Politique de Sécurité Cloud

Neo Financia

RÉFÉRENCE: PSSI-CLOUD-NF-2025
CLASSIFICATION: INTERNE
VERSION: 1.0
DATE D'APPROBATION: 21 avril 2025
APPROBATION: Conseil d'Administration de Neo Financia
PROPRIÉTAIRE: RSSI
PÉRIODICITÉ DE RÉVISION: Annuelle

Table des matières

---

1. Introduction et objectifs

1.1 Contexte et portée

La présente Politique de Sécurité Cloud (PSC) établit le cadre de sécurité applicable à l'ensemble des services cloud utilisés par Neo Financia. En tant que néobanque opérant exclusivement sur des infrastructures cloud, Neo Financia reconnaît que la sécurité de ces environnements est fondamentale pour garantir la confiance de ses clients et assurer la conformité réglementaire.

Cette politique s'applique à :

- L'ensemble des services financiers hébergés dans le cloud
- Tous les environnements cloud utilisés (Azure 70%, OVHcloud 20%, AWS 10%)
- L'ensemble des collaborateurs, prestataires et partenaires accédant à ces environnements
- Tous les modèles de service (IaaS, PaaS, SaaS)
- Toutes les phases du cycle de vie des services cloud (évaluation, adoption, exploitation, désengagement)

Neo Financia, en tant qu'établissement bancaire soumis à des exigences similaires à celles des Opérateurs d'Importance Vitale (OIV), applique des normes de sécurité particulièrement strictes à ses environnements cloud.

1.2 Objectifs de la politique

Cette politique vise à :

- Garantir la sécurité et la résilience des services financiers hébergés dans le cloud
- Établir un cadre clair pour la mise en œuvre des contrôles de sécurité adaptés aux risques spécifiques du cloud
- Assurer la conformité aux exigences réglementaires applicables (DORA, NIS2, RGPD, ACPR, DSP2)
- Définir les responsabilités en matière de sécurité cloud au sein de l'organisation
- Protéger les données des clients contre les accès non autorisés, les fuites et les altérations
- Maintenir la disponibilité et l'intégrité des services financiers en ligne
- Prévenir et détecter les activités frauduleuses
- Fournir un cadre d'amélioration continue pour atteindre un niveau de maturité supérieur

1.3 Définitions et terminologie cloud

Pour assurer une compréhension commune, les définitions suivantes s'appliquent :

- **IaaS (Infrastructure as a Service)** : Modèle de service fournissant des ressources informatiques virtualisées via le cloud (serveurs, stockage, réseaux)
- **PaaS (Platform as a Service)** : Modèle de service fournissant une plateforme permettant de développer, exécuter et gérer des applications
- **SaaS (Software as a Service)** : Modèle de service fournissant des applications logicielles hébergées et gérées par le fournisseur
- **Multi-cloud** : Utilisation de services cloud provenant de plusieurs fournisseurs
- **CSPM (Cloud Security Posture Management)** : Solution de gestion et d'évaluation continue des postures de sécurité cloud
- **CWP (Cloud Workload Protection)** : Solutions protégeant les charges de travail cloud (VM, conteneurs, etc.)
- **CASB (Cloud Access Security Broker)** : Outil de sécurité contrôlant l'accès aux ressources cloud
- **Shadow IT** : Utilisation de ressources IT non approuvées par la DSI
- **Infrastructure as Code (IaC)** : Gestion et provisionnement de l'infrastructure par le code plutôt que des processus manuels

2. Stratégie et gouvernance cloud

2.1 Approche multi-cloud

Neo Financia a adopté une stratégie multi-cloud s'appuyant sur trois fournisseurs principaux :

- **Microsoft Azure** (70% des charges) : Principalement pour les services bancaires critiques, les systèmes d'authentification et les applications principales
- **OVHcloud** (20% des charges) : Pour certains services nécessitant une hébergement en France et les environnements de développement
- **Amazon Web Services** (10% des charges) : Pour des services analytiques et certaines fonctionnalités spécifiques

Cette approche vise à :

- Réduire la dépendance vis-à-vis d'un fournisseur unique
- Optimiser les coûts et les performances
- Améliorer la résilience globale
- S'adapter aux spécificités réglementaires et territoriasles
- Bénéficier des forces spécifiques de chaque fournisseur

2.2 Organisation et responsabilités

La gouvernance de la sécurité cloud est structurée selon le modèle suivant :

Cloud Security Board

- Composition : RSSI, DSI, Architectes Cloud, Représentants métiers
- Fréquence : Mensuelle
- Responsabilités :
  - Validation des politiques et standards de sécurité cloud
  - Arbitrage des exceptions et dérogations
  - Supervision des risques majeurs
  - Validation des architectures de référence

Guilde Cloud

- Composition : Experts cloud, Architectes de sécurité, Représentants des équipes d'exploitation
- Fréquence : Bimensuelle
- Responsabilités :
  - Définition des bonnes pratiques
  - Développement et maintenance des standards techniques
  - Partage de connaissances et expertise
  - Conseil et assistance aux projets

Cloud Security Team

- Rattachement : Direction de la Sécurité des Systèmes d'Information
- Composition : Spécialistes de la sécurité cloud
- Responsabilités :
  - Mise en œuvre opérationnelle de la sécurité cloud
  - Surveillance continue des environnements
  - Réponse aux incidents de sécurité cloud
  - Évaluations de sécurité des configurations

Cloud Operations Team

- Rattachement : Direction des Systèmes d'Information
- Composition : Ingénieurs cloud, DevOps
- Responsabilités :
  - Déploiement et maintenance des infrastructures cloud
  - Application des contrôles de sécurité
  - Gestion des configurations
  - Surveillance opérationnelle

2.3 Processus de gouvernance

Les processus suivants encadrent la gouvernance de la sécurité cloud :

Processus d'évaluation et d'adoption des services cloud

1. **Demande initiale** : Formalisation du besoin métier ou technique
2. **Évaluation préliminaire** : Analyse du service par la Guilde Cloud
    - Adéquation technique
    - Compatibilité avec l'architecture existante
    - Analyse préliminaire des risques
3. **Évaluation de sécurité** : Analyse approfondie par la Cloud Security Team
    - Identification des risques de sécurité
    - Vérification des certifications de sécurité
    - Analyse de la conformité réglementaire
    - Évaluation des mécanismes de protection des données
4. **Validation architecturale** : Revue par les architectes de la Guilde Cloud
    - Cohérence avec l'architecture cible
    - Intégration avec les services existants
    - Résilience et performances
5. **Validation réglementaire et juridique** : Revue par les fonctions de conformité
    - Conformité RGPD, DORA, DSP2, NIS2
    - Exigences ACPR
    - Revue des conditions contractuelles
6. **Décision finale** : Validation par le Cloud Security Board
    - Pour les services critiques : validation COMEX requise
    - Pour les services non-critiques : validation DSI et RSSI
7. **Documentation** : Formalisation des décisions, contrôles et exceptions
8. **Mise en œuvre** : Déploiement selon les standards de sécurité

Ce processus doit être appliqué pour tout nouveau service cloud avant son adoption.

