REPUBLIQUE TUNISIENNE
MINISTERE DES TECHNOLOGIES DE LA COMMUNICATION

Référentiel de labélisation des fournisseurs de services d'informatique en nuage (N-Cloud et G-Cloud)

version 1.1 du 27 Décembre 2023

AGENCE NATIONALE DE LA CYBERSECURITE

VERSION	DATE	CRITERE DE DIFFUSION
1.1	27/12/2023	PUBLIC

VERSIONS DU REFERENTIEL

La présente version du référentiel est la version 1.1, ayant été examinée et validée par le comité de lecture sectoriel, instauré par décision ministérielle en date du 1er décembre 2023. Le tableau ci-dessous expose l'évolution chronologique des modifications et des différentes versions de ce document, qui demeure constamment accessible au grand public en vue de recueillir des commentaires pour contribuer d'une manière continue et participative à son amélioration.

DATE	VERSION	EVOLUTION DU DOCUMENT	AUTEUR
26/07/2023	1.0	Version initiale, non publiée et préparée par l'équipe de l'ANCS et soumise à un groupe d'experts pour lecture et amélioration.	ANCS
27/12/2023	1.1	Version publiée et adoptée pour le processus le labélisation N-Cloud et G-Cloud et ouverte pour commentaires en guise d'amélioration.	MTC/ANCS

NB : les commentaires sur le présent document doivent être adressés à l'Agence Nationale de la Cybersécurité à l'adresse électronique labelisation_cloud@ancs.tn ou à l'adresse postale 49 Avenue Jean Jaurès, 1000 Tunis, Tunisie.

CLASSIFICATION DU DOCUMENT

PUBLIC	X	INTERNE		CONFIDENTIEL		SECRET	

SOMMAIRE

1. Avant-propos

Dans le cadre de la stratégie digitale nationale 2025, la Tunisie a mis en place une stratégie nationale pour le Cloud, confiant à l'Agence Nationale de la Cybersécurité l'autorité de labéliser les fournisseurs de services d'hébergement. Les objectifs escomptés de ce nouveau framework de qualification est de :

— Encadrer les projets nationaux de cloudification et bien valoriser les ressources et les solutions basées sur le Cloud,
— Garantir la souveraineté numérique et mettre en œuvre sur le marché, une offre de Cloud souverain pour bien maitriser la localisation de l'hébergement et la dépendance technologique,
— Etendre d'une manière sécurisée le périmètre du Cloud national et du Cloud gouvernemental et améliorer la capacité ainsi que la qualité d'hébergement des applications et des services à l'échelle nationale.

D'une manière générale, les services d'informatique en nuage non qualifiés peuvent potentiellement accroitre l'exposition des clients à divers risques tels que la perte de données, l'indisponibilité des systèmes d'information, la compromission et la fuite d'informations confidentielles et sensibles. Pour toutes ces raisons, la mise en place d'un processus de labélisation va offrir aux consommateurs de services Cloud l'assurance des solutions recommandées par l'Etat dont le niveau de sécurité et la localisation d'hébergement ont été évalués de manière approfondie puis approuvés conformément à la réglementation en vigueur. Quant aux fournisseurs certifiés, la labélisation leur apporte davantage de clients, garantit leur capacité de prétendre à un marché en plein essor et leur offre la possibilité de se distinguer dans un domaine concurrentiel.

La politique de labellisation des fournisseurs de services informatiques en nuage est actuellement stipulée par le décret-loi n°17 de 2023 relatif à la cybersécurité et le présent référentiel présente les exigences minimales de la sécurité de l'information nécessaires pour évaluer et qualifier les prestataires de services d'hébergement et les fournisseurs de services d'informatiques en nuages ci-après nommés fournisseurs de services Cloud souhaitant loger des infrastructures, des plateformes ou des services informatiques pour le compte d'autrui. D'une part, la labélisation des fournisseurs de services Cloud est nécessaire pour instaurer un climat de confiance auprès des divers usagers et des diverses entreprises clientes, qu'elles soient publiques ou privées, souhaitant externaliser l'hébergement de leurs infrastructures, plateformes ou services informatiques. D'autre part, cette nouvelle orientation stratégique va renforcer davantage le partenariat public/privé dans le secteur du Cloud computing et contribuer au développement, d'une manière collaborative, du Cloud national et du Cloud gouvernemental nécessaires pour accélérer la transformation digitale en Tunisie.

2. Termes et définitions

Les termes et les définitions utilisés au niveau du présent référentiel ainsi que dans toute la documentation afférente au processus de labélisation des prestataires de services d'hébergement ou des fournisseurs de services d'informatique en nuage sont comme suit:

Nuage ou Cloud	:	Un centre de données accessible par des réseaux de télécommunications.
Centre de données ou Datacenter	:	Est l'ensemble des serveurs, des unités de stockage et des équipements réseau nécessaires pour héberger les plateformes électroniques, déployer les logiciels et stocker les données.
Informatique en nuage ou Cloud computing	:	Le modèle de transfert des ressources, du traitement et de transfert du stockage des données vers le Cloud, et ainsi que les modalités d'accès de l'usager à ces données à travers le réseau de télécommunications. Remarque : l'expression « informatique en nuage » utilisée au sein de ce référentiel ne sous-entend pas forcément l'usage de la virtualisation.
Cloud privé	:	Un environnement d'hébergement propriétaire, dédié à une seule entreprise et hébergé en interne ou en collocation chez un fournisseur de services d'hébergement.
Cloud public	:	Un environnement d'hébergement détenu et géré par un tiers fournisseur d'hébergement et mis à la disposition des clients.
Cloud hybride	:	Un environnement d'hébergement mixte dans lequel des applications s'exécutent en utilisant une combinaison de ressources de calcul, de stockage et de services de différents environnements Cloud privés et publics.
Cloud communautaire	:	Un environnement d'hébergement Cloud partagé entre plusieurs entreprises ayant des besoins opérationnelles communes et des exigences Cloud similaires en termes de qualité et de sécurité.
Fournisseur de services d'informatique en nuage	:	Prestataire de service Cloud offrant au moins un des services Cloud suivants : — Infrastructure en tant que service (IaaS) — Plateforme en tant que Service (PaaS) — Logiciel en tant que Service (SaaS)
Infrastructure en tant que service (IaaS) :	:	Modèle basé sur la fourniture d'un espace sécurisé et des ressources cloud essentielles et nécessaires pour héberger un centre de données.
Plateforme en tant que Service (PaaS)	:	Modèle basé sur la fourniture d'un environnement d'exploitation permettant au client du cloud d'héberger et de déployer ses applications informatiques.
Logiciel en tant que Service (SaaS)	:	Modèle basé sur la fourniture des applications informatiques au client du cloud à travers le réseau de télécommunication.
Labélisation	:	Processus de vérification des exigences par rapport aux stipulations de l'arrêté du ministre des technologies de la communication du 13 septembre 2023 et à un ensemble de référentiels adoptés par l'Agence Nationale de la Cybersécurité et selon une portée bien définie.
Commission de labélisation	:	Commission sectorielle technique qui examine les demandes de labélisation, de renouvellement et de retrait de labels des fournisseurs de services d'hébergement.
Portée de la labélisation	:	Périmètre choisi par le fournisseur soumissionnaire du dossier d'obtention du label et confirmé par la commission technique de labélisation. La portée de la labélisation couvre les possibilités suivantes : {IaaS, PaaS, SaaS} ou {IaaS,PaaS} ou {PaaS,SaaS} ou {IaaS} ou {PaaS} ou {SaaS}. Remarque : Dans le cas du SaaS, seules les applications auditées feront partie du périmètre de la labélisation et seront mentionnées dans le certificat du label attribué.

Fournisseur labélisé	:	Le prestataire de service d'hébergement ou fournisseur de service Cloud ayant obtenu le label N-Cloud ou G-Cloud après avoir justifié un haut niveau de compétence et de qualité de service en matière de cybersécurité.
Cloud souverain	:	Un modèle de déploiement et de fourniture de services Cloud dans lequel l'hébergement et l'ensemble des traitements effectués sur des données du Cloud sont physiquement réalisés dans les limites du territoire national tunisien et par une entité de droit tunisien, qualifié et qui respecte les lois en vigueur.
Client	:	L'entité commanditaire faisant appel à un fournisseur labélisé pour héberger une infrastructure en collocation ou pour se procurer des ressources et des services Cloud.
Exigence de labélisation	:	Un ensemble de mesures de sécurité à mettre en œuvre par le prestataire de service d'hébergement ou fournisseur de services Cloud.
Système d'information	:	Ensemble des ressources matérielles et immatérielles, outils et dispositifs isolés ou interconnectés, permettant la gestion de l'information et assurant les opérations de collecte, de stockage, de traitement, d'envoi de données.
Audit de sécurité du système d'information	:	Un processus méthodique, indépendant et documenté permettant d'évaluer un système d'information, d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits. L'audit de sécurité du système d'information comporte les éléments essentiels suivants : — Evaluation des aspects structurels, organisationnels et opérationnels de la sécurité des systèmes d'information, — Audit technique de la sécurité des composants du système d'information et test de leur immunité face aux incidents cybernétiques, — Analyse et évaluation des risques cybernétiques et présentation d'un plan de traitement afin d'éliminer ou de réduire le dégât des incidents cybernétiques. Remarque : l'audit de la sécurité du SI mentionné dans le présent référentiel doit être effectué par un auditeur accrédité et doit aboutir un rapport approuvé par l'Agence Nationale de la Cybersécurité.
Champ d'audit	:	Etendue d'un audit, le champ décrit généralement les lieux, les unités organisationnelles, les activités et les processus ainsi que la période couverte.
Critères d'audit	:	L'ensemble de politiques, procédures ou exigences déterminées par rapport auxquelles la conformité du système d'information est évaluée (la norme ISO/IEC 27002:2022 et la norme ISO/IEC 27017:2015).
Plan d'audit	:	Description des activités et des dispositions nécessaires pour réaliser un audit, préparée par le responsable de l'audit, en commun accord entre l'équipe de l'audit et l'audité pour faciliter la programmation dans le temps et la coordination des activités d'audit.
Preuve d'audit	:	Enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et qui sont vérifiables. Les preuves d'audit peuvent être qualitatives ou quantitatives et sont classées en quatre catégories : — Preuve physique sous forme de constatation ou observation — Preuve testimoniale sous forme de témoignage — Preuve documentaire sous forme de procédure, politique, rapport, compte rendu ou n'importe quel document de travail interne — Preuve analytique sous forme de calcul, déduction ou de comparaisons diverses
Constats d'audit	:	Résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit.

