

NAËL GUERIN CONSULTING

CATALOGUE DE PRESTATIONS

Audit IT & Cybersécurité

Sécurisation du système d'information, optimisation de l'infrastructure réseau et mise en conformité aux normes ISO, avec un scoring de maturité clair pour piloter vos progrès.

4 pôles d'expertise

Audit de sécurité · Optimisation réseau · Conformité ISO & réglementaire · Résilience & réponse à incident

contact@naelguerin.com · +33 6 68 84 93 76 · www.naelguerin.com

Interventions sur toute la France & en remote · Réponse sous 24 h

En un coup d'œil

4 pôles d'expertise, 17 prestations modulaires. Chacune peut être menée séparément ou combinée au sein d'une mission globale, 3 packs prêts à l'emploi sont proposés en fin de catalogue. Chaque audit donne lieu à un score de maturité chiffré (voir section 03).

Pôle A — Audit de sécurité

Réf.	Prestation
A1	Audit de sécurité du système d'information
A2	Revue de sécurité Active Directory
A3	Audit des accès & de la gestion des identités (IAM)
A4	Durcissement des systèmes (hardening)
A5	Audit de sécurité Microsoft 365 & cloud NOUVEAU
A6	Sensibilisation & formation à la cybersécurité

Pôle B — Optimisation de l'infrastructure réseau

Réf.	Prestation
B1	Audit & optimisation de l'infrastructure réseau
B2	Audit & configuration des pare-feux (firewall)
B3	Sécurisation du réseau WiFi
B4	Sécurisation de la messagerie (SPF, DKIM, DMARC) NOUVEAU
B5	Supervision & surveillance de l'infrastructure

Pôle C — Mise en conformité ISO & réglementaire

Réf.	Prestation
C1	Analyse d'écart (gap analysis) ISO 27001
C2	Analyse & gestion des risques (ISO 27005)
C3	Accompagnement à la conformité NIS 2 & RGPD
C4	Élaboration de la politique de sécurité (PSSI)

Pôle D — Résilience & réponse à incident

Réf.	Prestation
D1	Audit des sauvegardes & plan de reprise d'activité (PRA / PCA) NOUVEAU
D2	Préparation à la réponse à incident & exercice de crise NOUVEAU

01 Notre approche

Naël Guerin Consulting accompagne entreprises, PME et collectivités dans la sécurisation et l'optimisation de leur système d'information. Nos prestations d'audit IT et de cybersécurité reposent sur une expertise technique de terrain, une méthodologie structurée et une restitution claire, sans jargon inutile.

Chaque mission fait l'objet d'un cadrage préalable et d'un devis sur mesure, adapté à la taille de votre organisation, à votre périmètre technique et à vos objectifs de conformité.

Chaque audit est restitué avec un score de maturité chiffré et une grille de criticité des constats : vous savez précisément où vous en êtes, ce qui est urgent, et comment mesurer vos progrès dans le temps (voir section 03).

4 pôles d'expertise complémentaires

- ▶ Audit de sécurité — identifier les vulnérabilités réelles de votre SI (Active Directory, accès, systèmes, cloud).
- ▶ Optimisation de l'infrastructure réseau — fiabiliser, segmenter et sécuriser votre réseau, vos équipements et votre messagerie.
- ▶ Mise en conformité ISO & réglementaire — préparer votre organisation aux exigences des normes et réglementations en vigueur.
- ▶ Résilience & réponse à incident — garantir votre capacité à redémarrer et à réagir face à un incident majeur (ransomware, panne, sinistre).

02 Normes & référentiels couverts

Nos prestations s'appuient sur les principaux référentiels de sécurité et aident votre organisation à répondre à leurs exigences. Le périmètre normatif exact est défini avec vous lors du cadrage.