2.4 Standards et documentation

La documentation de sécurité cloud est structurée en trois niveaux :

1. **Politique de Sécurité Cloud** (le présent document)
    - Document stratégique définissant les principes et exigences générales
    - Révisé annuellement ou lors de changements majeurs
    - Approuvé par le Conseil d'Administration
2. **Standards de Sécurité Cloud**
    - Documents techniques détaillant les exigences par domaine ou technologie
    - Révisés tous les 6 mois
    - Approuvés par le Cloud Security Board
    - Exemples :
        - Standard de sécurité des environnements Azure
        - Standard de sécurité des conteneurs
        - Standard de sécurité des services managés
        - Standard de chiffrement cloud
3. **Guides et procédures opérationnelles**
    - Instructions techniques détaillées pour la mise en œuvre
    - Révisés en continu
    - Approuvés par la Guilde Cloud
    - Exemples :
        - Guide de durcissement des machines virtuelles

    - Procédure de gestion des droits d'accès cloud
    - Guide d'implémentation des contrôles de sécurité réseau

L'ensemble de cette documentation est centralisé dans le référentiel documentaire de l'entreprise, avec des contrôles d'accès appropriés.

3. Modèle de responsabilité partagée

3.1 Principes du modèle

La sécurité des environnements cloud repose sur un modèle de responsabilité partagée entre Neo Financia et ses fournisseurs de services cloud. Ce modèle définit clairement quelles responsabilités de sécurité incombent à chaque partie selon le type de service utilisé.

Principes généraux :

- Les fournisseurs cloud sont responsables de la sécurité DE l'infrastructure cloud
- Neo Financia est responsable de la sécurité DANS l'infrastructure cloud
- La répartition précise des responsabilités varie selon le modèle de service (IaaS, PaaS, SaaS)
- Neo Financia conserve toujours la responsabilité finale de la protection des données de ses clients

3.2 Matrice de responsabilités

Le tableau suivant détaille la répartition des responsabilités selon le modèle de service :

Domaine de sécurité	IaaS	PaaS	SaaS
Données clients	Neo Financia	Neo Financia	Neo Financia
Accès et identités utilisateurs	Neo Financia	Neo Financia	Neo Financia
Applications	Neo Financia	Neo Financia	Partagée
Middleware	Neo Financia	Fournisseur	Fournisseur
Système d'exploitation	Neo Financia	Fournisseur	Fournisseur
Virtualisation	Fournisseur	Fournisseur	Fournisseur
Infrastructure réseau	Fournisseur	Fournisseur	Fournisseur
Sécurité physique	Fournisseur	Fournisseur	Fournisseur
Configuration de sécurité	Neo Financia	Partagée	Partagée
Surveillance de sécurité	Partagée	Partagée	Partagée
Gestion des patchs et vulnérabilités	Neo Financia (OS)	Partagée	Fournisseur

Gestion des incidents	Partagée	Partagée	Partagée
Reprise d'activité	Partagée	Partagée	Partagée

3.3 Responsabilités spécifiques de Neo Financia

Quels que soient le modèle de service et le fournisseur cloud, Neo Financia conserve les responsabilités suivantes :

Protection des données

- Classification et inventaire des données
- Chiffrement des données sensibles
- Gestion des clés de chiffrement
- Contrôles d'accès aux données
- Surveillance des accès aux données sensibles

Gestion des identités et des accès

- Définition et application des politiques d'accès
- Gestion du cycle de vie des comptes
- Configuration de l'authentification multifacteur
- Revue régulière des droits d'accès
- Gestion des accès privilégiés

Sécurité applicative

- Développement sécurisé des applications
- Tests de sécurité avant déploiement
- Configuration sécurisée des applications
- Gestion des vulnérabilités applicatives
- Protection contre les attaques web

Configuration des services cloud

- Durcissement des configurations
- Application des bonnes pratiques de sécurité
- Respect des architectures de référence
- Désactivation des services non nécessaires
- Surveillance des dérives de configuration

Surveillance et réponse aux incidents

- Détection des comportements suspects
- Analyse des journaux de sécurité
- Réponse aux alertes
- Gestion des incidents de sécurité
- Coordination avec les fournisseurs cloud

4. Sécurisation des environnements cloud

4.1 Architecture de sécurité cloud

Neo Financia applique une approche de défense en profondeur pour ses environnements cloud, avec plusieurs couches de protection complémentaires.

Principes architecturaux fondamentaux

- **Segmentation** : Séparation stricte des environnements (production, test, développement)
- **Moindre privilège** : Attribution des droits minimaux nécessaires
- **Défense en profondeur** : Multiples couches de contrôles de sécurité
- **Réduction de la surface d'attaque** : Limitation des composants et services exposés
- **Automatisation** : Déploiement et configuration via Infrastructure as Code (IaC)
- **Surveillance continue** : Détection des anomalies et comportements suspects
- **Principe du "Zero Trust"** : Vérification systématique des accès, quel que soit le point d'origine

Architectures de référence standardisées

Neo Financia maintient des architectures de référence documentées et validées, couvrant :

- Landing zones sécurisées pour chaque fournisseur cloud
- Modèles de déploiement pour les charges de travail courantes
- Configurations de référence pour les services managés
- Patterns d'intégration avec les systèmes existants
- Solutions de continuité de service multi-régions

Ces architectures de référence sont obligatoires pour tous les déploiements cloud et toute exception doit être formellement approuvée par le Cloud Security Board.

4.2 Sécurité réseau cloud

La sécurité réseau cloud comprend les contrôles suivants :

Segmentation réseau

- Réseaux virtuels/VPC distincts par environnement et fonction
- Micro-segmentation des charges de travail critiques
- Utilisation de sous-réseaux dédiés par type de service
- Séparation des flux de données et d'administration
- Isolation des composants selon leur niveau de criticité

Contrôle des flux

- Filtrage à chaque niveau de l'architecture
- Groupes de sécurité et ACL configurés selon le principe du moindre privilège
- Documentation et justification de toutes les règles de flux
- Révision périodique (trimestrielle) des règles de flux
- Blocage par défaut avec autorisation explicite des flux légitimes

Protection périmétrique

- Pare-feu nouvelle génération (NGFW) pour les zones exposées
- Web Application Firewall (WAF) pour les services exposés sur Internet
- Protection DDoS avancée pour les services critiques
- Bastion sécurisé pour l'accès aux environnements
- Systèmes de détection/prévention d'intrusion (IDS/IPS)

Services d'accès privés

- Utilisation des endpoints/liens privés pour les services managés
- Connexions privées entre les environnements on-premises et cloud
- ExpressRoute/Direct Connect pour les connexions critiques

- Chiffrement des communications inter-régions et inter-clouds
- Évitement du transit par Internet pour les flux sensibles

4.3 Sécurisation des services managés

Les services managés (PaaS, SaaS) utilisés par Neo Financia doivent respecter les exigences suivantes :

Bases de données managées

- Accès exclusivement via des endpoints privés
- Authentification forte avec contrôles IAM et MFA
- Chiffrement transparent des données au repos
- Protection des sauvegardes par chiffrement
- Journalisation complète des accès et requêtes
- Séparation des environnements (pas de partage de ressources)

Stockage d'objets et de fichiers

- Accès public désactivé par défaut
- Chiffrement systématique des données (SSE avec clés gérées par Neo Financia si possible)
- Signatures d'accès temporaires avec durée limitée
- Journalisation des accès et des opérations
- Protection contre la suppression accidentelle
- Réplication sécurisée pour la résilience

