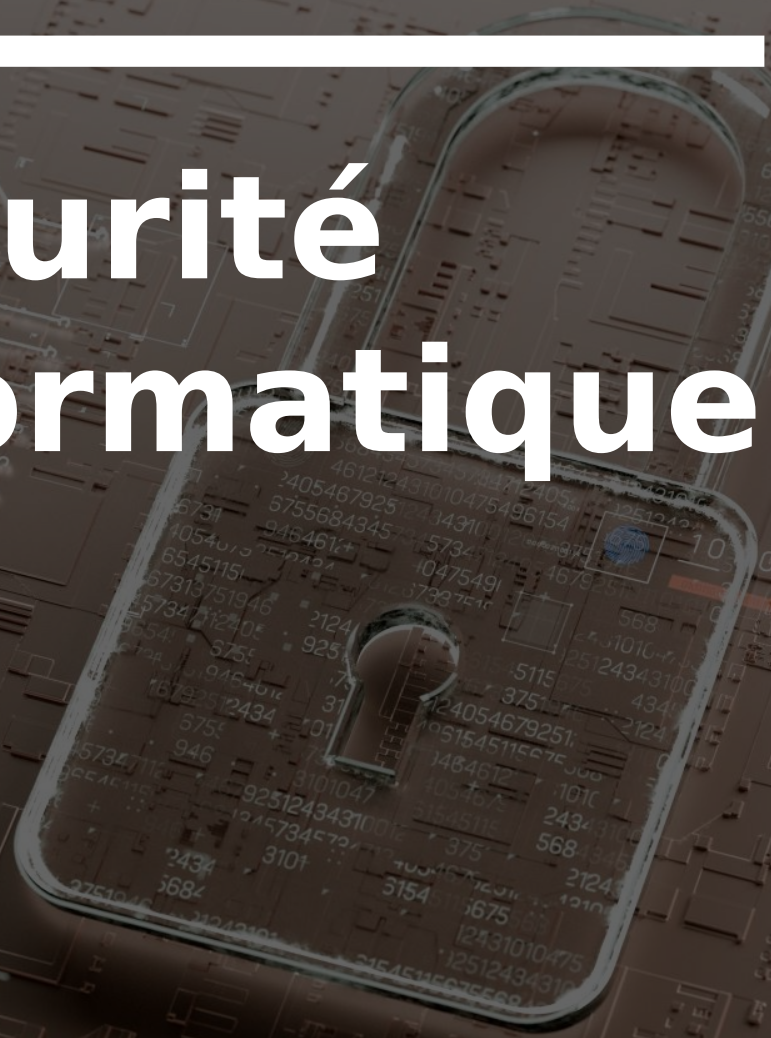
Sécurité informatique



Management de la sécurité et PSSI

Evaluation

Comprendre les besoins, identifier et évaluer

Comprendre les besoins

La cybersécurité est au service de la stratégie d’une entreprise

Elle revêt donc une dimension « macro » au sein du management global.

Les politiques et procédures se rattachant à la cybersécurité sont mises en place dans le but d’assurer la qualité et la continuité de l’activité de l’entreprise

Manager la sécurité

La sécurité des systèmes d’information (SSI) doit s’entendre comme un ensemble de moyens techniques, organisationnels, juridiques et humains ayant pour but de conserver, rétablir et garantir la sécurité du système d’information.

Cette sécurité vise à la fois à assurer :

- La disponibilité des données aux utilisateurs autorisés,
- A en préserver l’intégrité,
- A en garantir la confidentialité en interdisant tout usage à des tiers non autorisés,
- Et à assurer surveillance et traçabilité

Identifier les ressources

L’objectif est de connaître le périmètre lié à la sécurité

Il faut lister les services (authentification, contrôles d’accès physiques et logiques, disponibilité, intégrité et confidentialité) utilisés sur le réseau d’entreprise (postes clients, réseaux LAN et WAN)

À chaque sous-ensemble du périmètre correspond un niveau de sécurité différent selon les menaces possibles et en fonction de la valeur des informations à protéger.