3. Modèles de déploiement du Cloud

Une variété de modèles de déploiement et d'acteurs de service Cloud est disponible sur le marché national. Le choix de la bonne solution dépend essentiellement de la nature des projets (dimensionnement, sensibilité, cible, …) et du budget alloué (Voir Figure 1).

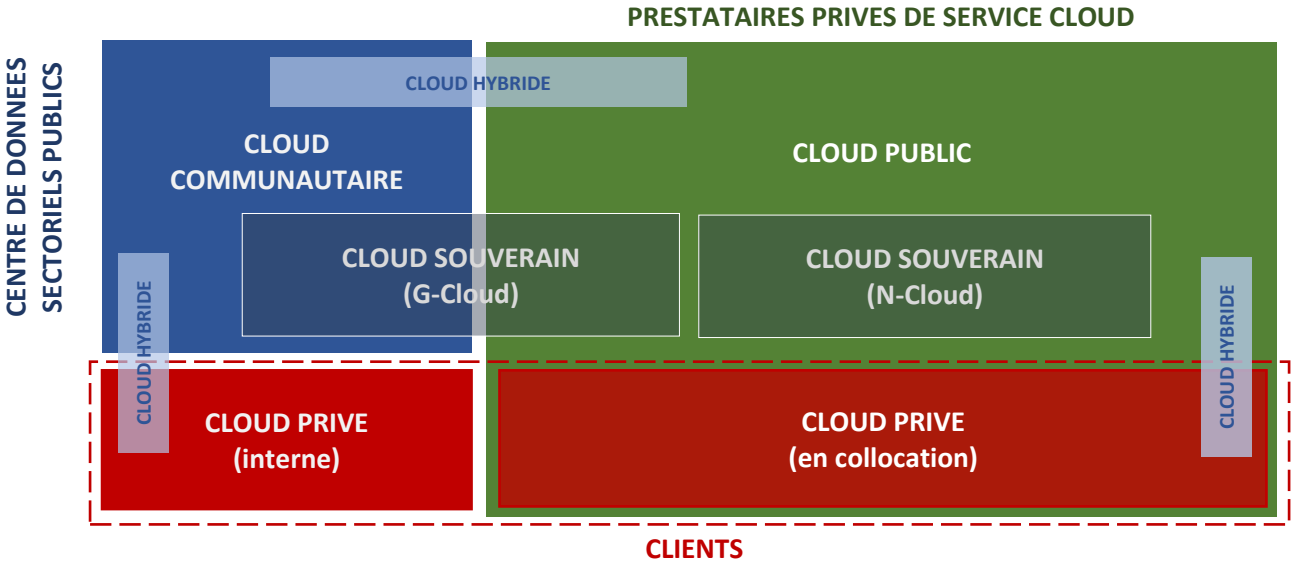

Figure 1. Cartographie des modèles de déploiement du Cloud

4. Objectif du document

Ce référentiel comprend la démarche et les modalités de labélisation des fournisseurs de service d'hébergement et des fournisseurs de services Cloud souhaitant obtenir les labels N-Cloud et G-Cloud conformément au décret-loi n°17 relatif à la cybersécurité. Il énonce les exigences de sécurité auxquelles doivent satisfaire les fournisseurs de services d'hébergement labélisés pour le maintien d'un système de gestion de la sécurité de l'information, de l'environnement d'hébergement soumis à l'évaluation pour l'obtention du label. La commission technique de labélisation doit se baser sur le présent référentiel pour qualifier les fournisseurs et émettre son avis par rapport à l'octroi des labels, et ceci conformément à l'arrêté du ministre des technologies de la communication du 13 septembre 2023, fixant les procédures et les conditions d'octroi, de renouvellement et de retrait du label « Fournisseur de services informatiques en nuage gouvernemental (G-Cloud) » et du label « Fournisseur de services informatiques en nuage national (N-Cloud). Ce référentiel comprend également les exigences que l'expert auditeur accrédité doit vérifier lors de la mission d'audit de sécurité réglementaire propre aux prestataires de services d'hébergement ou fournisseurs de services Cloud, et ceci conformément à l'arrêté du ministre des technologies de la communication du 12 septembre 2023, fixant les critères techniques d'audit de sécurité des systèmes d'information et les modalités de suivi de la mise en œuvre des recommandations contenues dans son rapport d'audit.

5. Public cible

Le présent référentiel est un document de référence destiné pour :

— Les membres de la commission sectorielle technique en charge de l'étude des dossiers soumis pour l'obtention du Label N-Cloud ou G-Cloud, afin de les guider dans le processus de labélisation des fournisseurs.
— Les experts auditeurs qui réalisent les missions d'audit, afin de les accompagner à conduire la mission conformément aux exigences applicables aux prestataires de services d'hébergement ou fournisseurs de services Cloud.
— Les fournisseurs de service d'hébergement ou audités ou encore soumissionnaires des dossiers de labélisation, pour bien se préparer à l'audit et/ou au processus de la qualification pour l'obtention du label.
— Les clients qui souhaitent connaitre les garanties de la qualité de l'hébergement et les exigences de sécurité respectées par les fournisseurs labélisés et à qui les données, les applications ou les infrastructures sont confiées.
— Les professionnels du métier (formateur, expert, consultant, etc) pour connaitre les normes et les bonnes pratiques applicables aux prestataires de services d'hébergement et fournisseurs de services Cloud labélisés à l'échelle nationale.

6. Domaine d'application

Ce document constitue le référentiel de l'ensemble des normes et des exigences applicables à un prestataire de services d'hébergement ou fournisseur de services Cloud, ci-après dénommé le « fournisseur labélisé ». Le fournisseur labélisé est tout prestataire de service d'hébergement ou fournisseur de service Cloud, de droit tunisien, appartenant au secteur public ou privé, ayant obtenu le label de « Fournisseur de services informatiques en nuage gouvernemental (G-Cloud) » et/ou le label de « Fournisseur de services informatiques en nuage national (N-Cloud) » et ce conformément à la réglementation en vigueur.

Le présent document est aussi une référence pour le client qui souhaite faire appel à un fournisseur labélisé pour héberger une infrastructure en collocation ou pour se procurer des ressources et des services Cloud pour son système ou environnement d'hébergement principal ou de réplication, et ceci sur le territoire Tunisien. Le domaine d'application de ce référentiel concerne les services Cloud suivants :

1. **Infrastructure en tant que service (IaaS)**

   La mise des ressources de stockage, de calcul et de réseau à la disposition du client. Le modèle IaaS permet au client de louer un accès à une infrastructure externalisée, virtuelle, extensible et évolutive. Le client ne se soucie plus de la mise en place et de la maintenance de l'infrastructure physique et garde généralement le contrôle et la

gestion des systèmes d'exploitation, des applications métier et du stockage des données. Dans ce cas de figure, le fournisseur de service IaaS sera évalué, lors du processus de la labélisation, sur la gestion de l'infrastructure physique ainsi que les services supplémentaires offerts au client tels que la journalisation, la supervision, la résilience de stockage et la sécurité.

Dans ce modèle de service Cloud, le client pourrait également héberger du matériel en colocation en mode mutualisé ou privatif et sera responsable de son installation et de sa maintenance. Dans ce cas, le fournisseur de service de colocation sera évalué, lors du processus de la labélisation, sur la gestion de l'infrastructure de base et les diverses servitudes englobant l'alimentation d'électricité, la climatisation, la surveillance et le contrôle d'accès physique, l'accès Internet et la haute disponibilité de cet environnement de colocation.