Référentiel	Ce qu'il encadre
ISO/IEC 27001	Système de management de la sécurité de l'information (SMSI), la norme de référence pour structurer et certifier votre sécurité.
ISO/IEC 27002	Bonnes pratiques et mesures de sécurité concrètes à mettre en œuvre (contrôles de l'annexe A).
ISO/IEC 27005	Gestion des risques liés à la sécurité de l'information, méthode d'analyse et de traitement des risques.
ISO 22301	Continuité d'activité, exigences pour les plans de reprise et de continuité (PRA / PCA).
NIS 2	Directive européenne renforçant la cybersécurité des entités essentielles et importantes (obligations de sécurité et de notification).
RGPD	Protection des données personnelles, sécurité et confidentialité des traitements, registre, notification des violations.
Guides ANSSI	Recommandations et guides d'hygiène informatique de l'agence nationale (bonnes pratiques, durcissement).
CIS Benchmarks	Référentiels internationaux de durcissement des systèmes et services (Windows, Linux, cloud, M365).

Note : la conformité complète à une norme relève d'une démarche organisationnelle globale. Nos audits en constituent une étape technique clé et préparent le terrain à une éventuelle certification.

03 Méthodologie d'évaluation & scoring

Un audit n'a de valeur que si ses conclusions sont mesurables et comparables dans le temps. Chaque mission d'audit est donc restituée avec deux outils de pilotage : un score de maturité global et une grille de criticité des constats.

3.1 — Le score de maturité cyber (sur 100)

Votre posture de sécurité est évaluée sur 6 domaines, chacun noté selon une échelle de maturité en 5 niveaux inspirée des pratiques ANSSI et ISO 27001. La moyenne pondérée de ces domaines produit un score global sur 100, présenté sous forme de radar dans le rapport de restitution.

Domaine évalué	Ce qui est mesuré
1. Gouvernance & organisation	Politique de sécurité, rôles et responsabilités, gestion documentaire, pilotage.
2. Identités & accès	Comptes, privilèges, MFA, cycle de vie des habilitations, comptes dormants.
3. Réseau & infrastructure	Segmentation, filtrage, exposition des services, WiFi, accès distants.
4. Systèmes & applications	Durcissement, mises à jour, journalisation, configuration cloud.
5. Résilience & continuité	Sauvegardes, PRA/PCA, capacité de détection et de réponse à incident.
6. Facteur humain	Sensibilisation, exposition au phishing, charte informatique, culture sécurité.

Niveau de maturité	Score	Description
Niveau 1 — Initial	0 à 20	Pratiques inexistantes ou improvisées, aucune formalisation.
Niveau 2 — Reproductible	21 à 40	Pratiques présentes mais partielles, dépendantes des individus.
Niveau 3 — Défini	41 à 60	Pratiques formalisées et documentées, application inégale.
Niveau 4 — Maîtrisé	61 à 80	Pratiques appliquées, contrôlées et mesurées régulièrement.
Niveau 5 — Optimisé	81 à 100	Amélioration continue, anticipation, sécurité intégrée aux projets.

À l'issue de la mission, vous disposez d'un score par domaine et d'un score global, un langage simple pour communiquer avec votre direction, prioriser les budgets et suivre l'évolution année après année.

3.2 — La grille de criticité des constats (alignée CVSS)

Chaque vulnérabilité ou écart identifié est classé selon la méthode CVSS (Common Vulnerability Scoring System), avec un délai de remédiation recommandé. Le plan d'action qui vous est remis est trié selon cette grille : vous savez immédiatement par quoi commencer.

Criticité	Score CVSS	Signification	Remédiation conseillée
Critique	9,0 – 10,0	Compromission possible du SI ou des données. Traitement immédiat.	Sous 48 h
Élevée	7,0 – 8,9	Vulnérabilité exploitable avec impact majeur.	Sous 2 semaines
Moyenne	4,0 – 6,9	Risque réel mais exploitation plus complexe ou impact limité.	Sous 1 à 3 mois

Criticité	Score CVSS	Signification	Remédiation conseillée
Faible	0,1 – 3,9	Écart aux bonnes pratiques, faible impact direct.	Amélioration continue

3.3 — Le suivi dans le temps

- ▶ Chaque rapport conserve la trace du score initial : un audit de suivi permet de mesurer objectivement la progression après remédiation.
- ▶ Un tableau de bord synthétique (une page) est fourni à destination de la direction : score global, radar par domaine, top 5 des risques.
- ▶ En option, une revue annuelle légère permet de réévaluer le score et d'actualiser le plan d'action sans refaire un audit complet.