Le lien avec le risque

Afin de définir les objectifs de sécurité, il est d’abord nécessaire de définir le risque

Pour cela, l’analyse de risque est une étape essentielle AVANT de mettre en place des stratégies de protection ou des politiques de cybersécurité

L’analyse de risque peut être réalisée grâce à plusieurs outils ou méthodes (MONARC, EBIOS, MEHARI, etc.)

Adopter une approche par le risque

Ce type d’approche permet de prioriser les moyens en fonction des besoins

Elle dimensionne les mesures en fonction de la criticité du risque et/ou de sa probabilité.

La décision est prise au cas par cas, en fonction du risque associé

Management du risque

Le management du risque se résume en cinq étapes :

- Identification : identification des ressources, vulnérabilités, menaces
- Evaluation : notation, poids, priorisation
- Planification de la réponse : détermination du plan d’action
- Implémentation
- Evaluation et surveillance

La réponse au risque peut prendre plusieurs formes:

- Evitement du risque
- Réduction du risque
- Partage du risque
- Rétention (acceptation) du risque

Evaluer les exigences métier

Quelle est la durée d’interruption maximale admissible? (DMIA)

Quelle est la perte de données maximale admissible? (PDMA)

Selon l’étude 2020 du CLUSIF, 50% des entreprises n’ont pas évalué les exigences métier

Le bilan d'impact sur l'activité consiste à identifier les exigences de délivrance des produits/services et les délais prioritaires pour le rétablissement de l'activité et des ressources.

L’importance du BIA

Le BIA permet de mettre en lumière l’impact réel d’un incident sur l’activité de l’entreprise

Sa constitution est la première étape vers l’établissement de deux documents importants :

- Le PCA, qui vise à lister les procédures, moyens et les politiques visant à assurer la continuité de l’activité
- Ou à défaut le PRA qui vise à définir les procédures à mettre en œuvre suite à un incident pour retrouver un niveau d’activité acceptable

La méthode EBIOS RM

Cette méthode est publiée par l'ANSSI et reste très utilisée, notamment en France

Elle s'articule autour de 5 « ateliers » :

- Atelier 1 : Cadrage / socle de sécurité.
- Atelier 2 : Sources de risque
- Atelier 3 : Scénarios stratégiques.
- Atelier 4 : Scénarios opérationnels.
- Atelier 5 : Traitement du risque

- https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

La méthode MEHARI

La méthode MEHARI (Méthode Harmonisée d’Analyse de Risques) est une méthode d’analyse de risques développée par le CLUSIF (Association Française des professionnels de la sécurité de l’information).

Créée en 1995, elle permet d’évaluer et de gérer les risques associés aux scénarios.

Cette méthode se décline en quatre phases distinctes qui sont les suivantes :

- Phase 1 : Analyse des enjeux et classement
- Phase 2 : Évaluation des services de sécurité
- Phase 3 : Analyse des risques
- Phase 4 : Élaboration de plans de sécurité

- https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/

Mise en œuvre de la SSI

NIST FRamework

Les modèles

Il existe de nombreux modèles de mise en œuvre de la SSI (ex : ici)

Ces modèles visent à apporter une méthodologie d'application et de suivi de la SSI

Le framework du NIST* permet d'établir une stratégie alignée sur les objectifs de l'entreprise.

De plus, il se réfère aux différentes normes applicables, comme ISO 27001 ou COBIT

**National Institute of Standards and*

Les composants du NIST CSF

Framework Core:

- Fournit un ensemble d’activités à réaliser
- Visant à atteindre l’objectif fixé
- Comprends 5 fonctions clé

Tiers :

- Décrivent des degrés de rigueurs et complexité
- Ils indiquent le degré d’information et d’implication

Profil :

- Combinaison du Tiers et du Framework Core
- Par différentiation des profils actuels et visés, on peut définir les actions à mener pour améliorer la sécurité