2. **Plateforme en tant que Service (PaaS)**

   La mise de la plateforme logicielle à la disposition du client. Le modèle PaaS permet au client de gérer généralement la plateforme logicielle et ses propres applications sans se soucier de l'installation et de l'entretien de l'infrastructure physique et logique. Dans ce cas, le fournisseur de service PaaS sera évalué, lors du processus de la labélisation, sur son rôle lié à la gestion de l'infrastructure physique comme le cas des fournisseurs IaaS et sera également évalué sur son rôle de gestion de l'infrastructure logique lié à la maintenance des serveurs, aux mises à jour du logiciel de l'infrastructure et lié à la configuration de la plateforme mise à la disposition des clients pour la gestion de leurs applications métier.

3. **Logiciel en tant que Service (SaaS)**

   La mise de l'application, ainsi que la plateforme sur laquelle l'application s'exécute, en plus de l'infrastructure sous-jacente à la plateforme, à la disposition du client. Le modèle SaaS est un modèle d'exploitation commerciale et de distribution des logiciels à travers le Cloud. Ce modèle permet uniquement au client d'effectuer quelques paramétrages métier dans l'application Cloud mise à sa disposition sous forme d'abonnement.

   Dans ce cas, le fournisseur de service SaaS sera évalué, lors du processus de la labélisation, sur son rôle lié à la gestion de l'infrastructure physique et logique, de la plateforme et des applications mises à la disposition des clients et le label dans ce cas sera uniquement pour les applications auditées.

   Remarque : si le fournisseur de service d'hébergement ou Cloud sous-traite une ou plusieurs parties de son activité à des prestataires d'hébergement tiers alors ceux-ci doivent être qualifiés sinon ils feront aussi l'objet d'évaluation. La qualification pour attribution de labels est faite selon le modèle de répartition des responsabilités entre le client et les divers prestataires.

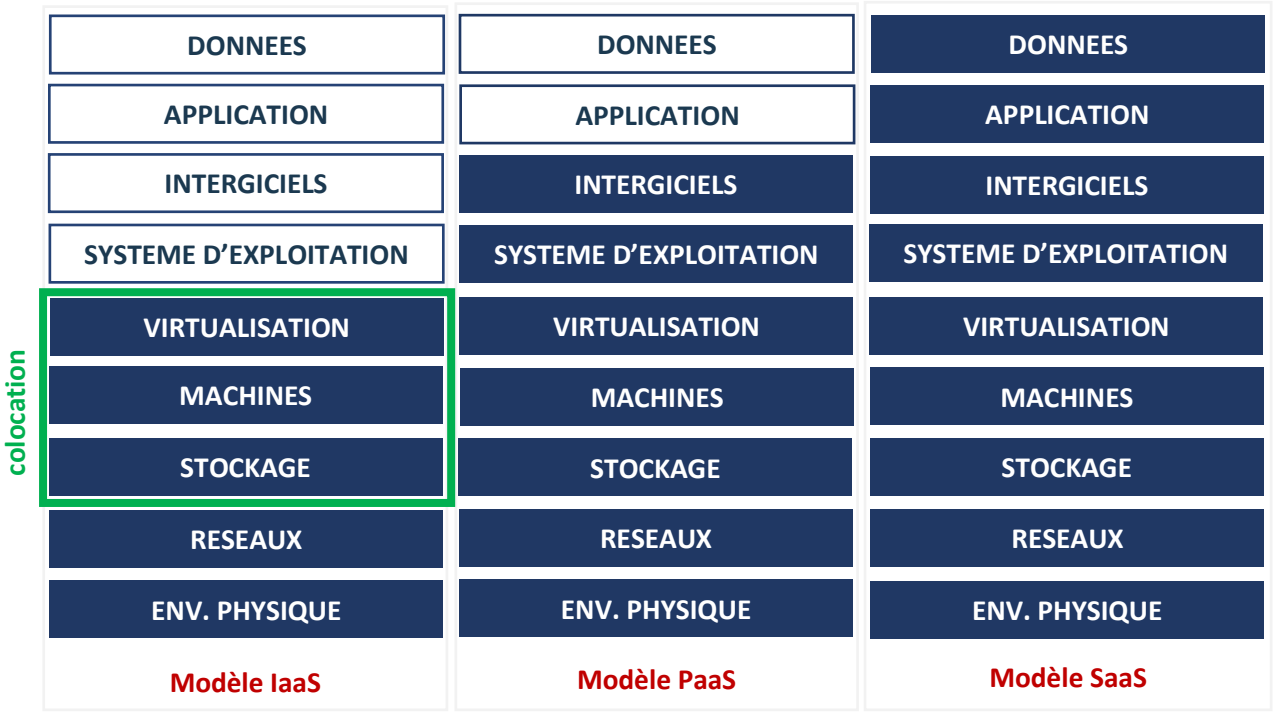

Figure 2. Périmètre du processus de la labélisation pour l'obtention du Label N-Cloud ou G-Cloud (en bleu)

7. Modalités de la labélisation

Les demandes d'obtention du label G-Cloud et N-Cloud et les demandes de renouvellement doivent être déposées auprès de l'Agence Nationale de la Cybersécurité par lettre recommandée ou par voie électronique avec un accusé de réception ou directement à l'agence sous pli fermé contre récépissé de dépôt.

Le dossier de la demande de labélisation doit obligatoirement inclure :

— Une fiche signalétique contenant des informations sur les centres de données principaux et de secours dont il est propriétaire et la nature des services de cloud qu'il fournit,
— Une copie du registre de commerce,
— Une copie des certificats de conformité en cybersécurité et de continuité d'activité ou du rapport d'audit de sécurité des systèmes d'information approuvé par l'Agence Nationale de la Cybersécurité datant de moins de douze mois,
— Les modèles des contrats de services qui seront adoptés dans la fourniture des services cloud,
— Une liste des prestataires auxquels sont sous-traités la réalisation d'une partie des tâches,
— Une copie du contrat de raccordement au réseau national intégré de l'administration concernant le demandeur du label « Fournisseur de services informatiques en nuage gouvernemental (G-cloud) ».

L'examen des dossiers de labélisation est assuré par une commission de labélisation présidée par le directeur général de l'Agence Nationale de la Cybersécurité ou son délégué. L'Agence Nationale de la Cybersécurité accorde le label N-Cloud ou G-Cloud sur la base de la décision de la ladite commission selon la démarche suivante :

1. Vérification de la complétude du dossier présenté pour l'obtention du label N-Cloud ou G-Cloud selon la réglementation en vigueur (Voir Annexe A).
2. Vérification des preuves présentées attestant la conformité du fournisseur aux exigences du référentiel (certifications de conformité, rapports d'audit, etc).
3. Vérification du périmètre de la labélisation de tous les prestataires de services Cloud invoqués au niveau du dossier et concernés par ce périmètre.
4. Emission de la décision d'octroi du label N-Cloud ou G-Cloud en précisant la portée du label et les éventuelles restrictions. Il est possible de rajouter à la décision des recommandations à titre de bonnes pratiques. Dans ce cas, ces recommandations ne font pas l'objet de vérification pour l'obtention du label. Dans le cas échéant, la commission technique présente la cause du refus au niveau de ladite décision.
5. Accord du label N-Cloud ou G-Cloud par l'Agence Nationale de la Cybersécurité sur la base de la décision favorable de la commission dans un délai n'excédant pas un mois à compter de la date de la réunion de la commission de labélisation. La labélisation accordée reste valable pour une durée d'un an.

8. Exigences de la labélisation

Les exigences de la labélisation (Voir Annexe B) doivent être respectées par le prestataire d'hébergement ou le fournisseur de service Cloud souhaitant obtenir et maintenir le label N-Cloud ou G-Cloud. Dans le dossier présenté pour l'obtention du label, le fournisseur peut soit présenter les certifications de conformité valides prouvant le respect des exigences de sécurité requises pour l'obtention des labels, soit un rapport d'audit de sécurité réglementaire élaboré selon le présent référentiel, par un auditeur accrédité par l'Agence Nationale de la Cybersécurité et ne dépassant pas la période d'un an.

Le fournisseur doit exiger des prestataires tiers, participant à la mise en œuvre de ses services (IaaS, PaaS ou SaaS), le respect des exigences et l'assurance d'un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il est fortement recommandé d'avoir les exigences de la labélisation dans les clauses des contrats et des accords conclus avec tous les tiers qui contribuent dans la fourniture des services sujet de la labélisation. Le dossier présenté pour l'obtention du label N-Cloud ou G-Cloud doit inclure les preuves de la qualification ou de la conformité des tiers à la pyramide des exigences de sécurité requises comme présenté au niveau de la figure 3.