04 Catalogue des prestations

Les prestations ci-dessous sont modulaires : elles peuvent être réalisées séparément ou combinées au sein d'une mission globale. Toutes sont proposées sur devis, après cadrage.

Pôle A — Audit de sécurité

A1 Audit de sécurité du système d'information

Un état des lieux complet de votre posture de sécurité, pour savoir où vous en êtes et par où commencer.

Ce que comprend la prestation

- ▶ Cartographie de votre système d'information et de vos actifs sensibles
- ▶ Analyse des vulnérabilités techniques et organisationnelles
- ▶ Revue des politiques de sécurité et des pratiques existantes
- ▶ Rapport détaillé avec score de maturité (sur 100) et criticité CVSS des constats
- ▶ Plan d'action priorisé et présentation de restitution à la direction

Cible	Toute organisation souhaitant un diagnostic global avant d'investir en sécurité.
Contribue à	ISO 27001 · ISO 27005 · Hygiène ANSSI

A2 Revue de sécurité Active Directory

L'annuaire Active Directory est la clé de voûte de la sécurité Windows, et la cible n°1 des attaquants.

Ce que comprend la prestation

- ▶ Audit des comptes, privilèges et groupes d'administration
- ▶ Détection des chemins d'escalade de privilèges (analyse ACL / BloodHound)
- ▶ Revue des politiques de mots de passe et des GPO
- ▶ Identification des faiblesses (Kerberoasting, AS-REP Roasting, délégations)
- ▶ Recommandations de durcissement et feuille de route de remédiation

Cible	Organisations disposant d'un domaine Active Directory (majorité des SI Windows).
Contribue à	ISO 27001 (A.9 contrôle d'accès) · ISO 27002 · ANSSI

A3 Audit des accès & de la gestion des identités (IAM)

Qui a accès à quoi, et pourquoi ? Une revue rigoureuse des identités et des habilitations de votre organisation.

Ce que comprend la prestation

- ▶ Revue des comptes utilisateurs, de service et à privilèges
- ▶ Application du principe du moindre privilège et revue des comptes dormants
- ▶ Audit ou mise en place de l'authentification unique (SSO : SAML, OAuth, OIDC)
- ▶ Revue de l'authentification multifacteur (MFA) et des politiques d'accès
- ▶ Sécurisation des annuaires LDAP / LDAPS

Cible	Organisations avec de nombreux utilisateurs, applications ou prestataires externes.
Contribue à	ISO 27001 (A.9) · RGPD · NIS 2

A4 Durcissement des systèmes (hardening)

Réduire la surface d'attaque de vos serveurs et postes en appliquant les standards de sécurité reconnus.

Ce que comprend la prestation

- ▶ Durcissement des serveurs Windows Server (référentiel CIS Benchmark)
- ▶ Durcissement des systèmes Linux (Debian, CentOS)
- ▶ Revue des services actifs et des ports exposés
- ▶ Définition d'une politique de mises à jour et de correctifs
- ▶ Mise en place de la journalisation et de la supervision de sécurité

Cible	Organisations souhaitant sécuriser durablement leurs serveurs et postes de travail.
Contribue à	ISO 27002 · Hygiène ANSSI · NIS 2 · CIS

A5 Audit de sécurité Microsoft 365 & cloud

Votre SI vit aussi dans le cloud : Microsoft 365 concentre messagerie, documents et identités, et mérite le même niveau d'exigence que votre réseau interne.

Ce que comprend la prestation

- ▶ Audit de la configuration Microsoft 365 / Entra ID (référentiel CIS M365)
- ▶ Revue des accès conditionnels, du MFA et des comptes administrateurs cloud
- ▶ Sécurisation d'Exchange Online, Teams, SharePoint et OneDrive (partages externes)
- ▶ Analyse des applications tierces connectées (OAuth) et de leurs permissions
- ▶ Revue de la journalisation, des alertes et du score Microsoft Secure Score

Cible	Toute organisation utilisant Microsoft 365, Google Workspace ou des services cloud.
Contribue à	ISO 27001 · ISO 27002 · CIS M365 · NIS 2

A6 Sensibilisation & formation à la cybersécurité

Le premier rempart, ce sont vos collaborateurs. Des équipes sensibilisées réduisent drastiquement le risque.

