



RÉPUBLIQUE TOGOLAISE

Repertoire des standards TIC



Contrôle des modifications du document :

Historique des validations			
Numéro de version	Date	Rôle/Instance/Entité	Auteur
1	29-01-2023	Directeur	Mohamed Wassel BELHADJ
2	20-02-2023	Consultante	Senda GHALLEB
3	22-05-2023	Consultant	Mahdi EZZINE
4	06-07-2023	Consultant	Mahdi EZZINE

Historique des révisions			
Numéro de version	Date	Brève description du changement	Auteur

SOMMAIRE

SOMMAIRE	3
Contexte et objectif du Catalogue de Standards TIC	4
1. Contexte :	5
2. Objectifs du Catalogue de Standards TIC :	6
PRESENTATION DES STANDARDS TIC.....	7
1. Périmètre des Standards TIC :	8
2. Présentation des domaines des standards TIC :	9
Benchmark et répertoire des standards.....	10
1. Benchmark par pays.....	11
2. Pourquoi un benchmark par pays ?.....	13
3. Collecte de standards par famille :	14
4. Tableau des familles de normes préférées et raisons.....	15
.....	17
Liste des standards	17
1. Security Standards	18
2. Interoperabilty Standards	44
3. Data Standard.....	68
4. Identity & Access Management Standards.....	84
5. Development Standards.....	106
6. Artificial Intelligence Standards.....	116
7. User and accessibility Standards	122
8. E-Signature & Transaction Standards.....	133
9. Infrastructure standard	138
Centre de Standardisation	139

Contexte et objectif du Catalogue de Standards TIC

1. Contexte :

Dans le cadre de la feuille de route gouvernementale 2025, l'Agence Togo Digital créée par décret N°2021-102/PR du 29 septembre 2021 accompagne les administrations publiques et parapubliques dans le processus de digitalisation de leur service et des services offerts aux citoyens.



Le gouvernement togolais a initié quarante-deux (42) projets de réforme dans sa feuille de route. Trois quarts de ces projets inclus une composante de digitalisation. La stratégie Togo Digital compte trois (3) axes :

Le succès des projets de digitalisation ou projets à composante digitale inscrits sur la feuille de route gouvernementale 2025 et dans la stratégie Togo Digital 2025 dépend fortement d'une infrastructure digitale cohérente. Cette cohérence est garantie par la capacité de standardisation et d'interopérabilité des systèmes d'information et s'appuie sur des normes permettant d'aider les agences gouvernementales à fournir de meilleurs services aux citoyens, à réduire les coûts et à garantir la protection des informations sensibles contre les cybermenaces.

Les standards de eGovernment désignent les lignes directrices et les spécifications techniques utilisées pour assurer l'interopérabilité, la sécurité et l'accessibilité des services et de l'information électroniques du gouvernement. Ces normes peuvent inclure des lignes directrices sur la structure et le format des sites Web gouvernementaux, l'utilisation des signatures électroniques et de l'authentification, et l'échange sécurisé de données entre les organismes gouvernementaux. L'objectif des normes de eGovernment est d'améliorer l'efficience et l'efficacité des services gouvernementaux et de les rendre plus accessibles aux citoyens et aux entreprises.

2. Objectifs du Catalogue de Standards TIC :

La digitalisation n'est pas un but en elle-même. Elle permet à un gouvernement et ses administrations d'améliorer la qualité des services offerts aux citoyens tout en améliorant l'efficacité, la fiabilité et la productivité dans la délivrance de ces services.

Le cadre d'interopérabilité est un ensemble d'accords et de lignes directrices visant à garantir la cohérence des systèmes d'information dans les évolutions programmées.

Les standards TIC jouent un rôle primordial dans la facilitation de l'interopérabilité syntaxique et lexicale entre les systèmes d'information tout en assurant l'adoption de normes approuvées au niveau international.

Les objectifs spécifiques des standards TIC du Togo sont les suivants :



Dans l'ensemble, les objectifs des normes relatives à l'administration en ligne sont d'améliorer la prestation des services gouvernementaux, d'accroître l'efficacité et la transparence des opérations gouvernementales et d'améliorer la qualité de vie globale des citoyens et des entreprises.

PRESENTATION DES STANDARDS TIC

1. Périmètre des Standards TIC :

Le champ d'application des standards TIC couvre trois types d'interactions :

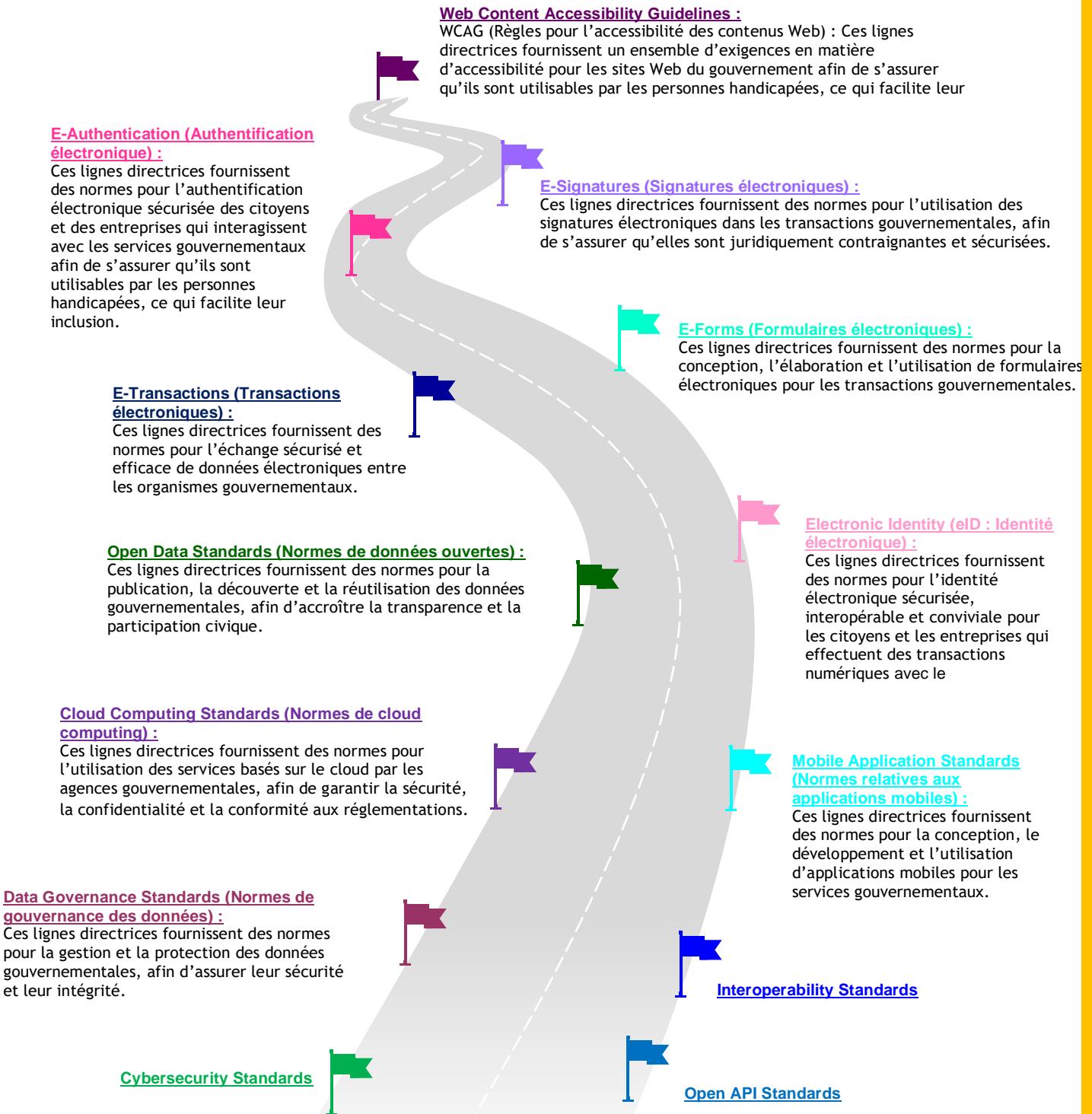


Ainsi, différents types d'acteurs prennent part aux échanges couverts par le périmètre du cadre d'interopérabilité :



2. Présentation des domaines des standards TIC :

Plusieurs normes de eGovernment peuvent être utilisées au niveau du Togo, notamment :



Benchmark et répertoire des standards

1. Benchmark par pays

Pays	Raison de la sélection	Normes numériques uniques	Taux de digitalisation (%)	Source
Singapour	Leader mondial en matière de transformation numérique et investissement important dans les infrastructures numériques.	Gouvernement engagé dans la numérisation, programmes de formation pour les travailleurs de la technologie	98%	Digital Readiness Blueprint (2021)
Royaume-Uni	Culture de l'innovation forte, adoption large des technologies numériques, initiatives de transformation numérique du gouvernement	Engagement du gouvernement en faveur de l'ouverture des données, normes élevées en matière de protection des données	96%	Global Digital Report (2021)
Corée du Sud	Adoption rapide des technologies de l'information, infrastructure de connectivité solide, investissements gouvernementaux dans la recherche et l'innovation, initiatives gouvernementales pour encourager l'innovation	Initiative de gouvernement électronique, cybersécurité, technologies de l'information et de la communication avancées	95%	Global Digital Report (2021)
Australie	Adoption rapide des technologies de l'information, infrastructure de connectivité solide, investissements gouvernementaux dans l'innovation et la recherche.	Normes strictes en matière de cybersécurité, initiatives gouvernementales pour encourager l'innovation.	86%	Global Digital Report (2021)
Union Européenne	Normes élevées en matière de protection des données, initiatives de transformation numérique de l'UE, cybersécurité, développement de l'infrastructure numérique européenne, initiatives	Règlement général sur la protection des données, stratégie pour le marché unique numérique, programmes de recherche et d'innovation numériques	85%	Digital Economy and Society Index 2020

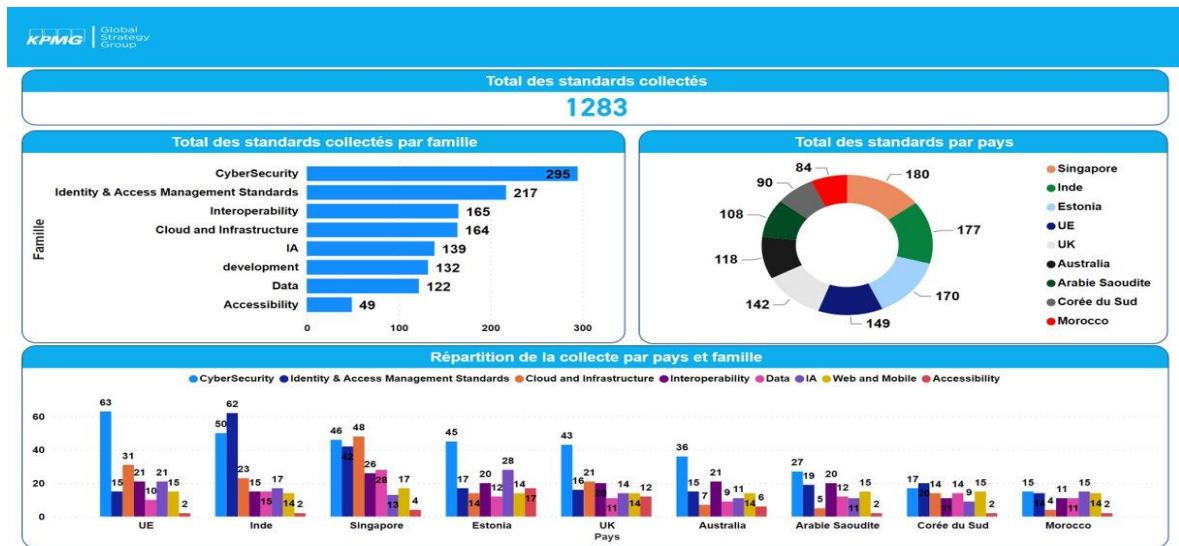
	pour encourager l'innovation			
Estonie	Première nation e-gouv du monde, programmes de numérisation des services publics, normes élevées en matière de cybersécurité	Infrastructures numériques avancées, normes de confidentialité élevées pour les données des citoyens	76%	Global Digital Report (2021)
Arabie Saoudite	Stratégie nationale de transformation numérique, forte utilisation des technologies émergentes, investissements dans les infrastructures de connectivité	Forte adoption des technologies de l'information par le gouvernement, initiatives de cybersécurité	73%	Global Digital Report (2021)
Maroc	Stratégie nationale de transformation numérique, développement rapide de l'écosystème de start-ups	Projet de cyberparc technologique, engagement du gouvernement en faveur de la modernisation des services publics	68%	Global Digital Report (2021)
Inde	Forte adoption de technologies numériques dans les secteurs public et privé, investissement important dans les infrastructures numériques	Une plateforme numérique pour les services aux citoyens (Aadhaar), des initiatives de Smart City et une infrastructure de cybersécurité solide	34%	Global Digital Report (2021)

2. Pourquoi un benchmark par pays ?

Le benchmarking des standards par pays permet de :

- ❖ Le benchmarking des standards utilisés par différents pays permet de comprendre les meilleures pratiques en matière de normes et de réglementations. Cela permet d'identifier les pays qui ont mis en place des normes efficaces et bien adaptées, et d'apprendre de leurs expériences.
- ❖ Le benchmarking permet d'évaluer la conformité des normes et des réglementations dans différents pays. Cela permet de comparer les exigences et les obligations imposées aux organisations en matière de données, de confidentialité, de sécurité, etc. Cela peut aider les organisations à s'assurer qu'elles respectent les normes internationales et les exigences locales.
- ❖ Le benchmarking peut contribuer à l'harmonisation des pratiques et des normes entre les pays. En identifiant les similitudes et les différences dans les normes utilisées, il est possible de favoriser une meilleure coopération et une meilleure coordination entre les pays pour promouvoir des normes communes et alignées.
- ❖ Le benchmarking des standards utilisés par les pays fournit des informations précieuses pour la prise de décision éclairée. Cela permet aux décideurs, aux régulateurs et aux acteurs concernés de comprendre les forces et les faiblesses des normes en vigueur dans différents pays, ce qui peut orienter les politiques et les stratégies en matière de données, de protection de la vie privée, de sécurité, etc.

3. Collecte de standards par famille :



Au total, 1283 normes ont été recensées dans le cadre de l'étude. Les quatre familles de normes les plus fréquemment mentionnées sont la cybersécurité (en première position), l'identity & Access Management (en deuxième position), l'interopérabilité (en troisième position) et Cloud & Infrastructure (en quatrième position). Les pays ayant le plus grand nombre de normes recensées sont Singapour, l'Inde, l'Estonie, l'UE et le Royaume-Uni. On observe que la majorité des pays sont en tête dans le domaine de la cybersécurité. La domination exceptionnelle de l'Inde dans le domaine de l'identity & AccessManagement est remarquable.

À la suite de notre collecte des standards présents dans les différents pays suivants tels que :

Le Singapour 180 standards, L'inde 173 standards, L'Estonie 161 standards, l'UE 143 standards, Le Royaume Uni 136 standards , L'Australie 113 standards, La Corée du Sud 81 standards , L'Arabie Saoudite 102 standards et Le Maroc 78.

On constate que la majorité des standards collectés se retrouvent dans la famille de CyberSecurity avec un total de 295 standards, Identity & Access Management Standards avec un total de 217, ensuite l'interopérabilité avec 165 Standards, Cloud and Infrastructure Standards avec un total de 164 ,IA Standards avec un total de 139, Le Développement Standards avec un total de 132, data management standards avec un total de 122 et L'accessibilité avec 49 Standards.

4. Tableau des familles de normes préférées et raisons

Famille	Définition	Raisons du choix	Normes spécifiques ou références	Défis ou problèmes visés
User Centric & Accessibility	Standards visant à assurer une expérience conviviale pour tous les utilisateurs, en mettant l'accent sur l'accessibilité pour les personnes ayant des capacités spécifiques.	Assurer une expérience conviviale pour tous les utilisateurs, indépendamment de leurs capacités spécifiques.	WCAG 2.1 (Web Content Accessibility Guidelines)	Accès équitable aux services et aux informations pour les personnes handicapées ou ayant des limitations
Identity & Access Management	Standards pour garantir la sécurité des informations personnelles, prévenir les accès non autorisés et faciliter l'authentification des utilisateurs.	Garantir la sécurité des informations personnelles, prévenir les accès non autorisés et faciliter l'authentification des utilisateurs.	OAuth 2.0, SAML (Security Assertion Markup Language)	Prévention des violations de données, contrôle des accès non autorisés, protection de l'identité des utilisateurs
Development	Standards pour améliorer la qualité, la fiabilité et la maintenabilité des applications logicielles, tout en favorisant la collaboration entre les développeurs.	Améliorer la qualité, la fiabilité et la maintenabilité des applications logicielles tout en favorisant la collaboration entre les développeurs.	Agile, DevOps	Gestion des projets complexes, amélioration de la qualité du code, réduction des délais de développement
Artificial Intelligence	Standards pour assurer la responsabilité, l'éthique et la transparence de l'utilisation de l'intelligence artificielle (IA) et garantir des systèmes d'IA fiables et respectueux de la vie privée	Assurer la responsabilité, l'éthique et la transparence de l'utilisation de l'intelligence artificielle (IA) et garantir des systèmes d'IA fiables et respectueux de la vie privée	Ethical AI Framework, IEEE P7003 (Standard for Algorithmic Bias Considerations)	Prévention des discriminations, transparence dans les décisions automatisées, responsabilité des systèmes d'IA

	vie privée.			
Interoperability	Standards visant à favoriser l'échange de données et la communication entre différents systèmes, facilitant l'intégration et l'interopérabilité des solutions informatiques.	Favoriser l'échange de données et la communication entre différents systèmes, faciliter l'intégration et l'interopérabilité des solutions informatiques.	HL7 (Health Level Seven), DICOM (Digital Imaging and Communications in Medicine)	Incompatibilité des systèmes, fragmentation des données, obstacles à la communication entre les applications
Data Management	Standards pour assurer la qualité, l'intégrité, la confidentialité et la conformité des données collectées, stockées et gérées.	Assurer la qualité, l'intégrité, la confidentialité et la conformité des données collectées, stockées et gérées.	GDPR (General Data Protection Regulation), ISO/IEC 27001	Gestion des risques liés aux données, respect de la vie privée des individus, maintien de l'intégrité des données
Infrastructure	Standards définissant des spécifications techniques et des bonnes pratiques pour la conception, la construction et la maintenance de l'infrastructure informatique.	Définir des spécifications techniques et des bonnes pratiques pour la conception, la construction et la maintenance de l'infrastructure informatique.	ITIL (Information Technology Infrastructure Library), ISO/IEC 20000	Stabilité, performances et disponibilité de l'infrastructure informatique
Security	Standards pour garantir la sécurité des systèmes, des données et des utilisateurs, prévenir les attaques et assurer la conformité aux réglementations en matière de sécurité	Garantir la sécurité des systèmes, des données et des utilisateurs, prévenir les attaques et assurer la conformité aux réglementations en matière de sécurité.	ISO/IEC 27001, NIST Cybersecurity Framework	Gestion des risques liés aux données, respect de la vie privée des individus, maintien de l'intégrité des données

Liste des standards

1. Security Standards

Les normes de cybersécurité sont un ensemble de lignes directrices, de spécifications et de meilleures pratiques pour protéger les systèmes d'information et les réseaux contre les cybermenaces. Les normes visent à fournir un langage et un cadre commun permettant aux organisations de comprendre et de gérer leurs risques de cybersécurité, ainsi que d'aider les organisations à se conformer aux réglementations et aux lois pertinentes dans ce domaine.

Voici une liste de normes de cybersécurité :

ID	Standard/Norme	Version	date de publication	Description	Url Documentation
Cyber_TG_01	CIS Controls	-	2008	Les CIS Controls sont organisés en une liste de 20 contrôles de sécurité essentiels, classés par ordre de priorité, et conçus pour aider les organisations à se protéger contre les cyberattaques courantes. Les contrôles sont conçus pour être pratiques et réalisables, quel que soit le niveau de maturité de la sécurité de l'organisation.	https://www.cisecurity.org/controls
Cyber_TG_02	ISO/IEC 27035	2016	1 juin 2011	Elle fournit des directives pour la gestion des incidents de sécurité de l'information et la réponse aux incidents.	https://www.iso.org/fr/standard/60803.html
Cyber_TG_03	ISO/IEC 27701	2019	6 août 2019	ISO/IEC 27701 est une extension de la norme ISO/IEC 27001, qui est axée sur la gestion de la sécurité de l'information. La norme ISO/IEC 27701 s'applique spécifiquement à la protection des informations personnelles, conformément aux principes et aux exigences du Règlement général sur la protection des données (RGPD) de l'Union européenne.	https://www.iso.org/g/standard/71670.html

Cyber_TG_04	NIST 800	-	décembre 2005	La série de publications NIST 800 couvre différents domaines de la cybersécurité, tels que la gestion des risques, la gestion de la sécurité, la sécurité des systèmes d'information, la sécurité des réseaux, la cryptographie, la sécurité des applications, la sécurité des données, etc.	https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
Cyber_TG_05	ANRT Guidelines	-	2022	Les "ANRT Guidelines" couvrent un large éventail de sujets liés aux télécommunications, tels que l'accès à Internet, la téléphonie mobile, la connectivité, les services de communication, la protection des données personnelles, la sécurité des réseaux, etc.	https://www.anrt.ma/en/reglementation/decisions
Cyber_TG_06	APRA CPS 234	-	1 juillet 2019	CPS 234 est conçu pour renforcer la résilience des institutions financières face aux cybermenaces et pour assurer la protection des données sensibles et des systèmes d'information.	https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
Cyber_TG_07	ASD Essential Eight	-	44888	Ensemble de pratiques de sécurité recommandées développées par l'Agence de la sécurité des systèmes d'information australienne (Australian Signals Directorate - ASD). Ces pratiques visent à aider les organisations à renforcer leur posture de sécurité et à atténuer les risques d'incidents de cybersécurité.	https://www.cyber.gov.au/about-us/news/essential-eight-assessment-guidance-package
Cyber_TG_08	Australian Privacy Principles (APP)	-	12 mars 2014	Les Australian Privacy Principles (APP) sont un ensemble de principes de confidentialité qui régissent la collecte, l'utilisation, la divulgation et la gestion des informations personnelles en Australie. Ils font partie de la loi sur la protection des renseignements personnels et de la Loi sur la confidentialité de 1988 (Privacy Act 1988) de l'Australian Government.	https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles

Cyber_TG_09	BS 10012	-	31 janvier 2017	Elle vise à aider les organisations à mettre en place des processus et des contrôles appropriés pour la gestion de la confidentialité des informations personnelles conformément aux réglementations sur la protection des données.	https://www.bsigroup.com/LocalFiles/en-GB/bs-10012/resources/BSI-BS-10012-Client-Guide-UK-EN.pdf
Cyber_TG_13	CIS Benchmarks	-	2000	Les CIS Benchmarks fournissent des recommandations de configuration spécifiques pour divers systèmes d'exploitation, logiciels, applications et infrastructures, afin d'améliorer leur sécurité. Ils sont élaborés par des experts en sécurité et sont continuellement mis à jour pour tenir compte des nouvelles menaces et des dernières vulnérabilités.	https://www.cisecurity.org/cis-benchmarks
Cyber_TG_14	CISCO SAFE	-	2000	CISCO SAFE fournit des lignes directrices, des bonnes pratiques et des recommandations pour concevoir, déployer et gérer une infrastructure de sécurité efficace. Il couvre divers domaines de sécurité, tels que la protection des périmètres, la prévention des menaces, la sécurisation des communications, la gestion des identités et des accès, la protection des données, etc.	https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html
Cyber_TG_15	CLS	-	4 fevrier 2022	Le Cybersecurity Labelling Scheme (CLS) est un programme de certification et de marquage de la cybersécurité mis en place à Singapour. Il vise à aider les consommateurs et les entreprises à identifier les produits et les solutions qui répondent à des normes de sécurité spécifiques.	https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme

Cyber_TG_16	Code of Practice for Cybersecurity for IOT Systems	-	44409	document qui fournit des lignes directrices et des recommandations pour renforcer la cybersécurité des systèmes IoT	https://www.tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20practice.pdf
Cyber_TG_17	Common Criteria	-	1996	Le Common Criteria (Critères communs) est un ensemble de normes internationales utilisées pour évaluer la sécurité et la fiabilité des produits et des systèmes informatiques.	https://fr.wikipedia.org/wiki/Crit%C3%A8res_communis
Cyber_TG_18	CPS PWG Framework	-	2017	Ce cadre vise à fournir des recommandations et des bonnes pratiques pour garantir la sécurité et la fiabilité des CPS, qui sont des systèmes composés à la fois de composants informatiques et de composants physiques interconnectés. Les CPS comprennent des systèmes tels que les voitures autonomes, les systèmes de contrôle industriel, les systèmes de santé connectés, etc.	http://sewiki.ru/CPS_PWG_Framework
Cyber_TG_20	Cyber Essentials	-	juin 2014	Cyber Essentials est un programme de certification développé par le gouvernement britannique pour aider les organisations à mettre en œuvre des mesures de base de cybersécurité. Il fournit un cadre clair et pratique pour protéger contre les cyberattaques courantes.	https://en.wikipedia.org/wiki/Cyber_Essentials
Cyber_TG_21	Cyber Essentials Scheme/Summary (BIS/14/696)(PDF)	-	2014	Ce document fournit un résumé du Cyber Essentials Scheme, qui est un programme de certification de la cybersécurité destiné aux organisations de toutes tailles.	https://irp-cdn.multiscreensite.com/965ebc71/files/uploaded/Cyber-Essentials-scheme-summary%20%281%29.pdf
Cyber_TG_22	Cyber Essentials technical requirements updated for April 2023	-	avril 2023	Les exigences techniques de Cyber Essentials fournissent un ensemble de contrôles de cybersécurité et de bonnes pratiques que les organisations devraient mettre en œuvre pour	https://www.ncsc.gov.uk/information/cyber-essentials-technical-controls-

				renforcer leur posture de sécurité.	<u>grace-period-update</u>
Cyber_TG_23	Cyber Security Information Sharing Partnership (CiSP)	-	2013	CiSP est une initiative conjointe de l'industrie et du gouvernement mise en place pour échanger des informations sur les cybermenaces en temps réel, dans un environnement sécurisé, confidentiel et dynamique, augmentant la connaissance de la situation et réduisant l'impact sur les entreprises britanniques.	https://www.gov.uk/government/specifications/cyber-security-information-sharing-programme
Cyber_TG_24	Cyber Swachhta Kendra	-	fevrier 2017	Cyber Swachhta Kendra (CSK) est une initiative du gouvernement indien visant à fournir des services de nettoyage et de sécurisation des systèmes informatiques pour les utilisateurs finaux en Inde. Le CSK est géré par le Centre national de réponse aux incidents informatiques (CERT-In), qui est l'agence nationale indienne responsable de la réponse aux incidents de sécurité informatique.	https://www.csk.gov.in/
Cyber_TG_25	Cybersecurity Act	-	5 fevrier 2018	Etablit un cadre réglementaire pour la cybersécurité, notamment la protection des infrastructures critiques, la prévention des cyberattaques et la réponse aux incidents de cybersécurité. Il permet également la mise en place d'une autorité de cybersécurité, le Cyber Security Agency of Singapore (CSA).	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
Cyber_TG_26	Cybersecurity and Critical Infrastructure Protection (CCP)	-	mars 2022	CCP peut également faire référence à la branche de l'Agence de la cybersécurité et de la sécurité des infrastructures (ACSI) aux États-Unis, chargée de la cybersécurité	https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/public/legacy_files/

				et de la protection des infrastructures critiques du pays.	bs/0601_cscip_preliminary.pdf
Cyber_TG_27	Cybersecurity Capability Maturity Model (C2M2)	V2	2021	Il fournit une structure pour évaluer les capacités actuelles de cybersécurité d'une organisation et identifier les domaines d'amélioration	https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf
Cyber_TG_28	Cybersecurity Code of Practice	V2.0	2022	Le "Cybersecurity Code of Practice" est un document publié par le gouvernement du Royaume-Uni qui fournit des conseils pratiques aux entreprises sur les mesures de sécurité à prendre pour protéger leurs systèmes informatiques et leurs données contre les cybermenaces. Le code de pratique est conçu pour aider les organisations à mettre en place des mesures de sécurité solides et à réduire les risques liés à la cybercriminalité.	https://www.csa.gov.sg/docs/default-source/legislation/cop_second-edition.pdf?sfvrsn=b2ab666a_2
Cyber_TG_29	Cybersecurity Labelling Scheme (CLS)	-	2022	L'Agence de cybersécurité de Singapour (CSA) a lancé le système d'étiquetage de cybersécurité (CLS) pour les appareils intelligents grand public, dans le cadre des efforts visant à améliorer la sécurité de l'Internet des objets (IoT), à relever les niveaux globaux de cyberhygiène et à mieux sécuriser le cyberspace de Singapour.	https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme
Cyber_TG_30	Cybersecurity Labelling Scheme (CLS) Publication No. 1	-	2023	Le Cybersecurity Labelling Scheme (CLS) est un schéma de marquage volontaire. Les produits qui postulent pour l'obtention du label de cybersécurité doivent passer une série d'évaluations et de tests, en fonction du niveau de label de cybersécurité que le	https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/pub-cls-public-1-overview-of-cls-

				développeur souhaite atteindre.	v12.pdf?sfvrsn=b559ba25_0
Cyber_TG_31	ECSM	-	octobre 2012	l'ECSM vise à promouvoir la sensibilisation, l'éducation et la sécurité en ligne au sein de l'Union européenne.	https://cybersecuritymonth.eu/
Cyber_TG_33	ENISA Cybersecurity Certification Framework	-	2021	Cette initiative de l'ENISA vise à établir un cadre harmonisé pour la certification de la cybersécurité des produits, des services et des processus.	https://www.enisa.europa.eu/topics/certification/eu-cybersecurity-certification-faq
Cyber_TG_34	ENISA Threat Landscape	-	2010	L'ENISA publie régulièrement des rapports sur le paysage des menaces en matière de cybersécurité, fournissant des informations sur les tendances, les risques et les recommandations de mitigation.	https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
Cyber_TG_35	Essentials Scheme: Requirements for basic technical protection from cyber attacks (BIS/14/696) (PDF)	-	2014	Ce guide vise à fournir des exigences de base pour la protection technique contre les attaques cybérénétiques.	https://www.cyberisksinsuranceforum.com/sites/default/files/Cyber_Essentials_Requirements.pdf
Cyber_TG_36	EU Cybersecurity Act	-	7 juin 2019	Le règlement établit un cadre réglementaire pour la certification de la cybersécurité des produits et services numériques, ainsi que pour la création d'un cadre de coopération en matière de cybersécurité au niveau de l'UE.	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
Cyber_TG_37	GDPR	-	42494	GDPR vise à renforcer et à harmoniser la protection des données personnelles des citoyens de l'UE et à responsabiliser les organisations qui collectent, traitent et stockent ces données.	https://gdpr-info.eu/

Cyber_TG_38	GDS Web Security	-	2011	L'objectif de GDS Web Security est de garantir que les sites Web gouvernementaux offrent un niveau élevé de sécurité et de protection des informations sensibles des utilisateurs. Cela inclut la protection contre les cyberattaques, la sécurité des données, la protection de la vie privée des utilisateurs et la conformité aux normes de sécurité établies.	https://www.getgds.com/services/security/web-security
Cyber_TG_40	Health Informatics Society of Australia (HISA) Cybersecurity Guidelines	-	1993	HISA a créé une communauté de pratique de la cybersécurité pour informer et impliquer toutes les parties prenantes sur la cybersécurité dans les soins de santé et influencer l'application de bonnes pratiques. L'utilisation élargie de la technologie en réseau, des appareils, des applications et des ensembles de données électroniques compatibles avec Internet, utilisés pour une gamme de fonctions cliniques, financières et administratives, a considérablement réduit le nombre d'étapes manuelles et de processus chronophages dans les flux de travail des soins de santé.	https://www.hisa.org.au/
Cyber_TG_41	HIPAA	-	21 aout 1996	Une loi américaine qui a été adoptée en 1996 pour protéger la confidentialité, la sécurité et l'intégrité des informations de santé. La loi HIPAA s'applique principalement aux organisations et aux professionnels de la santé aux États-Unis, tels que les médecins, les hôpitaux, les assureurs maladie et d'autres entités qui traitent des informations de santé.	https://www.hhs.gov/hipaa/index.html

Cyber_TG_42	IASME Cyber Assurance	-	25 juillet 2022	Vise à aider les organisations à améliorer leur posture de sécurité et à démontrer leur engagement envers la protection des données et des informations sensibles. Le programme IASME Cyber Assurance se base sur des normes internationales telles que l'ISO/IEC 27001 et l'ISO/IEC 27002, ainsi que sur des réglementations telles que le RGPD.	https://www.cybertecsecurity.com/cyber-security-services/iasme-cyber-assurance/
Cyber_TG_43	IASME Cyber Assurance	-	25 juillet 2022	L'objectif principal de l'IASME Cyber Assurance est d'aider les organisations de toutes tailles à améliorer leur posture de sécurité et à démontrer leur engagement envers la protection des données et des informations sensibles.	SAME comme en haut
Cyber_TG_44	IMDA IoT Cyber Security Guide (2019)	-	2019	Ce guide sert de guide pratique pour les utilisateurs d'entreprise ayant l'intention de déployer des solutions IoT ainsi que pour leurs fournisseurs, en fournissant des recommandations de base, des concepts fondamentaux et des listes de contrôle, en mettant l'accent sur les aspects de sécurité pour l'acquisition, le développement, les opérations et la maintenance de Systèmes IOT.	https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-iot-cyber-security-guide.pdf
Cyber_TG_45	Internet of Things (IoT) Cyber Security Guide	-	2020	Le guide de cybersécurité de l'Internet des objets (IoT) est une ressource qui fournit des lignes directrices et des bonnes pratiques pour sécuriser les dispositifs et les systèmes IoT contre les cybermenaces.	https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf

Cyber_TG_47	ISA/IEC 62443 Series of Standards	-	2009	<p>La série de normes ISA/IEC 62443 est une série de normes internationales développées conjointement par l'International Society of Automation (ISA) et l'International Electrotechnical Commission (IEC). Ces normes visent à fournir un cadre complet pour la cybersécurité des systèmes de contrôle industriel (ICS) et des systèmes automatisés.</p>	https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
Cyber_TG_48	ISM	-	1996	<p>ISM (Information Security Manual) est un document publié par l'Agence australienne de cybersécurité (Australian Cyber Security Centre - ACSC) qui établit les principes et les contrôles de sécurité de l'information pour les organisations gouvernementales australiennes. L'ISM fournit des directives détaillées pour la mise en œuvre d'un cadre de sécurité de l'information solide afin de protéger les informations sensibles et les systèmes informatiques.</p>	https://www.cyber.gov.au/sites/default/files/2023-03/Information%20Security%20Manual%20-%2028March%202023%29.pdf
Cyber_TG_49	ISO/CEI 27005	2011	2011	<p>ISO/CEI 27005 établit un cadre pour l'identification, l'évaluation et la gestion des risques de sécurité de l'information au sein d'une organisation. Elle aide les organisations à mettre en place un processus structuré pour identifier les risques potentiels, évaluer leur impact et leur probabilité, et prendre des mesures pour les traiter.</p>	https://www.iso.org/fr/standard/56742.html
Cyber_TG_50	ISO/CEI 27799	2016	2016	<p>La norme ISO/IEC 27799 est basée sur la norme ISO/IEC 27002, qui est un ensemble plus large de bonnes pratiques en matière de sécurité de l'information. Elle est conçue pour aider les organisations du secteur de la santé à mettre en place des mesures de sécurité</p>	https://www.iso.org/standard/62777.html

				appropriées pour protéger les informations de santé sensibles, telles que les dossiers médicaux électroniques, les données des patients et les systèmes d'information liés aux soins de santé.	
Cyber_TG_51	ISO/IEC 15408	2022	2022	L'ISO/IEC 15408 spécifie un processus d'évaluation de la sécurité selon des critères communs convenus au niveau international. Elle permet d'évaluer la sécurité des produits logiciels, matériels et des systèmes dans le but de déterminer leur niveau de résistance face aux menaces et aux attaques potentielles.	https://www.iso.org/standard/72891.html
Cyber_TG_52	ISO/IEC 27000	2018	2018	ISO/IEC 27000 est une série de normes internationales qui définit les bonnes pratiques et les exigences pour la gestion de la sécurité de l'information (Information Security Management System - ISMS).	https://www.iso.org/standard/73906.html
Cyber_TG_53	ISO/IEC 27001	2022	2022	Norme internationale pour la gestion de la sécurité de l'information, utilisée pour établir, mettre en œuvre, maintenir et améliorer un système de gestion de la sécurité de l'information.	https://www.iso.org/standard/27001
Cyber_TG_54	ISO/IEC 27002	2022	2022	Code de bonnes pratiques pour la gestion de la sécurité de l'information, qui fournit des directives détaillées sur les mesures de sécurité à prendre pour protéger les informations sensibles.	https://www.iso.org/standard/75652.html
Cyber_TG_55	ISO/IEC 27003	2017	2017	ISO/IEC 27003 est une norme internationale publiée par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC). Elle fournit des lignes directrices pour la mise en œuvre d'un système de gestion de la sécurité de l'information.	https://www.iso.org/standard/63417.html

				(SMSI) conformément à la norme ISO/IEC 27001.	
Cyber_TG_56	ISO/IEC 27013:2021/CD Amd 1	2021	25 novembre 2021	La norme ISO/IEC 27013 concerne la gouvernance de la sécurité de l'information et fournit des lignes directrices pour l'intégration de la sécurité de l'information dans la gouvernance globale d'une organisation. Elle vise à assurer une coordination et une collaboration efficaces entre la sécurité de l'information et les autres disciplines de gouvernance de l'organisation.	https://www.iso.org/standard/85922.html
Cyber_TG_57	ISO/IEC 27014	2020	2020	Ce document fournit des conseils sur les concepts, les objectifs et les processus de gouvernance de la sécurité de l'information, par lesquels les organisations peuvent évaluer, diriger, surveiller et communiquer les processus liés à la sécurité de l'information au sein de l'organisation.	https://www.iso.org/standard/74046.html
Cyber_TG_58	ISO/IEC 27032	2012	2012	Elle fournit des directives pour la cybersécurité, en se concentrant spécifiquement sur les problématiques liées à la sécurité de l'information dans le contexte des communications interconnectées.	https://www.iso.org/standard/44375.html
Cyber_TG_59	ISO/IEC 27035	2016	2016	La norme ISO/IEC 27035 concerne la gestion des incidents de sécurité de l'information et des événements liés à la cybersécurité. Elle fournit des lignes directrices et des bonnes pratiques pour la préparation, la réponse, l'analyse et l'amélioration des incidents de sécurité de l'information.	https://www.iso.org/standard/60803.html

Cyber_TG_60	ISO/IEC 27036-1	2021	2021	This document is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. This document addresses perspectives of both acquirers and suppliers.	https://www.iso.org/standard/82905.html
Cyber_TG_61	ISO/IEC 27036-2	2022	2022	Ce document spécifie les exigences fondamentales en matière de sécurité de l'information pour définir, mettre en œuvre, exploiter, surveiller, réviser, maintenir et améliorer les relations avec les fournisseurs et les acquéreurs.	https://www.iso.org/standard/82060.html
Cyber_TG_62	ISO/IEC 27040	2015	2015	La norme ISO/IEC 27040 fournit des directives et des recommandations pour établir, mettre en œuvre, maintenir et améliorer la gestion de la sécurité des informations liée à la continuité des activités. Elle vise à assurer la protection des informations critiques et des systèmes d'information en cas d'incidents majeurs ou de perturbations.	https://www.iso.org/standard/44404.html
Cyber_TG_63	ISO/IEC 27400	2022	2022	Ce document fournit des lignes directrices sur les risques, les principes et les contrôles pour la sécurité et la confidentialité des solutions Internet des objets (IoT).	https://www.iso.org/standard/44373.html
Cyber_TG_64	ISO/IEC 29151	2017	2017	Cette norme adopte la norme internationale ISO/IEC 29151 et fournit des directives pour la protection des informations personnelles identifiables (PII) dans les systèmes d'information.	https://www.iso.org/standard/62726.html

Cyber_TG_65	ISO/IEC 30162	2022	2022	Le présent document spécifie les modèles de réseau pour la connectivité IIoT et les exigences générales de compatibilité pour les dispositifs et les réseaux au sein des systèmes IIoT	https://www.iso.org/standard/53282.html
Cyber_TG_66	ISO/IEC DIS 27402	-	-	Ce document fournit des exigences de base pour les appareils IoT afin de prendre en charge les contrôles de sécurité et de confidentialité.	https://www.iso.org/standard/80136.html
Cyber_TG_67	ISO/IEC TR 27103	-	30 octobre 2018	ISO/IEC TR 27103 est un Rapport Technique (TR) qui fournit des directives sur la gestion des risques de cybersécurité dans le contexte des systèmes de gestion de la sécurité de l'information (SMSI) basés sur ISO/IEC 27001. TR 27103 s'intitule "Systèmes de gestion de la sécurité de l'information - Lignes directrices pour la gestion des risques de cybersécurité".	https://www.iso.org/standard/72437.html
Cyber_TG_68	ISO/IEC WD TR 27103	-	fevrier 2018	ISO/IEC TR 27103:2018 fournit des conseils sur la manière d'exploiter les normes existantes dans un cadre de cybersécurité.	https://www.iso.org/standard/85057.html
Cyber_TG_69	ISO/IEEE 11073-40101	2022	2022	La norme ISO/IEEE 11073-40101 contribue ainsi à améliorer l'efficacité et la sécurité des systèmes de santé en garantissant une communication cohérente et interopérable entre les dispositifs médicaux et les systèmes d'information de santé.	https://www.iso.org/standard/83502.html
Cyber_TG_70	IT Act 2000	-	2000	Une législation indienne qui a été introduite pour faciliter le commerce électronique, l'e-gouvernance et pour aborder diverses cybercriminalités et préoccupations en matière de cybersécurité.	https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

Cyber_TG_71	KS C ISO/IEC 27018	2019	2019	Cette norme adopte la norme internationale ISO/IEC 27018 et définit les bonnes pratiques pour la protection des informations personnelles dans le cloud computing.	https://www.iso.org/fr/standard/76559.html
Cyber_TG_72	KS C ISO/IEC 27032	2023	2023	Cette norme adopte la norme internationale ISO/IEC 27032 et fournit des lignes directrices pour la cybersécurité dans le contexte des réseaux informatiques.	https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf
Cyber_TG_73	MTCS	-	2013	MTCS (Multi-Tier Cloud Security) est un ensemble de normes et de pratiques de sécurité spécifiquement conçues pour l'évaluation et la certification de la sécurité des services cloud à Singapour.	http://cpg.global/wp-content/uploads/2017/09/SS-584-Multi-Tier-Cloud-Security.pdf
Cyber_TG_74	NCSC Cyber Assessment Framework (CAF)	V3.1	2022	Le NCSC Cyber Assessment Framework (CAF) est un cadre d'évaluation de la cybersécurité développé par le National Cyber Security Centre (NCSC) du Royaume-Uni. Le CAF fournit une approche complète pour évaluer la posture de sécurité d'une organisation et identifier les domaines nécessitant des améliorations.	https://www.ncsc.gov.uk/files/NCSC-CAF-v3-1.pdf
Cyber_TG_75	NCSS	-	1921	La NCSS est élaborée par les autorités compétentes en matière de cybersécurité et peut être spécifique à chaque pays.	https://resilience.enisa.europa.eu/enias-ncss-project
Cyber_TG_76	NIST Cybersecurity Framework (CSF)	-	fevrier 2014	Un cadre développé par le National Institute of Standards and Technology (NIST) des États-Unis, utilisé comme référence pour évaluer et améliorer la posture de cybersécurité des organisations.	https://www.nist.gov/itl/smallbusiness/cyber/planning-guides/nist-cybersecurity-framework
Cyber_TG_77	NIST SP 800-146	-	45057	Ce document fournit un aperçu du cloud computing et des recommandations pour son adoption sécurisée.	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf

Cyber_TG_78	NIST SP 800-61	Rev. 2	2012	NIST SP 800-61 établit une approche méthodique pour la gestion des incidents de sécurité, en mettant l'accent sur la coordination et la collaboration entre les différentes parties prenantes, telles que les équipes de sécurité informatique, les équipes de réponse aux incidents, les responsables des systèmes informatiques et les parties prenantes internes et externes.	https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
Cyber_TG_79	NISTIR 8259	-	2020	Le NISTIR 8259, également connu sous le nom de "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline", est un rapport spécial du National Institute of Standards and Technology (NIST) aux États-Unis. Ce rapport fournit des recommandations pour les fabricants de dispositifs IoT (Internet des objets) afin de renforcer la cybersécurité des appareils.	https://csrc.nist.gov/publications/detail/nistir/8259/final
Cyber_TG_80	NISTIR 8259A	-	octobre 2020	Le NISTIR 8259A est un rapport spécial du National Institute of Standards and Technology (NIST) aux États-Unis. Intitulé "Cybersecurity Framework Manufacturing Profile", ce rapport fournit des lignes directrices spécifiques pour l'application du NIST Cybersecurity Framework (CSF) dans le secteur manufacturier.	https://csrc.nist.gov/publications/detail/nistir/8259a/final
Cyber_TG_81	Norme COBIT	COBIT 5	1996	COBIT (Control Objectives for Information and Related Technologies) est un cadre de gouvernance et de gestion des technologies de l'information largement utilisé. Il fournit des bonnes pratiques pour la gouvernance et le contrôle des systèmes d'information au sein d'une organisation.	https://www.freshworks.com/freshservice/fr/cobit-blog/

Cyber_TG_82	Norme de protection des données personnelles (PDPA)	-	2 janvier 2013	Loi singapourienne qui établit les exigences pour la collecte, l'utilisation, la divulgation et le traitement des données personnelles, y compris les mesures de sécurité appropriées.	https://www.entrust.com/fr/digital-security/hsm/solutions/compliance/apac/thailands-personal-data-protection-act
Cyber_TG_83	NTIA IoT Security (National Telecommunications and Information Administration IoT Security)	-	décembre 2019	La sécurité IoT de NTIA (Administration nationale des télécommunications et de l'information) fait référence aux initiatives et aux lignes directrices élaborées par la National Telecommunications and Information Administration, une division du département du commerce des États-Unis, pour améliorer la sécurité des appareils et des systèmes de l'Internet des objets (IoT).	https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_09.12.17.pdf
Cyber_TG_85	O-ISM3	-	2011	O-ISM3, abréviation de "Open Information Security Management Maturity Model", est un modèle de maturité de gestion de la sécurité de l'information. Il fournit un cadre et des bonnes pratiques pour évaluer, planifier, mettre en œuvre et améliorer la gestion de la sécurité de l'information au sein d'une organisation.	https://ism3.com/
Cyber_TG_86	OWASP	-	2001	OWASP (Open Web Application Security Project) est une communauté mondiale dédiée à l'amélioration de la sécurité des applications web. Elle fournit des ressources, des outils, des lignes directrices et des bonnes pratiques pour aider les organisations à développer, déployer et maintenir des applications web sécurisées.	https://owasp.org/
Cyber_TG_87	PAS 555	-	2013	Cette PAS détaille un cadre pour la gouvernance et la gestion des risques de cybersécurité. Les exigences de cette PAS (spécification accessible au	Norme PAS 555:2013 (afnor.org)

				public) définissent les résultats d'une cybersécurité efficace et incluent des mesures techniques, physiques, culturelles et comportementales, ainsi qu'un leadership et une gouvernance efficaces. Il est conçu pour être évolutif et convient donc aux entreprises de toutes tailles.	
Cyber_TG_88	PCI-DSS	-	décembre 2004	Il s'agit d'un ensemble de normes de sécurité établies par le Conseil des normes de sécurité de l'industrie des cartes de paiement (Payment Card Industry Security Standards Council - PCI SSC) pour assurer la protection des données des titulaires de cartes de paiement et la sécurité des transactions.	https://fr.wikipedia.org/wiki/Norme de sécurité de l'industrie des cartes de paiement
Cyber_TG_89	Plan Maroc Cybersecurity	-	2013	Le "Plan Maroc Cybersecurity" est une stratégie nationale de cybersécurité élaborée par le Maroc pour renforcer la sécurité des systèmes d'information et protéger les infrastructures critiques du pays contre les cybermenaces.	https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf
Cyber_TG_90	PSPF	-	1 octobre 2018	PSPF (Protective Security Policy Framework) est un cadre de politique de sécurité protectrice utilisé en Australie. Il est géré par l'Agence australienne de cybersécurité (Australian Cyber Security Centre - ACSC) et le Département australien des affaires intérieures (Department of Home Affairs). Le PSPF vise à fournir des directives et des normes de sécurité pour protéger les informations, les biens et les personnes dans les organisations gouvernementales australiennes.	https://www.protectivesecurity.gov.au/

Cyber_TG_91	PSPF (Protective Security Policy Framework)	-	1 octobre 2018	Il s'agit d'un cadre de politique de sécurité qui établit les exigences pour la protection des informations gouvernementales en Australie. Il fournit des directives sur la gestion des risques, la sécurité physique, la sécurité des systèmes d'information et la gestion des incidents.	https://www.prote ctivesecurity.gov.au
Cyber_TG_92	SAMA Cybersecurity Framework	Version 1.0	45063	Le SAMA (Saudi Arabian Monetary Authority) Cybersecurity Framework est un cadre de cybersécurité spécifique développé par l'autorité monétaire saoudienne pour aider les institutions financières à protéger leurs systèmes d'information et à prévenir les cyberattaques.	https://www.sama.gov.sa/en-US/RulesInstructions/Cyber%20Security%20Framework.pdf
Cyber_TG_94	SOC 2 (Service Organization Control 2)	-	2010	Il s'agit d'une norme d'audit qui évalue les contrôles et les pratiques de sécurité de l'information d'une organisation.	https://www.aicpacima.com/resources/landing/system-and-organization-controls-soc-suite-of-services
Cyber_TG_95	SP 800-150	-	octobre 2016	Cette publication fournit des lignes directrices pour établir et participer à des relations de partage d'informations sur les cybermenaces. Ces conseils aident les organisations à établir des objectifs de partage d'informations, à identifier les sources d'informations sur les cybermenaces, à définir les activités de partage d'informations, à élaborer des règles qui contrôlent la publication et la distribution d'informations sur les menaces, à s'engager avec les communautés de partage existantes et à utiliser efficacement les informations sur les menaces à l'appui de l'organisation. pratiques globales de cybersécurité.	https://csrc.nist.gov/publications/detail/sp/800-150/final

Cyber_TG_96	SS 507	-	2020	Le standard SS 507 fait référence à la norme de Singapour pour les bonnes pratiques en matière de sécurité des systèmes d'information.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/12691c57-e1a4-4387-87b1-fe62d31f2731
Cyber_TG_97	ss 584	-	2020	Il s'agit d'une norme nationale de Singapour qui fournit des directives et des bonnes pratiques pour la gestion de la cybersécurité dans les organisations.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/b5430dc1-27f3-4203-bd8e-00345da6bed5
Cyber_TG_98	SS 638	-	2018	Cette norme vise à fournir des directives et des bonnes pratiques pour la sécurité des systèmes de contrôle industriel (ICS) utilisés dans les infrastructures critiques, telles que les centrales électriques, les usines de traitement chimique, les installations de traitement de l'eau, etc. Elle est conçue pour aider les organisations à protéger leurs systèmes de contrôle industriels contre les cybermenaces potentielles.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/fd1f48ab-6e55-49f4-a725-5addcb22654e
Cyber_TG_99	SS ISO 22301	-	2019	La norme ISO 22301 est une norme internationale qui spécifie les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de gestion de la continuité des activités (SGCA). Elle fournit un cadre pour aider les organisations à anticiper, prévenir, répondre et se rétablir face à des incidents perturbateurs.	https://www.socotec-certification-international.sg/certification/management-systems-certification/ss-iso-22301-2019-business-continuity-management-system
Cyber_TG_100	Telework Cybersecurity Controls (TCC)	-	2021	Le document vise à contribuer à éléver le niveau de cybersécurité au niveau national en permettant à l'organisation d'effectuer son travail à distance de manière sécurisée et de s'adapter aux changements de l'environnement des affaires et des systèmes de télétravail, et en améliorant	https://www.nca.gov.sa/en/legislation?item=193&slug=controls-list

				les capacités de cybersécurité de l'organisation et sa résilience face aux cybermenaces lors de la fourniture de travail à distance. Ces contrôles sont une extension des contrôles essentiels de cybersécurité (ECC).	
Cyber_TG_102	The Estonian Information System Security Framework (ISKE)	-	2007	The Estonian Information System Security Framework (ISKE) is a comprehensive set of guidelines and best practices for ensuring the security of information systems in Estonia.	https://ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its
Cyber_TG_105	TR 64 : 2018 Guidelines for IoT security for smart nation	-	2018	Cette référence technique présente les concepts de sécurité fondamentaux et la terminologie des systèmes de l'Internet des objets (IoT) et démontre leurs applications. Une approche holistique pour identifier et atténuer les menaces et les vulnérabilités des systèmes IoT est également introduite. Des conseils sont fournis sur la manière de procéder à la modélisation des menaces pour IoT.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/3ee3386a-4332-45be-903b-afef1dfb6770
Cyber_TG_106	TR 91 : 2021	-	2021	Étiquetage de cybersécurité pour l'IoT grand public	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/41f0e637-22d6-4d05-9de3-c92a53341fe5
Cyber_TG_107	TRM (Technology Reference Model)	-	2019	Un cadre utilisé pour guider la prise de décision technologique dans une organisation. Le TRM définit les blocs de construction technologiques qui sont utilisés pour fournir des services et des applications gouvernementales à Singapour. Il fournit une approche standardisée de la conception et de la mise	https://pubs.opengroup.org/architecture/togaf8-doc/arch/chap19.html

				en œuvre de solutions informatiques. Le TRM est géré par l'Agence gouvernementale de technologie (GovTech) et est utilisé comme guide pour l'approvisionnement informatique, la conception et la mise en œuvre de l'architecture. Il fait partie du cadre plus large de l'architecture d'entreprise du gouvernement de Singapour (SGEA).	
Cyber_TG_108	ISO/IEC AWI 27090	2022	2022	Ce document fournit des conseils aux organisations pour faire face aux menaces de sécurité et aux défaillances des systèmes d'intelligence artificielle (IA).	https://www.iso.org/standard/56581.html
Cyber_TG_109	ISO/IEC AWI 27091	2023	2023	Ce document fournit des conseils aux organisations pour faire face aux risques de confidentialité dans les systèmes d'intelligence artificielle (IA) et les modèles d'apprentissage automatique (ML).	https://www.iso.org/standard/56582.html
Cyber_TG_110	EVS-EN 17640	-	2022	Ce document décrit la méthodologie d'évaluation de la cybersécurité pour les produits TIC. Il est destiné à être utilisé pour les trois niveaux d'assurance tels que définis dans la loi sur la cybersécurité (c'est-à-dire basique, substantiel et élevé)	https://www.evs.ee/en/evs-en-17640-2022
Cyber_TG_111	EVS-ISO/IEC 27032	-	2018	La présente Norme internationale fournit des lignes directrices pour l'amélioration de l'état de la cybersécurité	https://www.evs.ee/en/evs-iso-iec-27032-2018
Cyber_TG_112	SOC for Cybersecurity	-	-	Le rapport SOC pour la cybersécurité vise à aider les organisations à démontrer l'efficacité de leurs efforts de gestion des risques de cybersécurité auprès des parties prenantes, notamment les clients, les partenaires commerciaux et les organismes de réglementation. Le rapport	https://www.aicpacima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity

				fournit des informations détaillées sur les contrôles, les processus et les activités de gestion des risques de cybersécurité de l'organisation.	
Cyber_TG_113	ISO/IEC 29128-1	2023	2023	Ce document établit un cadre pour la vérification des spécifications du protocole cryptographique conformément aux meilleures pratiques académiques et industrielles.	https://www.iso.org/standard/78931.html
Cyber_TG_114	ISO/IEC 27559	2022	2022	This document provides a framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data.	https://www.iso.org/standard/71677.html
Cyber_TG_115	ASTM F3286-17	-	2017	Ce guide répond au besoin de l'entreprise ou de l'organisation gouvernementale d'atténuer la probabilité de cyberattaques et de réduire l'étendue des cyberattaques potentielles, qui peuvent laisser des données personnelles sensibles, des informations d'entreprise et des infrastructures critiques vulnérables aux attaquants.	https://webstoreansi.org/standards/astm/astmf328617
Cyber_TG_116	ISO/IEC 27009:2020	-	2020	ISO 27009 traite de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée.	https://www.iso.org/standard/73907.html
Cyber_TG_117	ISO/IEEE 11073-40102	-	2022	Dans le contexte de l'interopérabilité plug-and-play sécurisée, la cybersécurité est le processus et la capacité d'empêcher l'accès ou la modification non autorisés, l'utilisation abusive, le refus d'utilisation ou l'utilisation non autorisée des informations stockées, accessibles depuis ou transférées vers et depuis un doctorat/PoCD.	https://www.iso.org/standard/83503.html

Cyber_TG_118	ETSI TR 103 305-1	V2.1.1	2016	Le présent document décrit un ensemble spécifique de mesures techniques disponibles pour détecter, prévenir, réagir et atténuer les dommages des cyberattaques les plus courantes aux plus avancées. Les mesures reflètent les connaissances combinées d'attaques réelles et de défenses efficaces.	https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/02.01.01_60/tr_10330501v020101p.pdf
Cyber_TG_119	ETSI EN 303 645	V2.1.1	2020	Le présent document spécifie des dispositions de haut niveau en matière de sécurité et de protection des données pour les dispositifs IoT grand public qui sont connectés à l'infrastructure du réseau (tel qu'Internet ou le réseau domestique) et leurs interactions avec les prestations de service.	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
Cyber_TG_120	ISO/IEC TS 27100	2020	2020	Ce document: — décrit la cybersécurité et les concepts pertinents, y compris la façon dont elle est liée et différente de la sécurité de l'information — établit le contexte de la cybersécurité ; — ne couvre pas tous les termes et définitions applicables à la cybersécurité — ne limite pas les autres normes dans la définition de nouveaux termes liés à la cybersécurité à utiliser	https://www.iso.org/standard/72434.html
Cyber_TG_121	IS/ISO/IEC 24761	2019	2019	Ce document définit la structure et les éléments de données du contexte d'authentification pour la biométrie (ACBio), qui est utilisé pour vérifier la validité du résultat d'un processus d'inscription et de vérification biométrique exécuté sur un site distant.	https://www.iso.org/standard/71163.html
Cyber_TG_122	ISO/IEC 24745	2022	2022	Ce document couvre la protection des informations biométriques selon diverses exigences de confidentialité, d'intégrité et de renouvellement/révocabilité	https://www.iso.org/standard/75302.html

				pendant le stockage et le transfert. Il fournit également des exigences et des recommandations pour la gestion et le traitement sécurisés et conformes à la confidentialité des informations biométriques.	
Cyber_TG_123	ISO/IEC 20547-4	2020	2020	Ce document spécifie les aspects de sécurité et de confidentialité applicables à l'architecture de référence des mégadonnées (BDRA), y compris les rôles, les activités et les composants fonctionnels des mégadonnées, et fournit également des conseils sur les opérations de sécurité et de confidentialité pour les mégadonnées.	https://www.iso.org/fr/standard/71278.html
Cyber_TG_124	ISO/IEC 19792	2009	2009	ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system.	https://www.iso.org/standard/51521.html
Cyber_TG_125	SSL/TLS	-	-	SSL (Secure Sockets Layer) et TLS (Transport Layer Security) sont des protocoles de sécurité utilisés pour établir des connexions sécurisées sur Internet. Ils sont principalement utilisés pour sécuriser les communications entre les clients (par exemple, navigateurs Web) et les serveurs (par exemple, sites Web) en chiffrant les données échangées.	https://fr.wikipedia.org/wiki/Transport_Layer_Security
Cyber_TG_126	NIST SP 800-53	Rev. 5	2020	NIST SP 800-53 est une publication spéciale du National Institute of Standards and Technology (NIST) des États-Unis qui fournit des directives et des contrôles de sécurité pour les systèmes d'information et les infrastructures informatiques. Cette publication, intitulée "Security and Privacy Controls for Information Systems and	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

				Organizations" (Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations), énonce un ensemble complet de contrôles de sécurité pour aider les organisations à protéger leurs informations sensibles.	
Cyber_TG_127	ITIL	-	-	ITIL (Information Technology Infrastructure Library) est un ensemble de bonnes pratiques et de recommandations pour la gestion des services informatiques. Il fournit un cadre de référence pour la planification, la conception, la mise en œuvre et la gestion des services informatiques au sein d'une organisation.	https://fr.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

En adhérant aux normes de cybersécurité, les organisations peuvent réduire le risque de cyberattaques, assurer la confidentialité et la sécurité des informations sensibles et accroître la confiance des clients.

Les normes de cybersécurité sont un élément important d'une stratégie de cybersécurité globale pour le eGovernment du Togo. Les normes fournissent un ensemble de pratiques exemplaires et de lignes directrices pour la sécurisation des systèmes d'information et des réseaux contre les cybermenaces et sont utilisées pour évaluer l'efficacité des mesures de cybersécurité du eGovernment.

Voici quelques avantages clés de l'utilisation des normes de cybersécurité :

Amélioration de la sécurité : Les normes de cybersécurité fournissent un cadre permettant aux organisations d'identifier et de gérer les risques liés à la cybersécurité et de mettre en œuvre les contrôles et les mesures nécessaires pour atténuer ces risques	Conformité : Le respect des normes de cybersécurité peut aider les organisations à répondre aux exigences réglementaires et à se conformer aux normes de sécurité spécifiques à l'industrie, telles que HIPAA pour les organisations de soins de santé et PCI DSS pour les organisations qui traitent les transactions par carte de crédit.	Confiance accrue : En démontrant leur conformité aux normes de cybersécurité, les organisations peuvent établir une relation de confiance avec leurs clients, leurs partenaires et leurs parties prenantes, et montrer qu'elles s'engagent à protéger les informations sensibles.
Amélioration des opérations : Les normes de cybersécurité peuvent aider les organisations à améliorer leur efficacité opérationnelle en rationalisant les processus et en réduisant le risque d'incidents de sécurité.	Meilleure gestion des risques : En suivant les normes de cybersécurité, les organisations peuvent mieux comprendre leurs risques de cybersécurité et mettre en œuvre une approche proactive pour gérer ces risques.	

2. Interoperability Standards

Les normes d'interopérabilité font référence aux directives et aux meilleures pratiques pour la connexion et l'intégration de systèmes et d'applications, tels que les bases de données, les moteurs de workflow et les services Web (webservices).

Voici une liste de normes d'interopérabilité :

ID	Standard/Norme	Version	date de publication	Description	Url Documentation
INT_TG_01	CSV (valeurs séparées par des virgules)	1.10.0 (2 fevrier 2023)	1970	Format indépendant de la plate-forme pour la soumission des données de feuille	https://fr.wikipedia.org/wiki/Comma-separated_values
INT_TG_02	HTML (HyperText Markup Language)	HTML 5.3 (28 janvier 2021)	mars 1993	langage de balisage hypertexte pour la création de documents Web	https://html.spec.whatwg.org/multipage/
INT_TG_03	JPEG (Joint Photographic Experts Group)	JPEG ITU-T T.81 (avril 2018)	septembre 1992	JPEG (Joint Photographic Experts Group) est un format de compression d'images numériques largement utilisé	https://jpeg.org/about.html
INT_TG_04	ISO 19115	2003	décembre 2003	L'ISO 19115 est une norme internationale développée par l'Organisation internationale de normalisation (ISO) qui fournit des directives pour la description, le contenu et la gestion des métadonnées géospatiales. Les métadonnées géospatiales sont des informations descriptives qui décrivent les données géographiques, telles que les données cartographiques, les images satellites, les données topographiques, etc.	https://www.iso.org/standard/26020.html
INT_TG_05	MPEG (Moving Picture Experts Group)	MPEG 4 Part 3 (juillet 2020)	mai 1992	format vidéo	https://www.mpeg.org/

INT_TG_06	ODF (Open Document Format)	0.11.0 (21 décembre 2022)	mai 2005	format de document ouvert pour applications bureautiques	https://opendocumentformat.org/aboutODF/
INT_TG_07	PDF (Portable Document Format)	2022 standard/Pro	juin 1993	format de document indépendant de la plateforme	https://www.adobe.com/acrobat/about-adobe-pdf.html
INT_TG_08	SOAP (Simple Object Access Protocol)	SOAP 1.2 (avril 2017)	mars 1999	SOAP (Simple Object Access Protocol) est un protocole de communication basé sur XML (eXtensible Markup Language) qui permet l'échange de messages entre des applications distribuées sur un réseau. Il est souvent utilisé dans les services web pour la communication entre des systèmes hétérogènes.	https://www.w3.org/TR/2000/NOTE-SOAP-20000508/
INT_TG_09	PNG (Portable Network Graphics)	PNG Specification 1.2 (octobre 2003)	octobre 1996	PNG (Portable Network Graphics) est un format de fichier d'image numérique largement utilisé. Il a été développé pour remplacer les anciens formats d'image tels que GIF (Graphics Interchange Format) en offrant une compression sans perte et une prise en charge de la transparence.	http://www.libpng.org/pub/png/
INT_TG_10	SVG (Scalable Vector Graphic)	SVG 2 (21 mai 2022)	septembre 2001	un format de fichier d'image basé sur XML (eXtensible Markup Language) qui permet de décrire des graphiques vectoriels bidimensionnels.	https://www.adobe.com/creativecloud/file-types/image/vector/svg-file.html
INT_TG_11	TIFF (format de fichier d'image marquée)	TIFF 6.0 (juin 1992)	juin 1987	TIFF (Tagged Image File Format), également connu sous le nom de format de fichier d'image marquée, est un format de fichier d'image populaire et polyvalent.	https://www.adobe.com/creativecloud/file-types/image/raster/tiff-file.html
INT_TG_12	TXT (Texte brut, fichier texte)	-	novembre 1971	TXT (Text) est un format de fichier courant utilisé pour stocker du texte brut, également appelé fichier texte. Il s'agit d'un format simple et universel qui peut être ouvert et lu par la plupart des éditeurs de texte et des programmes de traitement de texte.	https://docs.fileformat.com/fr/word-processing/txt/