Services d'application

- HTTPS obligatoire avec TLS 1.2+ uniquement
- Configuration durcie des services
- Authentification des API avec OAuth 2.0 et OpenID Connect
- Rate limiting pour prévenir les abus
- Intégration avec les solutions de surveillance centralisées
- Isolation réseau via intégration VNet/VPC quand disponible

Services analytiques

- Pseudonymisation ou anonymisation des données sensibles
- Séparation des environnements de production et d'analyse
- Contrôles d'accès granulaires sur les données
- Chiffrement de bout en bout des flux
- Traçabilité des traitements de données

4.4 Configuration sécurisée et durcissement

Neo Financia applique une approche systématique pour le durcissement des configurations cloud :

Standards de configuration

- Utilisation des benchmarks CIS (Center for Internet Security) adaptés à chaque service
- Application des recommandations de sécurité des fournisseurs
- Configuration alignée avec les normes sectorielles (ex: PCI-DSS pour les composants de paiement)
- Documentation des écarts aux standards avec justification

Processus de durcissement

1. Utilisation de modèles validés et durcis (templates IaC, images de base sécurisées)
2. Déploiement automatisé via des pipelines validés
3. Vérification post-déploiement par des outils de scanning
4. Correction des écarts identifiés
5. Validation de conformité avant mise en production
6. Surveillance continue des déviations

Gestion des configurations

- Approche "Configuration as Code" pour tous les environnements
- Gestion des versions des configurations
- Processus formel de validation des changements
- Tests de sécurité avant application des changements
- Sauvegarde des configurations fonctionnelles
- Capacité de rollback en cas de problème

5. Gestion des identités et des accès cloud

5.1 Architecture IAM centralisée

Neo Financia met en œuvre une architecture centralisée de gestion des identités et des accès pour tous ses environnements cloud :

Principes fondamentaux

- Source d'autorité unique pour les identités (Azure AD)
- Fédération avec tous les fournisseurs cloud
- Single Sign-On (SSO) pour tous les services
- Authentification forte et contextuelle
- Traçabilité complète des accès et actions

Composants clés

- Service d'annuaire central avec synchronisation vers les environnements cloud
- Solution de gestion du cycle de vie des identités
- Système de gestion des accès privilégiés (PAM)
- Plateforme d'authentification multifacteur
- Service de gestion des accès d'urgence

Modèle d'autorisation

- Approche Role-Based Access Control (RBAC) par défaut
- Complétée par Attribute-Based Access Control (ABAC) pour les cas complexes
- Définition de rôles standards avec permissions minimales
- Attribution basée sur les fonctions et responsabilités
- Séparation des tâches pour les opérations sensibles

5.2 Gestion des accès et privilèges

Neo Financia applique les principes suivants pour la gestion des accès aux environnements cloud :

Classification des accès cloud

Niveau	Description	Exigences

d'accès		
Standard	Accès aux applications et ressources non critiques	MFA obligatoire, revue semestrielle
Sensible	Accès aux données clients et services importants	MFA renforcé, approbation manager, revue trimestrielle
Critique	Accès aux systèmes stratégiques et aux données sensibles	MFA renforcé, approbation N+2, revue mensuelle
Administratif	Accès privilégiés aux infrastructures et services	Accès temporaire, workflow d'approbation, enregistrement des sessions

Processus de gestion des accès

1. **Demande** : Formalisation via le système de workflow dédié
    - Justification business
    - Périmètre précis
    - Durée d'accès
    - Approbation hiérarchique
2. **Approbation** :
    - Validation par les propriétaires des ressources
    - Validation par la sécurité pour les accès sensibles et critiques
    - Workflow d'approbation adapté au niveau de sensibilité
3. **Attribution** :
    - Configuration des droits minimaux nécessaires
    - Activation des accès avec durée limitée si applicable
    - Notification aux parties prenantes
4. **Surveillance** :
    - Journalisation de toutes les actions
    - Détection des comportements anormaux
    - Alertes sur les actions sensibles
5. **Revue périodique** :
    - Certification formelle par les managers
    - Vérification des accès inutilisés
    - Contrôle des cumuls de droits
6. **Révocation** :
    - Processus automatisé lié au cycle de vie RH
    - Révocation immédiate en cas de départ ou changement de fonction
    - Suppression des accès temporaires à échéance

5.3 Gestion des accès privilégiés cloud

Les accès privilégiés aux environnements cloud font l'objet de contrôles renforcés :

Principes de gestion

- Accès Just-In-Time (JIT) : Attribution temporaire avec durée limitée
- Accès Just-Enough-Access (JEA) : Droits minimaux nécessaires
- Séparation des privilèges : Fragmentation des droits administratifs
- Surveillance renforcée : Enregistrement et analyse de toutes les actions
- Double validation : Approbation par deux personnes pour les actions critiques

Mécanismes techniques

- Solution PAM (Privileged Access Management) dédiée
- Coffre-fort pour les identifiants privilégiés
- Authentification multifacteur renforcée
- Enregistrement vidéo des sessions privilégiées
- Analyses comportementales des actions administratives

Contrôles administratifs

- Formation spécifique obligatoire avant attribution de droits privilégiés
- Engagement écrit de respect des procédures
- Background check renforcé pour les administrateurs
- Renouvellement formel des accès privilégiés (trimestriel)
- Audit régulier des actions administratives

5.4 Authentification sécurisée

Neo Financia applique des mécanismes d'authentification robustes pour tous les accès aux environnements cloud :

Exigences d'authentification

- Authentification multifacteur (MFA) obligatoire pour tous les accès
- Mots de passe forts (minimum 14 caractères, complexité élevée)
- Authentification contextuelle basée sur le risque
- Détection des comportements de connexion suspects
- Verrouillage progressif après échecs d'authentification

Moyens d'authentification

- Application d'authentification mobile (prioritaire)
- Tokens matériels FIDO2 pour les accès critiques
- Certificats pour les connexions système et service-à-service
- Biométrie lorsque disponible et pertinent
- SMS ou email uniquement en dernier recours

Facteurs contextuels

L'authentification prend en compte les facteurs contextuels suivants :

- Localisation géographique
- Appareil utilisé (connu/inconnu)
- Heure de connexion
- Comportement utilisateur
- Niveau de risque de l'opération demandée

5.5 Accès d'urgence (break-glass)

Neo Financia maintient un processus d'accès d'urgence pour les situations exceptionnelles :

Procédure d'accès d'urgence

1. **Identification de la situation d'urgence** :
    - Incident majeur affectant l'accès normal aux systèmes
    - Perte d'accès aux mécanismes d'authentification standard
    - Situation critique nécessitant une intervention immédiate
2. **Activation** :
    - Validation par le RSSI ou son délégué
    - Documentation de la justification
    - Déverrouillage des identifiants d'urgence
3. **Utilisation** :
    - Accès strictement limité à la résolution du problème
    - Double contrôle pendant l'utilisation si possible
    - Journalisation renforcée de toutes les actions
4. **Désactivation** :
    - Réinitialisation des identifiants après usage
    - Revue des actions effectuées
    - Documentation complète de l'intervention

Gestion des identifiants d'urgence

- Conservation sécurisée (coffre physique et/ou numérique)
- Rotation régulière des identifiants (trimestrielle)
- Test périodique de fonctionnement (semestriel)
- Accès sous double contrôle
- Alertes automatiques en cas d'utilisation

6. Protection des données dans le cloud

6.1 Classification et localisation des données

Neo Financia applique une politique stricte de classification et localisation des données dans ses environnements cloud :