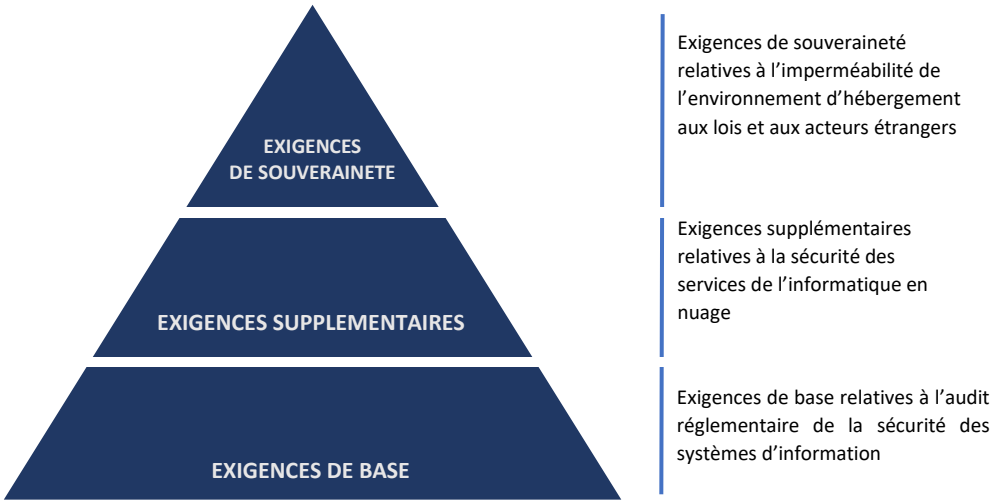

Figure 3. Pyramide des exigences applicables aux fournisseurs de services d'informatique en nuage souhaitant obtenir les labels N-Cloud et G-Cloud

9. Retrait du label N-Cloud ou G-Cloud

Les décisions de retrait du label N-Cloud ou G-Cloud sont prises par la commission sectorielle technique en cas de :

— Manquement aux obligations requises pour la labélisation de fournisseur de service Cloud gouvernemental et/ou national,
— Demande d'annulation déposée par le fournisseur d'une manière volontaire, et ce à cause d'un changement majeur dans sa politique d'hébergement qui n'est plus conforme avec les exigences du label obtenu.

Le non-respect aux obligations peut être constaté lors d'une mission d'audit sur site ou par suite d'une réclamation fondée d'un client ou d'un tiers, déposé contre un prestataire labélisé. Le manquement observé doit faire l'objet d'examen par la commission sectorielle technique afin de :

— Confirmer que le constat concerne le service labélisé
— Faire l'appréciation du constat (niveau gravité, impact, etc)
— Emettre la décision par rapport au retrait définitif du label

10. Points d'attention

— Un environnement de Cloud hybride ou encore multicloud ne peut pas être labélisé comme étant un seul environnement et ne donne pas au(x) prestataire(s) concerné(s) le droit à la qualification pour l'obtention d'un label pour la totalité de l'environnement. Dans le cas du Cloud hybride, chaque partie doit être évaluée séparément.
— En l'absence des certifications nécessaires pour l'éligibilité à la labélisation des fournisseurs d'hébergement, un audit de sécurité selon le présent référentiel doit être assuré par un expert auditeur accrédité par l'Agence Nationale de la Cybersécurité.

- La labélisation accordée aux prestataires d'hébergement ne garantit pas le respect de certains textes juridiques spécifiques tels que les codes relatifs à la télémédecine, au télétravail et autres. Tout besoin spécifique doit faire l'objet d'une mission d'évaluation dédiée.
- Les fournisseurs labélisés conservent la faculté de fournir leurs services en dehors du périmètre pour lequel ils sont qualifiés, mais ne peuvent se prévaloir de la labélisation obtenue sur ces services. Les prestations additionnelles fournies au client autres que l'hébergement tels que le développement, le conseil, la formation et autres, ne font pas partie de la portée de la labélisation et n'entrainent pas la perte du bénéfice de la labélisation, qui est obtenu uniquement sur la fourniture du service d'hébergement.
- Le client peut exiger la labélisation N-Cloud ou G-Cloud lors de l'achat d'un service Cloud (appel d'offres ou autres) et stipuler dans le contrat de service ou convention que la prestation réalisée soit une prestation labélisée et que le fournisseur doit s'engager à maintenir la labélisation souhaitée.
- Les références normatives présentées au niveau du présent document étaient la source de base pour l'élaboration des exigences de sécurité nécessaires pour mener une mission d'audit de sécurité pour les fournisseurs de services d'informatique en nuage : exigences de base, supplémentaires et de souveraineté. Le présent référentiel va évoluer dans le temps en fonction de l'évolution de ces normes. La référence documentaire servira également à la commission technique pour savoir la liste des certifications et des classifications à considérer pour l'attribution des labels.

11. Référencement des fournisseurs labélisés

L'Agence Nationale de la Cybersécurité publie périodiquement, au niveau de son site officiel, la liste des fournisseurs labélisés ainsi que la référence du label, le type et la période de validité accordée, dans l'objectif de mieux orienter les clients vers l'achat de services Cloud labélisés. La liste des labels expirés ou retirés sera également mise en ligne à titre indicatif.

12. Certificat de labélisation

Le certificat du label N-Cloud ou G-Cloud attribué aux fournisseurs de services cloud comprend :

- La raison sociale du fournisseur du service cloud ayant obtenu le label,
- Le type du label attribué (N-Cloud ou G-Cloud),
- La date de délivrance et la durée de validité du certificat de labélisation,
- Identifiant unique du certificat de labélisation attribué,
- Le cachet électronique visuel (TN CEV 2D-Doc) protégeant le document conformément à la législation en vigueur.

13. Règles d'usage de la marque de labélisation

Les marques de labélisation N-Cloud et G-Cloud sont représentées en langue Arabe et Français comme suite :

Labels en Français **Labels en Arabe**

Bleu : #063C5E
Blanc : #FFFFFF

Rouge : #CE1E28
Blanc : #FFFFFF

Bleu : #063C5E
Blanc : #FFFFFF

Rouge : #CE1E28
Blanc : #FFFFFF

L'entité labélisée devra respecter tous les éléments de la charte graphique du label N-Cloud ou G-Cloud. L'usage de la marque, telle que présentée ci-dessus, est réservée à l'Agence Nationale de la Cybersécurité et au fournisseur labélisé qui peut reproduire cette identité visuelle sur tous ses supports de communication, documents administratifs, commerciaux et promotionnels, brochures ou publicités, y compris sur le papier à en-tête, sites internet et en signature de courriers électroniques.

14. Références documentaires

Le référentiel adopté pour la labélisation des fournisseurs de services d'hébergement ou de services Cloud se base sur la législation en vigueur et l'ensemble des normes et standards suivants :

— Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
— Loi n°2000-83 du 9 aout 2000, relative aux échanges et au commerce électronique
— Décret-Loi n°2023-17 du 11 Mars 2023, relatif à cybersécurité
— Arrêté du ministre des technologies de la communication du 13 septembre 2023, fixant les procédures et les conditions d'octroi, de renouvellement et de retrait du label « Fournisseur de services informatiques en nuage gouvernemental (G-cloud) » et du label « Fournisseur de services informatiques en nuage national (N-cloud)
— Arrêté du ministre des technologies de la communication du 12 septembre 2023, fixant les critères techniques d'audit de sécurité des systèmes d'information et les modalités de suivi de la mise en œuvre des recommandations contenues dans son rapport d'audit
— Circulaire du président du gouvernement n°24 du 5 novembre 2020, portant sur le renforcement des mesures de sécurité informatique dans les structures administratives

- La norme ISO 18045:2022 relative aux critères d'évaluation pour la sécurité des technologies de l'information
- La norme ISO 19011:2018 relative aux lignes directrices pour l'audit des systèmes de management
- La norme ISO 22301:2019 relative aux systèmes de management de la continuité d'activité
- La norme ISO/IEC 27001:2022 relative aux systèmes de management de la sécurité de l'information
- La norme ISO/IEC 27002:2022 relative aux mesures de sécurité de l'information
- La norme ISO/IEC 27017:2015 relative au code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage
- La norme ISO/IEC 27005:2022 relative à la gestion du risque en sécurité de l'information
- La norme ISO/IEC 22123:2023 relative à l'informatique en nuage – partie 1, 2 et 3 vocabulaire, concepts, architecture de référence
- Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA), version 4
- Classification TIER 1, 2, 3 et 4 des datacenters de l'Uptime Institute

15. Conclusion

La Tunisie dispose actuellement d'un large tissu d'entreprises locales et de startups, exprimant une demande croissante pour des services Cloud. Cependant, pour répondre efficacement à ces besoins, il est impératif de développer un marché de datacenters à la fois vaste et mature, soutenu par une politique de labélisation rigoureuse mise en place par l'État. Cette démarche est essentielle afin d'assurer la qualité et la souveraineté des services Cloud proposés.

Bien que la certification des fournisseurs de services Cloud soit actuellement facultative, il est recommandé aux entreprises publiques et privées d'exiger ce label lors de l'acquisition de services d'hébergement. Cette exigence s'avère cruciale tant pour garantir la performance, la qualité ainsi que la sécurité, avec une assurance supplémentaire assurée par l'État. En conséquence, la mise en place d'une politique de labélisation efficace devrait être encouragée, promouvant ainsi les standards d'excellence dans le domaine du Cloud en Tunisie.