INT_TG_13	XAdES (signatures électroniques avancées XML)	XADES 2.2.1 (juillet 2012)	mars 2002	XAdES (XML Advanced Electronic Signatures) est un ensemble de normes utilisées pour la création et la vérification de signatures électroniques avancées dans des documents XML	http://www.yoodesign.org/doc/w3c/xades/
INT_TG_14	XML (Langage de balisage hypertexte extensible)	XML 1.0 2008	fevrier 1998	XML (eXtensible Markup Language) est un langage de balisage hypertexte extensible qui permet de structurer et de stocker des données de manière lisible par les humains et les machines. Il est utilisé pour décrire et échanger des informations structurées entre différentes applications et plates-formes.	https://developer.mozilla.org/fr/docs/Web/XML/XML_introduction
INT_TG_15	XSL (langage de style extensible)	XSTL 3.0 (aout 2022)	octobre 1999	XSL (eXtensible Stylesheet Language) est un langage de style extensible utilisé pour transformer et formater les données XML. Il est utilisé en conjonction avec XML pour définir des feuilles de style et spécifier la présentation visuelle des données XML.	https://www.w3.org/TR/xslt/all/
INT_TG_16	JSON (JavaScript Object Notation)	RFC 8259 (decembre 2017)	decembre 2001	JSON est un format de données léger et facile à lire/écrire pour l'échange de données. Il est largement utilisé dans les applications web et les services web pour représenter et échanger des données structurées.	https://www.json.org/json-en.html
INT_TG_17	REST (Representational State Transfer)	-	2000	REST est un style architectural pour la conception de services web. Il utilise les méthodes HTTP standard (GET, POST, PUT, DELETE) pour accéder et manipuler les ressources sur le web.	https://en.wikipedia.org/wiki/Representational_state_transfer
INT_TG_18	OData (Open Data Protocol)	Odata 4.01 (mars 2020)	mars 2012	OData est un protocole basé sur les standards du web pour l'échange de données. Il permet d'accéder et de manipuler des données à travers des interfaces RESTful, en utilisant des formats tels que XML ou JSON.	https://www.odata.org/
INT_TG_19	HL7 (Health Level 7)	HL7 version 2.8 (1999)	1987	HL7 est un ensemble de normes internationales pour l'échange d'informations de santé électroniques. Il définit des formats de messages et des protocoles de communication pour faciliter	https://www.hl7.org/

				l'interopérabilité des systèmes d'information de santé.	
INT_TG_20	DICOM	DICOM 3.0 (juin 2020)	1983	Digital Imaging and Communications in Medicine (DICOM) est une norme pour la transmission, le stockage et le partage d'images médicales et d'informations connexes. Elle garantit l'interopérabilité entre différents appareils et systèmes d'imagerie médicale, permettant l'échange fluide de données patient.	https://www.dicomstandard.org/
INT_TG_21	FHIR (Fast Healthcare Interoperability Resources)	FHIR R4 (2019)	juin 2014	FHIR est un standard d'interopérabilité de données de santé basé sur les API web. Il est utilisé à Singapour pour faciliter l'échange de données de santé entre les différentes applications et systèmes, permettant une meilleure coordination des soins et une meilleure accessibilité aux informations médicales.	https://ecqi.healthit.gov/fhir
INT_TG_22	Electronic Data Interchange (EDI)	EDI X12 version 5010 (janvier 2012)	1968	L'EDI est une méthode standardisée d'échange électronique de données commerciales. Il est utilisé dans différents secteurs à Singapour pour faciliter les transactions commerciales, les échanges de documents et la collaboration entre les partenaires commerciaux.	https://www.edibasics.com/what-is-edi/
INT_TG_23	XBRL (eXtensible Business Reporting Language)	XBRL 2.1 (octobre 2013)	avril 2001	Langage de balisage standardisé utilisé pour la création, l'échange et l'analyse de rapports financiers et commerciaux. Il permet de structurer les informations financières et les données d'entreprise de manière cohérente et compréhensible par les machines, facilitant ainsi leur intégration, leur comparaison et leur analyse.	https://www.xbrl.org/the-standard/what-an-introduction-to-xbrl/
INT_TG_24	OPenAPI	OpenAPI Specification 3.1.0 (juillet 2021)	juillet 2011	OpenAPI favorise l'interopérabilité en permettant aux différentes parties prenantes, qu'il s'agisse de développeurs internes ou externes, d'utiliser et de développer des applications	https://www.openapis.org/

				qui se connectent et communiquent efficacement avec les API exposées.	
INT_TG_25	DDOC (Digital Document)	DDOC 1.3 (decembre 2020)	novembre 2000	un format de fichier utilisé en Estonie pour les documents numériques sécurisés et signés. Il s'agit d'un format spécifique à l'Estonie qui permet de créer, de partager et de stocker des documents électroniques tout en garantissant leur authenticité, leur intégrité et leur validité légale.	https://www.tradefinanceglobal.com/legal/digital-negotiable-instruments/digital-documents/
INT_TG_26	GZIP	RFC 1952 (mai 1996)	mai 1992	GZIP est un format de compression de données utilisé pour réduire la taille des fichiers et faciliter leur transfert et leur stockage.	https://www.gzip.org/
INT_TG_27	PDF/A	ISO 19005-1:2020 (septembre 2020)	septembre 2005	PDF/A (Portable Document Format/Archival) est une norme de format de fichier utilisée spécifiquement pour l'archivage à long terme des documents électroniques. Il s'agit d'une version du format PDF conçue pour garantir la préservation à long terme des documents, en veillant à ce qu'ils puissent être ouverts et lus de manière cohérente dans le futur, même avec l'évolution des logiciels et des technologies.	https://fr.wikipedia.org/wiki/PDF/A
INT_TG_28	The Estonian Interoperability Framework	2.4 (novembre 2020)	mars 2005	Un ensemble de directives et de recommandations visant à promouvoir l'interopérabilité des systèmes d'information en Estonie. Il définit les principes, les normes et les bonnes pratiques à suivre pour permettre l'échange d'informations et la collaboration entre les différents acteurs du secteur public, du secteur privé et de la société civile.	https://joinup.ec.europa.eu/collection/eprocurement/discussion/estonian-interoperability-framework

INT_TG_29	UBL (Universal Business Language)	UBL 2.3 (octobre 2018)	fevrier 2006	langage de modélisation et de normalisation des échanges de données commerciales électroniques. Il s'agit d'un standard international développé par l'Organisation internationale de normalisation (ISO) et le Comité technique ISO/IEC JTC 1/SC 34.	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=UBL
INT_TG_30	SEMIC	SEMIC 2.3 (juin 2019)	fevrier 2008	Initiative européenne visant à promouvoir l'interopérabilité sémantique dans le domaine des services publics en ligne. SEMIC est soutenu par la Commission européenne et vise à faciliter l'échange d'informations entre les administrations publiques et les parties prenantes en utilisant des standards communs et des technologies sémantiques.	https://joinup.ec.europa.eu/collection/semic-support-centre
INT_TG_31	National Information Interoperability Framework (NIIF)	NIIF 2.1 (février 2017)	decembre 2008	NIIF vise à établir des normes, des directives et des principes communs pour permettre l'échange efficace, sécurisé et interopérable de l'information entre les organismes gouvernementaux, les organisations et les parties prenantes. Il peut inclure des spécifications techniques, des modèles de données, des protocoles d'échange et des politiques de gouvernance pour faciliter l'interopérabilité des systèmes d'information.	https://joinup.ec.europa.eu/collection/eprocurement/discussion/nif-national-ict-interoperability-framework
INT_TG_32	OASIS BDX (Business Document Exchange)	BDXR 1.0 (mai 2018)	2 mai 2012	OASIS BDX (Business Document Exchange) est une spécification développée par l'Organisation for the Advancement of Structured Information Standards (OASIS). Il s'agit d'un cadre de travail qui vise à faciliter l'échange électronique de documents commerciaux entre les organisations.	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=bdxr
INT_TG_33	ISO 20022	-	novembre 2004	ISO 20022 est une norme internationale pour l'échange de messages électroniques structurés entre les institutions financières et les organisations. Elle fournit un cadre commun pour la définition des messages financiers et des processus associés, permettant ainsi une	https://www.iso20022.org/

				interopérabilité améliorée et une communication plus efficace entre les différents acteurs du secteur financier.	
INT_TG_34	TCP/IP	RFC 9293 (18 aout 2022)	1 janvier 1983	TCP/IP (Transmission Control Protocol/Internet Protocol) est un ensemble de protocoles de communication utilisé pour interconnecter des réseaux d'ordinateurs et permettre la transmission de données sur Internet.	https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf
INT_TG_35	SOA	SOA Suite 12c (juin 2014)	décembre 1996	SOA (Service-Oriented Architecture) est un style d'architecture logicielle qui favorise la création de systèmes modulaires, flexibles et interopérables.	https://home.cs.colorado.edu/~ken/a/classes/5828/s10/presentations/soa.pdf
INT_TG_36	WS-I	8.5.5.23 (13 fevrier 2023)	fevrier 2002	L'objectif principal de WS-I était de définir des profils d'interopérabilité qui spécifient comment les différentes spécifications de services web peuvent être combinées pour assurer une interopérabilité harmonieuse. Ces profils étaient basés sur les standards existants tels que SOAP (Simple Object Access Protocol), WSDL (Web Services Description Language) et UDDI (Universal Description, Discovery, and Integration).	http://www.ws-i.org/
INT_TG_37	HTTP	HTTP 3 (2022)	mai 1996	Le protocole de communication standard utilisé pour le transfert de données sur le web.	https://developer.mozilla.org/en-US/docs/Web/HTTP?retiredLocale=de
INT_TG_38	WSDL (Web Services Description Language)	WSDL 2.0 (2007)	mars 2001	Un langage basé sur XML utilisé pour décrire les services web et leurs interfaces.	https://fr.wikipedia.org/wiki/Web_Services_Description_Language
INT_TG_40	ISO/IEC 21823-4	ISO/IEC 21823-4:2017 (octobre 2017)	juin 2018	ISO/IEC 21823-4:2022 établit des directives et des exigences pour assurer l'interopérabilité syntaxique des systèmes de l'IoT, en décrivant les principes, les exigences et le cadre pour le développement	https://www.iso.org/standard/84773.html

				de règles d'échange d'informations entre les appareils de l'IoT.	
INT_TG_41	HL7 CDA (Clinical Document Architecture)	HL7 CDA Release 2.1 (juillet 2005)	novembre 2000	Standard pour l'échange de documents cliniques dans le domaine de la santé.	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC130066/
INT_TG_44	X-Road	X-Road 6 (janvier 2020)	mars 2001	X-Road est une infrastructure de gouvernance électronique sécurisée et décentralisée développée en Estonie. Il s'agit d'un système d'échange de données sécurisé et interopérable conçu pour faciliter la communication et la collaboration entre les différents systèmes d'information utilisés par les institutions gouvernementales et les organisations privées.	https://x-road.global/
INT_TG_45	X-tee	X-tee 6 (janvier 2020)	juillet 2001	X-tee fournit une infrastructure fiable et sécurisée pour l'échange de données sensibles et confidentielles. Il est conçu pour garantir l'intégrité, la confidentialité et la disponibilité des informations échangées entre les différents acteurs.	https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee
INT_TG_46	e-Government Interoperability Framework	NAN	45023	Le cadre d'interopérabilité de l'administration électronique (e-Government Interoperability Framework) est un ensemble de principes, de normes et de directives qui facilite l'interopérabilité des systèmes d'information utilisés par les administrations publiques. Il vise à promouvoir l'échange efficace et sécurisé de données et de services entre les différentes entités gouvernementales.	https://www.unapict.org/sites/default/files/2019-01/e-Government%20Interoperability%20-%20Guide.pdf
INT_TG_47	LTI (Learning Tools Interoperability)	LTI 1.3 (mars 2019)	mars 2010	LTI (Learning Tools Interoperability) est un standard de l'industrie de l'éducation qui facilite l'intégration et l'interopérabilité des outils et des plates-formes d'apprentissage en ligne. Il permet aux systèmes	https://en.wikipedia.org/wiki/Learning_Tools_Interoperability

				d'apprentissage numériques, tels que les plates-formes d'apprentissage en ligne, les systèmes de gestion de l'apprentissage (LMS) et les outils d'enseignement numérique, de se connecter et de collaborer de manière transparente.	
INT_TG_48	SCORM (Sharable Content Object Reference Model)	SCORM 2004 4th Edition (janvier 2009)	janvier 2000	SCORM (Sharable Content Object Reference Model) est un ensemble de normes et de spécifications techniques utilisées dans l'industrie de l'e-learning pour la création et la distribution de contenus pédagogiques en ligne. Il permet de rendre les contenus d'apprentissage compatibles et interchangeables entre différentes plates-formes d'apprentissage et systèmes de gestion de l'apprentissage (LMS).	https://scorm.com/scorm-explained/one-minute-scorm-overview/
INT_TG_49	IMS Learning Tools Interoperability	LTI 1.3 (mars 2019)	avril 2005	IMS Learning Tools Interoperability (LTI) est un standard de l'industrie de l'éducation qui facilite l'intégration et l'interopérabilité des outils et des plates-formes d'apprentissage en ligne. Il permet aux systèmes d'apprentissage numériques, tels que les plates-formes d'apprentissage en ligne et les systèmes de gestion de l'apprentissage (LMS), de se connecter et de collaborer de manière transparente.	http://www.imsglobal.org/activity/learning-tools-interoperability
INT_TG_50	IMS Common Cartridge	Common Cartridge 1.3 (mars 2012)	janvier 2008	IMS Common Cartridge est une norme de l'industrie de l'éducation qui permet l'emballage et la distribution de contenus d'apprentissage numériques. Il fournit un format standardisé pour regrouper des ressources pédagogiques, telles que des cours, des modules, des activités, des évaluations, des médias, etc., afin de faciliter leur partage et leur utilisation sur différentes plates-formes d'apprentissage.	http://www.imsglobal.org/activity/common-cartridge

INT_TG_51	EBICS (Electronic Banking Internet Communication Standard)	EBICS version 3.0 (septembre 2017)	septembre 2003	EBICS (Electronic Banking Internet Communication Standard) est un standard de communication utilisé dans le domaine des services bancaires électroniques en Europe. Il définit un protocole sécurisé pour l'échange de données entre les clients (entreprises, institutions financières) et les banques.	https://www.ebics.org/en/home
INT_TG_52	TR 50	TR 50: 2016	septembre 2009	Interopérabilité des informations et des services de l'Internet des objets pour Smart Nation	https://standards.tiaonline.org/all-standards/committees/tr-50
INT_TG_53	XML Schema	XML Schema 1.1 (avril 2012)	mai 2001	pour spécifier les contraintes auxquelles ces données doivent se conformer.	XML Schema
INT_TG_54	RDF	RDF 1.1 (février 2014)	fevrier 1999	cadre de description des métadonnées, pour accéder aux données du Web	https://www.w3.org/RDF/
INT_TG_55	API RESTful	44893	2000	API signifie Interface de Programmation d'Application, et une API RESTful est un style architectural pour concevoir des applications en réseau. REST signifie Representational State Transfer, ce qui signifie que l'API est basée sur des méthodes HTTP standard telles que GET, POST, PUT et DELETE pour effectuer des opérations sur des ressources.	https://aws.amazon.com/fr/what-is/restful-api/
INT_TG_56	ISO 6709	2022	2022	La norme ISO 6709 appartient à la famille des normes ISO 6709 relatives à la représentation géographique des emplacements. Cette norme spécifie la syntaxe et les règles pour représenter les coordonnées géographiques (latitude, longitude et altitude) dans un format textuel standardisé. Elle est largement utilisée pour l'échange et la communication d'informations de localisation géographique.	https://www.iso.org/standard/75147.html

INT_TG_57	ISO 19136-1	2020	2020	La norme ISO 19136-1, également connue sous le nom de "ISO Geographic information - Geography Markup Language (GML) - Part 1: XML Schema language for geographic information", est une norme internationale qui spécifie le langage de balisage XML pour les informations géographiques, appelé GML (Geography Markup Language)	https://www.iso.org/standard/75676.html
INT_TG_58	ISO 19136-2	2015	2015	Le langage de balisage géographique (GML) est un codage XML conforme à la norme ISO 19118 pour le transport et le stockage d'informations géographiques modélisées conformément au cadre de modélisation conceptuelle utilisé dans la série de normes internationales ISO 19100 et comprenant à la fois les données spatiales et non géographiques. propriétés spatiales des caractéristiques géographiques.	https://www.iso.org/standard/61585.html
INT_TG_59	CBOR	-	-	CBOR (Concise Binary Object Representation) est un format binaire compact et efficace pour représenter et échanger des données structurées. Il a été défini par l'IETF (Internet Engineering Task Force) dans la spécification RFC 7049.	https://en.wikipedia.org/wiki/CBOR
INT_TG_60	CWT	-	2018	CWT (CBOR Web Token) est un format de jeton basé sur CBOR (Concise Binary Object Representation) utilisé pour sécuriser et échanger des informations entre des parties dans des environnements web et IoT. CWT est défini par la spécification RFC 8392.	https://datatracker.ietf.org/doc/html/rfc8392
INT_TG_61	gRPC	-	-	gRPC est un framework open source développé par Google pour la création d'applications client-serveur à grande échelle. Il permet aux développeurs de définir des services et des messages, puis de générer du code source dans différents langages pour faciliter la communication entre les clients et les serveurs.	https://fr.wikipedia.org/wiki/GRPC

INT_TG_62	SFTP	-	-	SFTP (SSH File Transfer Protocol) est un protocole sécurisé utilisé pour le transfert de fichiers sur un réseau. Contrairement au FTP traditionnel, qui utilise des canaux de communication non sécurisés, SFTP chiffre les données et les commandes de contrôle, offrant ainsi une communication sécurisée.	https://fr.wikipedia.org/wiki/SSH_File_Transfer_Protocol
INT_TG_63	FTP	-	-	FTP (File Transfer Protocol) est un protocole standard utilisé pour le transfert de fichiers sur un réseau. Il permet à un client d'envoyer ou de recevoir des fichiers depuis un serveur distant.	https://filezilla-project.org/
INT_TG_64	OWL	-	-	OWL (Web Ontology Language) est un langage de modélisation et de représentation des connaissances utilisé pour décrire les ontologies dans le domaine de la sémantique des données. Il fait partie des normes du W3C (World Wide Web Consortium) et offre une syntaxe formelle pour définir les concepts, les relations et les axiomes dans un domaine spécifique.	https://fr.wikipedia.org/wiki/Web_Ontology_Language
INT_TG_65	UML	-	-	UML (Unified Modeling Language) est un langage de modélisation graphique largement utilisé pour la conception et la documentation des systèmes logiciels. Il offre une notation standardisée pour représenter visuellement les différentes perspectives d'un système, y compris sa structure, son comportement, ses interactions et ses processus.	https://fr.wikipedia.org/wiki/UML_(informatique)
INT_TG_66	BPMN	-	-	BPMN (Business Process Model and Notation) est une notation graphique standard utilisée pour modéliser les processus métier. Elle fournit une représentation visuelle claire et cohérente des activités, des flux de travail, des décisions, des événements et des acteurs impliqués dans un processus métier.	Business_process_model_and_notation

INT_TG_67	EDIFACT	-	-	EDIFACT (Electronic Data Interchange for Administration, Commerce, and Transport) est un standard international de messagerie électronique largement utilisé pour l'échange de données commerciales et administratives entre les organisations. Il a été développé par l'Organisation des Nations Unies pour la coordination et le développement de l'échange électronique de données (UN/EDIFACT).	https://fr.wikipedia.org/wiki/%C3%89change_de_donn%C3%A9es_informatiques%C3%A9es_pour_l%27administration,_le_commerce_et_le_transport
INT_TG_68	ISA95	-	-	Norme pour l'interopérabilité des systèmes d'automatisation industrielle, souvent utilisée pour l'échange de données entre les différents niveaux hiérarchiques.	https://fr.wikipedia.org/wiki/ISA95
INT_TG_69	MQTT	-	-	Protocole de messagerie pour les communications machine à machine (M2M) et l'Internet des objets (IoT), souvent utilisé pour l'échange de données en temps réel.	
INT_TG_70	OPC UA	-	-	OPC UA (Open Platform Communications Unified Architecture) est un standard de communication industriel largement utilisé dans le domaine de l'automatisation industrielle. Il offre une infrastructure de communication interopérable et sécurisée pour l'échange de données entre les différents composants d'un système industriel, tels que les capteurs, les actionneurs, les machines, les logiciels de supervision, etc.	https://en.wikipedia.org/wiki/OPC_UA
INT_TG_71	NFS	-	-	NFS (Network File System) est un protocole de partage de fichiers utilisé pour permettre à des systèmes informatiques de partager des fichiers et des répertoires sur un réseau. Il a été développé par Sun Microsystems et est largement utilisé dans les environnements informatiques distribués.	https://fr.wikipedia.org/wiki/Network_File_System

INT_TG_72	ETL	-	-	ETL (Extract, Transform, Load) est un processus utilisé dans le domaine de l'informatique et de la gestion des données pour collecter, transformer et charger des données provenant de différentes sources dans un entrepôt de données ou une autre destination cible. Il s'agit d'une étape cruciale dans les pipelines de données et les projets de business intelligence.	https://fr.wikipedia.org/wiki/Extract-transform-load
INT_TG_73	ELT	-	-	processus similaire à ETL, mais avec une différence clé dans l'ordre des étapes. Au lieu de transformer les données avant de les charger dans l'entrepôt de données, les données sont d'abord chargées, puis transformées à l'intérieur de l'entrepôt de données	https://fr.wikipedia.org/wiki/Extract-transform-load
INT_TG_74	IPv6	-	-	IPv6 (Internet Protocol version 6) est la dernière version du protocole Internet (IP) utilisé pour l'acheminement des données sur Internet. Il a été développé pour remplacer progressivement IPv4 (Internet Protocol version 4), qui est la version précédente du protocole IP.	https://fr.wikipedia.org/wiki/IPv6
INT_TG_75	HTTPS	-	-	HTTPS (Hypertext Transfer Protocol Secure) est le protocole sécurisé utilisé pour sécuriser les communications sur Internet. Il est basé sur le protocole HTTP, qui est utilisé pour transférer des données entre un navigateur web et un serveur. HTTPS utilise le protocole SSL (Secure Sockets Layer) ou son successeur, le protocole TLS (Transport Layer Security), pour chiffrer les données échangées entre le client et le serveur, assurant ainsi leur confidentialité et leur intégrité.	https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

INT_TG_76	AS2	V2	-	AS2 (Applicability Statement 2) est un protocole de communication sécurisé et fiable utilisé pour l'échange électronique de données commerciales entre les partenaires commerciaux. Il est basé sur les spécifications de l'EDI (Electronic Data Interchange) et utilise le protocole HTTP ou HTTPS pour transférer les messages.	https://en.wikipedia.org/wiki/AS2
INT_TG_77	WMSWFS	-	-	WMS (Web Map Service) et WFS (Web Feature Service) sont deux normes liées aux services de géoservices dans le domaine de la cartographie et des systèmes d'information géographique (SIG).	https://www.sigeterritoires.fr/index.php/comprendre-les-geoservices-wms-et-wfs/
INT_TG_78	WMTS	-	-	WMTS (Web Map Tile Service) est un protocole standardisé pour la distribution de tuiles cartographiques sur le Web. Il fait partie des spécifications développées par l'Open Geospatial Consortium (OGC) pour les services de géoservices.	https://fr.wikipedia.org/wiki/Web_Map_Tile_Service
INT_TG_80	WCS	-	-	WCS (Web Coverage Service) est un standard développé par l'Open Geospatial Consortium (OGC) pour le partage et l'accès aux données de couverture géospatiales sur le Web. Il permet aux utilisateurs de récupérer des données de couverture géospatiales, telles que des images satellites, des modèles numériques d'élévation, des données météorologiques, etc., via des services web normalisés.	https://en.wikipedia.org/wiki/Web_Coverage_Service
INT_TG_81	WPS	-	-	WPS (Web Processing Service) est un standard développé par l'Open Geospatial Consortium (OGC) qui permet l'exécution et le partage de traitements géospatiaux sur le Web. Il offre une interface normalisée pour exécuter des algorithmes géospatiaux sur des données géographiques et récupérer les résultats de ces traitements.	

INT_TG_82	LDIF	-	-	LDIF (LDAP Data Interchange Format) est un format de fichier utilisé pour importer, exporter et échanger des données avec des serveurs LDAP (Lightweight Directory Access Protocol). Il s'agit d'un format texte structuré qui permet de représenter les entrées et les attributs d'un annuaire LDAP.	https://fr.wikipedia.org/wiki/LDAP_Data_Interchange_Format
INT_TG_83	SPARQL	-	-	SPARQL (SPARQL Protocol and RDF Query Language) est un langage de requête standardisé pour interroger et manipuler des données RDF (Resource Description Framework). Il est spécialement conçu pour extraire des informations à partir de graphes de connaissances représentés en RDF, qui est un format utilisé pour représenter des données structurées selon le modèle de triplet sujet-prédicat-objet.	https://fr.wikipedia.org/wiki/SPARQL
INT_TG_84	KML	-	-	KML (Keyhole Markup Language) est un langage de balisage basé sur XML (eXtensible Markup Language) utilisé pour représenter des données géographiques et des informations de localisation. Il a été développé par Keyhole Inc., une société acquise par Google, et est maintenant un format ouvert largement utilisé pour la visualisation et le partage de données géospatiales.	https://fr.wikipedia.org/wiki/Keyhole_Markup_Language
INT_TG_85	GeoJSON	-	-	GeoJSON est un format de données géospatiales basé sur la syntaxe JSON (JavaScript Object Notation). Il est utilisé pour représenter des données géographiques, telles que des points, des lignes et des polygones, ainsi que des informations attributaires associées.	https://fr.wikipedia.org/wiki/GeoJSON

INT_TG_86	GeoSpatial-Metadata	-	-	Les métadonnées géospatiales (GeoSpatial Metadata) sont des informations structurées qui décrivent les caractéristiques, les attributs et les propriétés des données géospatiales. Elles fournissent des détails sur la source, la qualité, la précision, l'étendue et d'autres aspects pertinents des données géographiques.	https://en.wikipedia.org/wiki/Geospatial_metadata
INT_TG_87	GML	-	-	GML (Geography Markup Language) est un langage de balisage basé sur XML (eXtensible Markup Language) utilisé pour représenter et échanger des données géographiques. Il a été développé par le consortium Open Geospatial Consortium (OGC) et est un standard largement utilisé dans le domaine des systèmes d'information géographique (SIG).	https://en.wikipedia.org/wiki/Geography_Markup_Language
INT_TG_88	Shapefile	-	-	Le shapefile est un format de fichier couramment utilisé dans le domaine des systèmes d'information géographique (SIG) pour stocker et échanger des données géographiques. Il a été développé par la société Esri (Environmental Systems Research Institute) et est devenu un standard de facto dans l'industrie géospatiale.	https://fr.wikipedia.org/wiki/Shapefile
INT_TG_89	GRAPHQL	-	-	GraphQL est un langage de requête et une spécification ouverte développée par Facebook. Il est utilisé pour l'interrogation et la manipulation des données côté serveur. Contrairement aux architectures REST traditionnelles, où plusieurs appels sont nécessaires pour récupérer différentes données, GraphQL permet aux clients de spécifier exactement les données dont ils ont besoin et d'obtenir une réponse contenant uniquement ces données.	https://graphql.org/

INT_TG_90	PAdES	-	-	PAdES (PDF Advanced Electronic Signatures) est un ensemble de normes et de spécifications pour les signatures électroniques avancées basées sur le format PDF (Portable Document Format). PAdES est développé par l'ETSI (European Telecommunications Standards Institute) et vise à assurer l'interopérabilité entre les différentes solutions de signature électronique basées sur PDF.	https://en.wikipedia.org/wiki/PAdES
INT_TG_91	XAdES	-	-	XAdES (XML Advanced Electronic Signatures) vise à garantir l'interopérabilité des signatures électroniques avancées basées sur le format XML. L'interopérabilité dans le contexte de XAdES signifie que les signatures électroniques créées conformément à la spécification XAdES peuvent être traitées et validées correctement par d'autres systèmes et applications qui prennent en charge également XAdES.	https://en.wikipedia.org/wiki/XAdES
INT_TG_92	CAdES	-	-	CAdES (CMS Advanced Electronic Signatures) vise à fournir une interopérabilité élevée pour les signatures électroniques avancées. L'interopérabilité se réfère à la capacité des systèmes et des technologies à fonctionner ensemble de manière transparente, indépendamment de leur fournisseur ou de leur plateforme.	https://en.wikipedia.org/wiki/CAdES_(computing)
INT_TG_93	IPSec	-	-	IPSec (Internet Protocol Security) est un ensemble d'protocoles largement utilisé pour sécuriser les communications sur Internet au niveau du réseau. Il offre des services de sécurité tels que l'authentification, la confidentialité et l'intégrité des paquets IP. IPSec est généralement mis en œuvre dans les réseaux privés virtuels (VPN) pour établir des connexions sécurisées via Internet.	https://fr.wikipedia.org/wiki/IPsec

INT_TG_94	UDP	-	-	UDP (User Datagram Protocol) est un protocole de communication sur IP (Internet Protocol) qui permet l'échange de datagrammes sans établissement de connexion préalable. Contrairement au protocole TCP (Transmission Control Protocol), UDP ne fournit pas de mécanismes de fiabilité, de contrôle de flux ou de retransmission des données. Il est considéré comme un protocole non fiable et orienté vers la simplicité et la rapidité.	https://fr.wikipedia.org/wiki/User_Datagram_Protocol
INT_TG_95	NTP	-	-	NTP (Network Time Protocol) est un protocole de réseau utilisé pour synchroniser l'horloge des systèmes informatiques sur un réseau. Son objectif principal est de fournir une référence de temps précise et cohérente à tous les appareils connectés, ce qui est essentiel pour des applications qui dépendent d'une synchronisation temporelle précise.	https://fr.wikipedia.org/wiki/Network_Time_Protocol
INT_TG_96	RTP	-	-	RTP (Real-time Transport Protocol) est un protocole de transport utilisé pour la transmission en temps réel de données audio et vidéo sur les réseaux IP. Il est conçu pour garantir une livraison rapide et fiable des flux multimédias en minimisant la latence et en assurant la synchronisation entre les différents éléments d'un système de communication en temps réel.	https://fr.wikipedia.org/wiki/Real-time_Transport_Protocol
INT_TG_97	SRTP	-	-	SRTP (Secure Real-time Transport Protocol) est une extension sécurisée du protocole RTP (Real-time Transport Protocol) utilisé pour le transport sécurisé des données audio et vidéo en temps réel sur les réseaux IP. SRTP ajoute des fonctionnalités de confidentialité (chiffrement) et d'intégrité (authentification) à RTP, ce qui garantit la sécurité des flux multimédias échangés.	https://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol

INT_TG_98	AMQP	-	-	AMQP (Advanced Message Queuing Protocol) est un protocole de messagerie avancé et ouvert conçu pour les systèmes de messagerie fiables, scalables et interopérables. Il fournit une infrastructure pour l'échange de messages entre différentes applications et composants logiciels, indépendamment du langage de programmation utilisé ou de la plateforme sur laquelle ils s'exécutent.	https://en.wikipedia.org/wiki/Advanced_Message_Queueing_Protocol
INT_TG_99	LDAP	-	-	LDAP (Lightweight Directory Access Protocol) est un protocole de communication utilisé pour accéder et gérer les services de répertoire. Il permet aux applications d'effectuer des opérations de recherche, de modification, d'ajout et de suppression de données dans un annuaire.	https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
INT_TG_100	OpenPGP	-	-	OpenPGP est un standard open source utilisé pour le chiffrement et la signature numérique des données, principalement utilisé pour sécuriser les communications électroniques, tels que les e-mails. Il fournit des fonctionnalités de confidentialité, d'intégrité des données et d'authenticité des utilisateurs.	https://www.openpgp.org/
INT_TG_101	SAMLv2.0	V2		SAML (Security Assertion Markup Language) est un protocole d'échange d'informations d'authentification et d'autorisation basé sur des assertions. SAML version 2.0 est la version actuelle et largement utilisée de ce protocole. Il permet l'échange sécurisé d'informations d'identification entre une entité d'authentification (l'identité fournisseur d'authentification - IdP) et une entité de service (le fournisseur de services - SP) dans un environnement de fédération d'identités.	https://en.wikipedia.org/wiki/SAML_2.0

INT_TG_102	Oauth 2.0	V2		OAuth 2.0 (Open Authorization 2.0) est un protocole d'autorisation et de délégation d'accès qui permet à une application tierce d'obtenir un accès limité à des ressources protégées au nom d'un utilisateur, sans avoir à connaître les identifiants d'authentification de l'utilisateur.	https://oauth.net/2/
INT_TG_103	Open ID connect	-	-	OpenID Connect est une extension du protocole OAuth 2.0 qui permet l'authentification et l'autorisation sécurisées des utilisateurs. Il fournit une couche d'identification et de profilage au-dessus d'OAuth 2.0, permettant aux utilisateurs d'accéder à des services en ligne avec leurs identifiants provenant d'un fournisseur d'identité.	https://fr.wikipedia.org/wiki/OpenID_Connect
INT_TG_104	UDDI	-	-	UDDI (Universal Description, Discovery, and Integration) est un protocole et une spécification de registre de services Web qui permet la publication, la recherche et la découverte des services Web dans un environnement distribué. Il fait partie de la pile de technologies des services Web.	https://fr.wikipedia.org/wiki/Universal_Description_Discovery_and_Integration
INT_TG_105	UTF-8	-	-	UTF-8 (Unicode Transformation Format 8-bit) est un encodage de caractères universel largement utilisé. Il permet de représenter les caractères de presque toutes les langues et de nombreux symboles spéciaux.	https://fr.wikipedia.org/wiki/UTF-8
INT_TG_106	Bzip2	-	-	Bzip2 est un algorithme de compression de données et un format de fichier associé. Utilisé pour compresser et décompresser des fichiers, réduisant ainsi leur taille et économisant de l'espace de stockage.	https://en.wikipedia.org/wiki/Bzip2
INT_TG_107	DocBook	-	-	DocBook est un langage de balisage XML (eXtensible Markup Language) conçu spécifiquement pour la création de documentation technique et de contenu structuré. Il fournit un ensemble de règles et de balises pour décrire différents	https://en.wikipedia.org/wiki/DocBook

				types de documents tels que des manuels, des guides de référence, des spécifications techniques, des livres électroniques, etc.	
INT_TG_108	CSS	-	-	CSS (Cascading Style Sheets) est un langage de feuilles de style utilisé pour décrire la présentation visuelle des documents HTML (Hypertext Markup Language) et XML (eXtensible Markup Language). Il permet de contrôler l'apparence et la mise en page des éléments d'une page web.	https://fr.wikipedia.org/wiki/Feuilles_de_style_en_cascade
INT_TG_109	CMIS	-	-	CMIS (Content Management Interoperability Services) est un ensemble de normes et de protocoles qui permettent l'interopérabilité entre différents systèmes de gestion de contenu (CMS) et repositories de contenu.	https://en.wikipedia.org/wiki/Content_Management_Interoperability_Services
INT_TG_110	DOM	-	2023	DOM (Document Object Model) est une interface de programmation normalisée par le W3C (World Wide Web Consortium) qui permet d'accéder et de manipuler les éléments d'un document HTML, XML ou XHTML. Le DOM représente la structure logique d'un document et fournit des méthodes et des propriétés pour interagir avec les éléments du document.	https://dom.spec.whatwg.org/
INT_TG_111	YAML	-	2001	YAML (YAML Ain't Markup Language) est un format de sérialisation de données utilisé pour représenter des informations structurées de manière lisible par les humains. Il est souvent utilisé comme langage de configuration ou de données dans de nombreux domaines, tels que le développement logiciel, l'infrastructure as code et la gestion des configurations.	https://fr.wikipedia.org/wiki/YAML

INT_TG_112	RAML	V1	2016	RAML (RESTful API Modeling Language) est un langage de modélisation conçu pour décrire et documenter les interfaces de programmation d'applications (API) RESTful. Il offre un moyen structuré de décrire les ressources, les méthodes, les paramètres, les types de données et les autres aspects d'une API, ce qui facilite la création et la maintenance de l'API.	https://en.wikipedia.org/wiki/RAML_(software)
INT_TG_113	iCalendar	-	-	iCalendar est un format de fichier standardisé utilisé pour créer, stocker et échanger des informations relatives aux calendriers, aux événements et aux tâches. Il permet aux utilisateurs de partager facilement des informations de calendrier entre différentes applications et plateformes.	https://fr.wikipedia.org/wiki/iCalendar
INT_TG_114	XSLT	V3	2017	XSLT (Extensible Stylesheet Language Transformations) est un langage de transformation utilisé pour convertir des documents XML en d'autres formats, tels que HTML, XHTML, XML ou même du texte brut. Il est basé sur la syntaxe XML et permet de définir des règles de transformation pour extraire, filtrer, trier et formater les données contenues dans un document XML.	https://www.w3.org/TR/xslt-30/
INT_TG_115	XPath	3.1	2017	XPath (XML Path Language) est un langage de requête utilisé pour naviguer et interroger des documents XML. Il permet de localiser et de sélectionner des éléments spécifiques dans une structure XML en utilisant des expressions basées sur la syntaxe XPath.	https://fr.wikipedia.org/wiki/XPath
INT_TG_116	XQuery			XQuery est un langage de requête conçu pour interroger et extraire des données à partir de documents XML. Il permet d'effectuer des requêtes complexes sur des données XML structurées, en utilisant des expressions et des opérations spécifiques.	https://fr.wikipedia.org/wiki/XQuery

INT_TG_117	XML Signature	V1.1	2013	XML Signature est une spécification du W3C (World Wide Web Consortium) qui définit un format standard pour la signature numérique des documents XML. Elle permet d'ajouter des signatures électroniques aux documents XML afin de garantir leur intégrité, leur authenticité et leur non-répudiation.	https://www.w3.org/TR/xmlsig-core1/
INT_TG_118	OpenLS	1.2	2005	OpenLS (Location Services) est un ensemble de spécifications permettant l'accès aux services de localisation basés sur le protocole OGC.	https://open-tablets.org/downloads
INT_TG_119	OWS Context	1	2013	OWS Context est un standard du Consortium Open Geospatial (OGC) qui définit un modèle de données XML pour décrire des contextes géospatiaux	https://www.ogc.org/standard/owc/
INT_TG_120	SLD	1.1.0	2003	SLD (Styled Layer Descriptor) est un standard du Consortium Open Geospatial (OGC) utilisé pour décrire le style d'affichage des données géospatiales.	https://wiki.gis.com/wiki/index.php/Styled_Layer_Descriptor
INT_TG_121	GeoTIFF	1.0.0.1	1995	GeoTIFF est un format de fichier d'image géoréférencée qui permet de stocker des données raster avec des informations géospatiales	https://en.wikipedia.org/wiki/GeoTIFF
INT_TG_122	ASIC		2014	ASIC (Associated Signature Containers) est un format de conteneur pour les signatures électroniques conformes aux normes PAdES, XAdES et CAdES.	https://en.wikipedia.org/wiki/Associated_Signature_Containers
INT_TG_123	IDMEF	2	2000	IDMEF (Intrusion Detection Message Exchange Format) est un format de message normalisé utilisé pour l'échange d'informations sur les détections d'intrusion	https://fr.wikipedia.org/wiki/IDMEF:_Intrusion_Detection_Message_Exchange_Format

INT_TG_124	IODEF	2	2004	IODEF (Incident Object Description Exchange Format) est un format de message normalisé utilisé pour l'échange d'informations sur les incidents de sécurité.	https://en.wikipedia.org/wiki/Incident_Object_Description_Exchange_Format
------------	-------	---	------	---	---

3. Data Standard

Les normes de gouvernance des données font référence aux lignes directrices et aux meilleures pratiques pour gérer, protéger et utiliser les données gouvernementales de manière sécurisée et responsable.