Le framework core

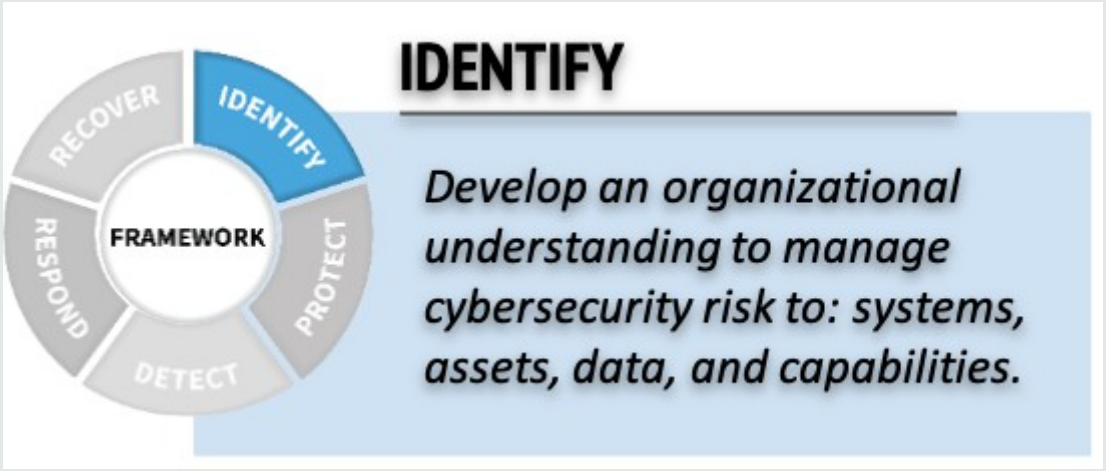
Le cadre est organisé en cinq fonctions clés:

- identify,
- protect,
- detect,
- response
- recover

Ces cinq termes lorsque considérés ensemble, donnent une vue d'ensemble du cycle de vie de la gestion de la cybersécurité dans le temps.

Chaque fonction est subdivisé en catégories puis en sous-catégories pour affiner l’analyse

Fonction Identify



Cette fonction permet d’établir une cartographie organisationnelle des composants de l’entreprise.

Exemples d’activités:

- Identifier les processus et les actifs critiques de l'entreprise
- Documenter les flux d'information
- Maintenir l'inventaire du matériel et des logiciels
- Établir des politiques de cybersécurité qui incluent les rôles et les responsabilités.
- Identifier les menaces, les vulnérabilités et les risques pour les actifs.

Fonction protect

Cette fonction décrit les mesures de sécurité appropriés pour assurer l’activité

Exemples d’activité:

- Gérer l'accès aux biens et aux informations
- Protéger les données sensibles
- Effectuer des sauvegardes régulières
- Protéger et gérer les vulnérabilités des appareils
- Former les utilisateurs

Fonction detect

Vise à mettre en œuvre des solution de détection d’évènements de cybersécurité.

Exemples d’activités :

- Tester et mettre à jour les processus de détection
- Maintenir et surveiller les journaux
- Connaître les flux de données de votre entreprise
- Comprendre l'impact des événements de cybersécurité

Fonction respond

L’objectif est de déployer les moyens et mesures pris lors de la détection d’un incident de cybersécurité

Exemples d’activités :

- Etablir des plans d’intervention
- Veiller à ce que les plans d'intervention soient testés
- Veiller à ce que les plans d'intervention soient mis à jour
- Coordonner avec les parties prenantes internes et externes

Fonction recover

Mise en œuvre des moyens et méthodes pour rétablir un service ou une activité impactée par un évènement de cybersécurité

Exemples d’activités:

- Etablir un PCA ou PRA
- Veillez à ce que les plans de reprise soient mis à jour
- Gérez les relations publiques et la réputation de l'entreprise

Panorama

Pour en savoir plus :
https://www.oas.org/fr/ssm/cicte/docs/OAS-AWS-Cadre-de-Cybersecurite-du-NIST-FRA.pdf

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018fr.pdf

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

La PSSI

L’outil indispensable

Objectifs

La politique de sécurité des systèmes d’information est un ensemble de documents stratégique.

Elle reflète la vision de la direction en matière de sécurité des SI et de gestion des risques.

On y trouve les différents éléments stratégiques (menaces, enjeux, besoins, etc.)