Ce que comprend la prestation

- ▶ Ateliers de sensibilisation au phishing et à l'ingénierie sociale
- ▶ Formation aux bonnes pratiques (mots de passe, MFA, données sensibles)
- ▶ Sensibilisation aux ransomwares et aux réflexes en cas d'incident
- ▶ Formation aux enjeux du RGPD pour les équipes
- ▶ Élaboration d'une charte informatique et de sécurité

Cible	Toute organisation, de la PME à la collectivité, souhaitant réduire le risque humain.
Contribue à	ISO 27001 (A.7 sécurité RH) · RGPD · NIS 2

B1 Audit & optimisation de l'infrastructure réseau

Un réseau bien conçu, c'est plus de performance, plus de fiabilité et une meilleure sécurité.

Ce que comprend la prestation

- Analyse de l'architecture réseau existante (LAN, WAN, WiFi)
- Revue de la segmentation et des VLAN
- Audit des flux et de l'exposition des services
- Recommandations de performance et de résilience
- Schéma de réseau cible documenté

Cible	Organisations dont le réseau a évolué au fil du temps sans refonte globale.
Contribue à	ISO 27001 · ISO 27002 · ANSSI

B2 Audit & configuration des pare-feux (firewall)

Le pare-feu est la porte d'entrée de votre réseau : ses règles doivent être maîtrisées et à jour.

Ce que comprend la prestation

- Revue des règles de filtrage (Fortinet, pfSense, OPNsense)
- Suppression des règles obsolètes ou trop permissives
- Optimisation de la politique de filtrage
- Audit et sécurisation des accès VPN (IPsec, SSL)
- Documentation de la configuration

Cible	Organisations disposant d'un ou plusieurs pare-feux à auditer ou reconfigurer.
Contribue à	ISO 27001 (A.13) · NIS 2 · ANSSI

B3 Sécurisation du réseau WiFi

Le WiFi est souvent le maillon faible : mal configuré, il ouvre une porte discrète sur tout votre SI.

Ce que comprend la prestation

- Audit de la couverture et de la configuration WiFi (cartes thermiques)
- Sécurisation de l'authentification (WPA2/WPA3-Enterprise)
- Séparation des réseaux invités et internes
- Détection des points d'accès non autorisés (rogue AP)
- Recommandations d'équipements et de configuration (Unifi, Cisco, Fortinet)

Cible	Bureaux, sites multiples, commerces, entrepôts et collectivités.
Contribue à	ISO 27001 · ISO 27002 · ANSSI

B4 Sécurisation de la messagerie

La messagerie est le premier vecteur d'attaque (phishing, usurpation, fraude au président). Protégez votre domaine et vos utilisateurs.

Ce que comprend la prestation

- Audit et mise en place des protocoles SPF, DKIM et DMARC
- Analyse de l'exposition du domaine à l'usurpation (spoofing)
- Revue des règles anti-phishing, anti-spam et des pièces jointes
- Sécurisation des transferts automatiques et des règles de boîtes aux lettres
- Rapport de conformité de la messagerie et suivi DMARC

Cible	Toute organisation, l'usurpation de domaine touche les PME comme les grands comptes.
Contribue à	ISO 27002 · ANSSI · NIS 2 · RGPD

B5 Supervision & surveillance de l'infrastructure

On ne protège bien que ce que l'on surveille. Mettez en place une visibilité continue sur votre SI.

Ce que comprend la prestation

- Mise en place d'une solution de supervision (LibreNMS ou équivalent)
- Surveillance des équipements réseau et serveurs critiques
- Alertes proactives sur les incidents et anomalies
- Tableaux de bord de disponibilité et de performance
- Accompagnement à la prise en main par vos équipes

Cible	Organisations souhaitant anticiper les pannes et détecter les comportements anormaux.
Contribue à	ISO 27001 (A.12) · NIS 2

C1 Analyse d'écart (gap analysis) ISO 27001

Où en êtes-vous par rapport à la norme ? Une photographie précise de l'écart entre votre situation et les exigences ISO 27001.