Voici une liste de normes de gouvernance des données :

ID	Standard/Norme	Version	Date publication	Description	Url Documentation
Data_TG_01	GDPR (General Data Protection Regulation)	JO L 127 du 23.5.2018	2018	Règlement européen sur la protection des données à caractère personnel, qui est entré en vigueur en mai 2018. Le GDPR renforce les droits des citoyens de l'UE en matière de protection de leurs données personnelles, tout en imposant des obligations strictes aux organisations qui traitent ces données.	https://gdpr-info.eu/
Data_TG_02	HIPAA	-	1996	Loi sur la portabilité et la responsabilité des assurances de santé	https://www.cdc.gov/phlp/publications/topic/hipaa.html
Data_TG_03	PDPA	2020 REVISED EDITION	45068	Personal Data Protection Act (Singapour)	https://sso.agc.gov.sg/Act/PDPA2012
Data_TG_04	ISO/IEC 27001	2022	2022	Standard de gestion de la sécurité de l'information	https://www.iso.org/fr/standard/27001

Data_TG_05	ISO/IEC 27701	2019	2019	Extension de l'ISO/IEC 27001 pour la protection des données à caractère personnel	https://www.iso.org/fr/standard/71670.html
Data_TG_06	SOC 2	-	-	évalue les contrôles de sécurité et la conformité des systèmes et des organisations qui gèrent des données sensibles pour des tiers, tels que des fournisseurs de services cloud, des centres de données ou des sociétés de traitement des paiements.	https://www.mperva.com/learn/data-security/soc-2-compliance/
Data_TG_07	UK Data Protection Act 2018	2018	2018	Le UK Data Protection Act 2018 est une loi du Royaume-Uni qui régit la protection des données à caractère personnel.	https://www.gov.uk/data-protection
Data_TG_08	Cloud Security Alliance (CSA) STAR	-	2018	Cadre de certification de sécurité pour les fournisseurs de services cloud, qui évalue la sécurité des offres de services cloud. Le CSA STAR fournit un registre public permettant aux fournisseurs de services cloud de démontrer leur niveau de conformité aux meilleures pratiques de sécurité.	https://cloudsecurityalliance.org/star
Data_TG_09	ISO/IEC 27017 Cloud security	2015	2015-12	Norme internationale pour la sécurité de l'information applicable aux services cloud. Elle fournit des directives et des mesures de sécurité spécifiques aux services cloud, en complément de l'ISO/IEC 27001.	https://www.iso.org/standard/43757.html
Data_TG_10	ISO/IEC 27018	2019	2019-01	Norme internationale qui établit des lignes directrices pour la protection des informations personnelles identifiables dans le cloud computing. Elle fournit des mesures de contrôle spécifiques pour les fournisseurs de services cloud traitant des données personnelles.	https://www.iso.org/fr/standard/76559.html
Data_TG_11	CCM (Cloud Controls Matrix)	Version 4	44354	Un cadre de contrôles de sécurité développé par le Cloud Security Alliance (CSA) pour aider les organisations à évaluer et attester la sécurité des services cloud. Le CCM fournit une liste exhaustive de contrôles de sécurité et des bonnes pratiques pour différentes	https://cloudsecurityalliance.org/research/cloud-controls-matrix/

				catégories de services cloud.	
Data_TG_12	NIST SP 800-146	-	5/1/2012	Guide du National Institute of Standards and Technology (NIST) des États-Unis pour l'adoption du cloud computing. Il fournit des recommandations pour les organisations qui envisagent de migrer vers le cloud, en abordant les considérations de sécurité, de confidentialité, d'intégrité et de disponibilité.	https://csrc.nist.gov/publications/detail/sp/800-146/final
Data_TG_13	NIST SP 800-144	-	12/1/2011	Guide du NIST sur la sécurité et la confidentialité dans le cloud computing. Il fournit une vue d'ensemble des concepts, des mécanismes de sécurité et des défis liés au cloud computing, ainsi que des recommandations pour la gestion des risques et la protection des données dans le cloud.	https://csrc.nist.gov/publications/detail/sp/800-144/final
Data_TG_15	GraphQL	-	Oct 26, 2021	Un langage de requête pour les API qui permet de demander des données spécifiques aux serveurs, offrant ainsi une flexibilité accrue par rapport aux requêtes REST traditionnelles	https://graphql.org/
Data_TG_16	NIST Privacy Framework	Version 1.1	April 16, 2018	Un cadre de référence élaboré par le National Institute of Standards and Technology (NIST) des États-Unis pour aider les organisations à gérer les risques liés à la vie privée. Il fournit des lignes directrices pour la gestion des données personnelles et la protection de la vie privée dans le contexte des activités commerciales.	https://www.nist.gov/privacy-framework
Data_TG_17	ISO/IEC 29100	2011	2011	Une norme internationale qui fournit des principes et des cadres pour la protection de la vie privée des individus dans le contexte de la technologie de l'information. Elle vise à aider les organisations à gérer les risques liés à la confidentialité des données personnelles.	https://www.iso.org/standard/45123.html

Data_TG_18	Singapore Data Exchange	-	2022	SDX facilite la collaboration et l'interopérabilité des données en fournissant des interfaces de données normalisées, un stockage sécurisé des données et des mécanismes de gouvernance des données. Elle contribue à rationaliser les processus de partage de données, à améliorer la qualité des données et à renforcer la prise de décisions basée sur les données au sein des organismes gouvernementaux.	https://www.mas.gov.sg/development/finTech/SGFinDex
Data_TG_19	Singapore Whole-of-Government Data Sharing Principles	-	-	Ensemble de principes directeurs établis par le gouvernement de Singapour pour guider le partage et l'échange de données entre les organismes gouvernementaux.	https://data.gov.sg/about
Data_TG_20	SS 584	2020	2020	La norme SS 584 établit les exigences et les meilleures pratiques pour les fournisseurs de services cloud afin de garantir la sécurité, la confidentialité et la fiabilité des services cloud. Elle vise à aider les organisations à évaluer et à sélectionner des fournisseurs de services cloud qui répondent à leurs besoins spécifiques en matière de sécurité des données et de gestion des risques.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/b5430dc1-27f3-4203-bd8e-00345da6bed5
Data_TG_21	ISO 19115	2014	2014-04	ISO 19115 est une norme internationale de métadonnées géospatiales. Elle fournit un cadre pour décrire, documenter et organiser les données géospatiales, facilitant ainsi leur découverte, leur utilisation et leur partage.	https://www.iso.org/standard/26020.html
Data_TG_22	ISO 19139	2019	2019-03	La norme ISO 19139 définit la syntaxe XML et les schémas de données nécessaires pour représenter les éléments de métadonnées définis dans la norme ISO 19115. Elle précise également les règles de validation et les règles de liaison entre les différentes parties des métadonnées.	https://www.iso.org/standard/32557.html

Data_TG_23	OpenDocument Format ODF	version 2.0	20 avril 2016	ODF est un format de fichier basé sur XML qui permet de stocker des documents texte, des feuilles de calcul, des présentations, des dessins et d'autres types de contenu bureautique de manière indépendante de l'application ou de la plate-forme utilisée.	https://opendocumentformat.org/aboutODF/
Data_TG_24	PDF	21.011.200 39	11 janvier 2022	Format de document indépendant de la plateforme	https://www.adobe.com/fr/acrobat/about-adobe-pdf.html
Data_TG_25	Singapore Open Data Licence	version 1.0	-	La Singapore Open Data Licence (Licence de données ouvertes de Singapour) est une licence utilisée pour la diffusion et l'utilisation des données ouvertes du gouvernement de Singapour. Elle vise à promouvoir la réutilisation et le partage des données gouvernementales dans un cadre ouvert et transparent.	https://www.mas.gov.sg/terms-of-use/open-data-licence
Data_TG_26	XML (Langage de balisage hypertexte extensible)	-	November 2008	XML (eXtensible Markup Language) est un langage de balisage hypertexte extensible qui permet de structurer et de stocker des données de manière lisible par les humains et les machines. Il est utilisé pour décrire et échanger des informations structurées entre différentes applications et plates-formes.	https://www.w3.org/standards/xml/core
Data_TG_27	JSON (JavaScript Object Notation)	-	December 2017	JSON est un format de données léger et facile à lire/écrire pour l'échange de données. Il est largement utilisé dans les applications web et les services web pour représenter et échanger des données structurées.	https://datatracker.ietf.org/doc/html/rfc8259
Data_TG_28	CSV	-	January 2014	CSV (Comma-Separated Values) est un format de fichier couramment utilisé pour stocker et échanger des données tabulaires sous forme de texte brut. Il s'agit d'un format simple et largement pris en charge par de nombreux logiciels et applications.	https://fr.wikipedia.org/wiki/Comma-separated_values

Data_TG_29	IDM Industry Data Model	-	-	Le modèle de données de l'industrie (IDM - Industry Data Model) est un modèle de données standardisé spécifiquement conçu pour représenter les concepts et les relations dans un domaine industriel particulier. Il offre une structure et une terminologie communes pour la modélisation des données dans ce domaine, facilitant ainsi l'intégration et l'échange de données entre les différentes organisations et systèmes.	https://www.teradata.fr/Resources/DataSheets/Industry-Data-Models-iDM
Data_TG_30	UBL Universal Business Language	UBL 2.3	UBL Universal Business Language	UBL (Universal Business Language) est un langage universel de commerce électronique basé sur XML. Il fournit une norme internationale pour la représentation des documents commerciaux, tels que les factures, les bons de commande, les bons de livraison, les devis, etc., dans un format électronique structuré et normalisé.	https://www.oasis-open.org/committees/tc_home.php?wg_abbr=UBL
Data_TG_31	EDXL Emergency Data Exchange Language	Version 1.1	2016	EDXL (Emergency Data Exchange Language) est un langage d'échange de données d'urgence qui vise à faciliter la communication et l'échange d'informations critiques entre les organisations et les systèmes impliqués dans la gestion des situations d'urgence. Il fournit une norme commune pour la représentation des données liées aux urgences, telles que les alertes, les rapports de situation, les ressources disponibles, les plans d'évacuation, etc.	https://www.oasis-open.org/standard/edxl-1/
Data_TG_32	EDXL-Common	Version 1.0	2015	Définit un modèle de données commun pour le partage des informations liées aux urgences	https://docs.oasis-open.org/emergency/edxl-ct/v1.0/edxl-ct-v1.0.html
Data_TG_33	EDXL-DE	Version 2.0	2013	Définit un élément de distribution pour l'échange de données d'urgence entre les systèmes.	https://docs.oasis-open.org/emergency/edxl-de/v2.0/edxl-de-v2.0.html

Data_TG_34	EDXL-HAVE	Version 1.0	2016	Définit une norme pour le partage des informations sur la disponibilité et l'état des hôpitaux pendant les urgences.	https://docs.oasis-open.org/emergency/edxl-have/v2.0/edxl-have-v2.0.html
Data_TG_35	EDXL-RM	Version 1.0	2009	Définit une norme de messagerie de ressources pour le partage d'informations sur les ressources en cas d'urgence.	https://docs.oasis-open.org/emergency/edxl-rm/v1.0/os/EDXL-RM-v1.0-OS.pdf
Data_TG_36	EDXL-SitRep	Version 1.0	06 Oct 2016	Définit une norme pour le partage des rapports de situation en cas d'urgence.	https://www.oasis-open.org/standard/edxl-sitrep/
Data_TG_37	ISO/IEC 27001	2022	2022	Cette norme définit les exigences pour la mise en place d'un système de gestion de la sécurité de l'information. Elle fournit un cadre pour établir, mettre en œuvre, maintenir et améliorer la sécurité de l'information dans un contexte de cloud computing.	https://www.iso.org/fr/standard/27001
Data_TG_38	ISO/IEC 17789	2014	2014	Cette norme décrit les exigences et les recommandations pour l'évaluation et l'assurance de la conformité dans le contexte du cloud computing. Elle fournit des directives pour l'évaluation de la sécurité, de la confidentialité, de la disponibilité et d'autres aspects pertinents des services de cloud computing.	https://www.iso.org/standard/60545.html
Data_TG_39	PSPF	-	-	PSPF (Protective Security Policy Framework) est un cadre de politique de sécurité utilisé en Australie. Il fournit des directives et des normes de sécurité pour aider les organisations à protéger leurs informations sensibles et à gérer les risques de sécurité.	https://ngm.com.au/protective-security-policy-framework
Data_TG_40	ISO/IEC 27701	2019	2019	La norme ISO/IEC 27701 fournit des lignes directrices sur les mesures de protection des informations personnelles, y compris la collecte, le traitement, le stockage, la conservation, la divulgation, la suppression et la	https://www.iso.org/standard/71670.html

				destruction de ces informations. Elle s'appuie sur les principes et les exigences énoncés dans la norme ISO/IEC 27001 pour assurer la conformité aux lois et réglementations en matière de protection des données personnelles.	
Data_TG_41	Data Protection Act 2018 (DPA 2018)	-	2018	Le DPA 2018 établit les principes fondamentaux de la protection des données et définit les droits des individus en ce qui concerne le traitement de leurs données personnelles. Il énonce les obligations des organisations qui collectent, traitent et stockent des données personnelles, et prévoit des sanctions en cas de non-respect de ces obligations.	https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
Data_TG_42	COBIT (Control Objectives for Information and Related Technologies)	version 5	avril 2012	Un cadre de gouvernance des technologies de l'information qui inclut également des aspects de gouvernance des données. COBIT fournit des objectifs de contrôle, des processus et des bonnes pratiques pour assurer la gouvernance et le contrôle des données au sein des organisations.	https://fr.wikipedia.org/wiki/COBIT
Data_TG_43	The Estonian Open Data Policy	-	31 January 2019	La "Politique estonienne en matière de données ouvertes" fait référence à l'approche adoptée par le gouvernement estonien pour promouvoir l'ouverture et l'accès aux données publiques dans le pays. Cette politique vise à encourager la transparence, l'innovation et la participation citoyenne en facilitant la disponibilité et l'utilisation des données publiques.	https://link.springer.com/chapter/10.1007/978-3-030-11410-7_3
Data_TG_44	The Estonian Personal Data Protection Act	-	31 January 2019	La "Loi estonienne sur la protection des données personnelles" régit la protection des données personnelles en Estonie. Elle établit les principes, les droits et les obligations relatifs au traitement des données personnelles par les organisations et les individus.	https://caseguard.com/articles/estonia-new-amendment-to-data-privacy-law-gdpr/

Data_TG_45	INSPIRE (Infrastructure for Spatial Information in the European Community)	-	2009	INSPIRE définit un cadre juridique et technique pour la collecte, la gestion et la diffusion des données spatiales dans différents domaines tels que l'environnement, l'agriculture, les transports, l'énergie, etc. Les données couvertes comprennent des informations géographiques telles que les cartes, les images satellite, les données topographiques, les données sur les sols, les données hydrographiques, etc.	https://ico.org.uk/media/about-the-ico/policies-and-procedures/2782/inspire-regulations_2009_and_the_role_of_the_ic.pdf
Data_TG_46	TR 82	2020	2020	Consignes pour la sécurité Cloud Native	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/db1a6d1a-35e1-43dc-ba89-a79c405bab14
Data_TG_47	TR 62	2018	2018	Lignes directrices pour la réponse aux incidents liés aux pannes de cloud (COIR)	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/b9377ccc-ae4f-4454-ad71-830d2c143636
Data_TG_48	ISO/IEC 29151	2017	2017-08	Cette norme internationale fournit des lignes directrices aux organisations sur la manière d'aborder la confidentialité et la protection des informations personnelles identifiables (PII) dans le contexte du cloud computing.	https://www.iso.org/standard/62726.html
Data_TG_49	GeoJSON	-	August 2016	Un format de données basé sur JSON spécifiquement conçu pour représenter des données géospatiales, telles que des points, des lignes et des polygones.	https://fr.wikipedia.org/wiki/GeoJSON
Data_TG_50	ISO 8000	2015	2015	Cette norme internationale fournit des lignes directrices et des principes pour la gestion de la qualité des données, y compris des recommandations sur les processus, les méthodes et les	https://www.iso.org/standard/60805.html

				mesures pour évaluer et améliorer la qualité des données.	
Data_TG_51	CCPA	-	2020	La CCPA est une loi californienne qui accorde aux consommateurs de Californie des droits concernant la confidentialité de leurs données personnelles. Elle exige des entreprises qu'elles fournissent des divulgations claires sur la collecte et l'utilisation des données personnelles, ainsi que des options pour limiter leur utilisation.	https://www.visitor-analytics.io/fr/glossaire/c/loi-californienne-sur-la-protection-de-la-vie-privee-des-consommateurs-ccpa/
Data_TG_52	APEC Cross-Border Privacy Rules (CBPR)	v6.1	2021	Developed by the Asia-Pacific Economic Cooperation (APEC) forum, the CBPR is a privacy framework that enables participating organizations to ensure the protection of personal information when transferred across borders within the APEC region.	http://mddb.apec.org/Documents/2021/CTI/WKSP9/21_cti_wksp9_010.pdf
Data_TG_53	NoSQL	-	2010	Catégorie de bases de données non relationnelles offrant une flexibilité et une évolutivité élevées pour la gestion de gros volumes de données.	https://fr.wikipedia.org/wiki/NoSQL
Data_TG_54	SP 800-145	2011	September 2011	Le cloud computing est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement provisionnés et libérés avec un effort de gestion minimal ou interactions avec le fournisseur de services. Ce modèle de cloud est composé de cinq caractéristiques essentielles, de trois modèles de service et de quatre modèles de déploiement.	https://csrc.nist.gov/publications/detail/sp/800-145/final

Data_TG_55	EVS-EN 14485	-	2004	La présente Norme européenne fournit des lignes directrices sur la protection des données pour les personnes impliquées dans l'informatique internationale applications qui impliquent la transmission de données de santé personnelles d'un État membre de l'UE vers un État non membre de l'UE. Son objectif est d'aider à l'application de la directive européenne sur la protection des données	https://www.evs.ee/en/evs-en-14485-2004
Data_TG_56	EVS-EN 17529	-	2022	Protection des données et confidentialité dès la conception et par défaut	https://www.evs.ee/en/evs-en-17529-2022
Data_TG_57	ISO/IEC 27555	-	2021	Ce document contient des lignes directrices pour l'élaboration et l'établissement de politiques et de procédures de suppression des informations personnelles identifiables (PII) dans les organisations	https://www.iso.org/standard/71673.html
Data_TG_58	Hadoop	-	-	Hadoop est un framework open source utilisé pour le stockage et le traitement distribué de grandes quantités de données sur des clusters de serveurs. Il est conçu pour traiter efficacement les données volumineuses et les tâches de traitement parallèles.	https://hadoop.apache.org/
Data_TG_59	Apache Kafka	-	-	Apache Kafka est une plateforme de streaming distribuée open source qui est largement utilisée pour la gestion et le traitement des flux de données en temps réel. Il fournit une architecture de messagerie hautement évolutive et tolérante aux pannes, capable de gérer des volumes massifs de données provenant de multiples sources et de les distribuer efficacement à des applications en temps réel.	https://kafka.apache.org/
Data_TG_60	SQL	-	-	SQL (Structured Query Language) est un langage de requête standardisé utilisé pour communiquer avec des bases de données relationnelles. Il permet de manipuler et de gérer les données stockées dans une base de données, notamment pour effectuer des opérations telles que la création, la modification, la	https://en.wikipedia.org/wiki/SQL

				suppression et la récupération des données.	
Data_TG_61	HDFS	-	-	HDFS (Hadoop Distributed File System) est un système de fichiers distribué conçu pour stocker de grandes quantités de données sur des clusters de serveurs. Il fait partie de l'écosystème Hadoop et est utilisé pour le stockage de données dans le cadre du traitement distribué et de l'analyse de données à grande échelle.	https://www.lebigdata.fr/hdfs-fonctionnement-avantages
Data_TG_62	Apache Hive	-	-	Apache Hive est un système de traitement et d'interrogation de données distribué, développé par la fondation Apache. Il fournit une interface SQL-like pour interagir avec des données stockées dans des systèmes de fichiers distribués, tels que Hadoop Distributed File System (HDFS), ainsi que d'autres systèmes de stockage compatibles.	https://fr.wikipedia.org/wiki/Apache_Hive
Data_TG_63	ISO/IEC 38500	2015	2015	L'ISO/IEC 38500 est une norme internationale qui fournit des lignes directrices pour la gouvernance des technologies de l'information (TI) au sein des organisations. Elle définit les principes et les recommandations permettant aux dirigeants et aux membres du conseil d'administration d'assumer leurs responsabilités en matière de gouvernance des TI.	https://www.iso.org/standard/62816.html
Data_TG_64	RDF (Resource Description Framework)	-	-	Le RDF (Resource Description Framework) est un cadre standardisé développé par le World Wide Web Consortium (W3C) pour représenter et échanger des informations structurées sur le web. Il fournit un modèle de données flexible et extensible permettant de décrire les ressources et leurs relations.	https://fr.wikipedia.org/wiki/Resource_Description_Framework

Data_TG_65	ODBC (Open Database Connectivity)	-	-	ODBC (Open Database Connectivity) est une interface de programmation standardisée qui permet aux applications d'accéder à des bases de données relationnelles de manière indépendante du système de gestion de bases de données (SGBD). Il a été développé par Microsoft dans les années 1990 et est désormais largement utilisé dans de nombreuses plateformes et systèmes d'exploitation.	https://www.netsuite.com/portal/partners.shtml
Data_TG_66	SGDSC	-	-	SGDSC (Singapore Government Data Sharing and Collaboration) Data Management est un ensemble de principes et de pratiques qui régissent la gestion des données au sein du gouvernement de Singapour. Ces principes et pratiques sont conçus pour garantir la qualité, la sécurité, l'intégrité et l'accessibilité des données utilisées par les agences gouvernementales.	
Data_TG_67	SDX	-	-	SDX fait référence à la Singapore Data Exchange (SDX), qui est une plateforme de données développée par le gouvernement singapourien pour faciliter l'échange de données entre les organisations.	
Data_TG_68	SWGDSP	-	-	SWGDSP (Singapore Whole-of-Government Data Sharing Principles) est un ensemble de principes directeurs qui régissent la manière dont les données sont partagées au sein du gouvernement de Singapour. Ces principes ont été développés dans le but de promouvoir l'échange de données entre les agences gouvernementales et de favoriser une utilisation efficace et sécurisée des données.	
Data_TG_69	DCAT-AP	-	-	DCAT-AP (Data Catalogue Application Profile) est un profil d'application du modèle DCAT (Data Catalog Vocabulary) développé par le groupe de travail W3C (World Wide Web Consortium) pour décrire et publier des catalogues de données. DCAT-AP fournit des spécifications et des bonnes pratiques pour l'échange de	https://www.w3.org/TR/vocab-dcat-3/

				métadonnées sur les ensembles de données dans le cadre de l'interopérabilité entre les catalogues de données.	
Data_TG_70	Dublin Core	-	-	Dublin Core est un ensemble de métadonnées standardisées utilisées pour décrire des ressources numériques telles que des documents, des images, des vidéos, des sites web, etc. Il s'agit d'une initiative visant à faciliter la recherche et la découverte de ces ressources en fournissant des informations essentielles sur leur contenu et leur contexte.	https://fr.wikipedia.org/wiki/Dublin_Core
Data_TG_71	XBRL	-	-	XBRL (eXtensible Business Reporting Language) est un langage de balisage basé sur XML utilisé pour l'échange électronique de données financières et comptables. Il a été spécifiquement développé pour faciliter la communication et l'analyse des rapports financiers et des informations comptables entre les organisations et les parties prenantes telles que les régulateurs, les investisseurs, les analystes financiers, etc.	https://en.wikipedia.org/wiki/XBRL
Data_TG_73	SODL	1	-	licence Singapore Open Data Licence (SODL) peut être appliquée pour régir la réutilisation des données ouvertes publiées par les organismes gouvernementaux.	https://dataall.ita.gov.sg/content/datamall/en/SingaporeOpenDataLicence.html
Data_TG_74	Python	-	-	Python est un langage de programmation polyvalent et populaire, apprécié pour sa simplicité, sa lisibilité et sa grande communauté de développeurs.	https://fr.wikipedia.org/wiki/Python_(language)
Data_TG_75	R	-	-	R est un langage de programmation et un environnement statistique largement utilisé pour l'analyse de données, la manipulation de données et la création de visualisations. Il est apprécié par les statisticiens, les scientifiques des données et les chercheurs pour sa richesse en fonctionnalités et sa flexibilité.	https://fr.wikipedia.org/wiki/R_(langage)

Data_TG_76	PostgresSQL	-	-	PostgreSQL, souvent appelé Postgres, est un système de gestion de base de données relationnelle (SGBDR) open source. Il est reconnu pour sa fiabilité, sa conformité aux standards SQL et sa richesse en fonctionnalités avancées.	https://fr.wikipedia.org/wiki/PostgreSQL
Data_TG_77	MySQL	-	-	MySQL est un système de gestion de base de données relationnelle (SGBDR) open source. Il est l'un des systèmes de base de données les plus populaires et largement utilisés dans le développement d'applications web et d'autres applications nécessitant un stockage et une gestion efficaces des données.	https://fr.wikipedia.org/wiki/MySQL
Data_TG_78	Maria DB	-	-	MariaDB est un système de gestion de base de données open source qui est une alternative compatible avec MySQL. Il a été développé par les développeurs originaux de MySQL après l'acquisition de MySQL par Oracle Corporation.	https://fr.wikipedia.org/wiki/MariaDB
Data_TG_79	Mongo DB	-	-	MongoDB est un système de gestion de base de données orienté document, open source et NoSQL (Not Only SQL). Contrairement aux bases de données relationnelles traditionnelles, MongoDB ne stocke pas les données dans des tables avec des lignes et des colonnes, mais plutôt dans des documents flexibles au format BSON (Binary JSON).	https://fr.wikipedia.org/wiki/MongoDB
Data_TG_80	Redis	-	-	Redis est un système de base de données en mémoire open source qui permet de stocker et de manipuler des données en utilisant une structure de données clé-valeur. Il se distingue par sa rapidité et sa flexibilité, ce qui en fait un choix populaire pour les applications nécessitant une manipulation rapide de données en mémoire.	https://fr.wikipedia.org/wiki/Redis
Data_TG_81	Memcached	-	-	Memcached est un système de mise en cache distribuée et en mémoire qui est largement utilisé pour améliorer les performances des applications web en stockant temporairement des données fréquemment utilisées en mémoire principale. Il agit	https://fr.wikipedia.org/wiki/Memcached

				comme un serveur de cache léger et rapide, permettant aux applications d'accéder rapidement aux données sans avoir à les récupérer à partir de sources de données plus lentes, telles que les bases de données.	
Data_TG_82	ISO 19157	2013	2013	ISO 19157 établit des principes, des spécifications et des directives pour évaluer et spécifier la qualité des données géographiques, y compris les données de géolocalisation, les cartes, les modèles numériques du terrain, etc. Elle fournit des lignes directrices pour la collecte, le traitement, la documentation et la communication des informations sur la qualité des données géographiques.	https://www.iso.org/standard/32575.html
Data_TG_83	WGS84	-	-	WGS84 (World Geodetic System 1984) est un système de référence géodésique mondial largement utilisé pour définir les coordonnées géographiques et altitudes. Il a été développé par le Département de la Défense des États-Unis pour une utilisation dans les systèmes de positionnement par satellite, notamment le GPS (Global Positioning System).	https://fr.wikipedia.org/wiki/WGS_84
Data_TG_84	ISO 19110	2016	2016	Elaborer un catalogue d'entités selon la norme ISO 19110 en décrivant les classes d'entités géographiques, leurs propriétés, leurs relations et leur regroupement	https://www.iso.org/obp/ui/#iso:std:iso:19110:ed-2:v1:fr

4. Identity & Access Management Standards

Les normes de gestion des identités et des accès (Identity & Access Management Standards) sont des directives et des pratiques établies pour assurer une gestion sécurisée et efficace des identités des utilisateurs et de leurs accès aux systèmes, applications et données.