Mais aussi les règles et procédures applicables en matière de sécurité

Formalisation

Quatre phases sont nécessaire à la formalisation de la PSSI.

Elle implique plusieurs acteurs au sein de l’entreprise, la direction, le DSI, le RSSI mais aussi les responsables métiers et les utilisateurs!

Les trois phases sont :

- Phase 0 : défini les objectifs et les moyens, elle se concrétise par la réalisation d’une note de cadrage
- Phase 1 : identification du périmètre, des enjeux, la réglementation le cas échéant et l’expression des besoins
- Phase 2 : synthèse des principes et règles de sécurité ainsi que les impacts (coûts, moyens, etc.)
- Phase 3 : finalisation et validation de la PSSI par le comité de sécurité, élaboration du plan d’action

Contenu d’une PSSI

- Version du document
- Objectif de la PSSI
- Périmètre de la PSSI
- Déclaration d’engagement du directeur général
- Objectifs de la sécurité de l’information
- Rôles et responsabilités en matière de sécurité de l’information
- Obligations légales et réglementaires
- Définitions et principes de sécurité
- Gestion des exceptions à la PSSI
- Gestion des non-conformités
- Amélioration continue

Grands chapitres de la PSSI

- gestion de la politique
- gestion des biens (inventaires et attributions)
- sécurité liée aux ressources humaines
- gestion des tiers
- habilitation
- sécurité des échanges de données
- sécurité des réseaux
- sécurité des applications
- mobilité
- projets, développements et maintenance
- sauvegardes
- continuité d’activité
- gestion des incidents
- etc.

Les normes, standards et référentiels

ISO 27001

Définition

Une norme est un document qui définit des exigences et donne des directives. Elle a pour but de garantir des produits ou des services et revêt un caractère obligatoire qui nécessite une certification.

Un standard est généralement un document élaboré par une entreprise ou un groupement d’entreprises qui préconise des exigences, des spécifications et des lignes directrices à appliquer.

Servant à donner un cadre, les référentiels sont souvent une sélection de normes, de bonnes pratiques et de travaux théoriques. Ils donnent des préconisation pour atteindre un niveau de service optimal

Norme : ISO27001

La norme ISO 27001 offre une démarche rigoureuse pour la prise en compte de la sécurité des informations numériques ou à vocation numérique. C’est une norme de gouvernance

La norme ISO 27001 est prescriptive, puisqu’elle formule des exigences. Toutefois, elle n’est pas limitative dans l’implémentation de ces dernières.

La norme 27001 ne précise pas « comment » traiter ses exigences, elle se limite à préciser le « quoi », dans le sens de ce qui doit être obligatoirement fait.

ISO27001 - suite

L’entreprise qui s’engage dans l’application de cette norme s’engage dans un processus de certification.

Ce processus comprend deux phases : la phase d’implémentation et la phase d’audit.

Le processus complet prend généralement 3 ans, la phase d’audit étant la finalité de laquelle découle la certification de l’entreprise.

Principes

L’ISO 27001 propose un modèle répondant aux enjeux d’une gouvernance optimisée et pérenne de la sécurité de l’information.

Ce modèle passe par la mise en place d’un Système de Management de la Sécurité de l’Information (SMSI).

Il se fonde sur 4 principes clés :

- Le pilotage par les risques
- L’approche processus
- L’implication du management
- L’amélioration continue (PDCA)

ISO 27002

Là ou ISO 27001 précise le « quoi », la norme 27002 précise le « comment ».

Il n’est pas fait obligation par la norme ISO 27001 de sélectionner les mesures dans le référentiel ISO 27002.

Selon son contexte métier, selon ses obligations réglementaires, il sera plus judicieux de se référer à des référentiels plus spécialisés et mieux adaptés à l’organisation.

L’ISO a par exemple dérivé du standard 27002 des listes de bonnes pratiques contextuelles : banque, industrie, etc.

Le SMSI

Le SMSI est avant tout un cadre pour atteindre des objectifs de sécurité de manière efficace.

