'équipement	Élimination ou réutilisation sécurisées de l'équipement ?	☐	
11.2.8	Équipement utilisateur sans surveillance	Une politique pour l'équipement utilisateur laissé sans surveillance est définie ?	☐	
11.2.9	Politique pour un bureau et un écran inutilisés	Une politique pour un bureau et un écran inutilisés est définie ?	☐	
12	***Sécurité liée à l'exploitation***			
12.1	**Procédures et responsabilités liées à l'exploitation**			
12.1.1	Procédures d'exploitation documentées	Une politique pour les procédures d'exploitation documentées est définie ?	☐	
12.1.2	Gestion des modifications	Une politique sur la gestion du changement est définie ?	☐	
12.1.3	Gestion des capacités	ne politique sur la gestion de la capacité est définie ?	☐	
12.1.4	Séparation des environnements de développement, de test et d'exploitation	Une politique pour la séparation des environnements de développement, de test et d'exploitation est définie ?	☐	
12.2	**Protection contre les logiciels malveillants**			
12.2.1	Contrôles contre les logiciels malveillants	Une politique pour les contrôles contre les logiciels malveillants est définie ?	☐	
12.3	**Sauvegarde du système**			
12.3.1	Sauvegarde	Une politique pour la sauvegarde des systèmes est définie ?	☐	
12.3.2	Sauvegarde des informations	Une politique pour la sauvegarde des informations est définie ?	☐	
12.4	**Journalisation et surveillance**			
12.4.1	Journalisation des événements	Une politique pour la journalisation des événements est définie ?	☐	

12.4.2	Protection des informations de journalisation	Une politique pour la protection des informations de journalisation est définie.	☐	
12.4.3	Journaux des administrateurs et des opérateurs	Une politique pour les journaux des administrateurs et des opérateurs est définie ?	☐	
12.4.4	Synchronisation des horloges	Une politique pour la synchronisation des horloges est définie ?	☐	
12.5	**Maîtrise des logiciels en exploitation**			
12.5.1	Installation de logiciels sur les systèmes opérationnels	Une politique pour l'installation de logiciels sur les systèmes opérationnels est définie ?	☐	
12.6	**Gestion des vulnérabilités techniques**			
12.6.1	Gestion des vulnérabilités techniques	Une politique pour la gestion des vulnérabilités techniques est définie ?	☐	
12.6.2	Restrictions à l'installation de logiciels	Une politique sur les restrictions à l'installation de logiciels est définie ?	☐	
12.7	**Considérations liées à l'audit des systèmes d'information**			
12.7.1	Contrôle de l'audit des systèmes d'information	Une politique pour le contrôle de l'audit des systèmes d'information est définie ?	☐	
13	***Sécurité des communications***			
13.1	**Gestion de la sécurité des réseaux**			
13.1.1	Contrôles réseau	Une politique pour les contrôles réseau est définie ?	☐	
13.1.2	Sécurité des services réseau	Une politique pour la sécurité des services réseau est définie ?	☐	
13.1.3	Ségrégation dans les réseaux	Une politique pour la ségrégation dans les réseaux est définie ?	☐	
13.2	**Transfert de l'information**			
13.2.1	Politiques et procédures de transfert d'informations	Une politique pour les politiques et procédures de transfert d'informations est définie ?	☐	
13.2.2	Accords sur le transfert d'informations	Une politique pour les accords sur le transfert d'informations est définie ?	☐	
13.2.3	Messagerie électronique	Une politique pour la messagerie électronique est définie ?	☐	
13.2.4	Accords de confidentialité ou de non-divulgation	Une politique pour les accords de confidentialité ou de non-divulgation est définie ?	☐	
13.2.5	Acquisition, développement et maintenance de systèmes	Une politique pour l'acquisition, le développement et la maintenance des systèmes est définie ?	☐	
14	***Acquisition, développement et maintenance de systèmes***			
14.1	**Exigences de sécurité applicables aux systèmes d'information**			
14.1.1	Analyse et la spécification des exigences en matière de sécurité des informations	Une politique définie pour l'analyse et la spécification des exigences en matière de sécurité des informations est définie ?	☐	

14.1.2	Sécurisation des services d'application sur les réseaux publics	Une politique pour la sécurisation des services d'application sur les réseaux publics est définie ?	☐	
14.1.3	Protection des transactions de services d'application	Une politique pour la protection des transactions de services d'application est définie ?	☐	
14.2	**Sécurité dans les processus de développement et d'assistance**			
14.2.1	Développement interne	Une politique pour le développement interne est définie ?	☐	
15	***Relations avec les fournisseurs***			
15.1.1	Relations avec les fournisseurs	Une politique sur les relations avec les fournisseurs est définie ?	☐	
16	***Gestion des incidents liés à la sécurité de l'information***			
16.1.1	Gestion de la sécurité de l'information	Une politique sur la gestion de la sécurité de l'information est définie ?	☐	
17	***Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité***			
17.1	**Continuité de la sécurité de l'information**			
17.1.1	Continuité de la sécurité de l'information	Une politique sur la continuité de la sécurité de l'information est définie ?	☐	
17.2	**Licenciements**			
17.2.1	Licenciements	Une politique pour les licenciements est définie ?	☐	
18	***Conformité***			
18.1	**Conformité aux obligations légales et réglementaires**			
18.1.1	Identification des lois applicables et des exigences contractuelles	Une politique pour l'identification des lois applicables et des exigences contractuelles est définie ?	☐	
18.1.2	Droits de propriété intellectuelle	Une politique pour les droits de propriété intellectuelle est définie ?	☐	
18.1.3	Protection des enregistrements	Une politique pour la protection des enregistrements est définie ?	☐	
18.1.4	Vie privée et la protection des informations personnellement identifiables	Une politique pour la vie privée et la protection des informations personnellement identifiables est définie ?	☐	
18.1.5	Régulation du contrôle cryptographique	Une politique pour la régulation du contrôle cryptographique est définie ?	☐	
18.1	**Examen indépendant de la sécurité de l'information**			
18.1.1	Conformité aux politiques et normes de sécurité	Une politique pour la conformité aux politiques et normes de sécurité est définie ?	☐	
18.1.2	Examen de la conformité technique	Une politique pour l'examen de la conformité technique est définie ?	☐	

EXCLUSION DE RESPONSABILITÉ

Tous les articles, modèles ou informations proposés par Smartsheet sur le site web sont fournis à titre de référence uniquement. Bien que nous nous efforcions de maintenir l'information à jour et exacte, nous ne faisons aucune déclaration, ni n'offrons aucune garantie, de quelque nature que ce soit, expresse ou implicite, quant à l'exhaustivité, l'exactitude, la fiabilité, la pertinence ou la disponibilité du site Web, ou des informations, articles, modèles ou graphiques liés, contenus sur le site. Toute la confiance que vous accordez à ces informations relève de votre propre responsabilité, à vos propres risques.

Ce modèle n'est fourni qu'à titre d'exemple. Ce modèle ne saurait en aucun cas être considéré comme des conseils juridiques ou de conformité. Les utilisateurs de ce modèle doivent déterminer les informations nécessaires dont ils ont besoin pour atteindre leurs objectifs.