Voici une liste de normes d'authentification et IAM :

ID	Standard/Norme	Version	Date de publication	Description	Url Documentation
IAM_TG_01	SAML	Version 2.0	mars 2005	Protocole de langage de balisage de sécurité basé sur XML pour l'authentification unique (SSO) et l'autorisation	https://developer.okta.com/docs/concepts/saml/
IAM_TG_02	OpenID Connect	-	-	Identity layer on top of OAuth 2.0	https://openid.net/connect/
IAM_TG_03	OAuth 2.0	2.1	2012-05-03	Authorization framework for third-party access to resources	https://fr.wikipedia.org/wiki/OAuth
IAM_TG_04	Kerberos	Version 5	26 May 2022	Network authentication protocol	https://en.wikipedia.org/wiki/Kerberos_(protocol)
IAM_TG_05	FIDO2	-	2015-09-04	Fast Identity Online Alliance 2.0	https://fidoalliance.org/fido2/
IAM_TG_06	Biometric Authentication	-	-	Authentication based on unique physical characteristics	https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

IAM_TG_07	JWT (JSON Web Tokens)	-	2015-01-01	Format compact et autonome pour transmettre des informations d'identité	https://jwt.io/introduction/
IAM_TG_08	SCIM (System for Cross-Domain Identity Management)	Version 2.0	2011-12-15	Protocole pour la gestion des identités entre systèmes	https://en.wikipedia.org/wiki/System_for_Cross-domain_Identity_Management
IAM_TG_09	OATH (Initiative for Open Authentication)	-	-	Standards d'authentification ouverte et basée sur les mots de passe	https://en.wikipedia.org/wiki/Initiative_for_Open_Authentication
IAM_TG_10	FIDO UAF (Universal Authentication Framework)	1.2.0	2016-01-08	Framework d'authentification basé sur des caractéristiques spécifiques de l'utilisateur	https://fidoalliance.org/specifications/
IAM_TG_11	XACML (eXtensible Access Control Markup Language)	3	2013-01-17	Langage de contrôle d'accès basé sur des politiques pour la gestion des autorisations	https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
IAM_TG_12	WebAuthn	-	2019-03-04	Norme W3C pour l'authentification sans mot de passe	https://fr.wikipedia.org/wiki/WebAuthn
IAM_TG_13	SSO (Single Sign-On)	Version 3.0	22 January 2013	Mécanisme permettant aux utilisateurs de se connecter une seule fois	https://auth0.com/docs/authenticate/single-sign-on
IAM_TG_14	Multi-Factor Authentication (MFA)	-	-	Utilisation de plusieurs méthodes d'authentification	https://www.onelogin.com/learn/what-is-mfa
IAM_TG_15	SingPass	-	-	SingPass, abréviation de "Singapore Personal Access", est un système d'identification électronique (e-Identification) utilisé à Singapour. Il permet aux résidents singapouriens d'accéder à un large éventail de services gouvernementaux en ligne de manière sécurisée et pratique.	https://www.singpass.gov.sg/main/

IAM_TG_16	CorpPass	-	2018	CorpPass est un système d'authentification électronique utilisé à Singapour pour les entreprises et les organisations	https://sleek.com/resources/what-is-corppass-and-how-does-it-work/
IAM_TG_17	2FA	-	-	La 2FA (Authentification à deux facteurs), également appelée authentification multi-facteurs (MFA), est une méthode de sécurité qui renforce le processus d'authentification en ajoutant une couche de vérification supplémentaire. Elle vise à renforcer la sécurité en exigeant deux facteurs distincts pour vérifier l'identité d'un utilisateur.	https://www.contentstack.com/docs/developers/security/two-factor-authentication/
IAM_TG_18	PKI	-	-	PKI (Public Key Infrastructure) est une infrastructure de gestion des clés publiques utilisée pour sécuriser les communications électroniques, les transactions en ligne et l'authentification des utilisateurs. Elle repose sur l'utilisation de la cryptographie à clé publique pour garantir la confidentialité, l'intégrité et l'authenticité des données.	https://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques
IAM_TG_19	NIST SP 800-63	-	19 juin 2017	NIST SP 800-63 est un ensemble de recommandations publié par le National Institute of Standards and Technology (NIST) des États-Unis concernant l'authentification électronique. Il fournit des directives pour l'identification et l'authentification des utilisateurs dans les systèmes informatiques.	https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines
IAM_TG_20	U2F (Universal Second Factor)	-	02/14/2023	Spécification de FIDO pour l'authentification à deux facteurs basée sur des clés de sécurité physiques.	https://www.okta.com/identity-101/u2f/
IAM_TG_21	ISO/IEC 27001	2022	2022	Norme internationale pour la gestion de la sécurité de l'information, qui inclut également des exigences pour la gestion des identités et des accès.	https://www.iso.org/fr/standard/27001
IAM_TG_22	myGovID	1.5.0.0	January 23, 2020	myGovID est un système d'identification numérique utilisé en Australie. Il s'agit d'une méthode d'authentification numérique permettant aux citoyens australiens de se connecter en toute sécurité aux services gouvernementaux en ligne. Le myGovID remplace progressivement les anciens	myGovID - Wikipedia

				systèmes d'authentification tels que les noms d'utilisateur et les mots de passe.	
IAM_TG_23	GovPass	-	-	GovPass est un système d'identification numérique utilisé à Singapour. Il s'agit d'un service gouvernemental qui permet aux résidents de Singapour de s'authentifier de manière sécurisée et d'accéder à une variété de services gouvernementaux en ligne.	https://www.nedapsecurity.com/insight/what-is-govpass-and-how-can-it-be-used/
IAM_TG_24	National e-Authentication Framework	-	January 2009	Le National e-Authentication Framework (NeAF) est un cadre d'authentification électronique . Il a été développé pour faciliter l'identification et l'authentification électronique sécurisées des utilisateurs lorsqu'ils accèdent à des services gouvernementaux en ligne.	https://qcert.org/sites/default/files/public/documents/au-bp-national_eauthenticaton_framework-eng-2009.pdf
IAM_TG_25	Identity Assurance Framework (IAF)	-	11 September 2015	Identity Assurance Framework (IAF) est un cadre d'assurance d'identité utilisé au Royaume-Uni. Il a été développé pour établir des normes et des exigences pour l'assurance des identités en ligne lors de l'accès aux services numériques gouvernementaux.	https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles
IAM_TG_26	EIDAS (Electronic Identification/ Authentication and Trust Services)	-	23 juillet 2014	EIDAS (Electronic Identification, Authentication, and Trust Services) est un règlement de l'Union européenne qui établit un cadre juridique pour les services d'identification électronique, d'authentification électronique et de services de confiance numérique au sein de l'UE.	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
IAM_TG_27	Smart-ID	-	November 2018	Smart-ID utilise la technologie des cartes à puce virtuelles pour stocker les certificats numériques d'authentification. Les utilisateurs doivent télécharger l'application Smart-ID sur leur smartphone et enregistrer leur identité en associant leur numéro d'identification personnel à leur appareil. L'application génère ensuite un certificat numérique unique qui est utilisé pour l'authentification et la signature.	https://www.smart-id.com/help/faq/general/can-use-smart-id-sign-documents-electronically/

IAM_TG_28	The Estonian ID Card	-	-	La carte d'identité estonienne (Estonian ID Card en anglais) est un document d'identification électronique délivré par le gouvernement en Estonie. Elle sert de pièce d'identité officielle et permet d'accéder à une large gamme de services en ligne sécurisés dans le pays.	https://visafoto.com/estonia/e-resident-digital-id-card-application
IAM_TG_29	Aadhaar	-	2018	Aadhaar est le nom du programme d'identification unique en Inde, mis en place par l'Autorité d'identification unique de l'Inde (UIDAI). Aadhaar est également utilisé pour désigner le numéro d'identification unique à 12 chiffres qui est attribué à chaque résident indien.	https://fr.wikipedia.org/wiki/Aadhaar
IAM_TG_30	eKYC	-	-	eKYC (Electronic Know Your Customer) fait référence à un processus électronique utilisé pour vérifier l'identité des clients lors de l'ouverture de comptes ou de l'accès à des services financiers. Il permet de simplifier et d'accélérer le processus de vérification d'identité en utilisant des technologies numériques et des informations déjà disponibles.	https://www.electronicid.eu/fr/blog/post/ekyc-electronic-know-your-customer/fr
IAM_TG_31	Aadhaar Act	-	2016	La loi Aadhaar établit les bases juridiques de la collecte, du stockage et de l'utilisation des données Aadhaar, qui comprennent des informations biométriques et démographiques des résidents indiens. Elle vise à faciliter la fourniture de services gouvernementaux, de subventions, d'avantages sociaux et d'autres prestations en utilisant le numéro Aadhaar comme identifiant unique.	Aadhaar Act - Unique Identification Authority of India Government of India (uidai.gov.in)
IAM_TG_32	OTP Authentication	-	2005	L'authentification par OTP (One-Time Password) est une méthode d'authentification qui utilise des mots de passe à usage unique. Lors de ce processus, un mot de passe généré de manière aléatoire est envoyé à l'utilisateur, généralement par SMS, e-mail ou via une application mobile dédiée.	https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp

IAM_TG_33	PIV	-	2005	PIV (Personal Identity Verification) fait référence à un standard d'identification et d'authentification utilisé principalement dans le gouvernement. Le PIV est basé sur des cartes à puce qui contiennent des informations biométriques et des certificats numériques pour vérifier l'identité des individus.	https://csrc.nist.gov/projects/piv/piv-standards-and-supporting-documentation
IAM_TG_34	UIDAI	-	2 July 2016	L'UIDAI (Unique Identification Authority of India) est une autorité indienne responsable de la mise en œuvre du programme Aadhaar. Créée en 2009, l'UIDAI est chargée de la gestion du système d'identification unique en Inde, qui attribue des numéros Aadhaar uniques à chaque résident.	https://en.wikipedia.org/wiki/Aadhaar
IAM_TG_35	PSD2	PSD2	25 novembre 2015.	PSD2 introduit l'authentification forte du client (SCA) pour les paiements électroniques afin de renforcer la sécurité. Cela signifie que les paiements en ligne nécessitent généralement une validation à deux facteurs pour vérifier l'identité de l'utilisateur.	https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/5402
IAM_TG_36	i-PIN	i-PIN 2.0	July 2, 2009	i-PIN (Internet Personal Identification Number) est un terme utilisé en Corée du Sud pour désigner un système d'authentification en ligne. Il s'agit d'un code à usage unique utilisé pour vérifier l'identité d'un utilisateur lorsqu'il accède à des services en ligne ou effectue des transactions.	https://en.wikipedia.org/wiki/I-PIN
IAM_TG_37	ITU-T X.1252	-	04/21	ITU-T X.1252 est une recommandation de l'Union internationale des télécommunications (UIT) qui définit les concepts et les principes fondamentaux de la gestion des informations d'identité numérique (Digital Identity Management) dans les environnements de télécommunication. Cette norme est utilisée pour faciliter l'identification et l'authentification des utilisateurs, ainsi que pour sécuriser les échanges d'informations numériques.	https://www.itu.int/rec/T-REC-X.1252-202104-I/en

IAM_TG_38	Authentication Step-Up Protocol and Metadata Version 1.0 OASIS Standard	Version 1.0	24 May 2017	Protocole de renforcement d'authentification vise à améliorer la sécurité de l'authentification numérique en ajoutant des mesures supplémentaires lorsque cela est nécessaire, tandis que la Version 1.0 des métadonnées établit des normes pour la gestion et l'échange de métadonnées, favorisant ainsi l'interopérabilité des systèmes et la qualité des informations.	https://www.oasis-open.org/standard/auth-step-v1-0/
IAM_TG_39	SS 529	2006	2006	This standard defines the data structure, security architecture and command set for a smart card with identification data. Some of the requirements are mandatory and some are optional. When optional parts are implemented, they shall comply with this standard.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/9a171587-b81c-49fa-8ad2-31da3e9b962d
IAM_TG_40	MINEX (MINutiae EXchange)	MINEX III	-	Cette norme définit un ensemble de méthodes de test pour évaluer les performances des systèmes de reconnaissance d'empreintes digitales.	https://www.nist.gov/itl/iad/image-group/ongoing-minex
IAM_TG_41	ISO/IEC 30107-3	2023	2023	Cette norme définit un ensemble de protocoles pour l'échange sécurisé de données biométriques, y compris des méthodes de cryptage et de signature des données biométriques.	https://www.iso.org/standard/79520.html
IAM_TG_42	ISO/IEC 30107-4	2020	2020	Cette norme définit un ensemble de protocoles pour le stockage sécurisé des données biométriques, y compris les méthodes de cryptage et de signature des données biométriques.	https://www.iso.org/standard/75301.html
IAM_TG_43	ISO/IEC 30107-2	2017	2017	Cette norme fournit des lignes directrices pour la gestion de la sécurité de l'information pour les systèmes liés à la biométrie, y compris des lignes directrices pour le contrôle d'accès, les pistes d'audit et la protection des données biométriques.	https://www.iso.org/standard/67380.html
IAM_TG_44	ISO/IEC 30107-4	2013	2013	Cette norme fournit des lignes directrices pour la création et la mise en œuvre de systèmes d'authentification électronique sécurisés, y compris des lignes directrices pour la création et la vérification d'identités numériques et des lignes	https://www.iso.org/standard/45138.html

				directrices pour la création et la vérification de signatures numériques.	
IAM_TG_45	ISO/IEC 30107-1	2016	2016	ISO/IEC 30107-1 est une norme internationale qui fait partie de la série ISO/IEC 30107 sur l'évaluation de la fiabilité de l'authentification biométrique. Plus précisément, la norme ISO/IEC 30107-1 traite des exigences relatives aux méthodes d'évaluation de la performance des systèmes biométriques.	https://www.iso.org/standard/53227.html
IAM_TG_46	RFC 4226	-	May 2011	L'algorithme HOTP est une méthode synchronisée dans le temps pour générer des mots de passe à usage unique (OTP). Il utilise une clé secrète partagée entre le serveur et le client, ainsi qu'une valeur de compteur, pour générer un OTP unique. L'algorithme utilise la fonction de chiffrement HMAC-SHA1 (Hash-based Message Authentication Code avec Secure Hash Algorithm 1) pour assurer l'intégrité et la sécurité du processus de génération de l'OTP.	https://datatracker.ietf.org/doc/html/rfc6238
IAM_TG_47	RFC 6238	-	May 2011	RFC 6238 établit les normes pour l'algorithme TOTP, qui permet de générer des mots de passe à usage unique basés sur l'horodatage et de les utiliser dans des systèmes d'authentification à deux facteurs basés sur le temps. Cet algorithme est couramment utilisé dans de nombreux systèmes et applications pour renforcer la sécurité des comptes utilisateur.	https://datatracker.ietf.org/doc/html/rfc6238
IAM_TG_48	ISO 19092	-	2023	Ce document spécifie le cadre de sécurité pour l'utilisation de la biométrie pour l'authentification des clients dans les services financiers, en se concentrant exclusivement sur les paiements de détail.	https://www.iso.org/standard/78308.html

IAM_TG_49	ISO/IEC TR 30125	-	2016	L'ISO/CEI TR 30125 fournit des lignes directrices pour le développement d'une méthode cohérente et sécurisée de personnalisation et d'authentification biométrique (seule ou non biométrique) dans un environnement mobile pour les systèmes achetés sur le marché libre.	https://www.iso.org/standard/53245.html
IAM_TG_50	IS/ISO/IEC 30136	-	2018	L'ISO/CEI 30136:2018 prend en charge l'évaluation de l'exactitude, de la confidentialité et de la confidentialité des schémas de protection des modèles biométriques.	https://www.iso.org/standard/53256.html
IAM_TG_51	ISO/IEC TR 29196	-	2018	Le document fournit des conseils sur la collecte et le stockage des données d'inscription biométriques et l'impact sur les processus dépendants de vérification et d'identification.	https://www.iso.org/standard/70951.html
IAM_TG_52	ISO/IEC 29109-1	-	2009	L'ISO/CEI 29109-1:2009 définit les concepts de test de conformité pour les formats d'échange de données biométriques et définit un cadre général de test de conformité.	https://www.iso.org/standard/45132.html
IAM_TG_53	ISO/IEC 29109-2	-	2010	L'ISO/CEI 29109-2:2010 spécifie les éléments de la méthodologie de test de conformité, les assertions de test et les procédures de test applicables à la norme de format d'échange de données biométriques relative aux données des détails des doigts (c'est-à-dire ISO/CEI 19794-2).	https://www.iso.org/fr/standard/50878.html
IAM_TG_54	ISO/IEC 29109-5	-	2019	Le présent document spécifie les éléments de la méthodologie de test de conformité, les assertions de test et les procédures de test applicables aux images faciales bidimensionnelles définies dans la norme de format d'échange de données biométriques ISO/IEC 19794-5:2005 pour les données d'images faciales.	https://www.iso.org/standard/73505.html
IAM_TG_55	ISO/IEC 29109-6	-	2011	Méthodologie d'essai de conformité pour les formats d'échange de données biométriques définis dans l'ISO/IEC 19794 — Partie 6: Données d'image de l'iris	https://www.iso.org/standard/50908.html

IAM_TG_56	ISO/IEC 19794-1	-	2011	L'ISO/CEI 19794-1:2011 décrit les aspects généraux et les exigences pour la définition des formats d'échange de données biométriques.	https://www.iso.org/standard/50862.html
IAM_TG_57	ISO/IEC 19794-2	-	2011	L'ISO/CEI 19794-2:2011 spécifie un concept et des formats de données pour la représentation des empreintes digitales en utilisant la notion fondamentale de minuties.	https://www.iso.org/standard/50864.html
IAM_TG_58	ISO/IEC 19794-3	-	2006	L'ISO/CEI 19794-3:2006, le format d'échange de données spectrales sur les modèles de doigts, spécifie les exigences pour la représentation des données spectrales locales ou globales dérivées d'une image d'empreinte digitale.	https://www.iso.org/standard/38747.html
IAM_TG_59	ISO/IEC 19794-4	-	2011	L'ISO/CEI 19794-4:2011 spécifie un format d'échange d'enregistrements de données pour le stockage, l'enregistrement et la transmission des informations d'une ou plusieurs zones d'image du doigt ou de la paume dans une structure de données ISO/CEI 19785-1	https://www.iso.org/standard/50866.html
IAM_TG_60	ISO/IEC 19794-5	-	2011	Biometric data interchange formats — Part 5: Face image data	https://www.iso.org/standard/50867.html
IAM_TG_61	ISO/IEC 19794-6	-	2011	L'ISO/CEI 19794-6:2011 spécifie les formats d'échange d'images d'iris pour les systèmes d'inscription, de vérification et d'identification biométriques.	https://www.iso.org/standard/50868.html
IAM_TG_62	ISO/IEC 19794-8	-	2011	L'ISO/CEI 19794-8:2011 décrit toutes les caractéristiques d'une empreinte digitale dans un petit enregistrement de données. Ainsi, il permet d'extraire à la fois des informations spectrales (orientation, fréquence, phase, etc.) et des caractéristiques (minuties, cœur, nombre de crêtes, etc.)	https://www.iso.org/standard/50869.html
IAM_TG_63	ISO/IEC 19794-9	-	2011	L'ISO/CEI 19794-9:2011 spécifie un format d'échange d'images pour les technologies biométriques d'identification ou de vérification de personnes qui utilisent des images biométriques vasculaires humaines et peuvent	https://www.iso.org/standard/56163.html

				être utilisées pour l'échange et la comparaison de données d'images vasculaires.	
IAM_TG_64	ISO/IEC 39794-1	-	2019	La norme ISO/IEC 39794-1 définit une structure de données et un format de fichier pour l'échange d'images d'empreintes digitales.	https://www.iso.org/standard/70788.html
IAM_TG_65	ISO/IEC 39794-2	-	-	La norme ISO/IEC 39794-2 définit une structure de données et un format de fichier pour l'échange des caractéristiques minutieuses des empreintes digitales.	https://www.iso.org/standard/72153.html
IAM_TG_66	ISO/IEC 19784-1	2018	2018	ISO/IEC 19784-1:2018 définit l'interface de programmation d'application (API) et l'interface de fournisseur de services (SPI) pour les interfaces standard au sein d'un système biométrique qui prennent en charge la fourniture de ce système biométrique à l'aide de composants de plusieurs fournisseurs. Elle assure l'interfonctionnement entre ces composants grâce au respect de la présente Norme internationale et d'autres Normes internationales.	https://www.iso.org/standard/70866.html
IAM_TG_67	ISO/IEC 19784-2	2007	2007	Information technology - Biometric application programming interface: Part 2 biometric archive function provider interface	https://www.iso.org/standard/43303.html
IAM_TG_68	ISO/IEC 19784-3	2020	2020	Technologies de l'information - Interface de programmation d'applications biométriques : partie 4 interface de fournisseur de fonction de capteur biométrique	https://www.iso.org/standard/72192.html
IAM_TG_69	ISO/IEC 19784-4	2011	2011	Technologies de l'information — Interface de programmation d'applications biométriques — Partie 4: Interface de fournisseur de fonction de capteur biométrique	https://www.iso.org/standard/50859.html

IAM_TG_70	ISO/IEC 19794-10	2007	2007	Technologies de l'information - Formats d'échange de données biométriques Partie 10 Géométrie des mains Données de silhouette	https://www.iso.org/standard/50859.html
IAM_TG_71	ISO/IEC 19794-11	2013	2013	Technologies de l'information - Formats d'échange de données biométriques Partie 11 Signature/Données dynamiques traitées par signature	https://www.iso.org/standard/51824.html
IAM_TG_72	ISO/IEC 19794-13	2018	2018	Technologies de l'information - Formats d'échange de données biométriques Partie 13 Données vocales	https://www.iso.org/standard/72276.html
IAM_TG_73	ISO/IEC 19794-14	2022	2022	Technologies de l'information - Formats d'échange de données biométriques : données d'ADN	https://www.iso.org/fr/standard/75402.html
IAM_TG_74	ISO/IEC 19794-15	2017	2017	Technologies de l'information - Format d'échange de données biométriques Partie 15 Données d'image du pli de la paume	https://www.iso.org/standard/63865.html
IAM_TG_75	ISO/IEC 19795-1	2021	2021	La norme ISO/IEC 19795-1, également connue sous le nom de "Information technology - Biometric performance testing and reporting - Part 1: Principles and framework", est une norme internationale qui fournit des lignes directrices pour les tests de performance et la présentation des résultats dans le domaine des technologies biométriques.	https://www.iso.org/standard/73515.html
IAM_TG_76	ISO/IEC 19795-2	2007	2007	TECHNOLOGIE DE L'INFORMATION TESTS ET RAPPORTS DE PERFORMANCE BIOMÉTRIQUE PARTIE 2 : MÉTHODES DE TEST POUR L'ÉVALUATION DES TECHNOLOGIES ET DES SCÉNARIOS	https://www.iso.org/standard/41448.html

IAM_TG_77	ISO/IEC 19795-3	2007	2007	TECHNOLOGIE DE L'INFORMATION TESTS DE PERFORMANCE BIOMÉTRIQUE ET RAPPORTS PARTIE 3 : TESTS SPÉCIFIQUES À LA MODALITÉ	https://www.iso.org/standard/41449.html
IAM_TG_78	ISO/IEC 19795-4	2008	2008	Information Technology - Biometric performance testing and reporting - part 4: Interoperability performance testing	https://www.iso.org/standard/46329.html
IAM_TG_79	ISO/IEC 19795-5	2011	2011	Technologies de l'information - Tests et rapports de performance biométrique - partie 5 : Scénario de contrôle d'accès et système de notation	https://www.iso.org/standard/51768.html
IAM_TG_80	ISO/IEC 19795-6	2012	2012	Technologies de l'information - Tests et rapports de performance biométrique - partie 6 : Méthodologies de test pour l'évaluation opérationnelle	https://www.iso.org/standard/50873.html
IAM_TG_81	ISO/IEC 19795-7	2011	2011	Information Technology - Biometric performance testing and reporting - part 7: Testing of on-card biometric comparison algorithms	https://www.iso.org/standard/53059.html
IAM_TG_82	ISO/IEC 19795-9	2019	2019	Technologies de l'information Tests et rapports de performance biométrique Partie 9 : Tests sur les appareils mobiles	https://www.iso.org/standard/78101.html
IAM_TG_83	ISO/IEC 29109-8	2011	2011	Technologies de l'information — Méthodologie d'essai de conformité pour les formats d'échange de données biométriques définis dans l'ISO/CEI 19794 — Partie 8: Données squelettiques sur les modèles de doigts	https://www.iso.org/standard/54279.html

IAM_TG_84	ISO/IEC 29109-9	2011	2011	L'ISO/CEI 19794-9:2007 spécifie un format d'échange d'enregistrements de données pour l'enregistrement, le stockage et la transmission d'une ou plusieurs images vasculaires de la main.	https://www.iso.org/standard/53321.html
IAM_TG_85	ISO/IEC 29109-10	2010	2010	Technologies de l'information — Méthodologie d'essai de conformité pour les formats d'échange de données biométriques définis dans l'ISO/IEC 19794 — Partie 10: Données de silhouette géométrique de la main	https://www.iso.org/standard/50909.html
IAM_TG_86	ISO/IEC 30107-1	2016	2016	La norme ISO/IEC 30107-1 fait partie de la série de normes ISO/IEC 30107, qui traite de la détection des attaques de présentation biométrique. Cette première partie spécifique, la norme ISO/IEC 30107-1, se concentre sur l'établissement d'un cadre général pour la détection des attaques de présentation dans les systèmes biométriques.	https://www.iso.org/standard/53227.html
IAM_TG_87	ISO/IEC 30107-2	2017	2017	La norme ISO/IEC 30107-2 fait partie de la série de normes ISO/IEC 30107, qui traite de la détection des attaques de présentation biométrique. Cette deuxième partie spécifique, la norme ISO/IEC 30107-2, se concentre sur les aspects liés aux tests et aux rapports pour la détection des attaques de présentation.	https://www.iso.org/fr/standard/67380.html
IAM_TG_88	ISO/IEC 30107-3	2023	2023	La norme ISO/IEC 30107-3 fait partie de la série de normes ISO/IEC 30107, qui traite de la détection des attaques de présentation biométrique. Cette troisième partie spécifique, la norme ISO/IEC 30107-3, se concentre sur les aspects liés aux tests et aux rapports spécifiques aux systèmes biométriques basés sur du matériel.	https://www.iso.org/standard/79520.html

IAM_TG_89	ISO/IEC 30107-4	2020	2020	Ce document est un profil qui fournit des exigences pour tester les mécanismes de détection d'attaque de présentation biométrique (PAD) sur les appareils mobiles avec reconnaissance biométrique locale.	https://www.iso.org/standard/75301.html
IAM_TG_90	ISO/IEC 39794-4	2019	2019	La norme ISO/IEC 39794-4:2019 fait partie de la série de normes ISO/IEC 39794, qui traite des cartes d'identification et des méthodes de test associées. Cette quatrième partie spécifique se concentre sur les cartes de proximité, qui sont des cartes dotées d'une technologie de communication sans contact pour l'échange de données avec des lecteurs compatibles.	https://www.iso.org/standard/72155.html
IAM_TG_91	ISO/IEC 29115	2013	2013	ISO/IEC 29115 est une norme internationale qui traite de la spécification et de la gestion des exigences de sécurité pour les produits et les systèmes d'information. Elle fournit des directives et des méthodes pour définir les exigences de sécurité à différents niveaux, de la conception initiale à la maintenance continue.	https://www.iso.org/standard/45138.html
IAM_TG_92	LDAP (Lightweight Directory Access Protocol)	-	-	LDAP (Lightweight Directory Access Protocol) est un protocole de communication utilisé pour accéder et gérer des services de répertoires. Il fournit un moyen standardisé d'interagir avec des services de répertoires qui stockent des informations hiérarchiques, telles que des annuaires d'utilisateurs, des coordonnées de contact, des informations d'authentification, etc.	https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
IAM_TG_93	UMA (User-Managed Access)	-	-	UMA (User-Managed Access) est une spécification qui permet aux utilisateurs de contrôler l'accès à leurs ressources en ligne par des services tiers. Elle vise à donner aux utilisateurs un contrôle plus granulaire sur leurs données personnelles et à faciliter le partage sélectif d'informations avec d'autres utilisateurs ou services.	https://fr.wikipedia.org/wiki/User-Managed_Access

IAM_TG_94	ISO 19989	-	-	ISO/IEC 19792 décrit ces aspects spécifiques à la biométrie et spécifie les principes à prendre en compte lors de l'évaluation de la sécurité des systèmes biométriques.	https://www.iso.org/standard/72402.html
IAM_TG_95	ISO 24760	2019	2019	Ce document définit les termes de la gestion d'identité et spécifie les concepts de base de l'identité et de la gestion d'identité et leurs relations.	https://www.iso.org/standard/77582.html
INFRA_TG_100	ITU-T G.653	-	2010	L'ITU-T G.653 est une norme technique émise par l'Union internationale des télécommunications (ITU) qui concerne les fibres optiques à dispersion décalée (DSF, Dispersion Shifted Fiber). Cette norme spécifie les caractéristiques et les performances des fibres optiques DSF utilisées dans les réseaux de communication à fibre optique.	https://www.itu.int/rec/T-REC-G.653-201007-I/en
INFRA_TG_101	G.652.D	-	2016	Cette norme spécifie les caractéristiques des fibres optiques à mode monomode non dispersif (SMF) utilisées dans les réseaux de communication à fibre optique.	https://www.itu.int/rec/T-REC-G.652-201611-I/fr
INFRA_TG_102	G.654.E	-	2020	Cette norme concerne les fibres optiques à dispersion décalée (DSF) pour les systèmes de télécommunications à très longue portée.	https://www.itu.int/rec/T-REC-G.654-202003-I/fr
INFRA_TG_103	G. 657.A2	-	2016	Cette norme définit les caractéristiques des fibres optiques à mode monomode pour les applications de raccordement d'abonnés.	https://www.itu.int/rec/T-REC-G.657-201611-I/en
INFRA_TG_104	G.657.B2	-	-	La norme ITU-T G.657.B2 fait référence à un type spécifique de fibre optique utilisé dans les réseaux de communication à fibre optique. Plus précisément, la G.657.B2 est une sous-catégorie de fibres optiques à mode monomode (SMF) qui est	http://wirerope.fr/bend-insensitive-optical-fiber-657b2/

				conçue pour faciliter le déploiement de réseaux de communication à fibre optique dans des environnements où l'espace est limité.	
INFRA_TG_1 05	ISO 13480	-	1997	Exigences relatives aux réseaux de tuyauteries industrielles	https://www.iso.org/fr/standard/22079.html
INFRA_TG_1 06	NF EN 12613	-	2021	Dispositifs avertisseurs à caractéristiques visuelles, en matière plastique, pour câbles et canalisations enterrés	https://www.boutique.afnor.org/fr-fr/norme/nf-en-12613/dispositifs-avertisseurs-a-caracteristiques-visuelles-en-matiere-plastique-/fa195965/238227
INFRA_TG_1 07	NF P 98050	-	-	Ouvrages souterrains d'hébergement de réseaux secs - partie 1 : chambres de tirage et de raccordements	https://www.boutique.afnor.org/fr-fr/norme/nf-p980501/ouvrages-souterrains-dhebergement-de-reseaux-secs-partie-1-chambres-de-tira/fa178768/58528
INFRA_TG_1 08	NF P 98051	-	2020	Chambres sans fond	https://www.boutique.afnor.org/fr-fr/norme/nf-p980501/ouvrages-souterrains-dhebergement-de-reseaux-secs-partie-1-chambres-de-tira/fa178768/58528
INFRA_TG_1 09	NF P 98311	-	2020	Fermeture des chambres de tirage	https://www.boutique.afnor.org/fr-fr/norme/nf-p98331/chaussees-et-dependances-tranchees-

					ouverture-remblayage-refection/fa193146/85652
INFRA_TG_1 10	EN –GJS–500–7	-	-	Matériau pour le tampon des chambres	http://www.steelnumber.com/en/steelcomposition_eu.php?name_id=1522
INFRA_TG_1 11	IEC 60794-1-2	-	2021	Câbles à fibres optiques - Spécification générique - Procédures fondamentales d'essais des câbles optiques	https://www.en-standard.eu/bs-ien-iec-60794-1-2-2021-optical-fibre-cables-generic-specification-basic-optical-cable-test-procedures-general-guidance/?msclkid=2a2d95f71a411d7e8082f16e8b2dfe71
INFRA_TG_1 12	NF EN 50289-4-17	-	2015	Méthodes d'essai pour évaluer la résistance aux UV des gaines des câbles électriques et des câbles à fibre optique	https://standards.globalspec.com/std/9968340/EN%2050289-4-17
INFRA_TG_1 13	IP 68	-	-	Indice de protection sur la pénétration de corps étranger et de l'eau	https://www.silamp.fr/pages/indice-de-protection-ip68
INFRA_TG_1 14	NFC 67.100	-	-	Poteaux en bois destinés à la construction des lignes aériennes électriques et de télécommunication	https://www.boutique.afnor.org/fr-fr/norme/nfc67100/poteaux-en-bois-specifications/fa017257/47249

INFRA_TG_15	NF C.67.200	-	-	Poteaux en béton armé destinés aux lignes électriques aériennes	Norme NF C67-200 (afnor.org)
INFRA_TG_16	NF C.67.250	-	1982	Poteaux en béton armé précontraint destinés aux lignes électriques aériennes	https://www.boutique.afnor.org/fr-fr/norme/nf-c67250/poteaux-en-beton-precontraint-specifications/fa016952/5124
INFRA_TG_17	UTE C15-400 F	-	2005	Installations électriques à basse tension - Guide pratique	https://www.boutique.afnor.org/fr-fr/norme/ute-c15400/installations-electriques-a-basse-tension-guide-pratique-raccordement-des-fa143321/25956
INFRA_TG_18	NF C 11201	-	1997	Réseaux de distribution publique d'énergie électrique des domaines de tension BT et HTA	https://www.boutique.afnor.org/fr-fr/norme/nf-c11201/reseaux-de-distribution-publique-denergie-electrique/fa042844/4065
INFRA_TG_19	NF EN 206-1	-	-	Béton - spécification, performances, production et conformité	http://www.ac-grenoble.fr/lycee/roger.deschaux/documents/Cours/Formulaires/Cisaillement/Etude%20de%20la%20norme_Beton_EN206-1.pdf
INFRA_TG_20	NF EN 61663-1	-	2000	Protection contre la foudre - Lignes de télécommunication - Partie 1 : installations à fibre optiques	https://standards.globalspec.com/std/841301/NF%20EN%2061663-1

INFRA_TG_1 21	NF EN 60794-3-10	-	2015	Câbles extérieurs – Spécification de famille pour les câbles optiques de télécommunications destinés à être installés dans des conduites, directement enterrés ou attachés en aérien	https://m.boutique.afnor.org/fr-fr/norme/nf-en-60794310/cables-a-fibres-optiques-partie-310-cables-exterieurs-specification-de-fami/fa059620/45312
INFRA_TG_1 22	NF EN 60794-3-11	-	2011	Câbles à fibre optique - 3-11 : Câbles extérieurs – Spécification de produit pour les câbles de télécommunications à fibres optiques unimodales, destinés à être installés dans des conduites, directement enterrés et en aériens ligaturés	https://m.boutique.afnor.org/fr-fr/norme/nf-en-60794311/cables-a-fibres-optiques-partie-311-cables-exterieurs-specification-de-prod/fa174081/38148
INFRA_TG_1 23	NF EN 60794-3-20	-	2017	Câbles extérieurs – Spécification de famille pour les câbles optiques de télécommunications aériens autoporteurs	https://www.boutique.afnor.org/fr-fr/norme/nf-en-60794320/cables-a-fibres-optiques-partie-320-cables-exterieurs-specification-de-fami/fa186723/58578
INFRA_TG_1 24	NF EN 60794-3-21	-	2018	Câbles extérieurs – Spécification particulière pour les câbles optiques de télécommunications aériens autoporteurs utilisés dans le câblage de locaux	https://m.boutique.afnor.org/fr-fr/norme/nf-en-60794321/cables-a-fibres-optiques-partie-321-cables-exterieurs-specification-de-prod/fa174130/80579
INFRA_TG_1 25	XP C 93-850-3-25	-	2022	Câbles à fibres optiques - 3-25 : Spécification particulière - Câbles de distribution à usage extérieur, en aérien ou en souterrain	https://standardstore.afnor.org/en-gb/standard/xp-c93850325/optical-fibre-cables-part-325-detail-specification-

					outdoor-distribution-cab/fa202267/32388073
INFRA_TG_1 26	XP C 93-850-6-25	-	2022	Câbles à fibres optiques – 6-25 : Spécification particulière – Câble de distribution à usage mixte (intérieur et extérieur)	https://www.boutique.afnor.org/fr-fr/norme/xp-c93850625/cables-a-fibres-optiques-partie-625-specification-particuliere-cables-de-di/fa198273/323880
INFRA_TG_1 27	NF EN 60794-4-20	-	2019	Optical fibre câbles – Part 4-20 : Câble optiques aériens sur ligne électrique – Spécifications de famille pour les câbles entièrement diélectriques et autoporteurs	https://www.boutique.afnor.org/fr-fr/norme/nf-en-iec-60794420/cables-a-fibres-optiques-partie-420-specification-intermediaire-cables-opti/fa192172/82191
INFRA_TG_1 28	XP C 93-850-3-22	-	2022	Câbles à fibres optiques – 3-22 : Spécification particulière – Câble optique de branchement à usage extérieur, aérien, façade ou conduite	https://www.normadoc.com/english/xpc93-850-3-22-04-2022.html
INFRA_TG_1 29	XP C 93-850-6-22	-	2020	Câbles à fibres optiques – 6-22 : Spécification particulière – Câble de branchement à usage mixte (intérieur et extérieur)	https://standards.globalspec.com/std/14257539/XP%20C93-850-6-22
INFRA_TG_1 30	NF EN 615376.2.1	-	2013	Exigences et essais pour les systèmes de chemin de câbles et les systèmes d'échelle à câbles prévus pour le support, le logement des câbles et éventuellement d'autres équipements électriques dans des installations électriques et/ou des systèmes de communication	https://www.boutique.afnor.org/fr-fr/norme/nf-en-6132621/materiel-electrique-de-mesure-de-commande-et-de-laboratoire-

					exigences-relat/fa172505/412 15
INFRA_TG_1 31	NF EN 61386-22	-	2004	Systèmes de conduits pour la gestion du câblage - Partie 22 : règles particulières - Systèmes de conduits cintrable	https://www.boutique.afnor.org/fr-fr/norme/nf-en-6138622/systemes-de-conduits-pour-la-gestion-du-cablage-partie-22-regles-particulie/fa124720/23363
INFRA_TG_1 32	NF EN 50085-2-1	-	2008	Systèmes de goulottes et systèmes de conduits-profilés pour installations électriques - Partie 2-1 : systèmes de goulottes et systèmes de conduits-profilés prévus pour être montés sur les murs et les plafonds	https://www.boutique.afnor.org/fr-fr/norme/nf-en-5008521/systemes-de-goulottes-et-systemes-de-conduitsprofiles-pour-installations-el/fa046519/29687
INFRA_TG_1 33	NF C 15-100	-	2015	Installations des réseaux de communication dans les bâtiments d'habitation	https://particuliers.promotelec.com/fiche-projet/nf-c-15-100-la-norme-de-reférence-pour-l'installation-electrique
INFRA_TG_1 34	NF C 32070 2.1	-	2004	Conducteurs et câbles isolés pour installations - Essais de classification des conducteurs et câbles du point de vue de leur comportement au feu	https://www.boutique.afnor.org/en-gb/standard/nf-c32070/insulated-cables-and-flexible-cords-for-installations-classification-tests-/fa111433/456#AreasStoreProductsSummaryView

INFRA_TG_1 35	NF EN 13501-6	-	2018	Classement au feu des produits et éléments de construction - Partie 6 : classement à partir des données d'essais de réaction au feu sur câbles de puissance, de commande et de communication	https://www.boutique.afnor.org/fr-fr/norme/nf-en-135016/classement-au-feu-des-produits-et-elements-de-construction-partie-6-classem/fa187540/82748
INFRA_TG_1 36	IEEE 802.8	-	-	Cette norme concerne les protocoles de réseau local à fibre optique.	https://fr.wikipedia.org/wiki/IEEE_802

5. Development Standards

Les normes de développement (Development Standards) sont des directives et des pratiques établies pour garantir la qualité, la cohérence et l'efficacité du processus de développement logiciel. Elles visent à améliorer la gestion de projet, la collaboration entre les équipes de développement, la reproductibilité des résultats et la qualité du code.