Niveaux de classification

Classification	Description	Exemples	Exigences de localisation
P3 - Critique	Données hautement sensibles et réglementées	Données d'authentification, identifiants, clés cryptographiques	France uniquement, fournisseurs qualifiés
P2 - Confidentiel	Données sensibles clients et métier	Données clients, données financières, données de transaction	UE uniquement (France préférentielle)
P1 - Interne	Données internes non sensibles	Documents de travail, communications, données analytiques agrégées	UE et UK

P0 - Public	Informations publiques	Marketing, informations produits, tarifs	Sans restriction géographique

Exigences de localisation

- **Données critiques (P3)** : Stockage exclusivement en France, de préférence chez des fournisseurs qualifiés SecNumCloud ou équivalent
- **Données confidentielles (P2)** : Stockage dans l'UE, avec préférence pour la France, réplication limitée à l'UE
- **Données internes (P1)** : Stockage dans l'UE ou UK, réplication limitée à ces zones
- **Données publiques (P0)** : Sans restriction géographique

Contrôles techniques

- Validation automatisée de la localisation des données
- Tags de classification sur les ressources de stockage
- Politiques de stockage par type de données
- Surveillance des mouvements de données transfrontaliers
- Contrôles d'accès adaptés à la classification

6.2 Stratégie de chiffrement

Neo Financia met en œuvre une stratégie de chiffrement complète pour protéger ses données dans les environnements cloud :

Principes de chiffrement

- Chiffrement par défaut des données au repos et en transit
- Niveau de protection adapté à la classification des données
- Gestion rigoureuse des clés de chiffrement
- Rotation périodique des clés
- Séparation des rôles pour l'administration des clés

Exigences par niveau de classification

Classification	Chiffrement au repos	Chiffrement en transit	Gestion des clés
P3 - Critique	AES-256 avec double chiffrement	TLS 1.3 avec PFS	HYOK (clés gérées on-premises)
P2 - Confidentiel	AES-256	TLS 1.3 avec PFS	BYOK (clés importées)
P1 - Interne	AES-256	TLS 1.2+	BYOK ou CSEK
P0 - Public	Standard (AES-256)	TLS 1.2+	Gérées par le fournisseur

Gestion des clés de chiffrement

- Utilisation d'un système centralisé de gestion des clés
- Infrastructure à clés publiques (PKI) interne pour les certificats
- Modules de sécurité matériels (HSM) pour les clés critiques
- Journalisation de toutes les opérations sur les clés

- Sauvegarde sécurisée et procédures de restauration
- Séparation des rôles pour l'administration des clés

Types de chiffrement déployés

- Chiffrement transparent des bases de données
- Chiffrement des volumes et disques virtuels
- Chiffrement des sauvegardes
- Chiffrement des communications (TLS)
- Chiffrement applicatif pour les données très sensibles
- Tokenisation pour certains usages spécifiques

6.3 Protection contre les fuites de données

Neo Financia déploie plusieurs mécanismes pour prévenir les fuites de données depuis ses environnements cloud :

Solutions techniques

- DLP (Data Loss Prevention) cloud-native
- CASB (Cloud Access Security Broker) pour le contrôle des flux
- Analyse comportementale des accès aux données (UEBA)
- Détection des transferts inhabituels de données
- Filtrage des informations sensibles dans les logs et traces

Contrôles préventifs

- Restrictions sur le partage externe des données
- Blocage des transferts non autorisés
- Validation des destinataires externes
- Chiffrement automatique des données partagées
- Watermarking des documents sensibles

Surveillance et détection

- Monitoring des accès aux données sensibles
- Alertes sur les volumes anormaux de téléchargement
- Détection des tentatives d'exfiltration
- Analyse des canaux de communication sortants
- Alertes sur les comportements utilisateurs atypiques

6.4 Cycle de vie des données cloud

Neo Financia gère de manière rigoureuse le cycle de vie complet des données dans ses environnements cloud :

Phases du cycle de vie

1. **Création/Collecte**
    - Classification automatique
    - Application des contrôles de sécurité appropriés
    - Minimisation des données collectées
    - Vérification de la base légale de traitement
2. **Stockage**
    - Stockage sécurisé selon la classification
    - Chiffrement approprié

    - Application des contrôles d'accès
    - Gestion de la redondance et des sauvegardes
3. **Utilisation/Traitement**
    - Contrôles d'accès basés sur les rôles
    - Journalisation des accès et traitements
    - Protection en cours d'utilisation
    - Détection des usages anormaux
4. **Partage/Distribution**
    - Canaux sécurisés pour les transferts
    - Contrôles sur les destinataires
    - Traçabilité des partages
    - Chiffrement des données partagées
5. **Archivage**
    - Stockage à long terme sécurisé
    - Rétention conforme aux exigences légales
    - Préservation de l'intégrité
    - Contrôles d'accès maintenus
6. **Suppression**
    - Effacement sécurisé
    - Vérification de la suppression effective
    - Documentation du processus
    - Respect des obligations de conservation légale

Politiques de rétention

- Définition des durées de conservation par type de données
- Alignement avec les exigences réglementaires (bancaires, RGPD, etc.)
- Mise en œuvre technique de l'application des durées
- Processus d'archivage intermédiaire si nécessaire
- Purge automatique à l'expiration de la durée

Suppression sécurisée

- Méthodes d'effacement adaptées à la sensibilité des données
- Vérification de la suppression effective
- Traitement particulier des copies et sauvegardes
- Prise en compte des spécificités cloud pour la suppression
- Documentation du processus de suppression

7. Sécurité des workloads cloud

7.1 Sécurisation des machines virtuelles

Neo Financia applique les contrôles suivants pour sécuriser ses machines virtuelles dans le cloud :

Durcissement des systèmes

- Utilisation d'images de base sécurisées et validées
- Configuration selon les benchmarks CIS

- Désactivation des services et comptes non nécessaires
- Application systématique des correctifs de sécurité
- Déploiement via des templates IaC validés

Contrôles d'accès système

- Gestion centralisée des identités
- Authentification forte pour tous les accès
- Accès SSH uniquement par clés (pas de mots de passe)
- Bastions sécurisés pour l'administration
- Pas d'accès direct depuis Internet

Protection en temps réel

- Solution EDR (Endpoint Detection and Response) sur toutes les VM
- Analyse antimalware en temps réel
- Protection contre les intrusions
- Surveillance de l'intégrité des fichiers
- Détection des comportements anormaux

Surveillance et journalisation

- Collecte centralisée des journaux
- Supervision des performances et de la disponibilité
- Alertes sur les événements de sécurité
- Analyse des comportements suspects
- Conservation des logs selon les exigences réglementaires

Sauvegarde et récupération

- Stratégie de sauvegarde adaptée à la criticité
- Chiffrement des sauvegardes
- Tests réguliers de restauration
- Protection contre les modifications non autorisées
- Conservation hors site des sauvegardes critiques

7.2 Sécurité des conteneurs

Pour ses environnements conteneurisés, Neo Financia implémente les mesures suivantes :

Sécurité des images

- Utilisation d'images de base minimales et durcies
- Scan automatique des vulnérabilités
- Interdiction des images non validées
- Registre privé sécurisé avec contrôle d'accès
- Signature et vérification des images

Sécurité de l'orchestration

- Configuration durcie des clusters Kubernetes
- Network Policies pour le contrôle des communications
- Pod Security Policies/Standards pour contraindre les pods
- RBAC strict pour l'administration des clusters
- Audit logging complet des opérations