Ce que comprend la prestation

- Évaluation de votre SI au regard des exigences ISO 27001 / 27002
- Identification des mesures de sécurité déjà en place
- Cartographie des écarts et des points de non-conformité
- Rapport d'analyse d'écart priorisé, avec taux de couverture par chapitre de la norme
- Feuille de route vers la conformité (ou la certification)

Cible	Organisations visant une certification ISO 27001 ou une mise en conformité structurée.
Contribue à	ISO 27001 · ISO 27002 · ISO 27005

C2 Analyse & gestion des risques (ISO 27005)

Une démarche de sécurité efficace commence par une bonne connaissance de ses risques.

Ce que comprend la prestation

- Identification et valorisation des actifs sensibles
- Analyse des menaces et des vulnérabilités
- Évaluation et hiérarchisation des risques (matrice probabilité × impact)
- Définition des mesures de traitement (réduire, transférer, accepter)
- Registre des risques exploitable dans le temps

Cible	Organisations souhaitant fonder leur sécurité sur une analyse de risque formelle.
Contribue à	ISO 27005 · ISO 27001 · NIS 2

C3 Accompagnement à la conformité NIS 2 & RGPD

Les nouvelles obligations réglementaires se durcissent. Anticipez plutôt que de subir.

Ce que comprend la prestation

- Évaluation de votre assujettissement à la directive NIS 2
- Revue des mesures de sécurité attendues (gouvernance, incidents)
- Analyse de conformité RGPD sur le volet sécurité des données
- Aide à la constitution du registre et des procédures de notification
- Plan d'action de mise en conformité priorisé

Cible	Entités concernées par NIS 2 et toute organisation traitant des données personnelles.
Contribue à	NIS 2 · RGPD · ISO 27001

C4 Élaboration de la politique de sécurité (PSSI)

Formaliser les règles du jeu : une politique de sécurité claire est le socle de toute démarche pérenne.

Ce que comprend la prestation

- ▶ Rédaction de la politique de sécurité du SI (PSSI)
- ▶ Définition des rôles et responsabilités
- ▶ Élaboration des procédures clés (accès, sauvegardes, incidents)
- ▶ Charte informatique à destination des collaborateurs
- ▶ Documentation prête à être adoptée par la direction

Cible	Organisations sans cadre de sécurité formalisé ou souhaitant le mettre à jour.
Contribue à	ISO 27001 (A.5) · ISO 27002 · ANSSI

D1 Audit des sauvegardes & plan de reprise d'activité (PRA / PCA)

La question n'est pas de savoir si un incident majeur surviendra, mais si vous pourrez redémarrer. Vos sauvegardes sont votre dernière ligne de défense.

Ce que comprend la prestation

- ▶ Audit de la stratégie de sauvegarde (règle 3-2-1, immuabilité, hors-ligne)
- ▶ Tests de restauration réels et mesure des délais (RTO / RPO)
- ▶ Vérification de la protection des sauvegardes contre les ransomwares
- ▶ Élaboration ou revue du plan de reprise et de continuité d'activité (PRA / PCA)
- ▶ Procédures de redémarrage documentées et priorisées par criticité métier

Cible	Toute organisation, 100 % des victimes de ransomware auraient aimé avoir testé leurs sauvegardes avant.
Contribue à	ISO 22301 · ISO 27001 (A.12, A.17) · NIS 2 · ANSSI

D2 Préparation à la réponse à incident & exercice de crise

Les premières heures d'un incident font toute la différence. Préparez vos réflexes avant d'en avoir besoin.