Voici une liste de normes Development :

ID	Standard/Norme	Version	Date de publication	Description	Url Documentation
Dev_TG_01	TR 67:2018	2018	2018	Fournit un cadre aux établissements de santé et aux professionnels pour atténuer les risques de sécurité des dispositifs médicaux connectés	https://www.singaporesstandardseshop.sg/Product/SSPDetail/386a8bb0-fda6-4b55-ba8b-614847b1566d

Dev_TG_02	Section 508	-	January 18, 2017	Il s'agit d'une loi fédérale américaine qui exige que les agences fédérales rendent leur technologie électronique et leurs informations accessibles aux personnes handicapées. Elle fixe des normes d'accessibilité pour les logiciels, les sites web et autres produits informatiques.	https://www.section508.gov/
Dev_TG_03	HTML	HTML 5	19 May 2023	HTML, qui signifie HyperText Markup Language (langage de balisage hypertexte), est le langage de base utilisé pour la création et la structuration du contenu sur le Web. Il définit la structure et la présentation des pages Web en utilisant des balises et des éléments.	https://en.wikipedia.org/wiki/HTML
Dev_TG_04	CSS	CSS4	2010	CSS, qui signifie Cascading Style Sheets (feuilles de style en cascade), est un langage de style utilisé pour définir la présentation et l'apparence des pages HTML. Il complète le HTML en permettant de contrôler le style, la mise en page et la mise en forme des éléments HTML d'une page Web.	https://www.w3.org/Style/CSS/Overview.en.html
Dev_TG_05	JavaScript	13 - ECMA-262	Juin 2022	JavaScript est un langage de programmation de haut niveau principalement utilisé pour ajouter de l'interactivité et du dynamisme aux pages Web. Il permet d'effectuer des manipulations du contenu HTML, de répondre aux actions de l'utilisateur, de communiquer avec des serveurs, de créer des animations...	https://developer.mozilla.org/en-US/docs/Web/javascript
Dev_TG_06	MWBP(Mobile Web Best Practices)	Version 1.0	29 July 2008	Un ensemble de bonnes pratiques pour garantir que le contenu Web est correctement optimisé pour les appareils mobiles	https://www.w3.org/TR/mobile-bp/
Dev_TG_07	MWABP(Mobile Web Application Best Practices)	-	14 December 2010	A set of best practices for developing mobile web applications that provide a high-quality user experience	https://www.w3.org/TR/mwabp/

Dev_TG_08	MW 2.0(Mobile Web 2.0)	Version 2.0	-	A set of best practices for developing web applications that are optimized for mobile devices and take advantage of the capabilities of those devices	https://fr.wikipedia.org/wiki/Web_2.0
Dev_TG_09	The developer's guide to the Human Interface Guidelines	-	June 19, 2020	Le Guide du développeur sur les directives relatives à l'interface humaine est une ressource complète qui fournit aux développeurs une compréhension approfondie des principes et des meilleures pratiques de conception d'interfaces utilisateur.	https://developer.apple.com/news/?id=yyz8lgtw
Dev_TG_10	Android MDG(Android Material Design Guidelines)	Material Design 3	-	Ces directives fournissent des recommandations et des bonnes pratiques pour concevoir des applications Android visuellement attrayantes, intuitives et conviviales.	https://developer.android.com/develop/ui/views/themes/look-and-feel
Dev_TG_11	MDM(Mobile Device Management)	-	2000	Un ensemble d'outils et de technologies pour gérer et sécuriser les appareils mobiles utilisés dans l'espace de travail	https://www.fortinet.com/resources/cyber glossary/mobile-device-management
Dev_TG_12	BYOD(Bring Your Own Device)	-	-	Une politique qui permet aux employés d'utiliser leurs appareils mobiles personnels à des fins professionnelles, tout en s'assurant que les appareils sont sécurisés et conformes aux politiques de l'entreprise	https://csrc.nist.gov/publications/detail/sp/1800-22/draft
Dev_TG_13	WCAG(Web Content Accessibility Guidelines)	WCAG 2.2	17 May 2023	Un ensemble de lignes directrices publiées par le World Wide Web Consortium (W3C) pour garantir que le contenu Web est accessible aux personnes handicapées.	https://www.w3.org/WAI/standards-guidelines/wcag/
Dev_TG_14	RWD(Responsive Web Design)	-	-	Une approche de la conception Web qui garantit que les pages Web sont facilement accessibles et utilisables sur une multitude d'appareils, y compris les ordinateurs de bureau, les tablettes et les smartphones.	https://developer.mozilla.org/en-US/docs/Learn/CSS/CSS_layout/R

					esponsive Design
Dev_TG_15	SSL/TLS(Secure Socket Layer / Transport Layer Security)	TLS v1.3	2018	Cryptographic protocols used to establish a secure communication channel between two systems over the internet. They ensure the confidentiality, integrity and authenticity of data transmitted between a client and a server. They are commonly used to secure web communications (HTTPS), email transmissions, instant messaging and other types of online transactions that require a high level of security	https://tswg.org/
Dev_TG_16	WSI(Web Services Interoperability)	-	-	Un ensemble de normes qui garantissent l'interopérabilité entre les services Web de différents fournisseurs	http://www.oasis-wsi.org/
Dev_TG_17	SGDS(Singapore Government Design System)	-	-	A set of design guidelines, standards and code that help government agencies create cohesive, user-centric digital services. SGDS provides a common design language, layout and visual elements to ensure consistency and accessibility across different government digital platforms. It also includes components, templates and design patterns that help designers and developers build and deliver digital services more efficiently. SGDS is open source.	https://www.developer.tech.gov.sg/products/categories/design/singapore-government-design-system/overview.html
Dev_TG_18	React	Version 18.2.0	14 juin 2022	Une bibliothèque JavaScript open-source développée par Facebook. Elle est utilisée pour construire des interfaces utilisateur interactives et réactives pour les applications Web.	https://react.dev/
Dev_TG_19	Government Design System (GDS)	v4.6.0	20 April 2023	Le Government Design System (GDS) est un système de conception gouvernemental utilisé au Royaume-Uni. Il s'agit d'un ensemble de principes, de lignes directrices	https://gds.blog.gov.uk/2018/06/22/introducing-the-gov-

				et de ressources de conception qui permettent aux organismes gouvernementaux de créer des services numériques cohérents et de haute qualité.	uk-design-system/
Dev_TG_20	EU Accessibility Act	-	April 2019	La "EU Accessibility Act" est une législation adoptée par l'Union européenne pour promouvoir l'accessibilité des produits et services aux personnes handicapées. L'objectif de cette loi est de garantir que les personnes handicapées puissent participer pleinement à la société en ayant accès à des produits, des services et des technologies numériques sans obstacles.	https://en.wikipedia.org/wiki/European_Accessibility_Act
Dev_TG_21	Korean National Web Accessibility Guidelines	-	30 June 2017	Les "Korean National Web Accessibility Guidelines" (Directives nationales coréennes en matière d'accessibilité Web) sont un ensemble de recommandations et de normes élaborées par le gouvernement coréen pour promouvoir l'accessibilité des sites Web aux personnes handicapées en Corée du Sud.	https://www.w3.org/WAI/policies/republic-of-korea/
Dev_TG_22	eGA Mobile, Estonian Public Sector Web Accessibility Guidelines	-	June 2021	Ces directives ont pour objectif de garantir que les sites Web du secteur public estonien sont conçus et développés de manière à être accessibles à tous les utilisateurs, y compris ceux ayant des limitations fonctionnelles, telles que les déficiences visuelles, auditives, motrices ou cognitives. Elles sont alignées sur les principes et les normes internationales d'accessibilité Web, tels que les Web Content Accessibility Guidelines (WCAG) du Web Accessibility Initiative (WAI).	https://digital-strategy.ec.europa.eu/en/policies/web-accessibility-directive-standards-and-harmonisation
Dev_TG_23	Apache Spark	Version 3.4.0	7 avril 2023	Système de traitement de données distribué open-source qui permet de traiter de grands ensembles de données de manière rapide et efficace.	https://spark.apache.org/

Dev_TG_24	Git	Version 2.40.1	25 avril 2023	Conçu pour gérer efficacement les modifications de code source dans un environnement de développement collaboratif	https://git-scm.com/
Dev_TG_25	Python	Python 3.9	5 octobre 2020	Utilisé pour le développement d'une variété d'applications, telles que des applications web, des applications de bureau, des scripts, des jeux, des outils d'analyse de données, et bien plus encore.	https://docs.python.org/3/
Dev_TG_26	Java	Java 17	14 septembre 2021	Utilisé pour développer des applications de bureau, des applications web, des applications mobiles, des jeux et bien plus encore	https://fr.wikipedia.org/wiki/Java_(langage)
Dev_TG_27	C++	C++20	décembre 2020	Langage de programmation orienté objet, qui est utilisé pour développer des applications à haute performance, telles que des systèmes d'exploitation, des jeux vidéo, des logiciels de CAO, et bien plus encore.	https://fr.wikipedia.org/wiki/C%2B%2B
Dev_TG_28	PHP	PHP 8.0	26 novembre 2020	Utilisé pour générer des pages web dynamiques et interactives, en utilisant des bases de données pour stocker et récupérer des informations.	https://www.php.net/
Dev_TG_29	Swift	Swift 5.5	septembre 2021	Utilisé pour le développement d'applications iOS, macOS, watchOS et tvOS, ainsi que pour le développement d'applications pour Linux.	https://www.lafinancepourtous.com/outils/questions-reponses/question-ce-que-swift/
Dev_TG_30	SQL	SQL:2016	2016	langage de programmation utilisé pour gérer et manipuler des données dans une base de données relationnelle	https://fr.wikipedia.org/wiki/Structured_Query_Language

Dev_TG_31	Eclipse	Version 4.27.0	4.27.0	Permet aux développeurs de travailler sur des projets logiciels en utilisant une variété de langages de programmation.	https://eclipside.org/
Dev_TG_32	Rust	version1.69.0	20 avril 2023	Langage de programmation open-source créé par Mozilla qui se concentre sur la sécurité, la performance et la concurrence.	https://www.rust-lang.org/
Dev_TG_33	C#	Version 11	8 novembre 2022	Utilisé pour le développement d'applications Windows, mais peut également être utilisé pour le développement d'applications Web, de jeux, de logiciels embarqués et d'autres types d'applications.	https://de.wikipedia.org/wiki/C-Sharp
Dev_TG_34	Angular	Version 16.0.0	3 mai 2023	Angular est un framework open-source de développement d'applications web	https://angular.io/
Dev_TG_35	Node.js	Version 20.2.0	16 mai 2023	Il permet aux développeurs d'écrire des applications côté serveur en utilisant JavaScript	https://nodejs.org/en
Dev_TG_37	SS 618	2016	2016	Lignes directrices sur la conception de l'interface utilisateur pour les personnes âgées	https://www.singaporestandardseshop.sg/Product/SSProductDetail/28b094be-a282-4c85-bdab-95d0afa6c4d8
Dev_TG_38	Scrum	-	-	Scrum est un cadre de gestion de projet agile largement utilisé dans le développement logiciel et d'autres domaines. Il se concentre sur la collaboration, la flexibilité et la livraison continue de valeur. Scrum permet aux équipes de travailler de manière itérative et itérative, en se concentrant	https://www.scrum.org/

				sur la livraison de produits fonctionnels à intervalles courts, appelés "itérations" ou "sprints".	
Dev_TG_39	Agile	-	-	Une méthode agile est une approche de gestion de projet qui se caractérise par sa flexibilité, sa collaboration et son orientation vers la livraison de valeur incrémentielle. Les méthodes agiles mettent l'accent sur la réactivité aux changements, la collaboration étroite entre les membres de l'équipe et la satisfaction du client.	https://fr.wikipedia.org/wiki/M%C3%A9thode_agile
Dev_TG_40	Singleton	-	-	Le pattern Singleton est un concept de conception logicielle qui vise à restreindre la création d'une classe à une seule instance. Il garantit qu'il n'y a qu'une seule instance de la classe et fournit un point d'accès global à cette instance.	https://en.wikipedia.org/wiki/Singleton_pattern
Dev_TG_41	Builder	-	-	Le pattern Builder est un pattern de conception logicielle qui est utilisé pour créer des objets complexes étape par étape. Il permet de séparer la construction d'un objet complexe de sa représentation afin que le même processus de construction puisse être utilisé pour créer différentes représentations.	https://en.wikipedia.org/wiki/Builder_pattern
Dev_TG_42	Prototype	-	-	Le pattern Prototype est un pattern de conception qui permet de créer de nouveaux objets en utilisant des objets existants comme modèles. Il permet de cloner et de créer de nouvelles instances d'objets à partir d'un prototype initial, évitant ainsi la nécessité de créer de nouvelles instances à partir de zéro.	https://en.wikipedia.org/wiki/Prototype_pattern
Dev_TG_43	Abstract Factory	-	-	Le pattern Abstract Factory est un pattern de conception qui fournit une interface pour créer des familles d'objets liés ou dépendants sans spécifier leurs classes concrètes. Il permet de créer des objets liés tout en isolant le code client de	https://fr.wikipedia.org/wiki/Fabrique_abstraite

				la connaissance des classes concrètes utilisées pour créer ces objets.	
Dev_TG_44	Facade	-	-	Le pattern Facade est un pattern de conception qui fournit une interface unifiée simplifiée pour un ensemble complexe de classes ou de systèmes. Il agit comme une couche d'abstraction supplémentaire en regroupant les fonctionnalités complexes et en exposant une interface simple et conviviale pour les clients.	https://fr.wikipedia.org/wiki/Fa%C3%A7ade_(patron_de_conception)
Dev_TG_45	Docker	-	-	Docker est une plateforme open-source qui permet de créer, déployer et exécuter des applications dans des conteneurs logiciels. Les conteneurs Docker offrent une méthode légère et portable pour encapsuler une application, ses dépendances et son environnement d'exécution, ce qui permet de les exécuter de manière cohérente sur différentes machines et environnements.	https://fr.wikipedia.org/wiki/Docker_(logiciel)
Dev_TG_46	CI&CD	-	-	CI/CD (Continuous Integration and Continuous Deployment/Delivery) est une approche de développement logiciel qui vise à automatiser et à améliorer la qualité du processus de livraison des logiciels. Il s'agit d'une pratique largement utilisée dans les méthodologies Agile et DevOps.	https://fr.wikipedia.org/wiki/CI/CD
Dev_TG_47	ECMAScript	-	-	ECMAScript (European Computer Manufacturers Association Script) est une spécification de langage de programmation qui définit les fonctionnalités et le comportement du langage de script JavaScript. Il s'agit d'un standard reconnu au niveau international et largement utilisé pour le développement d'applications Web et d'autres environnements d'exécution de	https://en.wikipedia.org/wiki/ECMAScript

				scripts.	
Dev_TG_48	WHATWG	-	-	WHATWG est la spécification HTML Living Standard, qui définit les normes actuelles du langage HTML et de ses fonctionnalités associées. Cette spécification est en constante évolution et est adoptée par de nombreux navigateurs web modernes.	https://fr.wikipedia.org/wiki/Web_Hypertext_Application_Technology_Working_Group
IAM_TG_94	SEO (Search Engine Optimization)	-	-	SEO (Search Engine Optimization) est une pratique qui vise à améliorer la visibilité et le classement d'un site web dans les résultats des moteurs de recherche tels que Google, Bing ou Yahoo. Le SEO consiste en un ensemble de techniques et de stratégies qui permettent d'optimiser les différents aspects d'un site web, tant sur le plan technique que sur le plan du contenu, afin de le rendre plus attractif et plus pertinent pour les moteurs de recherche.	https://fr.wikipedia.org/wiki/Optimisation_pour_les_moteurs_de_recherche

6. Artificial Intelligence Standards

Les normes de l'intelligence artificielle (Artificial Intelligence Standards) sont des directives et des pratiques établies pour promouvoir le développement et l'utilisation responsables, éthiques, sûrs et fiables de l'intelligence artificielle (IA). Ces normes visent à définir des principes et des lignes directrices pour guider la conception, l'implémentation et le déploiement de systèmes d'IA.

Voici une liste de normes IA :

ID	Standard/Norme	Version	Date de publication	Description	Url Documentation
IA_TG_01	ISO/IEC 23894	2023	2023	Norme pour l'évaluation des systèmes d'IA	https://www.iso.org/standard/77304.html
IA_TG_02	ISO/IEC 23053	2022	2022	Lignes directrices pour l'utilisation responsable de l'IA	https://www.iso.org/standard/74438.html
IA_TG_03	ISO/IEC 38507	2022	2022	Lignes directrices pour la gouvernance de l'IA	https://www.iso.org/standard/56641.html
IA_TG_04	ISO/IEC 22989	2022	2022-07	Cadre de compétences pour les professionnels de l'IA	https://www.iso.org/standard/74296.html
IA_TG_05	BS ISO/IEC 42001	2023	2023-02-01	Gestion de l'IA - Systèmes de gestion de l'IA	https://www.iso.org/standard/81230.html
IA_TG_06	AI Ethics Guidelines	-	2019	Lignes directrices éthiques pour l'utilisation de l'IA	https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

IA_TG_07	Singapore Model AI Governance Framework	-	25 May 2022	Cadre de gouvernance de l'IA de Singapour	https://www.pcp.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework
IA_TG_08	Australia AI Ethics Framework	-	7 November 2019	Cadre éthique de l'IA en Australie	https://www.industry.gov.au/publications/australia-artificial-intelligence-ethics-framework
IA_TG_09	UK AI Ethics Guidelines	-	10 June 2019	Lignes directrices éthiques pour l'IA au Royaume-Uni	https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety
IA_TG_10	IEEE P7000	-	2021-09-15	IEEE P7000 est une série de normes en développement par l'Institut des ingénieurs électroniciens et électriques (IEEE) qui traite de l'éthique des systèmes autonomes et intelligents. Cette série de normes vise à fournir des lignes directrices pour la conception, le développement et l'utilisation responsable des systèmes autonomes et intelligents dans divers domaines tels que l'intelligence artificielle, la robotique, les véhicules autonomes, etc.	https://standards.ieee.org/ieee/7000/6781/
IA_TG_11	TR 99	2021	2021	Ce TR sert de guide sur le premier cycle de vie d'un système d'IA, à savoir la phase de conception, pour la gestion des organismes.	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/53b4562-ef85-4ebb-bfeb-2b35beb1d29c
IA_TG_12	ISO/IEC TR 24030	2021	2021	This document provides a collection of representative use cases of AI applications in a variety of domains.	https://www.iso.org/standard/77610.html

IA_TG_13	ISO/IEC TR 24028	2020	2020	Ce document passe en revue les sujets liés à la fiabilité des systèmes d'IA	https://www.iso.org/standard/77608.html
IA_TG_14	ISO/IEC JTC 1/SC 42	2017	2017	JTC 1/SC 42 se concentre sur la normalisation des technologies de l'IA et des domaines connexes, tels que l'apprentissage automatique, les systèmes cognitifs, l'analyse de données, la robotique, l'interopérabilité et l'éthique de l'IA. Son objectif est de développer des normes internationales qui facilitent l'adoption, l'interopérabilité et la confiance dans les systèmes d'IA.	https://www.iso.org/committee/6794475.html
IA_TG_15	A guide to using AI in the public sector	-	10 June 2019	Le guide d'utilisation de l'IA dans le secteur public est un guide sur la façon de choisir, de construire et d'utiliser l'IA dans le secteur public pour s'assurer que le gouvernement maximise les avantages de cette technologie.	https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector
IA_TG_16	AI procurement guidelines	-	8 June 2020	The AI procurement guidelines are a guide that addresses the ethical uncertainty around AI procurement so that officials feel equipped to use innovative technology whilst being able to mitigate risks.	https://www.gov.uk/government/publications/guidelines-for-ai-procurement
IA_TG_17	TensorFlow	Version 2.12.0	23 mars 2023	TensorFlow est un framework open-source de machine learning	https://www.tensorflow.org/?hl=fr
IA_TG_18	Python	Python 3.9	5 octobre 2020	Utilisé pour le développement d'une variété d'applications, telles que des applications web, des applications de bureau, des scripts, des jeux, des outils d'analyse de données, et bien plus encore.	https://docs.python.org/3/
IA_TG_19	PyTorch	Version 2.0.0	15 mars 2023	PyTorch est un framework open-source de deep learning en Python,	https://pytorch.org/

IA_TG_20	Keras	Version 2.12.0	21 mars 2023	Une bibliothèque open-source de deep learning en Python	https://keras.io/
IA_TG_21	Scikit-learn	Version 1.2.2	9 mars 2023	Une bibliothèque open-source de machine learning en Python	https://fr.wikipedia.org/wiki/Scikit-learn
IA_TG_22	OpenCV	Version 4.7.0	29 décembre 2022	Une bibliothèque open-source de traitement d'images et de vision par ordinateur	https://opencv.org/
IA_TG_23	ISO/IEC AWI 27091	-	2023	Ce document fournit des conseils aux organisations pour faire face aux risques de confidentialité dans les systèmes d'intelligence artificielle (IA) et les modèles d'apprentissage automatique (ML).	https://www.iso.org/standard/56582.html
IA_TG_24	ISO/IEC AWI 27090	-	2022	Ce document fournit des conseils aux organisations pour faire face aux menaces de sécurité et aux défaillances des systèmes d'intelligence artificielle (IA).	https://www.iso.org/standard/56581.html
IA_TG_25	ISO/IEC DIS 5339	-	2023	Information technology — Artificial intelligence — Guidance for AI applications	https://www.iso.org/standard/81120.html
IA_TG_26	OWASP AI Security and Privacy Guide	-	15 February 2023	L'OWASP AI Security and Privacy Guide est un guide spécifique élaboré par l'OWASP pour aborder les enjeux de sécurité et de confidentialité liés à l'intelligence artificielle (IA). Ce guide vise à sensibiliser aux risques de sécurité et de confidentialité spécifiques aux systèmes basés sur l'IA, ainsi qu'à fournir des recommandations et des bonnes pratiques pour les atténuer.	https://owasp.org/www-project-ai-security-and-privacy-guide/

IA_TG_27	ETSI GR SAI 013	V1.1.1	2023	Sécurisation de l'Intelligence Artificielle (SAI) ; Cadre de preuves de concepts	https://cdn.standards.iteh.ai/samples/67260/7cc22a1d990547b6948e58a369093caf/ETSI-GR-SAI-013-V1-1-2023-03-.pdf
IA_TG_28	ETSI GR SAI 009	V1.1.1	2023	Le présent document décrit un cadre de sécurité d'une plate-forme informatique d'IA contenant du matériel et des logiciel pour protéger les actifs précieux tels que les modèles et les données déployés sur la plate-forme informatique d'IA	https://cdn.standards.iteh.ai/samples/63910/688602cb2fe6414889f9c842ed2117b5/ETSI-GR-SAI-009-V1-1-2023-02-.pdf
IA_TG_29	ETSI GR SAI 007	V1.1.1	2023	Le présent document identifie les étapes à suivre par les concepteurs et les implémentateurs de plateformes d'IA qui donnent l'assurance de l'explicabilité et la transparence du traitement de l'IA. Le traitement de l'IA comprend la prise de décision par l'IA et le traitement des données par l'IA.	https://www.etsi.org/deliver/etsi_gr/SAI/001_09/007/01.01.01_60/gr_SAI007v010101p.pdf
IA_TG_30	ETSI GR SAI 006	V1.1.1	2022	Le présent document identifie le rôle du matériel, à la fois spécialisé et généraliste, dans la sécurité de l'IA.	https://www.etsi.org/deliver/etsi_gr/SAI/001_09/006/01.01.01_60/gr_SAI006v010101p.pdf
IA_TG_31	ETSI GR SAI 005	V1.1.1	2021	The present document summarizes and analyses existing and potential mitigation against threats for AI-based systems as discussed in ETSI GR SAI 004	https://cdn.standards.iteh.ai/samples/59214/f9dc24e257f4466b18af69f37e4c2f1/ETSI-GR-SAI-005-V1-1-2021-03-.pdf
IA_TG_32	ETSI GR SAI 004	V1.1.1	2020	Le présent document décrit le problème de la sécurisation des systèmes et des solutions basés sur l'IA, en mettant l'accent sur la machine l'apprentissage, et les enjeux liés à la confidentialité, l'intégrité et la disponibilité à chaque étape de	https://cdn.standards.iteh.ai/samples/59209/d828e1afe6d34fc8842992c329195f5e/ETSI-GR-SAI-004-V1-1-2020-03-.pdf

				l'apprentissage automatique cycle de vie.	004-V1-1-1-2020-12-.pdf
IA_TG_33	ETSI GR SAI 002	V1.1.1	2021	Le présent document résume les méthodes actuellement utilisées pour obtenir des données pour la formation à l'IA, ainsi qu'un examen des initiatives existantes pour développer des protocoles de partage de données. Il fournit ensuite une analyse des lacunes sur ces méthodes et des initiatives visant à définir les exigences éventuelles en matière de normes garantissant l'intégrité et la confidentialité des données partagées, informations et commentaires	https://cdn.standards.iteh.ai/samples/58857/f9523b0864004e0092947e76227573ea/ETSI-GR-SAI-002-V1-1-1-2021-08-.pdf
IA_TG_34	ETSI GR SAI 001	V1.1.1	2022	Le présent document définit ce qu'est une menace d'intelligence artificielle (IA) et définit comment elle peut être distinguée de toute menace non liée à l'IA	https://www.etsi.org/deliver/etsi_gr/SAI/001_09/001/01.01.01_60/gr_SAI001v010101p.pdf
IA_TG_35	IS/ISO/IEC 24668	-	2022	Intelligence artificielle — Cadre de gestion des processus pour l'analyse de mégadonnées	https://www.iso.org/standard/78368.html
IA_TG_36	IS/ISO/IEC/TR 24372	-	2021	Ce document donne un aperçu de l'état de l'art des approches informatiques pour les systèmes d'IA, en décrivant : a) les principales caractéristiques informatiques des systèmes d'IA ; b) les principaux algorithmes et approches utilisés dans les systèmes d'IA, faisant référence aux cas d'utilisation contenus dans l'ISO/CEI TR 24030.	https://www.iso.org/standard/78508.html

IA_TG_37	ISO/IEC TR 24029-1	-	2021	Ce document fournit des informations sur les méthodes existantes pour évaluer la robustesse des réseaux de neurones.	https://www.iso.org/standard/77609.html
IA_TG_38	ISO/IEC TR 20547-1	-	2020	Ce document décrit le cadre de l'architecture de référence Big Data et le processus permettant à un utilisateur du document de l'appliquer à son domaine de problème particulier.	https://www.iso.org/standard/71275.html
IA_TG_39	EVS-ISO/IEC 2382-29:2001	-	2001	La présente partie de l'ISO/CEI 2382 est destinée à faciliter la communication internationale dans le domaine des technologies de l'information. Il présente les termes et les définitions de concepts sélectionnés pertinents pour le domaine des technologies de l'information en deux langues et définit les relations entre les articles. Pour faciliter la traduction dans d'autres langues, les définitions sont conçues pour exclure autant que possible les caractéristiques spécifiques à la langue. Cette section définit les concepts d'IA liés à la reconnaissance vocale et à la synthèse vocale.	https://www.evs.ee/en/evs-iso-iec-2382-29-2001
IA_TG_40	EVS-ISO/IEC 2382-34:2001	-	2001	Cette section définit les concepts d'IA liés aux réseaux de neurones, leurs composants, leurs connexions et leurs fonctions.	https://www.evs.ee/en/evs-iso-iec-2382-34-2001

7. User and accessibility Standards

Les normes relatives aux utilisateurs et à l'accessibilité sont des lignes directrices et des principes visant à garantir que les produits, services et environnements numériques sont utilisables et accessibles à un large éventail d'individus, y compris les personnes handicapées. Ces normes aident les concepteurs, développeurs et organisations à créer des expériences inclusives et conviviales qui répondent aux besoins divers des utilisateurs.