Sécurité runtime

- Isolation renforcée des conteneurs

- Détection des comportements anormaux
- Contrôle des privilèges et capabilities
- Protection contre les attaques sur la chaîne d'approvisionnement
- Microsegmentation des communications entre conteneurs

Surveillance dédiée

- Monitoring spécifique aux environnements conteneurisés
- Détection des vulnérabilités en temps réel
- Analyse comportementale des conteneurs
- Visibilité sur les communications entre conteneurs
- Alertes sur les activités suspectes

7.3 Sécurité des applications cloud-native

Neo Financia applique des contrôles spécifiques pour ses applications cloud-native :

Développement sécurisé

- Intégration de la sécurité dans le pipeline CI/CD
- Tests de sécurité automatisés (SAST, DAST, SCA)
- Revue de code pour les composants critiques
- Validation des dépendances tierces
- Standards de codage sécurisé

Architecture microservices sécurisée

- Authentification service-à-service
- Communication chiffrée entre services
- Isolation des domaines de sécurité
- Principe de moindre privilège pour chaque service
- Resiliency patterns implémentés

API Security

- Authentification et autorisation robustes
- Validation des entrées et sorties
- Rate limiting et protection contre les abus
- Passerelle API centralisée avec contrôles de sécurité
- Monitoring spécifique des API

Gestion des secrets

- Utilisation d'un coffre-fort pour les secrets
- Rotation automatique des credentials
- Utilisation d'identités managées lorsque possible
- Pas de secrets en clair dans le code ou les configurations
- Audit des accès aux secrets

7.4 Sécurité des services serverless

Pour ses fonctions et services serverless, Neo Financia implémente les contrôles suivants :

Sécurité du code

- Validation des entrées rigoureuse
- Analyse statique du code (SAST)
- Durcissement des dépendances

- Limitation du périmètre fonctionnel
- Contrôle de l'origine des déclencheurs

Contrôle d'exécution

- Principe du moindre privilège pour les IAM roles
- Timeouts adaptés pour limiter l'exposition
- Isolation des environnements d'exécution
- Limitation des ressources allouées
- Protection contre les attaques par déni de service

Sécurité des données

- Chiffrement des données en transit et au repos
- Épuration des données sensibles des logs
- Validation des sources et destinations de données
- Protection des informations d'authentification
- Isolation des données entre les exécutions

Surveillance

- Logging détaillé de toutes les exécutions
- Monitoring des erreurs et comportements anormaux
- Alertes sur les tentatives d'exploitation
- Analyse des patterns d'exécution
- Traçabilité des chaînes d'appels

8. Surveillance et gestion des incidents

8.1 Architecture de surveillance

Neo Financia a mis en place une architecture de surveillance complète de ses environnements cloud :

Principes de surveillance

- Visibilité centralisée sur tous les environnements cloud
- Détection en temps réel des incidents de sécurité
- Corrélation des événements multi-cloud
- Analyse comportementale pour identifier les menaces avancées
- Couverture de l'ensemble du cycle de vie cloud

Composants de l'architecture

- SIEM (Security Information and Event Management) centralisé
- Solutions CSPM (Cloud Security Posture Management)
- Outils de surveillance des workloads cloud (CWP)
- Sondes réseau et détection d'intrusion
- Analyse comportementale (UEBA)
- Gestion des vulnérabilités cloud

Sources de données de surveillance

- Logs des services cloud (niveau infrastructure et services)
- Logs des applications et bases de données
- Logs d'identité et d'authentification
- Flux réseau et analytics
- Métriques de performance et disponibilité

- Alertes de sécurité des fournisseurs cloud

Niveaux de monitoring

- Monitoring de la posture de sécurité (configurations, conformité)
- Monitoring des activités et comportements
- Monitoring des vulnérabilités et expositions
- Monitoring de la disponibilité et performance
- Monitoring des actions administratives et privilégiées

8.2 Détection des menaces

Neo Financia déploie une approche multicouche pour la détection des menaces dans ses environnements cloud :

Mécanismes de détection

- Détection basée sur les signatures (IoCs connus)
- Détection des anomalies comportementales
- Analyse avancée via machine learning
- Corrélation d'événements inter-services
- Détection contextualisée (tenant compte du risque métier)

Scénarios de détection prioritaires

- Compromission des identifiants et élévation de privilèges
- Mouvements latéraux entre services cloud
- Exfiltration de données sensibles
- Déploiement de charges malveillantes (cryptomining, etc.)
- Modification non autorisée des configurations et contrôles
- Attaques sur les API et services exposés
- Tentatives d'exploitation de vulnérabilités cloud

Intégration des sources de threat intelligence

- Flux de renseignements sur les menaces externes
- Partage d'information sectoriel (FS-ISAC, etc.)
- Alertes et bulletins des fournisseurs cloud
- Informations des CERTs nationaux
- Base de connaissances interne des incidents passés

Process d'amélioration continue

- Revue régulière des cas détectés et des faux positifs
- Ajustement des règles et seuils de détection
- Intégration du feedback des analyses d'incidents
- Simulations d'attaque pour tester l'efficacité
- Benchmark avec les bonnes pratiques du secteur

8.3 Réponse aux incidents cloud

Neo Financia a établi un processus structuré de réponse aux incidents spécifique aux environnements cloud :

Processus de réponse aux incidents cloud

1. **Préparation**
    - Documentation des procédures par type d'incident

- Formation des équipes d'intervention
- Mise en place d'outils spécialisés cloud
- Définition des canaux de communication
- Simulation régulière d'incidents

2. **Détection et analyse**
   - Identification de l'incident via monitoring
   - Qualification initiale (type, gravité, impact)
   - Escalade selon la matrice de criticité
   - Analyse préliminaire de la portée
   - Constitution de l'équipe d'intervention
3. **Confinement**
   - Isolation des ressources compromises
   - Préservation des preuves (snapshots, journaux)
   - Blocage des accès suspects
   - Limitation des mouvements latéraux
   - Mesures de stabilisation
4. **Éradication**
   - Suppression du vecteur d'attaque
   - Nettoyage des ressources compromise
   - Restauration à partir de sources saines
   - Renforcement des contrôles de sécurité
   - Vérification de l'efficacité des mesures
5. **Rétablissement**
   - Restauration contrôlée des services
   - Surveillance renforcée post-incident
   - Tests de sécurité avant remise en production
   - Validation fonctionnelle et technique
   - Communication aux parties prenantes
6. **Activités post-incident**
   - Analyse des causes profondes
   - Documentation complète de l'incident
   - Identification des améliorations nécessaires
   - Mise à jour des procédures
   - Partage des enseignements

Matrice de criticité des incidents cloud

Niveau	Critères	Temps de réponse	Escalade
Critique	Impact significatif sur les services financiers, données clients compromises, atteinte à la conformité réglementaire	Immédiat (15 min)	RSSI, COMEX, Régulateurs si nécessaire
Majeur	Perturbation importante d'un service, exposition potentielle de données, violation	< 1 heure	RSSI, Direction

	de contrôle critique		concernée
Modéré	Impact limité, vulnérabilité exploitable, déviation significative des contrôles	< 4 heures	Responsable sécurité cloud
Mineur	Anomalie sans impact immédiat, tentative non réussie, écart de configuration	< 24 heures	Équipe cloud ops

