Annexe C – Rôles adjacents à la cybersécurité au sein des organisations

En plus des rôles **principaux** qui définissent la profession en cybersécurité dont il est question dans cette NPN, il existe un certain nombre de rôles **adjacents** qui ont des responsabilités en matière de cybersécurité qui ne constituent normalement qu'une partie de leurs responsabilités générales au sein d'une organisation. Bien qu'ils soient souvent employés dans le domaine de la cybersécurité qu'à temps partiel, la portée et l'étendue dans laquelle ils remplissent ces rôles varient en fonction de la taille de l'organisation, du type et du degré d'infrastructure informatique ou Internet. Par exemple, pour les grandes organisations qui utilisent les technologies de l'information, tous les rôles suivants peuvent s'appliquer. Pour les petites organisations qui ne dépendent pas trop des TI ou de la connectivité Internet pour la conduite de leurs affaires, il est probable qu'une majorité de l'expertise et des services techniques seront externalisés. En conséquence, les autres responsabilités non techniques en matière de cybersécurité seront réparties au sein de l'organisation.

Ce tableau présente brièvement les rôles adjacents communs en matière de cybersécurité[9], l'ID NICE correspondante le cas échéant, la CNP associée et les principales responsabilités en matière de cybersécurité. En supposant que la majorité des personnes occupant ces fonctions possèdent déjà les compétences requises pour leurs rôles et fonctions principaux, seules les fonctions de cybersécurité sont dotées de compétences clés.[10] Plus précisément, pour la communauté de la main-d'œuvre existante et en particulier, les éducateurs, ceux-ci devraient orienter la discussion sur l'adaptation des programmes de formation et d'éducation afin de mieux refléter les réalités de la cybersécurité sur le marché du travail canadien.

[9] D'autres rôles seront ajoutés au fur et à mesure de leur détermination ou de leur émergence et suivront le processus de mise à jour de la NPN décrit dans la section *Examen et révision* présentée plus haut dans ce document.

[10] Le préfixe « cyber » indique une spécialisation dans le domaine cybernétique, mais tous les postes ci-dessous sont censés avoir les compétences requises pour soutenir leur fonction organisationnelle principale. Par exemple, un cyberinstructeur est censé avoir toutes les compétences nécessaires pour soutenir l'enseignement en plus de la connaissance/l'expérience du domaine cybernétique.

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
Supervision et gouvernance	Directeur général/haute direction/propriétaire	OV-EXL-001	0012 0013	Exécute les pouvoirs de décision et établit une vision et une orientation pour les ressources ou les opérations cybernétiques et connexes d'une organisation.	Cyberplanification stratégique Contexte d'entreprise et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité
	Directeur de l'informatique/directeur de la technologie	Aucune	0012 0013 0211 0213	Dirige et exécute les pouvoirs décisionnels liés aux TI organisationnelles, à l'infrastructure et aux services techniques. Cela inclut souvent les services de cybersécurité.	Cyberplanification stratégique Contexte d'entreprise et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité Évaluation et mesure de la cybersécurité
	Cyberconseiller juridique	OV-LGA-001	4112 4211	Fournit des conseils juridiques et des recommandations sur des sujets pertinents liés au droit de la cybernétique.	Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contexte de menace