Voici une liste de normes d'accessibilité :

ID	Standard/Norme	Version	Date de publication	Description	Url Documentation
ACC_TG_01	Web Content Accessibility Guidelines (WCAG)	WCAG 2.2	17 May 2023	Les Web Content Accessibility Guidelines (WCAG) sont des directives d'accessibilité pour le contenu web. Elles sont développées par le Web Accessibility Initiative (WAI) du World Wide Web Consortium (W3C), une organisation internationale qui travaille à rendre le Web accessible à tous, y compris aux personnes en situation de handicap.	https://www.w3.org/WAI/standards-guidelines/wcag/
ACC_TG_02	Section 508	-	2017	La Section 508 définit des normes d'accessibilité spécifiques pour divers types de produits et services TIC, tels que les sites web, les logiciels, les documents électroniques et les équipements de télécommunication. Ces normes sont basées sur les Web Content Accessibility Guidelines (WCAG) du World Wide Web Consortium (W3C) et comprennent également des exigences spécifiques aux États-Unis.	https://www.section508.gov/
ACC_TG_03	ISO 9241	-	2006	Normes internationales traitant de l'ergonomie de l'interaction homme-système et fournissent des lignes directrices pour l'évaluation et la conception des interfaces utilisateur.	https://fr.wikipedia.org/wiki/ISO_9241
ACC_TG_04	ARIA (Accessible Rich Internet Applications)	ARIA 1.2	2017	ARIA (Accessible Rich Internet Applications) est l'acronyme de "Applications Internet Riches Accessibles". Il s'agit d'un ensemble de normes web développées par le World Wide Web Consortium (W3C) dans le but d'améliorer l'accessibilité du contenu et des applications web pour les personnes en situation de handicap.	https://fr.wikipedia.org/wiki/Accessible_Rich_Internet_Applications

ACC_TG_05	Mobile Web Best Practices (MWBP)	v1	2008	Mobile Web Best Practices (MWBP) est un ensemble de recommandations pour la conception et le développement de sites web adaptés aux appareils mobiles. Bien qu'il n'existe pas de traduction officielle en français du terme "Mobile Web Best Practices", on peut le traduire littéralement par "Meilleures pratiques pour le web mobile".	https://www.w3.org/2007/02/mwbp_flip_cards
ACC_TG_06	ISO/IEC 40500	2012	2012	ISO/IEC 40500 est une norme internationale intitulée "Technologies de l'information - Critères d'accessibilité des sites web". Elle est également connue sous le nom de "WCAG 2.0 harmonisée" car elle adopte les principes et les lignes directrices des Web Content Accessibility Guidelines (WCAG) 2.0 du World Wide Web Consortium (W3C).	https://www.iso.org/standard/58625.html
ACC_TG_07	ATAG	(ATAG) 2.0	24 September 2015	Les Authoring Tool Accessibility Guidelines (ATAG) sont des directives développées par l'initiative pour l'accessibilité du Web (Web Accessibility Initiative - WAI) du World Wide Web Consortium (W3C). Ces directives se concentrent sur la promotion de l'accessibilité des outils de création, qui sont des applications logicielles utilisées pour créer et modifier du contenu web.	https://www.w3.org/WAI/standards-guidelines/atag/
ACC_TG_08	User Agent Accessibility Guidelines (UAAG)	UAAG 2.0	15 December 2015	Les User Agent Accessibility Guidelines (UAAG) sont des directives développées par le Web Accessibility Initiative (WAI) du World Wide Web Consortium (W3C). Ces directives se concentrent sur l'accessibilité des logiciels utilisateurs (user agents) tels que les navigateurs web, les lecteurs d'écran et autres applications qui permettent aux utilisateurs d'accéder à du contenu sur le Web.	https://www.w3.org/TR/UAAG20/

ACC_TG_09	RGAA (Référentiel Général d'Accessibilité pour les Administrations)	version 4	20 septembre 2019	RGAA (Référentiel Général d'Accessibilité pour les Administrations) est une norme française d'accessibilité spécifiquement conçue pour les services numériques et les sites web des administrations gouvernementales. Elle fournit des lignes directrices et des exigences visant à assurer l'accessibilité de ces ressources numériques aux personnes en situation de handicap.	https://designnumerique.gouv.fr/accessibilite-numerique/rgaa/
ACC_TG_10	Apple Human Interface Guidelines (HIG)	-	2022	Les directives d'interface utilisateur d'Apple fournissent des recommandations spécifiques pour la conception d'applications iOS et macOS afin d'offrir une expérience utilisateur cohérente et intuitive.	https://developer.apple.com/design/human-interface-guidelines/
ACC_TG_11	Material Design	version 4.4	-	Développé par Google, Material Design propose des principes de conception, des lignes directrices et des composants pour créer des interfaces utilisateur attrayantes et conviviales pour les applications et les sites web.	https://fr.wikipedia.org/wiki/Material_Design
ACC_TG_12	IBM Design Language	-	2014	IBM a développé son propre langage de conception axé sur l'expérience utilisateur, qui comprend des principes, des directives et des ressources pour créer des interfaces cohérentes et efficaces pour les produits IBM.	https://www.ibm.com/design/
ACC_TG_13	Android Compatibility Program	-	-	Le programme de compatibilité Android exige que les appareils fonctionnant sous Android respectent certaines exigences de sécurité définies par Google. Cela inclut des normes de sécurité pour le matériel, le système d'exploitation et les applications.	https://source.android.com/docs/compatibility/overview?hl=fr
ACC_TG_14	Web Performance Best Practices	-	-	Ces meilleures pratiques, définies par le World Wide Web Consortium (W3C), fournissent des recommandations pour améliorer les performances des sites web, y compris les sites web mobiles. Elles incluent des directives pour le	https://developer.mozilla.org/en-US/docs/Web/Performance

				chargement rapide des pages, l'optimisation des ressources, la mise en cache et la compression des données.	
ACC_TG_15	SS 618:2016	2016	2016	Fournit des conseils sur les principes de conception d'interfaces adaptées aux personnes âgées afin d'améliorer l'expérience utilisateur des personnes âgées. Non destiné aux personnes âgées souffrant de formes graves de déficiences. Fournit des exemples traitant des dispositions.	https://www.singaporestandardshospital.sg/Product/SPDtDetail/28b094be-a282-4c85-bdab-95d0afa6c4d8
ACC_TG_16	BS 8878	2010	2010	BS 8878 est une norme britannique intitulée "Web Accessibility - Code of Practice". Elle a été publiée par le British Standards Institution (BSI) et vise à fournir des directives pratiques pour la prise en compte de l'accessibilité web dans le processus de développement des sites web.	https://www.boutique.afnor.org/fr-fr/norme/bs-88782010/eu111647/213374
ACC_TG_17	ISO/IEC Guide 71	2014	2014	La norme ISO/IEC Guide 71, intitulée "Guide pour l'inclusion de l'accessibilité dans les normes", fournit des directives et des recommandations pour l'inclusion de l'accessibilité dans le processus de développement de normes. Elle a été développée par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) dans le but de promouvoir une approche inclusive de la normalisation.	https://www.iso.org/standard/57385.html
ACC_TG_18	ISO/IEC 10779	2020	2020	Le présent document spécifie les directives d'accessibilité à prendre en compte lors de la planification, du développement et de la conception de copieurs électrophotographiques, d'imprimantes de page et d'appareils multifonctions. Ces lignes directrices visent à améliorer l'accessibilité requise lorsque principalement des personnes âgées, des personnes handicapées et des	https://www.iso.org/obp/ui/#iso:std:iso-iec:10779:ed-2:v1:en

				personnes souffrant d'un handicap temporaire (ci-après dénommées personnes âgées et personnes handicapées) utilisent du matériel de bureau.	
ACC_TG_19	JIS X 8341-1	-	2010	Lignes directrices pour les personnes âgées et les personnes handicapées - Équipement, logiciels et services d'information et de communication - Partie 1 : Lignes directrices communes	https://www.boutique.afnor.org/fr-fr/norme/jis-x-83411/as020685/301150
ACC_TG_20	JIS X 8341-5	-	novembre 2014	La norme JIS X 8341-5 a été développée par le Japanese Industrial Standards Committee (JISC) et vise à fournir des directives et des recommandations pour rendre les contenus web accessibles aux personnes handicapées. Elle s'aligne sur les principes et les critères de conformité des Web Content Accessibility Guidelines (WCAG) du World Wide Web Consortium (W3C).	https://www.boutique.afnor.org/fr-fr/norme/jis-x-83412/as023860/290138
ACC_TG_21	JIS X 8341-3	-	juin 2016	Lignes directrices pour les personnes âgées et les personnes handicapées - Équipements, logiciels et services d'information et de communication - Partie 3 : Contenu Web / Remarque : Approuvé 2020-10-20 JIS	https://www.boutique.afnor.org/fr-fr/norme/jis-x-83413/as024697/290839
ACC_TG_22	IS X 8341-7	-	2011	La norme JIS X 8341-7 a été développée par le Japanese Industrial Standards Committee (JISC) et vise à fournir des directives et des recommandations pour rendre les outils d'auteur accessibles aux personnes handicapées. Ces outils d'auteur font référence aux logiciels utilisés pour créer des contenus numériques, tels que les éditeurs de texte, les systèmes de gestion de contenu (CMS) et les outils de développement web.	https://archive.org/details/jis.x.8341.7.e.2011

ACC_TG_23	Developing Websites for Older People: How Web Content Accessibility Guidelines (WCAG) 2.0 Applies, by W3C	-	-	Le WCAG 2.0 est une référence internationale pour l'accessibilité des contenus web, et ce document met l'accent sur l'application spécifique de ces lignes directrices pour répondre aux besoins des personnes âgées. Il reconnaît que les personnes âgées peuvent rencontrer des défis spécifiques lors de l'utilisation des sites web en raison de facteurs tels que la diminution de la vision, de l'ouïe, de la mobilité ou des capacités cognitives.	https://www.w3.org/WAI/older-users/developing/
ACC_TG_24	Usability for Senior Citizens, by Nielsen Norman Group	-	Usability for Senior Citizens, by Nielsen Norman Group	La convivialité (ou l'utilisabilité) des produits et des technologies pour les personnes âgées est un domaine d'importance croissante, compte tenu du vieillissement de la population dans de nombreux pays. Les personnes âgées peuvent faire face à des défis spécifiques lors de l'utilisation de technologies, et il est crucial d'adapter les produits pour répondre à leurs besoins.	https://www.nngroup.com/articles/usability-for-senior-citizens/
ACC_TG_26	EN 301 549	V3.2.1	2021-03	La norme EN 301 549 est basée sur les Web Content Accessibility Guidelines (WCAG) du World Wide Web Consortium (W3C) et couvre différents aspects de l'accessibilité des TIC, tels que les sites web, les applications mobiles, les documents électroniques, les logiciels, les produits matériels, etc. Elle fournit des exigences et des recommandations pour rendre ces produits et services accessibles aux personnes handicapées, en prenant en compte différents types de handicaps (visuels, auditifs, moteurs, cognitifs, etc.).	https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf
ACC_TG_27	ISO/IEC 30071-1	2019	2019	Ce document adopte une approche holistique de l'accessibilité des technologies de l'information et de la communication (TIC) en combinant des conseils sur la mise en œuvre de l'accessibilité des systèmes TIC (accessibilité des TIC) tant	https://www.iso.org/standard/70913.html

				au niveau organisationnel qu'au niveau du développement du système.	
ACC_TG_28	ISO/IEC TR 29138-2	2009	2009	La présente partie de l'ISO/CEI TR 29138 identifie un ensemble de documents qui fournissent des orientations sur la manière de répondre aux besoins des personnes handicapées. Bien que son public principal soit les développeurs de normes, il peut également être utile pour les développeurs de produits et services de technologie de l'information, les décideurs politiques, les acheteurs et les défenseurs de l'accessibilité.	https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:29138:-2:ed-1:v1:en
ACC_TG_29	ISO/IEC TR 29138-1	2018	2018	Ce document identifie un ensemble de besoins d'accessibilité des utilisateurs que les divers utilisateurs ont des systèmes TIC pour rendre ces systèmes accessibles à eux. Chaque besoin d'accessibilité de l'utilisateur peut être exigé d'un système par un individu. Différents utilisateurs peuvent avoir différents ensembles de besoins d'accessibilité utilisateur dans différents contextes.	https://www.iso.org/standard/71953.html
ACC_TG_30	ISO/IEC Guide 71	2014	2014	Le Guide ISO/CEI 71:2014 fournit des conseils aux développeurs de normes sur la façon de répondre aux exigences et aux recommandations d'accessibilité dans les normes qui se concentrent, directement ou indirectement, sur les systèmes (c'est-à-dire les produits, les services et les environnements bâtis) utilisés par les personnes.	https://www.iso.org/obp/ui/#iso:std:iso-iec:guide:71:ed-2:v1:en
ACC_TG_31	ISO/IEC 24786	2009	2009	ISO/IEC 24786:2009 spécifie les exigences et les recommandations pour rendre les paramètres d'accessibilité accessibles. Cela rendra les technologies de l'information plus accessibles en permettant aux personnes handicapées	https://www.iso.org/standard/41556.html

				de régler elles-mêmes les paramètres d'accessibilité.	
ACC_TG_32	ISO 9241-210	2019	2019	Ce document fournit des exigences et des recommandations pour les principes et activités de conception centrés sur l'humain tout au long du cycle de vie des systèmes interactifs informatisés. Il est destiné à être utilisé par ceux qui gèrent les processus de conception et concerne les moyens par lesquels les composants matériels et logiciels des systèmes interactifs peuvent améliorer l'interaction homme-système.	https://www.iso.org/standard/77520.html
ACC_TG_33	ISO/IEC 10779	2020	2020	Le présent document spécifie les directives d'accessibilité à prendre en compte lors de la planification, du développement et de la conception de copieurs électrophotographiques, d'imprimantes de page et d'appareils multifonctions. Ces lignes directrices visent à améliorer l'accessibilité requise lorsque principalement des personnes âgées, des personnes handicapées et des personnes souffrant d'un handicap temporaire (ci-après dénommées personnes âgées et personnes handicapées) utilisent du matériel de bureau.	https://www.iso.org/standard/77594.html
ACC_TG_34	ISO 9241-971:2020	2020	2020	Le présent document fournit des exigences et recommandations ergonomiques générales et spécifiques pour les systèmes interactifs tactiles/haptiques accessibles, y compris les interactions tactiles/haptiques accessibles.	https://www.iso.org/fr/standard/74511.html
ACC_TG_35	ISO/IEC TR 19765	2007	2007	L'ISO/CEI TR 19765:2007 présente des icônes et des symboles actuellement utilisés pour fournir un accès aux installations et aux outils pour répondre aux besoins des utilisateurs âgés et handicapés	https://www.iso.org/standard/33903.html

				des produits des technologies de l'information (TI), et pourrait constituer la base d'une future Norme internationale qui fournirait une collection recommandée d'icônes et de symboles.	
ACC_TG_36	ISO/IEC TR 19766	2007	2007	L'ISO/CEI TR 19766:2007 fournit des recommandations relatives à la conception d'icônes pour favoriser l'accessibilité par les personnes âgées et les personnes handicapées.	https://www.iso.org/standard/42128.html
ACC_TG_38	CEN/TR 17884:2022	2022	2022	Ce document précise les connaissances, les compétences, la responsabilité et l'autonomie des experts en TIC impliqués dans le développement de produits et services (y compris les contenus numériques) pour accroître les connaissances en matière d'accessibilité dans différents domaines, pour différentes compétences et responsabilités.	https://standards.it-eh.ai/catalog/stands/cen/c59502e6-c15f-4654-a826-68e951442b25/cen-tr-17884-2022
ACC_TG_39	EN 301549	V3.2.1	2021	Le présent document définit les exigences d'accessibilité fonctionnelle applicables aux produits et services TIC et fournit une description des modes opératoires d'essai et de la méthodologie d'évaluation pour chaque exigence d'accessibilité sous une forme adaptée à une utilisation dans le cadre des marchés publics en Europe. Le présent document est destiné à être utilisé avec les technologies Web, les technologies non Web et les hybrides utilisant les deux. Il couvre à la fois le logiciel et le matériel ainsi que les services. Il est destiné à être utilisé à la fois par les fournisseurs et les acheteurs, mais il est attendu qu'il sera également utilisé par beaucoup d'autres.	https://standards.it-eh.ai/catalog/stands/clc/12ae0c38-e6f2-41ef-8821-66a3492b6ec1/en-301549-2021
ACC_TG_40	CEN/CLC/ETSI TR 101550	V1.1.1	2022	Le présent document répertorie les documents utilisés dans la création de la norme EN 301 549 (V1.1.1) sur les exigences d'accessibilité pour les marchés publics de produits et	https://standards.it-eh.ai/catalog/stands/cen/05f05a91-7569-4c2f-8d5a-a0392528624e/cen

				services TIC en Europe et fournit une référence source pour tout autre document nécessaire à la mise en œuvre des procédures de test spécifiées dans cette norme.	<u>-clc-etsi-tr-101550-2022</u>
ACC_TG_41	ICT Accessibility Standards	-	-	Les normes d'accessibilité des technologies de l'information et de la communication (TIC) sont des directives et des spécifications techniques qui visent à rendre les produits, les services et les systèmes TIC accessibles aux personnes en situation de handicap.	https://ati.gmu.edu/web-standards-2-2/
ACC_TG_42	ISO 19128	2005	2005	la norme ISO 19128 spécifie l'interface pour les serveurs de cartes Web, permettant aux utilisateurs d'accéder et d'interagir avec des données cartographiques via des navigateurs Web. Elle facilite l'échange de données spatiales et définit les opérations et les requêtes de base pour la récupération de données cartographiques.	https://www.iso.org/standard/32546.html
ACC_TG_43	ADA	-	-	ADA, ou Americans with Disabilities Act, est une loi complète sur les droits civils aux États-Unis qui interdit la discrimination à l'égard des personnes handicapées dans divers domaines de la vie publique. Elle a été promulguée en 1990 et a depuis contribué à promouvoir l'égalité des chances et l'accès des personnes handicapées.	https://www.ada.gov/
ACC_TG_45	ISO/IEC 30071-1	2019	2019	Ce document donne des lignes directrices pour la construction et la maintenance de systèmes TIC (y compris les produits et services) qui sont accessibles à divers utilisateurs (y compris les utilisateurs handicapés et les personnes âgées).	https://www.iso.org/standard/70913.html
ACC_TG_46	XACML	V3	2013	XACML (eXtensible Access Control Markup Language) 3.0 est une norme développée par le comité technique de l'OASIS (Organization for the Advancement of Structured Information Standards). XACML est un langage de	https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

				contrôle d'accès basé sur XML conçu pour spécifier et gérer les politiques de contrôle d'accès dans les systèmes d'information.	
ACC_TG_47	APA	-	-	La mission du groupe de travail sur les architectures de plate-forme accessibles (APA WG) est de s'assurer que les spécifications du W3C prennent en charge l'accessibilité pour les personnes handicapées. Le groupe fait progresser cette mission grâce à l'examen des spécifications du W3C, au développement de supports techniques, à la collaboration avec d'autres groupes de travail et à la coordination de stratégies d'accessibilité harmonisées au sein du W3C.	https://www.w3.org/WAI/APA/

8. E-Signature & Transaction Standards

E-signature : Les signatures électroniques, également connues sous le nom de signatures numériques, sont utilisées pour signer électroniquement des documents et fournir un moyen sûr et juridiquement contraignant de signer des documents.

E-transaction : Les normes relatives aux transactions électroniques font référence aux lignes directrices et aux meilleures pratiques pour la réalisation de transactions électroniques dans une organisation.

Voici une liste de normes de E-transaction et E-Signature :

ID	Standard/Norme	Version	Date Publication	Description	Url Documentation
sig_tg_01	eSign-IO	-	-	eSign-IO est une plateforme en ligne spécialisée dans la gestion et la signature électronique des documents. Elle permet aux utilisateurs de créer, envoyer, signer et archiver des documents électroniques de manière sécurisée et légale.	https://esignature.s.io/

sig_tg_0 2	ETA (Electronic Transactions Act)	-	Mars 2021	Définit la reconnaissance légale des signatures électroniques à Singapour	https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations
sig_tg_0 3	PKI(Public Key Infrastructure)	-	-	Les gouvernements utilisent l'ICP pour émettre des certificats numériques pour l'authentification des signatures numériques	https://fr.wikipedia.org/wiki/Infrastructure%CA%A0_c%C3%A9%CA%9s_publiques
sig_tg_0 4	XML SSP(XML Signature Syntax and Processing)	Version 1.1	11 April 2013	Norme utilisée pour créer des signatures numériques pour les documents XML	https://www.w3.org/TR/xmlsig-core1/
sig_tg_0 5	PAdES(PDF Advanced Electronic Signatures)	-	10 Apr 2023	PDF-based electronic signature standard used by the Singapore government for signing PDF documents	https://www.pdf-tools.com/fr/pdf-knowledge/pades-pdf-advanced-electronic-signature/
sig_tg_0 6	AdES(Advanced Electronic Signatures)	-	2014	Une norme européenne utilisée pour les signatures électroniques qui offre un niveau de sécurité plus élevé qu'une signature électronique de base	https://en.wikipedia.org/wiki/Advanced_electronic_signature
sig_tg_0 7	eSign	-	2000	eSign, également connu sous le nom de signature électronique, fait référence à l'utilisation de méthodes électroniques pour signer des documents et les rendre juridiquement contraignants. Une signature électronique est l'équivalent électronique d'une signature manuscrite et elle est utilisée pour authentifier l'intégrité du contenu d'un document et l'identité de la personne qui le signe.	https://www.gonitro.com/fr/sign/esign-act
sig_tg_0 9	XAdES (XML Advanced Electronic Signatures)	-	20 February 2003	XAdES (XML Advanced Electronic Signatures) est une norme développée par l'ETSI (European Telecommunications Standards Institute) pour les signatures électroniques avancées basées sur des documents XML. Il s'agit d'une extension du format XML Signature défini par le W3C (World	https://www.w3.org/TR/XAdES/

				Wide Web Consortium) pour les signatures électroniques.	
sig_tg_10	UK Electronic Signature Regulations 2002	-	2002	Les UK Electronic Signature Regulations 2002 sont une législation au Royaume-Uni qui établit le cadre juridique pour l'utilisation des signatures électroniques. Ces réglementations ont été mises en place pour reconnaître la validité juridique des signatures électroniques et promouvoir leur utilisation dans les transactions électroniques.	https://www.legislation.gov.uk/ksi/2002/318/content/s/made
sig_tg_11	CAdES	-	February 2008	CAdES (CMS Advanced Electronic Signatures) est un ensemble de normes et de spécifications utilisées pour la création, la vérification et la validation de signatures électroniques avancées basées sur le format CMS (Cryptographic Message Syntax). CAdES est basé sur les standards du consortium ETSI (European Telecommunications Standards Institute).	https://www.rfc-editor.org/rfc/rfc5126
sig_tg_13	XMLDSig (XML Digital Signature)	Version 1.1	11 April 2013	XMLDSig (XML Digital Signature) est une norme du World Wide Web Consortium (W3C) qui définit un format pour les signatures numériques dans les documents XML. Elle permet de garantir l'intégrité et l'authenticité des données XML en utilisant des techniques de chiffrement et de hachage.	https://en.wikipedia.org/wiki/XML_Signature
sig_tg_14	eIDAS (Electronic Identification, Authentication and Trust Services)	-	2014	Ce règlement de l'UE fournit un cadre pour des transactions électroniques sécurisées et fiables, y compris les signatures électroniques. Il comprend des lignes directrices pour la création et la vérification des signatures numériques, ainsi que des lignes directrices pour les fournisseurs de services de confiance.	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
sig_tg_15	S/MIME (Secure/Multipurpose Internet Mail Extensions)	-	-	Cette norme fournit des instructions pour la création et la vérification de signatures numériques pour les messages électroniques, y compris des instructions pour le chiffrement des messages électroniques.	https://fr.wikipedia.org/wiki/S/MIME

sig_tg_16	ASiC (Advanced Signature Containers)	-	2011	cette norme fournit des directives pour la création et la vérification des conteneurs de signature numérique, y compris des directives pour l'horodatage et la validation à long terme	https://en.wikipedia.org/wiki/Associated_SignatureContainers
sig_tg_17	ETSI TS 102 778	-	2010	Cette norme fournit des lignes directrices pour la création et la vérification de signatures numériques pour les transactions électroniques, y compris des lignes directrices pour l'horodatage et la validation à long terme	https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations
sig_tg_18	ISO/IEC 14888-1	-	2008	Cette norme fournit des lignes directrices pour la création et la vérification de signatures numériques, y compris des lignes directrices pour la création et la vérification de signatures numériques basées sur le format ISO/IEC 14888-2 (CMS).	https://www.iso.org/fr/standard/44226.html
sig_tg_19	NIST SP 800-73	-	May 2015	Cette norme fournit des lignes directrices pour la création et la vérification de signatures numériques pour les cartes de vérification d'identité personnelle (PIV), y compris des lignes directrices pour la création et la vérification de signatures numériques basées sur le format ISO/IEC 7816-8 (PKCS#1).	https://csrc.nist.gov/publications/detail/sp/800-73/4/final
sig_tg_20	ETA(Electronic Transaction Act)	-	2010	Fournit un cadre juridique pour les transactions électroniques à Singapour, y compris les signatures électroniques et les contrats	https://www.imda.gov.sg/regulations-and-licensing-listing/electronic-transactions-act-and-regulations
sig_tg_21	PEPPOL (Pan-European Public Procurement On-Line)	-	-	Un ensemble de normes et de spécifications techniques permettant des processus de passation de marchés électroniques dans toute l'Europe. D'autres programmes d'administration en ligne non européens mettent en œuvre PEPPOL pour faciliter le commerce transfrontalier et la facturation électronique avec les États membres de l'UE.	https://peppol.eu/what-is-peppol/

sig_tg_2	NTP (Network Trade Platform)	-	-	Singapore government's nationwide e-invoicing network. It is a one-stop trade and logistics ecosystem which aims to provide a seamless and efficient end-to-end trade experience for business in Singapore. The platform is designed to connect players in the trade and logistics industry, including shippers, freight forwarders, carriers and customs brokers among others. It facilitates the exchange of information, streamlines trade processes and helps businesses to reduce costs and improve efficiency. NTP is operated by Singapore Customs in collaboration with other government agencies and private sector partners.	https://www.ntp.gov.sg/home/
sig_tg_2	ISO 20022	2022	February 2022	Une norme mondiale pour les messages financiers, utilisée pour les paiements et les transactions électroniques	https://www.iso20022.org/
sig_tg_2	SGQR	-	17 septembre 2020	A unified QR code payment system in Singapore that enables consumers to make payments to merchants by scanning a QR code.	https://www.mas.gov.sg/development/e-payments/sgqr
sig_tg_2	PayNow	-	10 July 2017	A peer-to-peer funds transfer service that allows users to transfer money instantly to anyone with a Singapore bank account, using only their mobile number or National Registration Identity Card (NRIC) number.	https://www.abs.oreg.sg/consumer-banking/pay-now
sig_tg_2	Payment Card Industry Data Security Standard (PCI DSS)	version 3.2	avril 2016	Le "Payment Card Industry Data Security Standard" (PCI DSS) est un ensemble de normes de sécurité des données qui réglemente la protection des informations des titulaires de cartes de paiement. Il a été développé par le Conseil des normes de sécurité PCI (PCI SSC) pour garantir la sécurité des transactions par carte de paiement et la protection des données des titulaires de cartes.	https://www.pcisecuritystandards.org/

sig_tg_2 7	PKCS	-	-	Les normes PKCS fournissent des spécifications pour les algorithmes, les formats de clés et les structures de données utilisées dans les systèmes de cryptographie à clé publique.	https://fr.wikipedia.org/wiki/Public_Key_Cryptographic_Standards
---------------	------	---	---	--	---

9. Infrastructure standard

Les standards d'infrastructures font référence aux normes et aux meilleures pratiques utilisées dans le domaine des technologies de l'information (IT) pour concevoir, déployer et gérer les infrastructures informatiques d'une organisation. Ces standards fournissent des lignes directrices et des recommandations pour assurer la cohérence, la fiabilité, la sécurité et la performance des systèmes et des réseaux informatiques.

Voici une liste de normes de Standards d'infrastructures :

id	Standard/Norme	Version	Date de publication	Description	Url Documentation
INFRA_TG_01	IPv6 (Internet Protocol version 6)	V6	2017	la dernière version du protocole Internet (IP), qui est utilisé pour identifier et localiser les appareils sur un réseau. IPv6 a été développé pour répondre aux limitations d'IPv4, qui est la version précédente et encore largement utilisée d'IP.	https://fr.wikipedia.org/wiki/IPv6
INFRA_TG_02	RFC 8200	-	2017	RFC 8200, intitulé "Internet Protocol, Version 6 (IPv6) Specification", est un document normatif publié par l'Internet Engineering Task Force (IETF) en juillet 2017. Il définit les spécifications techniques pour la version 6 du protocole Internet (IPv6).	https://www.rfc-editor.org/rfc/rfc8200.html
INFRA_TG_04	IEEE 802.3	-	-	IEEE 802.3 est une norme pour les réseaux informatiques édictée par l'Institute of Electrical and Electronics Engineers (IEEE). Cette norme est généralement connue sous le nom d'Ethernet. C'est aussi un sous-comité du comité IEEE 802 comprenant plusieurs groupes de travail	https://fr.wikipedia.org/wiki/IEEE_802.3

				distincts ayant chacun la responsabilité du développement et de la spécification d'un standard d'interconnexion entre équipements basés sur les liaisons filaires.	
INFRA_TG_05	IEEE 802.1X	-	2001	802.1X est un standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE (famille de la norme IEEE 802). Il permet de contrôler l'accès aux équipements d'infrastructures réseau (et par ce biais, de relayer les informations liées aux dispositifs d'identification).	https://fr.wikipedia.org/wiki/IEEE_802.1X
INFRA_TG_06	IEEE 802.1Q	-	1999	Il permet de modifier la trame Ethernet au niveau de la couche MAC afin de fournir un mécanisme d'étiquetage de trame très répandu et implanté dans de nombreux équipements de marques différentes. Il permet de propager plusieurs VLAN sur un même lien physique (trunk). Shortest Path Bridging (IEEE 802.1aq) Incorporé dans l'IEEE 802.1Q-20141	https://fr.wikipedia.org/wiki/IEEE_802.1Q
INFRA_TG_07	iSCSI	-	avril 2004	iSCSI (Internet Small Computer System Interface) est un protocole de stockage réseau qui permet de transférer des données sur un réseau IP en utilisant le modèle de commande/échange SCSI (Small Computer System Interface). Il permet aux systèmes informatiques d'accéder à des dispositifs de stockage distants, tels que des disques durs, des bandes magnétiques ou des lecteurs optiques, comme s'ils étaient connectés localement.	https://fr.wikipedia.org/wiki/iSCSI
INFRA_TG_08	ISO 22300	2022	2022	Le présent document définit les termes utilisés dans les normes relatives à la sécurité et à la résilience.	https://www.iso.org/fr/standard/72889.html

INFRA_TG_09	FCoE (Fibre Channel over Ethernet)	-	2009	FCoE (Fibre Channel over Ethernet) est une technologie qui permet de transporter des trames Fibre Channel (FC) sur un réseau Ethernet, combinant ainsi les avantages du protocole Fibre Channel pour le stockage avec l'infrastructure Ethernet utilisée couramment dans les réseaux informatiques.	https://fr.wikipedia.org/wiki/Fibre_Channel_over_Ethernet
INFRA_TG_10	ISO/CEI 11801	-	2017	ISO/CEI 11801 est une norme internationale qui spécifie les exigences et les recommandations pour les infrastructures de câblage des réseaux de communication. Elle fournit des directives détaillées sur la conception, l'installation et la maintenance des systèmes de câblage structuré.	https://fr.wikipedia.org/wiki/ISO/CEI_11801
INFRA_TG_11	Câble catégorie 7	-	-	Le câble catégorie 7 de classe F est spécifié par la norme ISO/CEI 11801:2002 qui est relative au câblage de type Ethernet. Celui-ci est partiellement compatible avec les câbles catégorie 5 et 6 et permet la transmission de données à des débits allant jusqu'à 40 Gbit/s et à des fréquences jusqu'à 600 MHz.	https://fr.wikipedia.org/wiki/C%C3%A2ble_cat%C3%A9gorie_7
INFRA_TG_12	Cat 6a	-	-	Un câble de Catégorie 6A, également connu sous le nom de Cat 6A, est une évolution du câble de Catégorie 6 (Cat 6) qui offre des performances améliorées en termes de débit de données et de qualité de transmission. Le "A" dans Cat 6A signifie "Augmented" (augmenté) pour indiquer les améliorations apportées par rapport au Cat 6.	https://fr.wikipedia.org/wiki/C%C3%A2ble_cat%C3%A9gorie_6a
INFRA_TG_13	IEEE 802.11ac	-	2014	IEEE 802.11ac est une norme de réseau sans fil qui définit les spécifications pour les réseaux Wi-Fi à haut débit. Également connu sous le nom de Wi-Fi 5, l'IEEE 802.11ac est une évolution de la norme précédente IEEE 802.11n (Wi-Fi 4) et offre des améliorations significatives en termes de vitesse et de performance.	https://fr.wikipedia.org/wiki/IEEE_802.11ac

INFRA_TG_14	DHCP	-	-	<p>Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau utilisé pour attribuer automatiquement les adresses IP et les paramètres de configuration réseau à des dispositifs sur un réseau. Il simplifie la configuration et la gestion des adresses IP en permettant aux appareils de se connecter à un réseau et d'obtenir automatiquement une adresse IP valide, ainsi que d'autres informations réseau nécessaires, sans intervention manuelle.</p>	https://fr.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
INFRA_TG_15	Border Gateway Protocol	BGP-4	1994	<p>Le Border Gateway Protocol (BGP) est un protocole de routage utilisé sur Internet pour échanger des informations de routage entre les systèmes autonomes (AS). Il est conçu pour prendre en charge le routage entre les réseaux externes et permet aux fournisseurs de services Internet (ISP) de s'interconnecter et de partager des informations de routage pour acheminer le trafic efficacement.</p>	https://fr.wikipedia.org/wiki/Border_Gateway_Protocol
INFRA_TG_16	Simple Network Management Protocol (SNMP)	-	1993	<p>Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.</p>	https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol
INFRA_TG_17	Network Time Protocol (NTP)	Version 4	2010	<p>Network Time Protocol (« protocole de temps réseau ») ou NTP est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.</p>	https://fr.wikipedia.org/wiki/Network_Time_Protocol

INFRA_TG_18	Domain Name System(DNS)	-	2019	Le Domain Name System (DNS) est un système de noms de domaine utilisé pour traduire les noms de domaine faciles à retenir en adresses IP numériques associées aux ressources réseau. Il agit comme un annuaire permettant de localiser et d'identifier les serveurs et les services sur Internet.	https://fr.wikipedia.org/wiki/Domain_Name_System
INFRA_TG_19	SD-WAN	-	2020	SD-WAN (Software-Defined Wide Area Network) est une technologie de réseau qui permet de gérer et d'optimiser les réseaux étendus (WAN) de manière centralisée à l'aide de logiciels. Contrairement aux réseaux WAN traditionnels qui étaient principalement basés sur des matériels propriétaires, le SD-WAN utilise des logiciels pour virtualiser et contrôler les fonctionnalités de gestion du réseau.	https://fr.wikipedia.org/wiki/SD-WAN
INFRA_TG_20	Software-defined networking	-	2012	Le Software-Defined Networking (SDN) est un concept et une approche de conception réseau qui vise à séparer le plan de contrôle (control plane) du plan de données (data plane) dans un réseau informatique. Il propose une architecture réseau plus flexible, programmable et centralisée, où la gestion et le contrôle du réseau sont définis par des logiciels.	https://en.wikipedia.org/wiki/Software-defined_networking
INFRA_TG_21	Multiprotocol Label Switching	-	-	Multiprotocol Label Switching (MPLS) est une technologie de réseau largement utilisée pour acheminer efficacement le trafic dans les réseaux de données. Elle est souvent utilisée dans les réseaux étendus (WAN) pour offrir des performances et une qualité de service (QoS) améliorées.	https://fr.wikipedia.org/wiki/Multiprotocol_Label_Switching