Pour initialiser une démarche de SMSI, l’organisme doit :

- déterminer le périmètre (fonctionnel, géographique, organisationnel, etc.) concerné,
- identifier parmi les processus de ce périmètre, ceux qui sont concernés par la sécurité de l’information, et leurs risques associés,
- déterminer les exigences (objectifs, référentiels, méthodes, etc.) nécessaires pour assurer la sécurité des processus,
- définir les mesures de sécurité nécessaires pour se conformer aux exigences exprimées.

Pourquoi?

Le Système de Management de la Sécurité de l’information sert à assurer la sécurité dans la durée, à rendre vérifiable de façon formelle cette sécurité et à fournir une confiance aux parties prenantes de l’organisme.

La mise en place d’un SMSI permet donc à l’organisme :

- d’assurer sa sécurité de l’information à court, moyen et long terme
- de se mettre à l’abri des tracasseries judiciaires en cas de préjudice du à une attaque de son système d’information.
- De bénéficier d’un cadre procédural vérifiable à tout moment

C’est un des socles de la mise en place d’ISO 27001

NIS

La nouvelle directive

Contexte

Le 10 novembre 2022, les députés européens votent la version 2 de la directive NIS

Network and Information Security est une directive datant de 2016 qui vise à augmenter le niveau de cybersécurité des acteurs majeurs de dix secteurs d’activité

Par exemple, elle oblige ces acteurs à déclarer les incidents de cybersécurité et de mettre en œuvre les mesures de sécurité nécessaires pour réduire fortement l’exposition de leurs systèmes

NISv2

Infrastructure numérique
Gestion des services TIC
Fabrication de produits informatiques
Fournisseurs numériques

La version 2 est beaucoup plus large.

Elle catégorise les entités en deux grandes catégories :

Secteurs hautement critiques : energie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène), transports (transports aériens, ferroviaires, par eau, routiers), secteur bancaire, infrastructures des marchés financiers, santé, eau potable, eaux usées, infrastructure numérique, gestion des services TIC, administration publique et espace

Secteurs critiques : services postaux et d’expédition, gestion des déchets, fabrication, production et distribution de produits chimiques, production, transformation et distribution des denrées alimentaires, fabrication (fabrication de dispositifs médicaux, de produits informatiques, électroniques et optiques, d’équipements électriques, de machines et équipements, de véhicules automobiles ou encore d’autres matériels de transport), fournisseurs numériques et recherche

Plus précisément

Dans son annexe, la directive détaille les types d’entreprises concernées.

Une variable d’application peut être faite en fonction de la taille (50 employés) ou du CA (10 M €)

Environ 600 types d’entités différentes seront concernés, parmi eux des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC40.