ANNEXE A – DOSSIER DE LA DEMANDE DE LABELISATION

L'Agence Nationale de la Cybersécurité attribue le label « Fournisseur de services informatiques en nuage national (N-Cloud) » ou le label « Fournisseur de services informatiques en nuage gouvernemental (G-Cloud) » à tout prestataire de services d'hébergement tunisien appartenant au secteur public ou privé qui remplit les conditions suivantes :

— Doit fournir au moins un des services informatiques en nuage IaaS, PaaS et SaaS,
— Doit fournir et utiliser des centres de données principaux et de secours situés sur le territoire tunisien,
— Doit être conforme aux normes internationales dans le domaine de la cybersécurité et de la continuité d'activité conformément au référentiel élaboré par l'ANCS,
— Doit être en mesure d'assurer le service de support et d'assistance technique 24/7 au profit des structures bénéficiaires des services cloud,
— Pour le label G-Cloud, le fournisseur de service d'hébergement doit être impérativement relié au réseau national intégré de l'administration et à la plateforme nationale d'interopérabilité.

Le dossier de la demande de labélisation doit obligatoirement inclure :

— Une fiche signalétique contenant des informations sur les centres de données principaux et de secours dont il est propriétaire et la nature des services de cloud qu'il fournit,
— Une copie du registre de commerce,
— Une copie des certificats de conformité en cybersécurité et de continuité d'activité ou du rapport d'audit de sécurité des systèmes d'information approuvé par l'Agence Nationale de la Cybersécurité datant de moins de douze mois,
— Les modèles des contrats de services qui seront adoptés dans la fourniture des services cloud,
— Une liste des prestataires auxquels sont sous-traités la réalisation d'une partie des tâches,
— Une copie du contrat de raccordement au réseau national intégré de l'administration concernant le demandeur du label « Fournisseur de services informatiques en nuage gouvernemental (G-cloud) ».

FICHE SIGNALETIQUE

Fournisseur de services d'informatique en nuage
(N-Cloud ou G-Cloud)

1 Renseignements généraux du fournisseur

1.1 Identité de la société

Raison Sociale :	.....	Sigle :	.....
Secteur d'Activité :	.....	Identifiant Fiscal :	.....
Date de Création :	.....	Jort n° :	du : .....
Registre du Commerce :	.....		

1.2 Identité du représentant juridique

Nom et Prénom :	.....	Nationalité :	.....
Date/Lieu Naissance :	.....	Fonction :	.....
CIN n° :	.....	Délivrée le :	.....
E-Mail :	.....	Tél :	.....

1.3 Coordonnées de la société

Adresse :	.....		
Tél :	.....	E-Mail :	.....
Site Web :	.....		

2 Renseignements techniques du fournisseur

2.1 Label demandé

☐	N-Cloud
☐	G-Cloud

2.2 Services offerts (portée du label)

☐	Infrastructure en tant que Service (IaaS) (collocation incluse)
☐	Plateforme en tant que service (PaaS)
☐	Logiciel en tant que service (SaaS)

2.3 Certifications en cybersécurité et continuité d'activité

Certification	Date d'obtention	Date d'échéance

2.4 Rapports d'audit de sécurité de l'information pour les services Cloud

Période de l'audit	Date d'approbation du rapport de l'audit par l'ANCS

2.5 Lieu d'hébergement

Centre de données	**Propriété du centre**	**Type** (Principal/Secours)	**Classification** (Tier 1-4, non-classifié,…)

2.6 Liste des prestataires

Prestataire (Raison sociale)	**Type de la prestation** (Hébergement, Sous-traitance technique, commerciale, assistance, …)	**Contrat** (Type (service, maintenance, …), Date de signature, Durée, …)

2.7 Service support pour les clients

Numéro d'appel :	……
Adresse électronique :	……
Formulaire Web :	……
Autres :	……

Je soussigné certifie sur l'honneur l'exactitude des renseignements fournis dans cette demande de labélisation.

Date et Signature / Cachet du Premier Responsable

ANNEXE B – Exigences de sécurité applicables aux fournisseurs labélisés

En plus des exigences définies dans le référentiel de l'audit réglementaire de la sécurité des systèmes d'information publié par l'Agence Nationale de la Cybersécurité, il faut considérer l'ensemble des exigences supplémentaires de mise en œuvre spécifiques aux services de nuage listées au niveau du tableau ci-dessous :

ID ANCS	Réf (ISO 27002/ ISO 27017)	Titre de la mesure de sécurité de l'information	Vérifications à effectuer	Moyens de vérification supplémentaires (sans s'y limiter)	Preuves
	5	**Mesures de sécurité organisationnelles**			
MS-01	5.1	Politiques de sécurité de l'information	• Si la politique de sécurité de l'information du fournisseur de services en nuage est renforcée afin de traiter la fourniture et l'utilisation de ses services en nuage	• Revue des documents de la PSI relative au service et des politiques spécifiques • Entretien avec le DG • Interviews d'un échantillon des utilisateurs • Revue des PVs de réunion du comité de sécurité	• Document de PSI relative au service approuvé par la DG • Documents de politiques spécifiques approuvés par le niveau de direction approprié • Historique des mises à jour de PSI et des politiques spécifiques • PV de réunion du comité de sécurité sur la màj de la PSI
MS-02	5.2	Fonctions et responsabilités liées à la sécurité de l'information	• S'il existe un document de répartition appropriée des rôles et des responsabilités en matière de sécurité de l'information concernant les clients et les prestataires contribuant à la fourniture des services en nuage • S'il y a une désignation du responsable de la sécurité des systèmes d'information et d'un responsable de la sécurité physique	• Revue de l'organigramme, des fiches de poste, des décisions et notes internes en relation avec la sécurité du SI • Entretien avec le DG • Interview du RSI (le cas échéant) • Revue des responsabilités et des fonctions en matière de sécurité dans le cadre du contrat de services en nuage	• Décision de nomination du RSI (conformément au circulaire n° 24 de 2020) et du responsable de la sécurité physique • Décision de mise en place du comité de sécurité • PVs de réunions du comité, • Fiches de poste • Contrat de services en nuage

MS-03	CLD.6.3.1	Partage des rôles et des responsabilités dans un environnement d'informatique en nuage	• Si le fournisseur de services en nuage documente et communique ses aptitudes, rôles et responsabilités en matière de sécurité de l'information pour l'utilisation de son service en nuage, ainsi que les rôles et responsabilités en matière de sécurité de l'information que le client du service en nuage devrait mettre en œuvre dans le cadre de son utilisation du service en nuage	• Revue des responsabilités et des fonctions en matière de sécurité dans le cadre du contrat de services en nuage	• Fiches de poste • Contrats de services en nuage
MS-04	5.4	Responsabilités de la direction	• Si les rôles et les responsabilités en matière de sécurité de l'information avec le personnel, les clients de services en nuage, les prestataires de services en nuage et les sous-traitants sont définis et revus régulièrement	• Revue de la note interne signée par le DG • Revue d'un échantillon de contrats avec les sous-traitants • Entretien avec le DG • Interview du DRH et du DAF	• Notes interne signée par le DG • Echantillons des contrats avec les sous-traitants comportant l'engagement pour appliquer les exigences de sécurité conformément aux politiques et aux procédures
MS-05	5.5	Contacts avec les autorités	• Si le fournisseur a informé le client des emplacements géographiques des centres de données (principal et secours)	• Revue des lieux d'hébergement et de la liste des emplacements géographiques des centres de données (principal et secours)	• Liste des emplacements géographiques des centres de données

MS-06	5.8	Sécurité de l'information dans la gestion de projet	• Si le fournisseur de services en nuage fournit des informations aux clients de services en nuage concernant les aptitudes en matière de sécurité de l'information qu'il utilise • Si ces informations de sécurité fournies sont informatives et ne contiennent pas des informations qui pourraient être utiles à une personne mal intentionnée • S'il existe un document pour une estimation des risques préalablement à tout projet pouvant avoir un impact sur le service, et ce quelle que soit la nature du projet	• Revue des informations fournies aux clients des services en nuage • Revue des SLA signés • Revue du document pour une estimation des risques	• SLA signés • Document pour une estimation des risques
MS-07	5.9	Inventaire des informations et autres actifs associés	• Si un inventaire ou registre des actifs du fournisseur de services en nuage est maintenu et si les données du client ainsi que les données obtenues à partir des services en nuage sont identifiés de manière explicite • Si le fournisseur s'assure de la validité des licences des logiciels tout au long de la prestation	• Revue de la PSI pour l'identification des règles relatives à l'inventaire • Revue des procédures d'inventaire des actifs • Revue de l'inventaire et vérification de son exhaustivité • Vérification de l'existence du nom du propriétaire pour les informations et autres actifs associés identifiés • Interviews du DAF et du DSI	• PSI • Procédures d'inventaire • Inventaire des informations et autres actifs associés

MS-08	CLD.8.1.5	Retrait des mesures relatives aux actifs du client de services d'informatique en nuage	• Si le fournisseur de services en nuage fournit des informations concernant les dispositions de restitution et de retrait des actifs du client de services en nuage au terme du contrat d'utilisation d'un service en nuage • Si les dispositions relatives à la restitution et au retrait des actifs sont documentées dans le contrat et appliquées en temps utile • Si les dispositions spécifient les actifs à restituer et à retirer	• Revue de la PSI pour l'identification des règles relatives à la restitution des actifs • Revue des procédures de restitution des actifs • Revue de l'inventaire et vérification de son exhaustivité • Interview du DAF • Interview du DSI	• PSI • Procédures de restitution des actifs • Inventaire des informations et autres actifs associés
MS-09	5.13	Marquage des informations	• Si des procédures pour le marquage de l'information sont élaborées et mises en œuvre conformément au plan de classification adopté par le fournisseur de services en nuage qui devrait documenter et divulguer toute fonctionnalité de service qu'il fournit permettant aux clients de services en nuage de classer et d'étiqueter leurs informations et actifs associés.	• Revue des procédures de marquage de l'information • Interview des responsables métier • Vérification de marquage sur un échantillon de documents • Revue des applications de services en nuage qui fournissent des fonctions de gestion de l'information en ajoutant des données issues de services en nuage aux données des clients de ces services	• Procédures de marquage des informations • Echantillon de documents • Imprimes écran des applications dédiées pour la gestion de l'information