Coordination avec les fournisseurs cloud

- Procédures d'escalade formalisées avec chaque fournisseur
- Points de contact dédiés préétablis
- Processus de partage d'information sécurisé
- Simulation conjointe pour les services critiques
- Revue post-incident partagée

8.4 Gestion du Shadow IT cloud

Neo Financia dispose d'un programme structuré pour la détection et la gestion du Shadow IT cloud :

Stratégie de détection

- Analyse du trafic réseau sortant
- Scan des domaines et certificats
- Monitoring des dépenses et cartes corporate
- Découverte via solutions CASB
- Programme de divulgation responsable interne

Processus de traitement

1. **Détection et inventaire**
    - Identification des services non autorisés
    - Documentation des usages et utilisateurs
    - Évaluation initiale des risques
2. **Évaluation des risques**
    - Analyse de la sensibilité des données concernées
    - Évaluation de la conformité du service
    - Analyse des contrôles de sécurité disponibles
    - Identification des alternatives approuvées
3. **Décision et traitement**
    - Intégration au catalogue officiel (si applicable)
    - Migration vers une alternative approuvée
    - Mise en conformité avec exigences de sécurité
    - Suppression et blocage (cas critiques)
4. **Prévention**
    - Sensibilisation des utilisateurs concernés
    - Amélioration du catalogue de services approuvés
    - Adaptation des procédures d'approbation
    - Contrôles techniques préventifs

Approche de remédiation

- Priorisation basée sur les risques
- Période de transition adaptée aux contraintes métier
- Accompagnement des utilisateurs
- Processus accéléré pour évaluation de nouveaux services
- Approche non punitive encourageant la transparence

9. Conformité et gestion des risques

9.1 Exigences réglementaires

Neo Financia, en tant qu'établissement bancaire, doit se conformer à plusieurs réglementations dans le cadre de l'utilisation des services cloud :

Principales réglementations applicables

Réglementation	Principales exigences pour le cloud	Application chez Neo Financia
DORA (Digital Operational Resilience Act)	Résilience opérationnelle numérique, gestion des tiers, tests de résilience, notification des incidents	Contrôles de résilience multi-cloud, tests réguliers, surveillance 24/7
NIS2	Mesures de sécurité pour entités essentielles, gestion des incidents, sécurité de la chaîne d'approvisionnement	Framework de sécurité aligné, procédures de notification, évaluation des fournisseurs
RGPD	Protection des données personnelles, transferts internationaux encadrés, sécurité des traitements	Contrôles de localisation, chiffrement, analyse d'impact, gestion des sous-traitants
Exigences ACPR	Maîtrise des risques liés à l'externalisation, réversibilité, audit, continuité d'activité	Due diligence renforcée, clauses contractuelles, stratégie de sortie, résilience multi-site
DSP2	Authentification forte, sécurité des paiements, sécurité des API, gestion des incidents	Mise en œuvre SCA, sécurisation des API, monitoring des transactions

Processus de conformité

Neo Financia a mis en place un processus continu pour garantir la conformité de ses environnements cloud :

1. **Veille réglementaire**
    - Suivi des évolutions des textes applicables
    - Analyse d'impact sur les services cloud
    - Participation aux groupes de travail sectoriels
2. **Traduction en exigences techniques**

    - Définition des contrôles requis
    - Intégration dans les standards techniques
    - Mise à jour des architectures de référence

3. **Implémentation et vérification**

    - Déploiement des contrôles nécessaires
    - Tests de conformité
    - Audits internes et externes

4. **Surveillance continue**

    - Monitoring de la conformité
    - Détection des dérives
    - Reporting aux instances de gouvernance

5. **Amélioration continue**

    - Analyse des écarts
    - Adaptation aux nouvelles exigences
    - Benchmarking avec les bonnes pratiques

9.2 Évaluation des risques cloud

Neo Financia a intégré l'évaluation des risques cloud dans son processus global de gestion des risques :

Catégories de risques cloud spécifiques

- **Risques stratégiques** : Dépendance aux fournisseurs, évolution des services, viabilité à long terme
- **Risques opérationnels** : Disponibilité, performances, résilience, incidents techniques
- **Risques de sécurité** : Compromission, malveillance, vulnérabilités, configuration incorrecte
- **Risques de conformité** : Évolutions réglementaires, localisation des données, audits
- **Risques contractuels et juridiques** : SLA, responsabilités, droits d'audit, litiges
- **Risques liés aux fournisseurs** : Défaillance, rachat, changement de stratégie, fin de service

Méthodologie d'évaluation

1. **Identification des risques**

    - Ateliers avec les parties prenantes
    - Analyse de la documentation technique
    - Retour d'expérience sur les incidents
    - Veille sur les menaces cloud

2. **Analyse des risques**

    - Évaluation de la probabilité
    - Évaluation de l'impact (financier, opérationnel, réputationnel, réglementaire)
    - Prise en compte des contrôles existants
    - Détermination du risque inhérent et résiduel

3. **Traitement des risques**
    - Acceptation (risques faibles)
    - Réduction (mise en place de contrôles supplémentaires)
    - Transfert (assurance, clauses contractuelles)
    - Évitement (changement d'approche ou de fournisseur)
4. **Surveillance des risques**
    - Indicateurs de risque clés (KRI)
    - Tableau de bord des risques cloud
    - Revue périodique (trimestrielle)
    - Réévaluation lors de changements significatifs

Intégration avec la gestion globale des risques

- Alignement avec la méthodologie générale de Neo Financia
- Reporting consolidé au Comité des Risques
- Cohérence des échelles d'évaluation
- Vision transverse des risques IT et métier

9.3 Stratégie de sortie cloud

Neo Financia a élaboré une stratégie de sortie complète pour chacun de ses principaux fournisseurs cloud :

Scénarios de sortie considérés

- Défaillance majeure ou cessation d'activité du fournisseur
- Dégradation significative et prolongée des services
- Évolution contractuelle ou tarifaire inacceptable
- Changement des exigences réglementaires rendant impossible l'utilisation
- Décision stratégique de changement de fournisseur
- Incident de sécurité majeur affectant la confiance

Principes de la stratégie de sortie

- Documentation complète des dépendances techniques
- Architecture favorisant la portabilité (évitement du vendor lock-in)
- Préférence pour les standards ouverts et les solutions interopérables
- Clauses contractuelles garantissant l'assistance à la sortie
- Maintenance de compétences internes sur les technologies alternatives
- Tests périodiques des capacités de migration

Plans de sortie documentés

Chaque plan de sortie inclut :

1. **Cartographie des services**
    - Inventaire détaillé des services utilisés
    - Identification des dépendances
    - Classification par criticité métier
    - Évaluation de la complexité de migration
2. **Destinations alternatives**
    - Identification des alternatives pour chaque service
    - Évaluation des écarts fonctionnels et techniques

    - Prérequis pour la migration
    - Estimation des coûts de transition
3. **Procédures de migration**
    - Séquence de migration par priorité
    - Méthodes d'extraction des données
    - Procédures de test et validation
    - Mécanismes de coexistence temporaire
4. **Organisation et ressources**
    - Équipes impliquées et responsabilités
    - Compétences nécessaires
    - Budget provisionné
    - Planning estimatif par phase
5. **Tests et validation**
    - Tests partiels réguliers
    - Vérification des procédures d'extraction
    - Validation des formats d'exportation
    - Exercices pour les services critiques