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Agent de protection de la vie privée/gestionnaire du respect de la vie privée	OV-LGA-002	0213	Élabore et supervise le programme de respect de la vie privée et le personnel chargé de ce programme, en soutenant les besoins des responsables de la protection de la vie privée et de la sécurité et de leurs équipes en matière de conformité, de gouvernance/politique et de réponse aux incidents.	Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contexte de menace Contrôles de sécurité relatifs à la protection de la vie privée
	Gestionnaire de la sécurité des communications (SECOM)	OV-MGT-002	0131 0213	Personne qui gère les ressources de sécurité des communications (SECOM) d'une organisation (CNSSI 4009) ou le gardien des clés d'un système de gestion de clés de chiffrement	Gestion du programme de sécurité PCA/PIC Gestion des risques liés à la chaîne d'approvisionnement Politiques, lignes directrices et exigences de gestion de la SECOM Comptabilité de la SECOM Infrastructure et applications de chiffrement/d'ICP Gestion des incidents de la SECOM
	Développeur et gestionnaire de la main-d'œuvre du cyberespace	OV-SPP-001	4156	Élabore des plans, des stratégies et des orientations pour la main-d'œuvre du cyberespace afin de répondre aux besoins en matière de main-d'œuvre, de personnel, de formation et d'éducation et de tenir compte des changements apportés à la politique, à la doctrine, au matériel, à la structure des forces et aux besoins en matière d'éducation et de formation dans le cyberespace.	Parcours professionnel dans le domaine de la cybersécurité Sources et renseignements sur le marché du travail en cybersécurité Normes professionnelles en matière de cybersécurité Certifications et accréditations de cybersécurité Évaluation des compétences en matière de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Développeur de programmes d'enseignement en ligne	OV-TEA-001	4011 4021 4216	Élabore, planifie, coordonne et évalue les cours, méthodes et techniques de cyberformation/d'éducation en fonction des besoins pédagogiques.	Connaissance pertinente du domaine cybernétique (par thème) Évaluation des compétences en matière de cybersécurité
	Cyberinstructeur	OV-TEA-002	4011 4021 4216	Élabore et mène la formation ou l'éducation du personnel dans le domaine cybernétique.	Connaissance pertinente du domaine cybernétique (par thème) Évaluation des compétences en matière de cybersécurité
	Planificateur de cyberpolitiques et de stratégies	OV-SPP-002	0412 4161	Élabore et maintient des plans, une stratégie et une politique de cybersécurité pour soutenir les initiatives organisationnelles de cybersécurité et la conformité réglementaire, et s'y aligner.	Gestion du programme de cybersécurité PCA/PIC Contexte juridique et politique du cyberespace Contexte d'entreprise et de menace Planification et développement de la cyberpolitique Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Gestionnaire de programme	OV-PMA-001	0012 0013 0211	Dirige, coordonne, communique et intègre la réussite globale du programme, et en est responsable, en veillant à l'alignement avec les priorités de l'agence ou de l'entreprise.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Gestion du programme de cybersécurité PCA/PIC Gestion des risques liés à la chaîne d'approvisionnement Modèles de cybermaturité Normes de cybersécurité Évaluation et mesure de la cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Chef de projet des TI	OV-PMA-002	0211 0213	Gère directement les projets de technologie de l'information.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Intégration des cybersystèmes Gestion de projets de cybersécurité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Gestionnaire du soutien des produits	OV-PMA-003	0211 0213	Gère l'ensemble des fonctions de soutien nécessaires pour mettre en œuvre et maintenir l'état de préparation et la capacité opérationnelle des systèmes et des composants.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Intégration des cybersystèmes Gestion de projets de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Processus d'essais et d'évaluation des produits de cybersécurité Gestion du cycle de vie des produits de cybersécurité
	Gestionnaire d'investissement/de portefeuille de TI	OV-PMA-004	0211 0213	Gère un portefeuille d'investissements dans les TI qui s'alignent sur les besoins globaux de la mission et les priorités de l'entreprise.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Gestion du programme de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Modèles de cybermaturité Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité
	Auditeur de programmes de TI	OV-PMA-005	0211 0213	Effectue des évaluations d'un programme de TI ou de ses composantes individuelles pour déterminer la conformité aux normes publiées.	Politiques, pratiques et procédures d'audit de cybersécurité Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Contexte juridique et politique Exigences de conformité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Évaluation de vulnérabilité Processus d'essai et d'évaluation de la cybersécurité
	Analyste commercial	Aucune	1122 2171 4162	Analyse et détermine les besoins, recommande des solutions qui apportent une valeur commerciale aux parties prenantes.	Gouvernance, rôles et responsabilités de la cybersécurité Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Contexte juridique et politique Exigences de conformité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Évaluation de vulnérabilité Processus d'essai et d'évaluation de la cybersécurité
	Analyste financier	Aucune	1112	Collecte et analyse les renseignements financiers et les risques. Fournit des estimations, des prévisions et des tendances financières connexes. Fournit des	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				conseils pour soutenir les activités financières et d'investissement.	Contexte juridique, politique et financier Exigences du programme de cybersécurité Approvisionnement et acquisition dans le domaine de la cybersécurité Évaluation et mesure de la cybersécurité
	Analyste des risques	Aucune	1112 4162	Collecte et analyse les risques organisationnels. Fournit des évaluations des risques connexes et des conseils sur les mesures d'atténuation.	Gestion des risques liés à la cybersécurité Méthodes d'évaluation de la menace et des risques Contexte d'entreprise et de menace Contexte juridique, politique et financier Exigences du programme de cybersécurité
	Spécialiste de la communication	Aucune	0124 1123	Planifie, organise et développe la publicité, le marketing et les relations publiques.	Contexte de la cybermenace Contexte juridique et politique Exigences de conformité PCA/PIC Communications lors d'un cyberincident (communications de crise)
	Webmestre/gestionnaire des communications en ligne	Aucune	2175	Recherche, conceptualise, développe et produit des sites Internet et intranet et de médias basés sur le Web.	Menaces à la cybersécurité Vulnérabilités des applications Web Essai et évaluation de logiciels Exigences en matière de réponse aux incidents de cybersécurité
	Spécialiste de l'apprentissage et du développement	Aucune	4011 4021 4216	Élabore, planifie, coordonne et évalue les programmes et activités d'apprentissage et de	Exigences organisationnelles en matière de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				perfectionnement organisationnel et individuel	Rôles et responsabilités en matière de cybersécurité Parcours professionnel dans le domaine de la cybersécurité Évaluation des compétences en matière de cybersécurité
	Planificateur de continuité des activités et de résilience	Aucune	1112 2171	Détermine, coordonne et supervise l'élaboration d'un plan de continuité des activités afin de soutenir la résilience de l'organisation face à la fraude, à la criminalité financière, aux cyberattaques, au terrorisme et aux défaillances des infrastructures.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Exigences organisationnelles en matière de cybersécurité Rôles et responsabilités en matière de cybersécurité Plans, processus et procédures de cybersécurité Gestion des incidents de cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)
	Spécialiste de l'approvisionnement	Aucune	1225	Détermine et acquiert des équipements généraux et spécialisés, des matériaux, des droits fonciers ou d'accès et des services commerciaux pour leur utilisation ou leur transformation ultérieure par leur organisation.	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Gestion de projets de cybersécurité Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Contrôles de cybersécurité (de gestion, opérationnels, techniques) Processus d'essais et d'évaluation des produits de cybersécurité Gestion du cycle de vie des produits de cybersécurité
Conception et développement (Fourniture sécurisée dans la NICE)	Autorisateur (souvent le DI ou le propriétaire du système)	SP-RSK-001	0012 0013 0211	Haut fonctionnaire ou cadre supérieur ayant le pouvoir d'assumer officiellement la responsabilité de l'exploitation d'un système d'information à un niveau de risque acceptable pour les opérations organisationnelles (y compris la mission, les fonctions, l'image ou la réputation), les actifs de l'organisation, les personnes, les autres organisations et la nation (CNSSI 4009).	Cyberplanification stratégique Contexte d'entreprise et de menace Gestion des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Gestion du programme de cybersécurité Évaluation et mesure de la cybersécurité
	Architecte d'entreprise	SP-ARC-001	0211 2147	Développe et maintient des processus d'affaires, des systèmes et des processus d'information pour soutenir les besoins de la mission de l'entreprise; développe des règles et des exigences en matière de technologie de l'information (TI) qui décrivent les architectures de base et cibles.	Cyberobjectifs organisationnels Architecture et conception de la cybersécurité Ingénierie de la cybersécurité Évaluation de la menace et des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Intégration des cybersystèmes Chiffrement/ICP
	Développeur de logiciels	SP-DEV-001	2241 2233 2243	Développe, crée, entretient et écrit/code de nouvelles applications informatiques, des logiciels ou des programmes utilitaires spécialisés (ou modifie ceux qui existent déjà).	Vulnérabilités des systèmes et des logiciels Essais et évaluation de la sécurité logicielle Outils, techniques et procédures de sécurité logicielle Pratiques et outils d'évaluation de la vulnérabilité et d'essais de pénétration Identité, justificatifs d'identité et authentification
	Planificateur des besoins en systèmes	SP-SRP-001	2147 2171 2261	Consulte les clients pour évaluer les exigences fonctionnelles et traduire ces exigences en solutions techniques	Cyberobjectifs organisationnels Architecture et conception de la cybersécurité Ingénierie de la cybersécurité Évaluation de la menace et des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement/ICP Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité Identité, justificatifs d'identité et authentification