MS-10	5.16	Gestion des identités	• Si le fournisseur de services en nuage fournit au client de services en nuage des fonctions de gestion des identités des utilisateurs finaux, ainsi que des spécifications pour l'utilisation de ces fonctions afin de gérer l'accès aux services en nuage	• Revue de l'accord signé entre le fournisseur de services en nuage et un échantillon des clients de services en nuage • Vérification au niveau des technologies d'identification des tiers et de gestion d'accès pour les services en nuage et les interfaces d'administration associées	• Accord signé entre le fournisseur de services en nuage et un échantillon des clients de services en nuage • Imprimes écran
MS-11	5.17	Informations d'authentification	• Si le fournisseur de services en nuage fournit des informations sur la procédure de gestion des informations d'authentification secrètes du client de services en nuage, y compris l'attribution de ces informations et l'authentification des utilisateurs finaux	• Revue de la procédure de gestion du fournisseur de services en nuage des informations d'authentification secrètes des clients • Entretien avec le RSI • Vérification des preuves de communication de la procédure	• Procédure de gestion du fournisseur de services en nuage des informations d'authentification secrètes des clients de services en nuage • Preuves de communication de la procédure
MS-12	5.18	Droits d'accès	• Si le fournisseur de services en nuage fournit des fonctions permettant la gestion des droits d'accès des utilisateurs du client de services en nuage, ainsi que des spécifications pour l'utilisation de ces fonctions	• Revue de l'accord signé entre le fournisseur de services en nuage et un échantillon des clients de services en nuage • Vérification au niveau des technologies d'identification des tiers et de gestion d'accès pour les services en nuage et les interfaces d'administration associées	• Accord signé entre le fournisseur de services en nuage et le client de services en nuage • Imprimes écran

			• Si le fournisseur de services en nuage prend en charge les technologies d'identification des tiers et de gestion d'accès pour ses services en nuage et les interfaces d'administration associées afin de faciliter l'intégration et l'administration de l'identité des utilisateurs entre les systèmes du client et le service en nuage avec la facilité d'utilisation de plusieurs services en nuage (via l'authentification unique (SSO) par exemple)		
MS-13	5.20	La sécurité de l'information dans les accords conclus avec les fournisseurs	• Si les mesures de sécurité de l'information qu'offre le fournisseur de services d'informatique en nuage sont spécifiées dans le cadre d'un accord avec le client de services en nuage • Si les mesures de sécurité de l'information spécifiées dans le cadre d'un accord avec le client de services en nuage sont mises en œuvre	• Revue d'un échantillon d'accords formels ou de contrats avec les clients de services en nuage • Vérification d'un échantillon de la mise en œuvre des mesures de sécurité de l'information spécifiées dans le cadre d'un accord avec le client de services en nuage	• Echantillon d'accords formels ou de contrats avec les clients de services en nuage • Liste des mesures de sécurité de l'information spécifiques à chaque type de service en nuage

MS-14	5.21	Gestion de la sécurité de l'information dans la chaîne	• Si le fournisseur de services en nuage fournit des objectifs de sécurité de l'information aux fournisseurs, lors de la fourniture de services en nuage basés sur une chaîne d'approvisionnement • Si le fournisseur de services en nuage met des obligations aux fournisseurs pour mener des activités de gestion des risques pour atteindre ces objectifs	• Revue des contrats avec les autres fournisseurs de services en nuage • Revue des objectifs de sécurité de l'information demandés aux autres fournisseurs de services en nuage • Revue des clauses relatives aux activités de gestion des risques dans les contrats avec fournisseurs de services en nuage	• Les contrats avec les autres fournisseurs de services en nuage • Document des objectifs de sécurité de l'information demandé aux autres fournisseurs de services en nuage
MS-15	5.24	Planification et préparation de la gestion des incidents de sécurité de l'information	• Si le fournisseur de services en nuage définit la répartition des responsabilités et des procédures en matière de gestion des incidents de sécurité de l'information entre le client et le fournisseur services en nuage • Si le fournisseur de services en nuage fournit un document qui contient : o l'étendue des incidents de sécurité de l'information o le niveau de divulgation de détection des incidents de sécurité de l'information et les réponses associées	• Revue de la procédure en matière de gestion des incidents et la répartition des responsabilités • Revue des documents qui contiennent les informations sur l'incident	• Procédures de gestion des incidents • Echantillon de fiches d'incidents

			○ Le délai cible dans lequel les notifications d'incident de l'information auront lieu ○ La procédure de notification des incidents ○ Les coordonnées des personnes à contacter pour le traitement des questions relatives aux incidents ○ Les recours possibles en cas de survenance de certains incidents		
MS-16	5.28	Recueil de preuves	• Si des procédures convenues entre le fournisseur de services en nuage et le client sont établies pour répondre aux demandes de preuves numériques potentielles ou d'autres informations provenant de l'environnement d'informatique en nuage	• Revue de la procédure d'identification, de collecte et de protection de l'information pouvant servir de preuve • Revue d'un échantillon de preuves • Interview du DSI, du RSI et du DRH	• Procédure d'identification, de collecte et de protection de l'information pouvant servir de preuve • Echantillon de preuves
MS-17	5.31	Exigences légales, statutaires, réglementaires et contractuelles	• Si le fournisseur de services en nuage informe le client des juridictions légales qui régissent le service en nuage • Si le fournisseur de service en nuage informe le client sur ses propres exigences légales pertinentes	• Revue des documents relatifs aux exigences réglementaires, contractuelles, et légales • Revue du document des mesures spécifiques et des responsabilités individuelles mises en place pour répondre à ces exigences	• Documents relatifs aux exigences réglementaires, contractuelles, et légales • Historique des MAJ de documents • Document des mesures spécifiques et des responsabilités individuelles

			• Si le fournisseur de services en nuage fournit les preuves de sa conformité actuelle avec la législation applicable et les exigences contractuelles	• Interview du DSI, du RSI, du responsable juridique et du DRH • Revue de la procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires	mises en place pour répondre à ces exigences, • Certifications par des auditeurs tiers
MS-18	5.32	Droits de propriété intellectuelle	• Si le fournisseur de services en nuage établit une procédure pour répondre aux plaintes relatives aux droits de propriété intellectuelle • Si le fournisseur de services en nuage dispose d'une procédure permettant d'identifier les exigences spécifiques au nuage en matière de licences avant de permettre l'installation de tout logiciel sous licence	• Revue de la procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires • Revue de l'inventaire des logiciels officiellement installés et déclarés sur chaque équipement informatique (serveurs, postes de travail, équipement réseau et de sécurité, …) • Revue du rapport d'audit de la conformité des logiciels installés aux logiciels déclarés • Revue du programme de sensibilisation réalisé et liste des bénéficiaires	• Procédure de vérification de la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires • Inventaire des logiciels officiellement installés et déclarés sur chaque équipement informatique (serveurs, postes de travail, équipement réseau et de sécurité, …) • Rapport d'audit de la conformité des logiciels installés • Programme de sensibilisation réalisé et liste de bénéficiaires

				• Interview du DSI et du RSI et d'un échantillon d'utilisateurs • Vérification sur un échantillon de serveurs du nombre d'utilisateurs réels et comparaison avec le nombre d'utilisateurs autorisés par la licence • Vérification sur un échantillon d'équipements informatiques des licences de logiciels installés	• Echantillon de licences de logiciels
MS-19	5.33	Protection des enregistrements	• Si le fournisseur de service en nuage fournit des informations sur la protection des enregistrements recueillis et stockés des utilisateurs des services en nuage	• Revue de la procédure de stockage et de manipulation des enregistrements • Interview du DAF, DRH, DSI et RSI • Audit des droits d'accès aux enregistrements au niveau des bases de données	• Procédure de stockage et de manipulation des enregistrements • Rapport d'audit des droits d'accès aux enregistrements
MS-20	5.35	Révision indépendante de la sécurité de l'information	• Si le fournisseur de service en nuage fournit des preuves documentées au client permettant d'étayer sa déclaration de mise en œuvre des mesures de sécurité de l'information conformément aux politiques et procédures	• Revue de la procédure de mise à jour des notes d'organisation relatives à la sécurité de l'information • Revue des rapports d'audit	• Procédure de mise à jour des notes d'organisation relatives à la sécurité de l'information, • Rapports d'audit