Ce que comprend la prestation

- ▶ Élaboration du plan de réponse à incident (rôles, escalade, communication)
- ▶ Procédures d'urgence : isolement, préservation des preuves, notification (CNIL, ANSSI)
- ▶ Constitution du kit de crise (contacts, annuaires hors-ligne, modèles de communication)
- ▶ Exercice de crise sur table (scénario ransomware ou fuite de données)
- ▶ Rapport d'exercice et axes d'amélioration du dispositif

Cible	Organisations souhaitant structurer leur capacité de réaction, notamment dans le cadre de NIS 2.
Contribue à	NIS 2 (notification 24/72 h) · ISO 27001 (A.16) · RGPD · ANSSI

05 Packs & missions combinées

Les prestations peuvent être librement combinées. 3 packs types répondent aux besoins les plus fréquents, chacun reste ajustable lors du cadrage, avec un tarif global adapté.

Pack Diagnostic Essentiel

Savoir où vous en êtes, le point de départ idéal.

- ▶ A1 — Audit de sécurité du système d'information
- ▶ B1 — Audit de l'infrastructure réseau
- ▶ D1 (volet audit) — Vérification des sauvegardes
- ▶ Livrables : score de maturité, top 10 des risques, plan d'action priorisé

Pour qui : PME et collectivités qui n'ont jamais fait auditer leur SI.

Pack Conformité

Se mettre en ordre de marche face à ISO 27001, NIS 2 et au RGPD.

- ▶ C1 — Analyse d'écart ISO 27001
- ▶ C2 — Analyse de risques ISO 27005
- ▶ C3 — Accompagnement NIS 2 & RGPD
- ▶ C4 — Rédaction de la PSSI et des procédures clés

Pour qui : Organisations soumises à NIS 2 ou visant une certification.

Pack Sérénité

Sécuriser, surveiller et savoir réagir — une couverture complète.

- ▶ A2 + A3 — Sécurisation Active Directory et des identités
- ▶ A5 — Audit Microsoft 365 & cloud
- ▶ B2 + B4 — Pare-feux et messagerie
- ▶ B5 — Supervision de l'infrastructure
- ▶ D1 + D2 — Sauvegardes, PRA et préparation à la réponse à incident

Pour qui : Organisations souhaitant une montée en sécurité globale et durable.

06 Comment se déroule une mission

Chaque prestation, quelle qu'elle soit, suit une démarche structurée en 4 temps, gage de clarté et d'efficacité.

Étape	Contenu
1. Cadrage & périmètre	Définition commune des objectifs, du périmètre technique et du calendrier. Signature d'un accord de confidentialité (NDA) le cas échéant. À l'issue de cette étape, vous recevez un devis sur mesure.
2. Collecte & reconnaissance	Inventaire de l'existant, cartographie de l'infrastructure et analyse de la documentation disponible.
3. Analyse & tests	Réalisation des audits et tests techniques, analyse des configurations, identification des vulnérabilités et calcul du score de maturité.
4. Restitution & accompagnement	Remise d'un rapport détaillé (synthèse direction + annexes techniques), présentation orale des résultats et accompagnement à la mise en œuvre du plan d'action.

Les livrables systématiques

- ▶ Une synthèse pour la direction (1 à 2 pages) : score de maturité, radar par domaine, risques majeurs.
- ▶ Un rapport technique détaillé : constats, preuves, criticité CVSS, recommandations.
- ▶ Un plan d'action priorisé et budgérable, exploitable par vos équipes ou votre prestataire.
- ▶ Une présentation orale de restitution, en présentiel ou en visio.

Tarification

L'ensemble des prestations est proposé sur devis. Chaque mission étant unique, par sa taille, son périmètre et ses enjeux, le tarif est établi après un échange de cadrage gratuit et sans engagement. Les prestations peuvent être combinées au sein d'une mission globale ou d'un pack, avec un tarif adapté.

NAËL GUERIN CONSULTING

PASSONS À L'ACTION

Discutons de votre projet

Un besoin précis, une question, ou simplement l'envie de faire le point sur la sécurité de votre système d'information ? Le premier échange de cadrage est gratuit et sans engagement.

Email contact@naelguerin.com

Téléphone +33 6 68 84 93 76

Zone Toute la France & en remote · Réponse sous 24 h

Naël Guerin Consulting — Gestion de projet · Audit IT & Cybersécurité · Formation IT