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
	Spécialiste d'essai et d'évaluation de système	SP-TST-001	2173 2171 2174 2283	Planifie, prépare et exécute des essais de systèmes pour évaluer les résultats par rapport aux spécifications et aux exigences, et analyse/rapporte les résultats des essais.	Vulnérabilités des systèmes et des logiciels Essais et évaluation de la sécurité des systèmes et des logiciels Outils, techniques et procédures de sécurité logicielle Pratiques et outils d'évaluation de la vulnérabilité et d'essais de pénétration Normes de cybersécurité Évaluation et mesure de la cybersécurité
	Développeur de systèmes	SP-SYS-002	2147 2173 2174	Conçoit, développe, met à l'essai et évalue les systèmes d'information tout au long du cycle de vie du développement de système.	Architecture et conception de la cybersécurité Ingénierie de la cybersécurité Évaluation de la menace et des risques Contexte juridique et politique du cyberespace Exigences de conformité en cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques) Intégration des cybersystèmes Chiffrement/ICP Normes de cybersécurité Évaluation et mesure de la cybersécurité Gestion du cycle de vie des produits de cybersécurité Identité, justificatifs d'identité et authentification
	Développeur Web	Aucune	2175	Recherche, conceptualise, développe et produit des sites	Menaces à la cybersécurité Vulnérabilités des applications Web