	6	Mesures de sécurité applicables aux personnes			
MS-21	6.3	Sensibilisation, enseignement et formation en sécurité de l'information	• Si tous les employés et les sous-traitants reçoivent périodiquement des sessions de sensibilisation et des formations adaptées en ce qui concerne le traitement approprié des données des clients de services en nuage et des données obtenues à partir des services en nuage • et s'ils reçoivent régulièrement les mises à jour des politiques et procédures s'appliquant à leurs fonctions	• Revue des programmes de formation et de sessions de sensibilisation • Interview du DRH pour l'identification des sujets des sessions de sensibilisation et de formation • Interview d'un échantillon d'employés ayant participé à ces sessions	• Programme de formation des années précédentes et de l'année en cours • Programme de sessions de sensibilisation réalisées et planifiées et bénéficiaires • Listes des participants aux sessions de formation et de sensibilisation
MS-22	6.8	Déclaration des événements de sécurité de l'information	• Si le fournisseur de services en nuage fournit un mécanisme d'échange qui permet de signaler un événement de sécurité de l'information et de suivi l'état d'un événement	• Revue de la procédure de déclaration des événements de sécurité de l'information • Revue d'un échantillon de fiches de déclaration des événements de sécurité de l'information • Interview du DSI, du RSI et d'un échantillon d'utilisateurs	• Procédure de déclaration des événements de sécurité de l'information • Echantillon de fiches de déclaration des événements de sécurité de l'information

	7	**Mesures de sécurité physique**			
MS-23	7.14	Élimination ou recyclage sécurisé(e) du matériel	• Si le fournisseur de services en nuage s'assure que des dispositions sont prises pour l'élimination ou le recyclage sécurisé(e) des ressources (par exemple, matériel, stockage de données, fichiers, mémoire) en temps opportun	• Revue des procédures d'élimination ou de recyclage sécurisé(e) des ressources par le fournisseur de services en nuage • Vérification de l'application des procédures d'élimination ou de recyclage sécurisé(e) des ressources par le fournisseur de services en nuage	• Procédures d'élimination ou de recyclage sécurisé(e) des ressources par le fournisseur de services en nuage
	8	**Mesures de sécurité technologiques**			
MS-24	CLD.13.1.4	Alignement du management de la sécurité pour les réseaux virtuels et physiques	• Si le fournisseur de services en nuages définit une politique de sécurité de l'information pour la configuration des réseaux virtuels • Si la politique de sécurité de l'information pour la configuration des réseaux virtuels est cohérente avec la politique de sécurité de l'information pour le réseau physique • Si la configuration du réseau virtuel respecte les exigences de la politique de sécurité pour la configuration des réseaux virtuels et qu'elle est cohérente avec le réseau physique	• Revue de la politique de sécurité de l'information pour la configuration des réseaux virtuels • Audit de l'architecture réseaux	• La politique de sécurité de l'information pour la configuration des réseaux virtuels • La politique de sécurité de l'information pour le réseau physique • Rapport d'audit de l'architecture réseaux

MS-25	8.2	Droits d'accès privilégiés	• Si le fournisseur de services en nuage fournit des techniques d'authentification suffisantes (ex : authentification multi-facteurs) pour authentifier les administrateurs du service en nuage du client conformément aux aptitudes administratives d'un service en nuage et en fonction des risques identifiés	• Revue du processus d'attribution des droits à privilèges et la conformité de sa mise en œuvre avec la politique de contrôle d'accès • Revue des comptes d'accès à privilèges • Revue des logs des accès • Interview des administrateurs systèmes, réseaux, BD et applications et des responsables métier pour l'identification des droits d'accès à privilèges et des conditions de leur expiration	• Politique de contrôle d'accès • Procédure de gestion des accès (règles d'attribution des droits d'accès à privilèges) • Liste des comptes d'accès à privilèges sur les applications, les BD, les serveurs et les équipements réseau et de sécurité • Paramètres des comptes d'accès à privilèges (droits accordés, délai d'expiration)
MS-26	8.3	Restrictions d'accès aux informations	• Si le fournisseur de services en nuage prévoit des contrôles d'accès qui permettent au client de services en nuage de restreindre l'accès à ses services, aux fonctions de ses services et aux données du client conservées dans le service	• Revue des rapports d'audit des techniques de contrôle d'accès fournies par le fournisseur de services en nuage au client • Interview des administrateurs système et réseau • Vérification des techniques de contrôle d'accès utilisées par le fournisseur de services en nuage pour permettre au client de services en nuage de restreindre l'accès aux informations du service en nuage conformément à sa propre politique de contrôle d'accès	• Politique de contrôle d'accès • Procédure de gestion des accès • Rapports d'audit des techniques de contrôle d'accès fournies par le fournisseur de services en nuage au client de services en nuage

MS-27	8.6	Dimensionnement	• Si le fournisseur de service en nuage fournit un mécanisme de surveillance de la capacité totale des ressources • Si le fournisseur de service en nuage fournit les dimensionnements exigés par le client • Si le fournisseur de service en nuage fournit une allocation flexible des ressources	• Revue des indicateurs et critères de performance des serveurs et des équipements réseaux • Revue de la procédure de gestion des changements • Interview du RSI et des administrateurs système, BD et réseau • Revue des contrats-cadre du service et d'un SLA connexe	• Indicateurs et critères de performance des serveurs et des équipements réseaux • Procédure de gestion des changements • Contrat qui contient les ressources (les logiciels, le matériel de traitement, le stockage des données et la connectivité au réseau)
MS-28	8.8	Gestion des vulnérabilités techniques	• Si le fournisseur de services en nuage met à la disposition du client des informations concernant la gestion des vulnérabilités techniques susceptibles d'affecter les services en nuage fournis	• Revue de la procédure de gestion de vulnérabilités • Revue des rapports des audits • Revue des documents résultants de l'installation des correctifs • Interview du RSI et des administrateurs système et réseau • Vérification du processus de veille sur les vulnérabilités • Revue de l'historique des installations des nouvelles versions et des correctifs • Interview des administrateurs système et réseau • Vérification des versions installées sur les serveurs, les équipements réseau et sécurité et les postes de travail	• Procédure de gestion de vulnérabilités techniques • Rapports des audits techniques • Documentation de l'installation des correctifs • Cellule de veille • Abonnement au CERT national (TunCERT) • Historique des installations des nouvelles versions et des correctifs

MS-29	8.13	Sauvegarde des informations	• Si le fournisseur de services en nuage fournit les spécifications de ses aptitudes de sauvegarde qui comprennent : ○ l'étendue et le calendrier de sauvegarde ○ les méthodes de sauvegarde et le format des données, y compris le cryptage ○ les périodes de conservation des données de sauvegardes ○ les procédures de vérification d'intégrité des données de sauvegarde ○ les procédures et les délais de restauration des données à partir des sauvegardes ○ les procédures de mise à l'essai des aptitudes de sauvegardes ○ le lieu de stockage des sauvegardes • Le fournisseur de services en nuage doit fournir un accès sécurisé et séparé aux sauvegardes	• Revue de la politique de sauvegarde • Revue des rapports d'audit du processus de sauvegarde • Interview des responsables métier • Interview du RSI et des administrateurs système, BD et réseau	• Politique de sauvegarde • Liste des responsables de sauvegardes • Rapports d'audit du processus de sauvegarde

MS-30	8.15	Journalisation	• Si le fournisseur de services en nuage fournit des aptitudes de journalisation • Si le fournisseur de services en nuage répond aux exigences du client en matière de journalisation des événements	• Revue du rapport d'analyse des besoins en termes de journalisation • Revue de la politique de journalisation • Interview des responsables métier • Interview du RSI et des administrateurs système, BD et réseau	• Rapport d'analyse des besoins en termes de journalisation • Politique de journalisation
MS-31	8.17	Synchronisation des Horloges	• Si le fournisseur de service en nuage fournit des informations concernant l'horloge utilisée par les systèmes et la manière de synchronisation des horloges locales avec l'horloge du service en nuage	• Interview des administrateurs système et réseau • Vérification de la synchronisation des horloges des serveurs et des équipements réseau et sécurité avec un serveur NTP unique	• Horloges des serveurs et des équipements réseau et sécurité synchronisées avec un serveur NTP unique
MS-32	8.18	Utilisation de programmes Utilitaires à privilèges	• Si le fournisseur de services en nuage identifie les exigences pour tout programme utilitaire utilisé au sein du service en nuage • Si le fournisseur de services en nuage s'assure que toute utilisation de programmes utilitaires capables de contourner les procédures de fonctionnement normal ou de sécurité est strictement limitée au personnel autorisé,	• Revue d'inventaire des programmes utilitaires utilisés au sein des services en nuage • Entretien avec le RSI du fournisseur de services en nuage Interview et de l'administrateur système • Vérification, par échantillonnage, de l'application des exigences identifiées pour l'utilisation d'un ensemble de programmes utilitaires	• Inventaire des programmes utilitaires utilisés au sein des services en nuage • Rapports d'audit relatifs à l'utilisation de ces programmes

			et que l'utilisation de ces programmes fait l'objet d'examens et d'audits réguliers	• Revue des rapports d'audit relatifs à l'utilisation de ces programmes	
MS-33	CLD.9.5.1	Séparation des environnements informatiques virtuels	• Si le fournisseur de services en nuage applique une séparation logique appropriée des données des clients, des applications virtualisées, des systèmes d'exploitation, du stockage et du réseau pour: ○ l'isolement approprié des ressources utilisées par les clients de services en nuage dans les environnements en multilocation ○ la séparation entre l'administration interne du fournisseur de services en nuage et les ressources utilisées par les clients de services en nuage • Si le fournisseur de services en nuage tient compte des risques liés à l'utilisation de logiciels fournis par les clients dans les services en nuage	• Interview des administrateurs système et réseau • Audit de configuration des solutions de virtualisation • Audit de configurations des équipements réseau et de sécurité • Revue du rapport d'analyse des risques liés à l'utilisation des services en nuage	• Rapport d'audit de configuration des solutions de virtualisation • Rapport d'audit de configuration des équipements réseau et de sécurité • Rapport d'analyse des risques liés à l'utilisation des services en nuage