Les entreprises concernées seront averties par un arrêté du premier ministre

La directive entre en application en octobre 2024

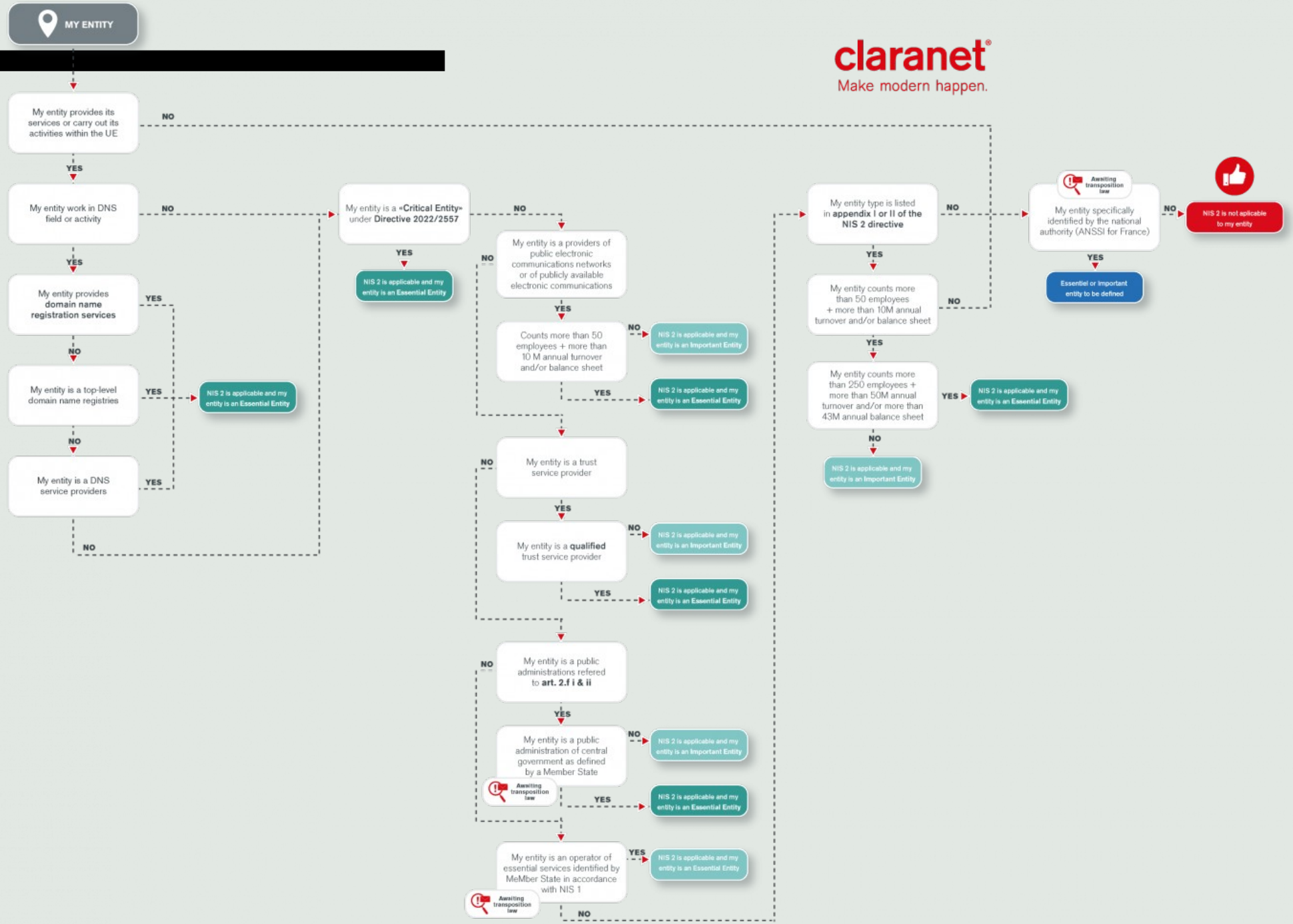
La prise en compte des prestataires

Si une entreprise n’est pas concernée par la directive, mais est prestataire d’une entreprise de secteur critique ou essentiel, elle sera de fait obligée de répondre aux exigences de la directive.

Prenons un exemple concret : si votre PME est fournisseur d’un service pour une entreprise chargé du traitement des déchets, qui elle, est soumise à NIS-2, et que vous avez un accès direct au système d’information de cette entreprise, vous serez également soumis à ces mêmes exigences dans le but d’éviter les attaques de type « Supply chain »

En
im
ag
es

claranet®
Make modern happen.



Concrètement

Les entreprises concernées devront se conformer à une liste de mesure contraignantes (pas de préconisations ici!)

Cela implique la mise en place de politiques axées sur l’analyse des risques cyber et la mise en place d’une politique de sécurité des systèmes d’information (PSSI).

Une gestion efficace des incidents sera aussi demandée, complétée par la mise en place d’un plan de continuité de l’activité (PCA) et d’un plan de reprise (PRA).

Au niveau organisationnel, les sous-traitants devront aussi s’assurer du contrôle d’accès, et de la gestion des actifs informatiques critiques (active directory, ldap …).

En application

Toute entreprise devant appliquer la nouvelle directive devra obligatoirement mener une analyse de risque cyber, selon la méthode qu’elle jugera nécessaire.

Au niveau des mesures, le cadre ressemble beaucoup à ISO 27001, son application peut être une réponse à la conformité à cette directive.