Continuité de service pendant la transition

- Stratégies de coexistence temporaire
- Mécanismes de synchronisation des données
- Processus de bascule progressive
- Plan de communication pour les utilisateurs

9.4 Audit et assurance

Neo Financia a mis en place un programme complet d'audit et d'assurance pour ses environnements cloud :

Programme d'audit cloud

Type d'audit	Fréquence	Périmètre	Responsable
Audit interne de sécurité cloud	Semestriel	Contrôles de sécurité, configurations, accès	Équipe d'audit interne
Scans de conformité automatisés	Continu	Dérives de configuration, vulnérabilités	Cloud Security Team
Tests de pénétration	Annuel	Services exposés, contrôles de sécurité	Prestataire externe
Audit de conformité réglementaire	Annuel	Exigences ACPR, DORA, RGPD, DSP2	Auditeur externe
Revue des droits d'accès	Trimestriel	Accès et privilèges cloud	IAM Team
Audit des fournisseurs cloud	Annuel (par rotation)	Contrôles de sécurité des fournisseurs	Équipe d'audit + RSSI

Due diligence des fournisseurs cloud

Neo Financia réalise une due diligence approfondie de ses fournisseurs cloud :

- Analyse des certifications (ISO 27001, SOC 2, etc.)
- Évaluation des contrôles de sécurité
- Revue des rapports d'audit tiers
- Évaluation de la viabilité financière
- Analyse des incidents historiques
- Vérification des capacités de support et d'intervention

Clauses d'audit contractuelles

Les contrats avec les fournisseurs cloud incluent :

- Droit d'audit explicite
- Modalités d'exercice du droit d'audit
- Accès aux rapports d'audit tiers (SOC 2, etc.)
- Obligation de fournir des preuves de conformité
- Procédure d'escalade en cas de défaillance identifiée

Certification et attestation

Neo Financia s'appuie sur les certifications des fournisseurs tout en réalisant ses propres validations :

- Vérification de la validité des certificats
- Analyse du périmètre couvert
- Examen des Statement of Applicability (SoA)
- Identification des exclusions et limitations
- Complémentarité avec les audits internes

10. Gestion des fournisseurs cloud

10.1 Sélection et évaluation des fournisseurs

Neo Financia applique un processus rigoureux pour la sélection et l'évaluation de ses fournisseurs cloud :

Critères d'évaluation

- **Sécurité et conformité**
  - Certifications de sécurité (ISO 27001, SOC 2 Type II, etc.)
  - Contrôles techniques et organisationnels
  - Conformité aux réglementations sectorielles
  - Transparence sur les incidents de sécurité
- **Résilience et continuité**
  - Architecture multi-régions et haute disponibilité
  - SLA documentés et historique de performance
  - Capacités de reprise après sinistre
  - Gestion des incidents et communication de crise
- **Juridique et contractuel**
  - Localisation des données et juridictions applicables

    - Clauses de responsabilité et limitation
    - Conditions de résiliation et assistance
    - Droits d'audit et de contrôle

- **Technique et opérationnel**

    - Adéquation aux besoins fonctionnels
    - Performances et évolutivité
    - Intégration avec l'existant
    - Support et maintenance

- **Financier et stratégique**

    - Stabilité financière du fournisseur
    - Pérennité des services
    - Roadmap d'évolution
    - Modèle de tarification et prévisibilité

Processus de qualification

1. **Présélection**

    - Request for Information (RFI)
    - Analyse du marché et benchmarks
    - Vérification des références sectorielles

2. **Évaluation approfondie**

    - Request for Proposal (RFP) détaillé
    - Questionnaire de sécurité et conformité
    - Démonstrations techniques
    - Visite des installations (si applicable)

3. **Due diligence**

    - Analyse financière
    - Vérification des certifications
    - Revue des incidents historiques
    - Évaluation des risques pays

4. **Contractualisation**

    - Négociation des SLA
    - Définition des KPI de performance
    - Établissement des clauses de sécurité et audit
    - Formalisation de la stratégie de sortie

10.2 Gestion contractuelle et des SLA

Neo Financia formalise ses exigences dans les contrats avec ses fournisseurs cloud :

Exigences contractuelles

- **Sécurité et confidentialité**

    - Obligations de protection des données
    - Mesures de sécurité minimales requises
    - Notification des incidents de sécurité
    - Modalités d'audit et de contrôle

- **Niveaux de service (SLA)**
  - Disponibilité minimale garantie (99,95% pour les services critiques)
  - Temps de réponse aux incidents
  - Métriques de performance
  - Pénalités en cas de non-respect
- **Continuité de service**
  - Plans de continuité d'activité obligatoires
  - Tests réguliers documentés
  - Objectifs de temps de reprise (RTO/RPO)
  - Procédures d'escalade en situation de crise
- **Conformité réglementaire**
  - Respect des exigences sectorielles
  - Engagement sur la localisation des données
  - Assistance pour les audits réglementaires
  - Documentation de conformité
- **Fin de contrat et réversibilité**
  - Assistance à la migration en sortie
  - Formats d'exportation des données
  - Durée de la période de transition
  - Suppression sécurisée des données

Surveillance des SLA

- Collecte automatisée des métriques de performance
- Tableau de bord de suivi des SLA
- Revue mensuelle des performances
- Processus d'escalade en cas de dégradation
- Documentation des incidents et calcul des pénalités

10.3 Gestion des risques fournisseurs

Neo Financia intègre la gestion des risques liés aux fournisseurs cloud dans son dispositif global :

Évaluation continue des risques

- Réévaluation annuelle de chaque fournisseur critique
- Surveillance des évolutions (acquisitions, restructurations)
- Veille sur les incidents de sécurité et interruptions
- Analyse d'impact des changements de services ou conditions
- Évaluation des risques de concentration

Surveillance opérationnelle

- Monitoring en temps réel des services critiques
- Suivi des bulletins de sécurité des fournisseurs
- Participation aux programmes de preview des changements
- Analyse des rapports d'incidents et post-mortem
- Évaluation des impacts des maintenances planifiées

Plans de mitigation

- Diversification des fournisseurs pour les services critiques
- Architectures multi-cloud pour les fonctions essentielles
- Capacités de repli interne pour les services vitaux
- Solutions alternatives identifiées et documentées
- Provisionning financier pour les transitions d'urgence

Gouvernance des risques fournisseurs

- Intégration dans le reporting au Comité des Risques
- Revue trimestrielle des risques fournisseurs critiques
- Coordination avec les équipes Achats et Juridique
- Plans d'action documentés pour les risques significatifs
- Simulations de défaillance fournisseur

10.4 Communication et coordination

Neo Financia établit des canaux structurés de communication avec ses fournisseurs cloud :

Niveaux de communication

- **Stratégique**
  - Revues exécutives semestrielles
  - Alignement des roadmaps
  - Évolution de la relation
  - Responsables : RSSI, DSI, Direction
- **Tactique**
  - Comités de pilotage trimestriels
  - Suivi des projets et initiatives
  - Résolution des problèmes récurrents
  - Responsables : Responsables Cloud, Sécurité
- **Opérationnel**
  - Points de suivi mensuels
  - Performance et incidents
  - Changements planifiés
  - Responsables : Cloud Operations, Support

Gestion de crise

- Procédures d'escalade documentées
- Contacts d'urgence 24/7 identifiés
- Canaux de communication sécurisés
- Simulation conjointe périodique
- Plan de communication coordonné