MS-34	CLD.9.5.2	Renforcement des machines virtuelles	• Si le fournisseur de services en nuage s'assure de la bonne application des mesures techniques appropriées pour chaque machine virtuelle utilisée (seulement les services nécessaires sont utilisés, protection contre les logiciels malveillants, journalisation, …)	• Entretien avec l'administrateur système, • Audit de configuration d'un échantillon de machines virtuelles	• Rapport d'audit de configuration d'un échantillon de machines virtuelles
MS-35	8.21	Cloisonnement des réseaux	• Si le fournisseur de services en nuage procède à la séparation de l'accès au réseau : ○ Si les réseaux des locataires du service en nuage dans un environnement en multi location sont séparés ○ Si l'environnement administratif interne du fournisseur de services en nuage et l'environnement informatique en nuage du client de services en nuage sont séparés • Si le fournisseur de services en nuage fournit aux clients des mécanismes de vérification de cloisonnement des réseaux	• Revue des architectures et des configurations des réseaux virtuels utilisés dans les environnements de Cloud • Revue des moyens de vérification des réseaux fournis aux clients de services en nuage	• Schéma synoptique de l'architecture du réseau pour les services en nuage • Diagramme des flux réseaux pour les environnements Cloud • Les moyens de vérification des réseaux fournis aux clients de services en nuage

MS-36	8.24	Utilisation de la cryptographie	• Si le fournisseur de services en nuage fournit des informations au client de services en nuage : ○ concernant les cas dans lesquelles il utilise la cryptographie pour protéger les informations qu'il traite ○ sur toutes les aptitudes qu'il fournit et qui peuvent aider le client à appliquer sa propre protection cryptographique • Si le fournisseur de services en nuage utilise des certificats à clés publiques issus par l'autorité nationale de certification (TunTrust)	• Revue de la politique du fournisseur de services en nuage spécifique à l'utilisation des mesures cryptographiques • Revue des procédures utilisées par le fournisseur de services en nuage pour gérer les clés liées au service en nuage • Revue d'un échantillon de clients par rapport au processus de communication concernant l'utilisation de la cryptographie	• Politiques d'utilisation des mesures cryptographiques • Procédures de gestion des clés cryptographiques • Processus de communication aux clients concernant l'utilisation de la cryptographie
MS-37	8.25	Cycle de vie de développement sécurisé	• Si des documents de bonnes pratiques de développement sécurisé ont été élaborées et mises en œuvre • Si le fournisseur de services en nuage fournit aux clients des informations sur les procédures et les pratiques de développement sécurisé (dans le cas où ces documents ne contiennent pas d'informations confidentielles)	• Revue des procédures et des documents de bonnes pratiques de développement sécurisé • Revue des informations sur les procédures et les pratiques de développement sécurisé fournies aux clients	• Procédures et documents de bonnes pratiques de développement sécurisé

MS-38	8.32	Gestion des changements	• Si le fournisseur de services en nuage fournit au client des informations concernant les changements apportés au service en nuage qui pourraient avoir un impact négatif sur celui-ci
			• Si le fournisseur de services en nuage fournit toutes les informations de changement dont il a besoin le client à savoir :
			  ○ catégories de changements
			  ○ date et heure prévues des changements
			  ○ description technique des changements apportés au service en nuage et aux systèmes sous-jacents
			  ○ notification du début et de la fin des modifications
			• Si le fournisseur de services en nuage informe le client des changements liés à d'autres fournisseurs de services en nuage utilisés par ce fournisseur
				• Revue des contrats ou les accords de niveau de service (SLA) avec les clients
				• Revue des moyens de notification sur les changements
				• Vérification sur un échantillon des informations de changements envoyés aux clients
					• Contrats ou accords de niveau de service (SLA) signés avec les clients
					• Moyens de notification sur les changements
					• Des informations de changements envoyés aux clients

MS-39	CLD.12.1.5	Sécurité opérationnelle de l'administrateur	• Si le fournisseur de services en nuages fournit une documentation concernant les opérations et les procédures qui l'exigent	• Revue des informations fournies aux clients des services en nuage • Revue des contrats SLA signés	• Politique de sécurité de l'information • Procédures relatives aux opérations d'administration de l'environnement

					• Contrats ou accords de niveau de service (SLA) signés avec les clients
MS-40	CLD.12.4.5	Surveillance des services en nuage	• Si le fournisseur fournit des mécanismes et des aptitudes permettant au client de services en nuage de surveiller des aspects spécifiés du fonctionnement des services en nuage qu'il juge pertinents • Si le fournisseur de services en nuages fournit des informations aux clients de services en nuage concernant les aptitudes de surveillance du service • Si les données de surveillance sont conformes aux journaux d'événements	• Revue de la politique de sécurité de l'information • Revue des procédures de surveillance des services en nuage • Revue des documents concernant les aptitudes de surveillance du service	• La politique de sécurité de l'information • Procédures de surveillance des services en nuage • Documents concernant les aptitudes de surveillance du service

A la liste des exigences de base relatives à la sécurité du système d'information et des exigences supplémentaires relatives aux fournisseurs de services d'informatique en nuage se rajoutent les exigences de souveraineté nécessaires pour garantir que les données et les applications nationales restent imperméables aux lois et aux acteurs étrangers. Les besoins relatifs à la résidence des données, aux divers accès depuis l'étranger à l'environnement d'hébergement et aux prestataires des services de confiance sont listés au niveau du tableau ci-dessous :

ID ANCS	Titre de la mesure de sécurité de l'information	Vérifications à effectuer
TN-01	Lieu d'hébergement	Les centres de données principaux et de secours doivent être localisés au niveau du territoire tunisien et gérés par des entités de droit tunisien
TN-02	Accès d'administration distant	Dans le cas d'une intervention d'administration ou de support technique sur le périmètre G-Cloud ou N-Cloud, réalisée à distance par une personne localisée hors du territoire national Tunisien, il est nécessaire d'informer le client et de déployer toutes les mesures de sécurité nécessaire pour protéger l'intervention à distance. Le fournisseur doit documenter la liste des opérations qui peuvent être effectuées depuis un emplacement hors du territoire Tunisien, et les mécanismes permettant d'en assurer le contrôle d'accès et la supervision.
TN-03	Protection des données à caractère personnel	La prise en compte de la réglementation nationale (autorisation, déclaration, etc) concernant la protection des données à caractère personnel est obligatoire lors de la collecte, l'enregistrement, la conservation, la consultation, l'organisation, la modification, l'exploitation, l'utilisation, l'expédition, la distribution, la diffusion, l'interconnexion, la communication, le transfert ou la destruction
TN-04	Usage des services de confiance	• Usage des mécanismes de chiffrement robustes pour les données stockées ou pour les flux de données respectant les recommandations de l'Agence Nationale de Certification Electronique • Usage des mécanismes de hachage fiables selon les recommandations de l'Agence Nationale de Certification Electronique • Usage des solutions de signature électronique homologuées par l'Agence Nationale de Certification Electronique • Usage des conteneurs sécurisés pour la conservation et l'usage des clés cryptographiques (HSM, Cartes à puce cryptographique, etc) • Usage des certificats électroniques issus d'une autorité de certification de confiance et pour les applications et les plateformes gouvernementales et sites e-Gov (.gov.tn, .tn), il est obligatoire d'utiliser des certificats émis par l'Agence Nationale de Certification Electronique

TN-05	Raccordement au réseau national intégré de l'administration	La labélisation G-Cloud pour les fournisseurs de services d'informatique en nuage nécessite un raccordement au réseau national intégré de l'administration qui est géré par le Centre National Informatique et conçu pour véhiculer les données et les services intergouvernementaux. • Un VRF prestataire doit être implémenté au niveau du Backbone IP/MPLS de l'opérateur réseau afin d'interconnecter les différents prestataires de service cloud au RNIA. La gouvernance et la gestion de ce VRF (adressage et routage) sont assurées par le CNI. • Interconnexion avec deux (02) accès en fibres optiques, actifs, prennent deux itinéraires différents et fonctionnent en partage de charges avec un débit de 10 Mbps qui peut évoluer vers 1GBps. • Mise en place d'un point d'accès contrôlé (FW + IPS) hautement disponible permettant le contrôle de trafic et la protection contre les intrusions qui sera géré par le centre national informatique.