INFRA_TG_22	Multiprotocol Label Switching Architecture	-	1996	L'architecture du Multiprotocol Label Switching (MPLS) comprend différents composants qui coopèrent pour permettre le fonctionnement de cette technologie de réseau.	https://fr.wikipedia.org/wiki/Multiprotocol_Label_Switching
INFRA_TG_23	Ethernet	-	-	Ethernet est une technologie de réseau local (LAN) largement utilisée pour la transmission de données entre les périphériques connectés au même réseau. Il est basé sur une série de normes, principalement définies par l'IEEE (Institute of Electrical and Electronics Engineers), dans la famille de normes IEEE 802.3.	https://fr.wikipedia.org/wiki/Ethernet
INFRA_TG_24	ISO/IEC/IEEE 8802-3:2021	-	2021	La norme ISO/IEC/IEEE 8802-3:2021 décrit les caractéristiques des couches physiques (PHY) et de la sous-couche de contrôle de liaison de données (MAC) pour les réseaux Ethernet. Elle spécifie les différentes variantes et classes d'Ethernet, y compris les vitesses de transmission, les types de câbles, les interfaces électriques et optiques, les mécanismes de contrôle d'accès au support (MAC), les formats de trame et les protocoles associés.	https://www.iso.org/standard/78299.html
INFRA_TG_25	Transmission Control Protocol(TCP)	-	1973	TCP/IP (Transmission Control Protocol/Internet Protocol) est un ensemble de protocoles de communication qui forme la base de l'Internet et de nombreux réseaux informatiques. Il définit comment les données sont transmises, acheminées et reçues entre les périphériques connectés à un réseau.	https://fr.wikipedia.org/wiki/Transmission_Control_Protocol
INFRA_TG_26	GPON	-	-	GPON est l'acronyme de Gigabit-capable Passive Optical Network. Cette technique est utilisée dans le domaine des réseaux de transmission de données et des réseaux d'accès à Internet à très haut débit.	https://fr.wikipedia.org/wiki/GPON

INFRA_TG_27	ANSI/TIA-942 STANDARD	-	-	Cette norme fournit des directives pour la conception et la mise en œuvre de l'infrastructure du centre de données, y compris le câblage, la distribution de l'alimentation, le refroidissement et la sécurité.	https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/
INFRA_TG_28	ISO/IEC 17788	-	2014	L'ISO/CEI 17788:2014 donne un aperçu de l'informatique en nuage ainsi qu'un ensemble de termes et de définitions. Il s'agit d'une base terminologique pour les normes de cloud computing.	https://www.iso.org/standard/60544.html
INFRA_TG_29	ISO/IEC 17789	-	2014	L'ISO/IEC 17789:2014 spécifie l'architecture de référence du cloud computing (CCRA). L'architecture de référence comprend les rôles de cloud computing, les activités de cloud computing et les composants fonctionnels de cloud computing et leurs relations.	https://www.iso.org/standard/60545.html
INFRA_TG_30	IEEE 802.11	-	-	IEEE 802.11 est un ensemble de normes qui définissent les spécifications de la communication par réseau local sans fil (WLAN). Il est communément appelé Wi-Fi et est largement utilisé pour les réseaux sans fil dans les maisons, les entreprises et les espaces publics.	https://fr.wikipedia.org/wiki/IEEE_802.11ac
INFRA_TG_31	IS-IS (Intermediate system to intermediate system)	-	-	IS-IS, qui signifie Intermediate System to Intermediate System (de système intermédiaire à système intermédiaire), est un protocole de routage utilisé couramment dans les réseaux IP à grande échelle, notamment dans les environnements de fournisseurs de services. Il s'agit d'un protocole de passerelle intérieure (IGP) qui permet aux routeurs au sein d'un système autonome d'échanger des informations de routage et de prendre des décisions de transfert éclairées.	https://fr.wikipedia.org/wiki/IS-IS

INFRA_TG_32	Uptime Institute Tier Standards (Tier I, II, III, IV)	-	-	Les Uptime Institute Tier Standards (Normes de Niveau de l'Uptime Institute) sont une classification utilisée pour évaluer la résilience et la disponibilité des centres de données. Les normes Tier définissent quatre niveaux de certification qui correspondent à différents niveaux de redondance et de fiabilité des infrastructures du centre de données.	https://fr.wikipedia.org/wiki/Uptime_Institute
INFRA_TG_33	ANSI/BICSI 002-2019	-	2019	La norme ANSI/BICSI 002-2019 aborde différents aspects liés aux centres de données, tels que l'infrastructure physique, les systèmes de câblage, les systèmes de refroidissement, l'alimentation électrique, la gestion des câbles, la sécurité, les contrôles environnementaux, et d'autres considérations clés. Elle vise à promouvoir des pratiques optimales pour assurer une conception efficace, une disponibilité élevée, une gestion simplifiée et une évolutivité future des centres de données.	https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-2019-data-center-design
INFRA_TG_34	ASHRAE TC 9.9	-	-	ASHRAE TC 9.9, ou Technical Committee 9.9 de l'American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE), est un comité technique qui se concentre sur les aspects liés à la conception et à l'exploitation des infrastructures de centres de données. TC 9.9 est spécifiquement dédié à l'étude des technologies de refroidissement, de la gestion thermique et de l'efficacité énergétique des centres de données.	https://www.ashrae.org/File%20Library/Technical%20Resources/Bookstore/ASHRAE_TC0909_Power_White_Paper_22_June_2016_RELISED.pdf
INFRA_TG_35	AWS Well-Architected Framework	-	2023	Le cadre Well-Architected d'AWS (Amazon Web Services) fournit un ensemble de meilleures pratiques et de directives pour concevoir, construire et exploiter des architectures cloud sur la plateforme AWS. Il est conçu	https://fr.wikipedia.org/wiki/IEEE_802.15.4

				pour aider les clients à prendre des décisions éclairées concernant leurs environnements cloud, à améliorer les performances, la sécurité et l'efficacité du système, et à fournir des solutions fiables et évolutives.	
INFRA_TG_36	IEEE 802.15.4	-	-	Le 802.15.4 est un protocole de communication défini par l'IEEE. Il est destiné aux réseaux sans fil de la famille des LR WPAN (Low Rate Wireless Personal Area Network) du fait de leur faible consommation, de leur faible portée et du faible débit des dispositifs utilisant ce protocole.	https://fr.wikipedia.org/wiki/IEEE_802.15.4
INFRA_TG_37	ISO/IEC 30134	-	2016	Gestion des installations et des infrastructures des centres de données - Cette norme fournit des directives pour la gestion des installations des centres de données, y compris les systèmes d'alimentation et de refroidissement, la sécurité physique, la surveillance de l'environnement et les processus de maintenance.	https://www.iso.org/standard/63450.html
INFRA_TG_38	NF EN 50600-1	-	2019	Cette norme européenne spécifie les exigences et les recommandations pour les installations et les infrastructures des centres de données, couvrant des domaines tels que l'alimentation électrique, le refroidissement, la sécurité physique et les contrôles environnementaux.	https://www.boutique.afnor.org/fr-fr/norme/nf-en-506001/technologie-de-linformation-installation-et-infrastructures-de-centres-de-t/fa191510/83211
INFRA_TG_39	5G (Fifth Generation)	-	-	La 5G (cinquième génération) est une norme de réseau de téléphonie mobile. Elle succède à la quatrième génération, appelée 4G1, en proposant des débits plus importants et une latence fortement réduite, tout en évitant le risque de saturation des réseaux lié à l'augmentation des usages numériques	https://fr.wikipedia.org/wiki/5G

INFRA_TG_40	ISO/IEC 19831	2015	2015	ISO/IEC 19831:2015 décrit le modèle et le protocole pour les interactions de gestion entre un fournisseur d'infrastructure en tant que service (IaaS) cloud et les consommateurs d'un service IaaS. Les ressources de base d'IaaS (machines, stockage et réseaux) sont modélisées dans le but de fournir un accès de gestion des consommateurs à une implémentation d'IaaS et de faciliter la portabilité entre les implémentations cloud qui prennent en charge la spécification. Ce document spécifie un protocole de type REST (Representational State Transfer) utilisant HTTP.	https://www.iso.org/standard/66296.html
INFRA_TG_41	ISO/IEC 22123-1	2023	2023	Ce document définit les termes utilisés dans le domaine du cloud computing.	https://www.iso.org/standard/82758.html
INFRA_TG_42	ISO/IEC FDIS 22123-2	-	-	L'ISO/CEI 17788:2014 donne un aperçu de l'informatique en nuage ainsi qu'un ensemble de termes et de définitions. Il s'agit d'une base terminologique pour les normes de cloud computing.	https://www.iso.org/standard/80351.html
INFRA_TG_43	ISO/IEC TR 30133:2023	2023	2023	Ce document décrit les pratiques généralement applicables pour améliorer l'efficacité des ressources des centres de données, indépendamment de leur(s) application(s).	https://www.iso.org/standard/53253.html
INFRA_TG_44	ISO/IEC 22237-1	2021	2021	Décrit les principes généraux des centres de données sur lesquels reposent les exigences de la série ISO/IEC22237 ;	https://www.iso.org/standard/78550.html

INFRA_TG_45	ISO/IEC TS 22237-2	2018	2018	L'ISO/CEI TS 22237-2:2018 traite de la construction de bâtiments et d'autres structures qui fournissent des logements pour les centres de données sur la base des critères et de la classification de la "sécurité physique" dans l'ISO/CEI TS 22237- 1 à l'appui de la disponibilité.	https://www.iso.org/standard/73009.html
INFRA_TG_46	ISO/IEC 22237-3	2021	2021	Ce document traite des alimentations électriques et de la distribution électrique au sein des centres de données en fonction des critères et des classifications de « disponibilité », « sécurité physique » et « activation de l'efficacité énergétique » dans la norme ISO/IEC 22237-1.	https://www.iso.org/standard/78551.html
INFRA_TG_47	ISO/IEC 22237-4	2021	2021	Ce document traite du contrôle environnemental dans les centres de données sur la base des critères et des classifications de "disponibilité", "sécurité" et "activation de l'efficacité énergétique" dans la norme ISO/CEI 22237- 1.	https://www.iso.org/standard/78552.html
INFRA_TG_48	ISO/IEC TS 22237-5	2018	2018	L'ISO/CEI TS 22237-5:2018 traite du large éventail d'infrastructures de câblage de télécommunications dans les centres de données sur la base des critères et des classifications de "disponibilité" de l'ISO/CEI TS 22237- 1.	https://www.iso.org/standard/73012.html
INFRA_TG_49	ISO/IEC TS 22237-6	2018	2018	Ce document traite de la sécurité physique des centres de données sur la base des critères et des classifications de "disponibilité", "sécurité" et "activation de l'efficacité énergétique" dans l'ISO/CEI TS 22237- 1.	https://www.iso.org/fr/standard/73013.html
INFRA_TG_50	ISO/IEC TS 22237-7	2018	2018	L'ISO/CEI TS 22237-7:2018 spécifie les processus de gestion et d'exploitation des centres de données. Ce document se concentre principalement sur les processus opérationnels nécessaires pour fournir le niveau attendu de résilience, de disponibilité, de gestion des risques, d'atténuation des risques, de planification des	https://www.iso.org/standard/73014.html

				capacités, de sécurité et d'efficacité énergétique.	
INFRA_TG_51	ISO/IEC 21836	2020	2020	Ce document spécifie une méthode de mesure pour évaluer et rapporter l'efficacité énergétique d'un serveur informatique.	https://www.iso.org/standard/71926.html
INFRA_TG_52	ISO/IEC 21878	2018	2018	Ce document spécifie les directives de sécurité pour la conception et la mise en œuvre des VS. Les considérations de conception axées sur l'identification et l'atténuation des risques, ainsi que les recommandations de mise en œuvre concernant les SV typiques sont traitées dans ce document.	https://www.iso.org/standard/72029.html
INFRA_TG_53	ISO/IEC 27018	2019	2019	Le présent document définit des objectifs de sécurité acceptés, des mesures de sécurité et des lignes directrices de mise en œuvre de mesures destinées à protéger les informations personnelles identifiables (PII) conformément aux principes de protection de la vie privée de l'ISO/IEC 29100 pour l'environnement informatique en nuage public.	https://www.iso.org/fr/standard/76559.html
INFRA_TG_54	ISO/IEC DIS 5140	2022	2022	Ce document fournit des concepts fondamentaux pour plusieurs services cloud, y compris le multi-cloud, le cloud hybride, le cloud inter-cloud et le cloud fédéré.	https://www.iso.org/standard/80910.html
INFRA_TG_55	BS ISO/IEC 19941	2017	2017	L'ISO/CEI 19941:2017 spécifie les types d'interopérabilité et de portabilité de l'informatique en nuage, la relation et les interactions entre ces deux aspects transversaux de l'informatique en nuage et la terminologie et les concepts communs utilisés pour	https://www.iso.org/standard/66639.html

				discuter de l'interopérabilité et de la portabilité, en particulier en ce qui concerne les services en nuage.	
INFRA_TG_56	BS EN IEC 61280-1-3	2021	2021	Cette norme spécifie les procédures de test pour les sous-systèmes de communication à fibre optique. Plus précisément, la partie 1-3 de la norme IEC 61280-1-3 se concentre sur les procédures de test des photomètres optiques, utilisés pour mesurer la puissance optique dans les fibres optiques et les câbles optiques.	
INFRA_TG_57	Uptime Institute Tiers	-	-	L'Institut Uptime est une organisation internationale qui se spécialise dans la classification et la certification des centres de données en fonction de leur disponibilité et de leur fiabilité. L'une des méthodes les plus couramment utilisées par l'Uptime Institute pour classer les centres de données est le système de classification Tier.	https://uptimeinstitute.com/tiers
INFRA_TG_58	G.657	-	2016	Caractéristiques des câbles et fibres optiques monomodes insensibles aux pertes par courbure	https://www.itu.int/rec/T-REC-G.657-201611-1/fr
INFRA_TG_59	G.652	-	2016	G.652 est une norme internationale qui décrit les attributs géométriques, mécaniques et de transmission d'une fibre optique et d'un câble monomodes, développée par le secteur de la normalisation de l'Union internationale des télécommunications (UIT-T) qui spécifie le type le plus populaire de Câble à fibre optique en mode (SMF).	https://www.itu.int/rec/T-REC-G.652-201611-1/en

INFRA_TG_60	IEC 61757	1	2018	La CEI 61757:2018 est une spécification générique couvrant les fibres optiques, les composants et les sous-ensembles dans la mesure où ils se rapportent spécifiquement aux applications de détection à fibre optique. Il a été conçu pour être utilisé comme un outil commun de travail et de discussion par les vendeurs de composants et sous-ensembles destinés à être intégrés dans des capteurs à fibre optique, ainsi que par les concepteurs, fabricants et utilisateurs de capteurs à fibre optique indépendamment de toute application ou installation.	https://webstore.iec.ch/publication/59554
INFRA_TG_61	IEC 60794-1-1	5	2023	L'objet du présent document est d'établir des exigences génériques uniformes pour les propriétés géométriques, de transmission, matérielles, mécaniques, de vieillissement (exposition à l'environnement), climatiques et électriques des câbles à fibres optiques et des éléments de câble, le cas échéant.	https://webstore.iec.ch/publication/68873
INFRA_TG_62	IEC 60793-1	-	-	La famille de normes IEC 60793 couvre les spécifications pour les fibres optiques utilisées dans les communications optiques et d'autres applications. Elle est composée de plusieurs parties qui définissent différents aspects des fibres optiques.	https://webstore.iec.ch/publication/76853
INFRA_TG_63	IS 16939	-	2018	Cette norme définit les exigences du câble à fibre optique monomode, utilisant une fibre optique conforme à la Rec. ITU-T Rec.G.657, pour les applications FTTx.	https://shop.standards.ie/en-ie/Standards/IS-16939-2018-1169658_SAIG_BIS_BIS_2785054/
INFRA_TG_64	IS/ISO/IEC 19944-1	-	2020	Ce document s'applique principalement aux fournisseurs de services cloud, aux clients de services cloud et aux utilisateurs de services cloud, mais également à toute personne	https://www.iso.org/fr/standard/79573.html

				ou organisation impliquée dans les implications juridiques, politiques, techniques ou autres des flux de données entre les appareils et les services cloud.	
INFRA_TG_65	TIA 942-A 2014	-	2014	<p>La norme TIA-942 couvre tous les aspects de l'infrastructure physique des centres de données, y compris l'architecture et la topologie, la conception environnementale, les systèmes d'alimentation et distribution, systèmes de refroidissement et distribution, systèmes de câblage, redondance, les voies, la sécurité et la sécurité physique. Un objectif clé de la norme TIA-942 est de définir comment un centre de données doit être construit et configuré pour fournir le niveau de la fiabilité et la résilience requises par les utilisateurs finaux. Il y a quatre cotes qui fournissent une manière impartiale pour les propriétaires et les utilisateurs de centres de données de définir leurs attentes en fonction des applications et des données stockées dans leur centre de données spécifique</p>	https://tiaonline.org/wp-content/uploads/dlm_uploads/2021/01/TIA-942-Standard_OnePage_r-110220.pdf
INFRA_TG_67	G.656	-	2010	Caractéristiques des fibres et câbles optiques à dispersion non nulle destinés au transport à large bande	https://www.itu.int/rec/T-REC-G.656-201007-I/en
INFRA_TG_68	G.655	-	2009	La norme spécifie les attributs géométriques, mécaniques et de transmission d'une fibre optique monomode ainsi que de son câble. La plage de diamètre de champ de mode autorisée dans G.655 est de 8 à 11 µm dans une fibre à dispersion décalée non nulle. La fibre G.655.C a une valeur	https://www.itu.int/rec/T-REC-G.655-200911-I/en

				de conception de liaison PMD maximale de 0,20 ps/km ² , qui est la valeur la plus basse recommandée par l'ITU-T. G.655 a la longueur d'onde de coupure du câble et les coefficients d'atténuation du câble dans les bandes C et L	
INFRA_TG_69	G.654	-	2020	La fibre G.654 recommandée par l'UIT-T est une fibre optique monomode à décalage de coupure spécialement utilisée pour la transmission longue distance à large bande passante. La fibre G. 654 est une fibre optique monomode et un câble qui a la dispersion nulle des longueurs d'onde de fibre optique autour de 1300 nm, la fibre avec une perte minimisée et une longueur d'onde de coupure décalée à environ 1550 nm. la norme de fibre a été introduite pour la première fois en 1988. La fibre ITU-T G.654 pourrait être appliquée dans des systèmes sous-marins à bande passante plus élevée, système de transport de retour.	https://www.itu.int/rec/T-REC-G.654-202003-I/fr
INFRA_TG_70	G.652	9.0	2016	La norme spécifie les attributs géométriques, mécaniques et de transmission d'une fibre optique monomode ainsi que de son câble.	https://www.itu.int/rec/T-REC-G.652-201611-I/en
INFRA_TG_71	ISO/IEC 27017	2015	2015	ISO/IEC 27017:2015 donne des lignes directrices pour les contrôles de sécurité de l'information applicables à la fourniture et à l'utilisation de services cloud en fournissant : - des conseils de mise en œuvre supplémentaires pour les contrôles pertinents spécifiés dans l'ISO/CEI 27002 ; - des contrôles supplémentaires avec des conseils de mise en œuvre	https://www.iso.org/standard/43757.html

				spécifiquement liés aux services cloud.	
INFRA_TG_72	ISO/IEC 17203	2017	2017	La spécification OVF (Open Virtualization Format) décrit un système ouvert, sécurisé, efficace et format extensible pour le conditionnement et la distribution de logiciels à exécuter dans des systèmes virtuels.	https://www.iso.org/standard/72081.html
INFRA_TG_73	NIST SP 500-293	-	2014	Cela fournit un cadre et une structure détaillés pour les infrastructures de cloud computing. Bien que conçu pour les applications gouvernementales, il peut également être utilisé dans le secteur privé.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-293.pdf
INFRA_TG_74	NIST SP 800-144	-	2011	Cette norme fournit des conseils et des recommandations pour la mise en œuvre d'un environnement sécurisé dans les services de cloud public.	https://csrc.nist.gov/publications/detail/sp/800-144/final
INFRA_TG_75	NIST SP 800-145	-	2011	Cette norme décrit des aspects importants du cloud computing et sert de référence pour comparer les services cloud et les stratégies de déploiement. Il fournit également une base pour les discussions sur le cloud computing et comment l'utiliser.	https://csrc.nist.gov/publications/detail/sp/800-145/final
INFRA_TG_76	ISO/IEC 17826	2.0.0	2022	cette norme concerne les développeurs de systèmes mettant en œuvre et utilisant le stockage en nuage.	https://www.iso.org/standard/83451.html

INFRA_TG_77	ISO/IEC 18384	-	2016	Cette norme définit le vocabulaire, les lignes directrices et les principes techniques généraux sous-jacents à la SOA, qui sont souvent déployées sur des plates-formes cloud.	https://www.techtarget.com/searchsecurity/tip/Top-cloud-security-standards-and-frameworks-to-consider
INFRA_TG_78	ISO/IEC TS 23167	2020	2020	Cette norme décrit les technologies et techniques utilisées dans le cloud computing, y compris les machines virtuelles, les hyperviseurs et les conteneurs.	https://www.iso.org/standard/74805.html
INFRA_TG_79	Organization for the Advancement of Structured Information Standards (OASIS)	-	-	Cette organisation à but non lucratif développe des normes ouvertes pour la sécurité, la technologie cloud, l'IoT, les technologies de contenu et la gestion des urgences. Ses divers comités techniques cloud incluent OASIS Cloud Application Management for Platforms, OASIS Identity in the Cloud et OASIS Topology and Orchestration Specification for Cloud Applications.	https://www.oasis-open.org/
INFRA_TG_80	NIST Special Publication 500-332	-	2020	Discute et met en évidence un ensemble d'exigences prioritaires pour l'adoption du cloud computing.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-332.pdf
INFRA_TG_81	IEC 60793-1	-	2022	Spécifications générales - Cette partie établit des définitions, des termes et des méthodes d'essai communs pour les fibres optiques.	https://standards.ieee.ai/catalog/standards/iec/dea8f0c9-607c-4a19-b165-f82e3d8e32a9/iec-60793-1-1-2022

INFRA_TG_82	ISO/IEC TR 23050	2019	2019	Ce document décrit le traitement des métriques du centre de données dans des circonstances où l'énergie électrique est stockée et exportée à l'intérieur des limites du centre de données d'autres normes de la série ISO/IEC 30134.	https://www.iso.org/standard/74405.html
INFRA_TG_83	EN 50600-2-1	-	-	Gestion de l'infrastructure de centres de données - Partie 2-1 : Terminologie - Cette norme établit la terminologie et les définitions de base utilisées dans le domaine des infrastructures de centres de données.	https://standards.iteh.ai/catalog/standards/clc/a9d359c5-b85a-4b92-a5e5-aebeb34f46d3/en-50600-2-1-2021
INFRA_TG_84	EN 50600-2-2	-	-	Gestion de l'infrastructure de centres de données - Partie 2-2 : Spécification de l'infrastructure de centres de données - Cette norme spécifie les exigences techniques pour la conception, la construction et l'exploitation des infrastructures physiques des centres de données, y compris les paramètres tels que l'alimentation électrique, le refroidissement, la sécurité, les câblages, etc.	https://standards.iteh.ai/catalog/standards/clc/7f86e177-a03c-4e5b-991b-27528436cf86/en-50600-2-2-2019
INFRA_TG_85	EN 50600-2-3	-	-	Gestion de l'infrastructure de centres de données - Partie 2-3 : Évaluation et classement de l'infrastructure de centres de données - Cette norme fournit des directives pour évaluer et classer les infrastructures de centres de données en fonction de différents critères tels que la disponibilité, la redondance, la résilience, la capacité, etc.	https://standards.iteh.ai/catalog/standards/clc/212dd9d2-d6ec-4e64-976b-0035b8f971d4/en-50600-2-3-2019
INFRA_TG_86	EN 50600-2-4	-	-	Gestion de l'infrastructure de centres de données - Partie 2-4 : Exigences de sécurité pour l'infrastructure de centres de données - Cette norme établit les exigences de sécurité physiques et techniques pour les infrastructures de centres de données, y compris les	https://standards.iteh.ai/catalog/standards/clc/bb5faca9-6ba9-429c-a04d-f3e2b46d90bc/en-50600-4-2-2016

				aspects tels que l'accès physique, la surveillance, la protection contre l'incendie, etc.	
INFRA_TG_87	EN 50600-2-5	-	-	Gestion de l'infrastructure de centres de données - Partie 2-5 : Gestion des risques pour l'infrastructure de centres de données - Cette norme fournit des directives pour l'identification, l'évaluation et la gestion des risques liés aux infrastructures de centres de données, y compris les risques liés à la sécurité, à l'environnement, aux opérations, etc.	https://standards.iteh.ai/catalog/standards/clc/e05a08b8-0699-4a11-b824-d36fae1bdd04/en-50600-2-5-2021
INFRA_TG_88	EN 50600-2-6	-	-	Gestion de l'infrastructure de centres de données - Partie 2-6 : Gestion de l'énergie pour l'infrastructure de centres de données - Cette norme spécifie les exigences et les bonnes pratiques pour la gestion de l'énergie dans les infrastructures de centres de données, y compris l'efficacité énergétique, la surveillance de la consommation, la planification énergétique, etc.	https://standards.iteh.ai/catalog/standards/clc/7f86e177-a03c-4e5b-991b-27528436cf86/en-50600-2-2-2019
INFRA_TG_89	ITU-T G.984	-	2010	ITU-T G.984 est une norme technique émise par l'Union internationale des télécommunications (ITU-T) qui définit les spécifications pour la technologie de réseau de fibre optique passive (PON) basée sur la norme Gigabit-capable Passive Optical Network (GPON).	https://en.wikipedia.org/wiki/GPON
INFRA_TG_90	ANSI/TIA-568	-	2015	L'ANSI/TIA-568 est une norme développée par l'American National Standards Institute (ANSI) et la Telecommunications Industry Association (TIA). Elle définit les normes et les exigences pour la conception, l'installation et la performance des systèmes de câblage	https://fr.wikipedia.org/wiki/ANSI/TIA-568

				structuré utilisés dans les réseaux de communication.	
INFRA_TG_91	TCP/IP	-	-	TCP/IP (Transmission Control Protocol/Internet Protocol) est une suite de protocoles de communication utilisés pour interconnecter des dispositifs sur Internet et sur de nombreux réseaux locaux (LAN) et étendus (WAN). Elle est devenue la base du fonctionnement d'Internet et est largement utilisée dans les réseaux informatiques du monde entier.	https://fr.wikipedia.org/wiki/Transmission_Control_Protocol
INFRA_TG_92	VPN	-	-	Un réseau privé virtuel (VPN, Virtual Private Network) est un service qui permet de créer une connexion sécurisée et cryptée entre un appareil et un réseau privé via un réseau public, tel qu'Internet. Le VPN permet de sécuriser les communications en ligne, de protéger la confidentialité des données et d'accéder à des ressources réseau de manière sécurisée, même à distance.	https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel
INFRA_TG_93	MPLS	-	-	MPLS (Multiprotocol Label Switching) est un protocole de commutation de paquets utilisé dans les réseaux de télécommunications pour acheminer efficacement les données d'un point à un autre. Il a été développé pour améliorer les performances et la qualité de service des réseaux IP.	https://fr.wikipedia.org/wiki/Multiprotocol_Label_Switching

INFRA_TG_94	Fibre optique	-	-	Un type de câble de transmission de données	https://fr.wikipedia.org/wiki/Fibre_optique
INFRA_TG_95	VoIP	-	-	une technologie de communication qui permet de transmettre des appels vocaux sur des réseaux IP, tels qu'Internet.	https://fr.wikipedia.org/wiki/Voix_sur_IP
INFRA_TG_96	UDP	-	-	UDP (User Datagram Protocol) est un protocole de communication utilisé dans les réseaux informatiques. Il fait partie de la couche de transport du modèle TCP/IP. Contrairement au protocole TCP, qui fournit une communication fiable et orientée connexion, UDP offre une communication non fiable et sans connexion.	https://fr.wikipedia.org/wiki/User_Datagram_Protocol
INFRA_TG_97	ISO/IEC 27001	-	-	Lorsqu'il s'agit de l'infrastructure de sécurité de l'information, ISO/IEC 27001 recommande d'identifier et d'évaluer les risques liés aux actifs informatiques, y compris les systèmes, les réseaux et les équipements utilisés pour traiter, stocker et transmettre les informations sensibles.	https://www.iso.org/fr/standard/27001
INFRA_TG_98	COBIT	-	-	COBIT (Control Objectives for Information and Related Technologies) est un cadre de gestion des technologies de l'information largement utilisé pour aider les organisations à atteindre leurs objectifs en matière de gouvernance et de gestion des technologies de l'information.	https://fr.wikipedia.org/wiki/CobiT

INFRA_TG_99	4G / 5G	-	-	Les normes 4G (quatrième génération) et 5G (cinquième génération) font référence aux normes de communication sans fil utilisées dans les réseaux mobiles. https://fr.wikipedia.org/wiki/5G	
-------------	---------	---	---	--	--

Centre de Standardisation

Centre de standardisation	Description	Url
ISO (International Organization for Standardization)	<p>L'Organisation internationale de normalisation (ISO), ou International Organization for Standardization en anglais, est une organisation internationale indépendante et non gouvernementale qui développe et publie des normes internationales. Les normes de l'ISO couvrent différents aspects de la technologie, de l'industrie et des affaires, et sont conçues pour assurer la cohérence, la sécurité et la qualité des produits, des services et des systèmes à travers le monde.</p>	<p>https://www.iso.org/about-us.html</p>
IEC International Electrotechnical Commission	<p>La Commission électrotechnique internationale (IEC, pour International Electrotechnical Commission en anglais) est une organisation internationale de normalisation qui développe et publie des normes internationales pour les technologies électriques et électroniques. Il s'agit d'une organisation à but non lucratif créée en 1906 et dont le siège se trouve à Genève, en Suisse.</p>	<p>https://www.iec.ch/homepage</p>
NIST National Institute of Standards and Technology	<p>NIST signifie National Institute of Standards and Technology. Il s'agit d'un laboratoire de normes de mesure et d'un organisme non réglementaire relevant du département du commerce des États-Unis. La mission du NIST est de promouvoir l'innovation et la compétitivité industrielle en faisant progresser la science des mesures, les normes et la technologie.</p>	<p>https://www.nist.gov/</p>
IEEE Institute of Electrical and Electronics Engineers	<p>L'IEEE, acronyme de l'Institute of Electrical and Electronics Engineers, est une organisation professionnelle internationale dédiée à l'avancement de la technologie dans les domaines de l'électricité, de l'électronique et de l'informatique. Fondée en 1963, l'IEEE compte des membres issus de diverses disciplines, notamment l'ingénierie électrique, l'informatique, les télécommunications, l'électronique, l'automatique,</p>	<p>https://www.ieee.org/</p>

	les sciences de l'information et bien d'autres.	
Estonian Centre for Standardisation and Accreditation	Le Centre estonien de normalisation et d'accréditation (Estonian Centre for Standardisation and Accreditation en anglais) est l'organisme national chargé de la normalisation, de l'accréditation et de la promotion de la qualité en Estonie. Il est responsable de l'élaboration et de la gestion des normes estoniennes dans différents domaines, ainsi que de la coordination des activités d'accréditation dans le pays.	https://www.evs.ee/en
Singapore Standards Council (SSC)	Le Singapore Standards Council (SSC) facilite le développement, la promotion et l'examen des normes de Singapour, des références techniques et des accords d'atelier à Singapour.	https://www.singaporestandardseshop.sg/Home/Index
BSI Group	BSI Group est un groupe institutionnel britannique d'organismes de services en normalisation, certification, formation et contrôle de conformité, opérant au Royaume-Uni sous charte royale en tant que société d'économie mixte à caractère commercial et industriel mais sans redistribution de profits. Le sigle BSI se réfère aux mots British Standards Institution, l'ancien nom d'une de ses branches jusqu'à la création du groupe, encore parfois utilisé au Royaume-Uni pour désigner l'institution entière.	https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/

Standards Australia	Standards Australia est l'organisme national de normalisation de l'Australie. Il s'agit d'une organisation à but non lucratif qui développe et publie des normes techniques dans divers secteurs industriels afin de promouvoir la sécurité, la qualité et l'efficacité des produits, des services et des processus.	https://www.standards.org.au/
ETSI	ETSI (European Telecommunications Standards Institute) est une organisation européenne de normalisation dans le domaine des télécommunications. Fondée en 1988, elle est chargée de développer des normes pour les réseaux et les services de télécommunications en Europe.	https://www.etsi.org/standards#Pre-defined%20Collections
IMDA (Infocomm Media Development Authority)	IMDA (Infocomm Media Development Authority) est l'autorité de développement des technologies de l'information et des médias à Singapour. Créeée en 2016, l'IMDA est chargée de promouvoir l'adoption et l'utilisation efficace des technologies de l'information et des médias pour stimuler la croissance économique, améliorer la qualité de vie des citoyens et renforcer le secteur des technologies de l'information et des communications (TIC) à Singapour.	https://www.imda.gov.sg/Business
Bureau of Indian Standards	Le Bureau of Indian Standards (BIS) est l'organisme national de normalisation de l'Inde. Il est responsable de l'élaboration, de la promotion et de la mise en œuvre de normes techniques dans différents domaines en Inde. Le BIS a été créé en 1986 en vertu de la loi BIS (Bureau of Indian Standards Act) pour harmoniser les normes et les spécifications techniques dans le pays.	https://www.services.bis.gov.in/php/BIS_2.0/eBIS/

CEN, the European Committee for Standardization	<p>Le Comité européen de normalisation est l'un des trois organismes européens de normalisation (avec le CENELEC et l'ETSI) qui ont été officiellement reconnus par l'Union européenne et par l'Association européenne de libre-échange (AELE) comme étant responsables du développement et de la définition des normes volontaires au niveau européen.</p>	<p>https://www.cencenelec.eu/about-cen/</p>
OGC Web Services (OWS)	<p>OGC (Open Geospatial Consortium) est une organisation internationale qui développe et promeut des standards ouverts pour l'interopérabilité des données géospatiales et des services associés. L'OGC travaille à la création et à la normalisation de spécifications techniques qui permettent aux différentes applications et systèmes de partager et d'intégrer facilement des données géospatiales.</p>	<p>https://www.ogc.org/standard/owc/</p>
Union Internationale des Télécommunications	<p>Agence des Nations Unies spécialisée dans les technologies de l'information et de la communication, dont le siège se trouve à Genève (Suisse). L'UIT est particulièrement impliqué dans la définition de standards technologiques.</p>	<p>https://www.itu.int/fr/Pages/default.aspx</p>