Partage d'information

- Échange d'informations sur les menaces
- Alertes de sécurité et vulnérabilités
- Communication préalable des maintenances
- Retours d'expérience post-incidents
- Programme d'amélioration continue

11. Amélioration continue

11.1 Mesure de la performance

Neo Financia a défini un ensemble d'indicateurs clés de performance (KPI) pour évaluer l'efficacité de sa sécurité cloud :

KPI de sécurité cloud

Catégorie	Indicateur	Objectif	Fréquence de mesure
Posture de sécurité	Score de conformité aux standards	≥ 95%	Mensuelle
Posture de sécurité	Délai moyen de remédiation des vulnérabilités critiques	< 7 jours	Mensuelle
Posture de sécurité	Nombre de dérives de configuration	Réduction de 10% par trimestre	Mensuelle
Gestion des identités	Taux de couverture MFA	100%	Mensuelle
Gestion des identités	Accès privilégiés avec JIT/PAM	100%	Trimestrielle
Gestion des identités	Taux de revue des accès	100% selon calendrier	Trimestrielle
Opérations	Taux de disponibilité des services critiques	≥ 99,95%	Mensuelle
Opérations	Délai de détection des incidents	< 15 minutes	Trimestrielle
Opérations	Temps de résolution des incidents critiques	< 4 heures	Trimestrielle
Données	Taux de chiffrement des données sensibles	100%	Trimestrielle
Données	Conformité à la politique de localisation	100%	Mensuelle
Données	Tests de restauration réussis	100%	Trimestrielle

Tableau de bord et reporting

- Tableau de bord consolidé des métriques de sécurité cloud
- Reporting mensuel au COSEC
- Reporting trimestriel au Comité des Risques
- Analyse des tendances et identification des améliorations
- Benchmarking avec les standards de l'industrie

11.2 Évaluation de la maturité

Neo Financia utilise un modèle d'évaluation de maturité pour sa sécurité cloud :

Modèle de maturité sécurité cloud

Niveau	Description	Caractéristiques
1 - Initial	Pratiques ad hoc et réactives	Actions non formalisées, dépendance aux individus, absence de visibilité complète
2 - Défini	Processus documentés mais application inconsistante	Documentation des contrôles, conscience des risques, implémentation partielle
3 - Géré	Processus standardisés et appliqués systématiquement	Contrôles déployés, surveillance active, mesures correctives
4 - Optimisé	Processus mesurés et en amélioration continue	Métriques détaillées, automatisation, amélioration proactive
5 - Innovant	Approche avancée avec optimisation constante	Innovation, intégration complète, adaptation rapide aux nouvelles menaces

État actuel et objectifs

- Niveau de maturité actuel : 3/5 (Géré)
- Objectif à 12 mois : 4/5 (Optimisé)
- Objectif à 24 mois : 4,5/5 (Optimisé tendant vers Innovant)

Domaines d'évaluation

- Gouvernance et stratégie cloud
- Gestion des identités et des accès
- Protection des données
- Sécurité des applications et workloads
- Surveillance et détection
- Réponse aux incidents
- Gestion des fournisseurs et de la conformité

Processus d'évaluation

- Auto-évaluation semestrielle
- Audit externe annuel
- Analyse d'écart et plans d'action
- Validation par le Cloud Security Board
- Rapports d'avancement trimestriels

11.3 Plan d'amélioration

Sur la base de son évaluation de maturité actuelle (niveau 3/5), Neo Financia a défini un plan d'amélioration structuré pour atteindre ses objectifs :

Plan d'action à 12 mois

Domaine	Actions prioritaires	Échéance	Responsable
Gouvernance	Mise en place d'un processus formel d'évaluation des services cloud	T2 2025	Cloud Security Board
Automatisation	Déploiement d'une solution CSPM	T3 2025	Cloud

	avancée avec remédiation automatique		Security Team
IAM	Généralisation de l'accès privilégié temporaire (PAM/JIT)	T2 2025	IAM Team
Surveillance	Implémentation d'une solution UEBA pour la détection avancée des menaces	T3 2025	SOC Team
Données	Déploiement du chiffrement E2E pour 100% des données critiques	T4 2025	Cloud Security Team
Résilience	Mise en œuvre d'architectures actif-actif multi-régions pour les services critiques	T4 2025	Cloud Architecture Team
Formation	Programme de certification cloud security pour toutes les équipes techniques	Continu	RSSI

Initiatives stratégiques à long terme

- Développement d'une plateforme de sécurité cloud native
- Intégration complète de la sécurité dans les pipelines CI/CD
- Mise en place d'un programme de Cloud Security Posture Management avancé
- Déploiement d'une solution Zero Trust Network Access (ZTNA) cloud-native
- Création d'un programme de threat hunting dédié aux environnements cloud
- Développement des capacités d'analyse de risque quantitative pour le cloud

Suivi et gouvernance

- Revue mensuelle de l'avancement par le Cloud Security Board
- Reporting trimestriel au COSEC
- Ajustement du plan en fonction des évolutions de la menace et de la technologie
- Allocation budgétaire dédiée et suivi des investissements
- Indicateurs de progression par initiative

12. Annexes

12.1 Glossaire des termes

Terme	Définition
BYOK (Bring Your Own Key)	Utilisation de clés de chiffrement propres dans les services cloud
CASB (Cloud Access Security Broker)	Solution contrôlant l'accès aux ressources cloud
CSPM (Cloud Security Posture Management)	Solution évaluant et corrigeant la posture de sécurité cloud
CWP (Cloud Workload Protection)	Solutions de protection des charges de travail cloud
HYOK (Hold Your Own Key)	Conservation des clés de chiffrement on-premises

IaaS (Infrastructure as a Service)	Fourniture d'infrastructures virtualisées via le cloud
IAM (Identity and Access Management)	Gestion des identités et des accès
IaC (Infrastructure as Code)	Gestion et provisionnement de l'infrastructure par code
JIT (Just-In-Time)	Accès temporaire fourni uniquement lorsque nécessaire
MFA (Multi-Factor Authentication)	Authentification à plusieurs facteurs
PAM (Privileged Access Management)	Gestion des accès privilégiés
PaaS (Platform as a Service)	Fourniture d'une plateforme de développement et d'exécution
SaaS (Software as a Service)	Fourniture d'applications logicielles hébergées et gérées
UEBA (User and Entity Behavior Analytics)	Analyse comportementale des utilisateurs et entités

12.2 Matrice de contrôles de sécurité cloud

[Note: Matrice détaillée des contrôles de sécurité par service cloud et par fournisseur]

12.3 Procédures associées

[Note: Liste des procédures opérationnelles liées à cette politique]

12.4 Références

- Recommandations ANSSI pour l'externalisation vers le cloud public
- Recommandations ENISA pour la sécurité cloud
- CSA Cloud Controls Matrix
- CIS Benchmarks pour les environnements cloud
- ISO/IEC 27017 (Sécurité cloud)
- ISO/IEC 27018 (Protection des données personnelles dans le cloud)
- NIST SP 800-144 (Guidelines on Security and Privacy in Public Cloud Computing)
- NIST SP 800-145 (Definition of Cloud Computing)
- NIST SP 800-146 (Cloud Computing Synopsis and Recommendations)

Document approuvé le 21 avril 2025 par le Conseil d'Administration de Neo Financia.
Propriétaire du document : RSSI
Classification : INTERNE