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				Internet et intranet et de médias basés sur le Web.	Essai et évaluation de logiciels Exigences en matière de réponse aux incidents de cybersécurité
	Administrateur des bases de données	OM-DTA-001	2172	Administre les bases de données ou les systèmes de gestion des données qui permettent le stockage, l'interrogation, la protection et l'utilisation des données en toute sécurité.	Sécurité des systèmes et des données Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification
	Analyste de données	OM-DTA-002	2172	Examine des données provenant de multiples sources disparates dans le but de fournir des renseignements sur la sécurité et la vie privée. Conçoit et met en œuvre des algorithmes personnalisés, des processus de flux de travail et des configurations pour des ensembles de données complexes à l'échelle de l'entreprise, utilisés à des fins de modélisation, d'exploration de données et de recherche.	Sécurité des systèmes et des données Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification
	Gestionnaire de l'information (gestionnaire des connaissances de la NICE)	OM-KMG-001	0213 1523	Responsable de la gestion et de l'administration des processus et des outils qui permettent à l'organisation de déterminer et de documenter le capital intellectuel et le contenu de l'information, et d'y accéder.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Catégorisation des renseignements/données Sécurité des systèmes et des données

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
					Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification
	Spécialiste en soutien technique	OM-STS-001	2281 2282	Fournit un soutien technique aux clients qui ont besoin d'aide en utilisant du matériel et des logiciels au niveau du client, conformément aux composantes des processus organisationnels établis ou approuvés (c'est-à-dire le plan directeur de gestion des incidents, le cas échéant).	Contexte d'entreprise et de menace Sécurité des systèmes et des données Sauvegarde et récupération des données Cybermenaces et vulnérabilités Réponse aux incidents Politiques, pratiques et opérations des cybersystèmes
	Spécialiste des opérations réseau	OM-NET-001	2281 2282	Planifie, met en œuvre et exploite des services/systèmes de réseau, y compris le matériel et les environnements virtuels.	Contexte d'entreprise et de menace Sécurité des systèmes et des données Sauvegarde et récupération des données Cybermenaces et vulnérabilités Réponse aux incidents Politiques, pratiques et opérations des cybersystèmes
	Administrateur du système	OM-ADM-001	2281	Responsable de la mise en place et de la maintenance d'un système ou d'éléments spécifiques d'un système (par exemple, installation, configuration et mise à jour du matériel et des logiciels; création et	Contexte d'entreprise et de menace Sécurité des systèmes et des données Sauvegarde et récupération des données

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				gestion des comptes d'utilisateurs; supervision ou réalisation de tâches de sauvegarde et de récupération; mise en œuvre de contrôles de sécurité opérationnels et techniques; et respect des politiques et procédures de sécurité organisationnelle).	Cybermenaces et vulnérabilités Réponse aux incidents Politiques, pratiques et opérations des cybersystèmes Identité, justificatifs d'identité et authentification
	Analyste des systèmes de données	Aucune	2172	Détermine, développe et analyse les besoins en matière de systèmes de données pour l'organisation. Prend en charge, conçoit et met en œuvre des systèmes de données.	Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Sécurité des systèmes et des données Menaces et vulnérabilités des systèmes de données Planification de la reprise après sinistre Sauvegarde et récupération des données Identité, justificatifs d'identité et authentification Outils, techniques et procédures de cybersécurité utilisés pour protéger les données et les systèmes de données Chiffrement et ICP
	Gestionnaire des systèmes (comprend les rôles de gestionnaire des systèmes, des logiciels et des systèmes de données)	Aucune	0213	Planifie, organise, dirige, contrôle et évalue les activités des organisations qui analysent, conçoivent, développent, mettent en œuvre, exploitent et administrent des logiciels informatiques et de	Évaluation de la menace et des risques Gestion des risques liés à la cybersécurité Contexte d'entreprise et de menace Contexte technique Intégration des cybersystèmes

Domaine d'activité/catégorie de travail	Titre ou rôle de travail commun	ID NICE	CNP	Responsabilité majeure en matière de cybersécurité (NICE et autres sources)	Compétences clés en matière de cybersécurité
				télécommunications, des réseaux et des systèmes d'information	Gestion de projets de cybersécurité Exigences en matière de cyberapprovisionnement Gestion des risques liés à la chaîne d'approvisionnement Normes de cybersécurité Évaluation et mesure de la cybersécurité Contrôles de cybersécurité (de gestion, opérationnels, techniques)