Pour les petites et moyennes entreprises qui intègreront le périmètre, le **Guide des TPE/PME** constitue par exemple une base solide de mesures concrètes et pérennes.

Les sanctions

Contrairement à son prédécesseur, NIS-2 prévoit des contrôles et des sanctions pour ceux qui ne se conforment pas.

Les amendes administratives peuvent aller jusqu'à 10 millions d'euros ou **2** % du chiffre d'affaires pour les entités essentielles

Jusqu’à 7 millions d'euros et 1,4 % du chiffre d'affaires pour les entités importantes.

En cas de négligence

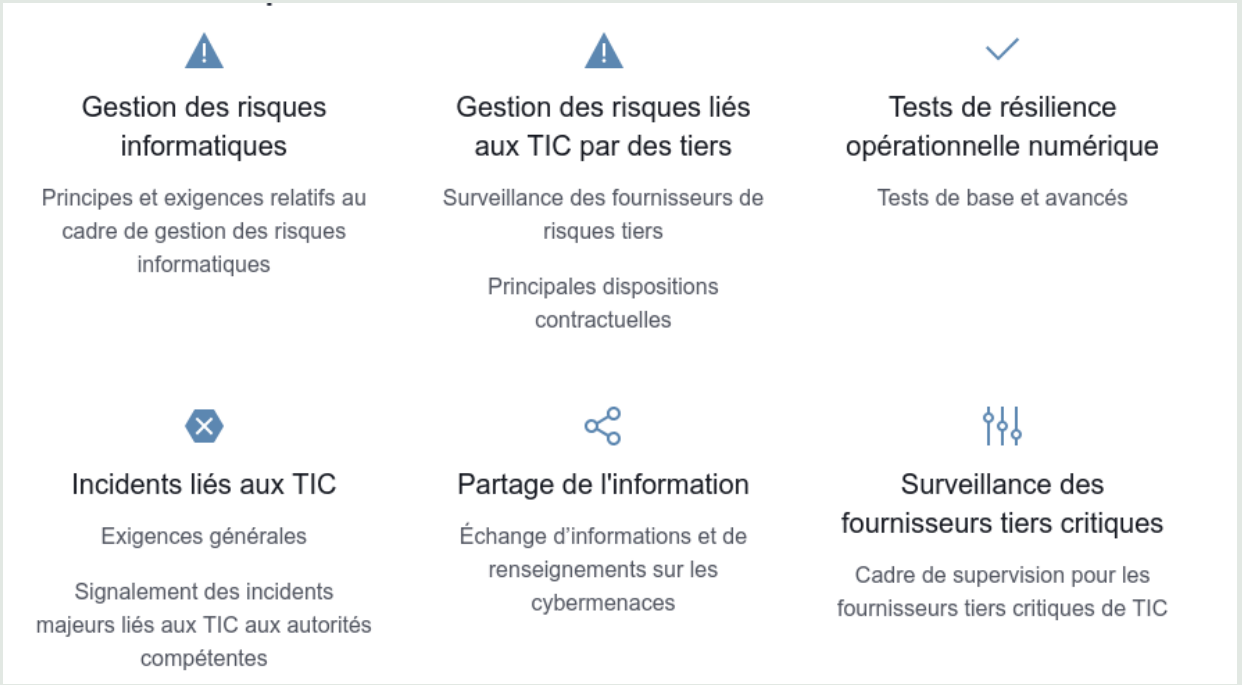
Dans le cadre de NIS2, si une négligence grave est établie à la suite d'un incident lié à la cybersécurité, les autorités des États membres peuvent :

- Exiger que les organisations divulguent publiquement les violations de conformité.
- Publier des annonces publiques mettant en lumière à la fois la ou les personnes physiques et morales responsables de la violation, en fournissant les détails.
- Les organisations classées comme entités essentielles doivent imposer une interdiction temporaire à certaines personnes d'assumer des rôles de direction si de telles violations devaient se reproduire.

DORA

Pour les établissements financiers

DORA



Titre complet : Digital Operational Resilience Act

Adoption : Adopté en décembre 2022 par l'Union Européenne

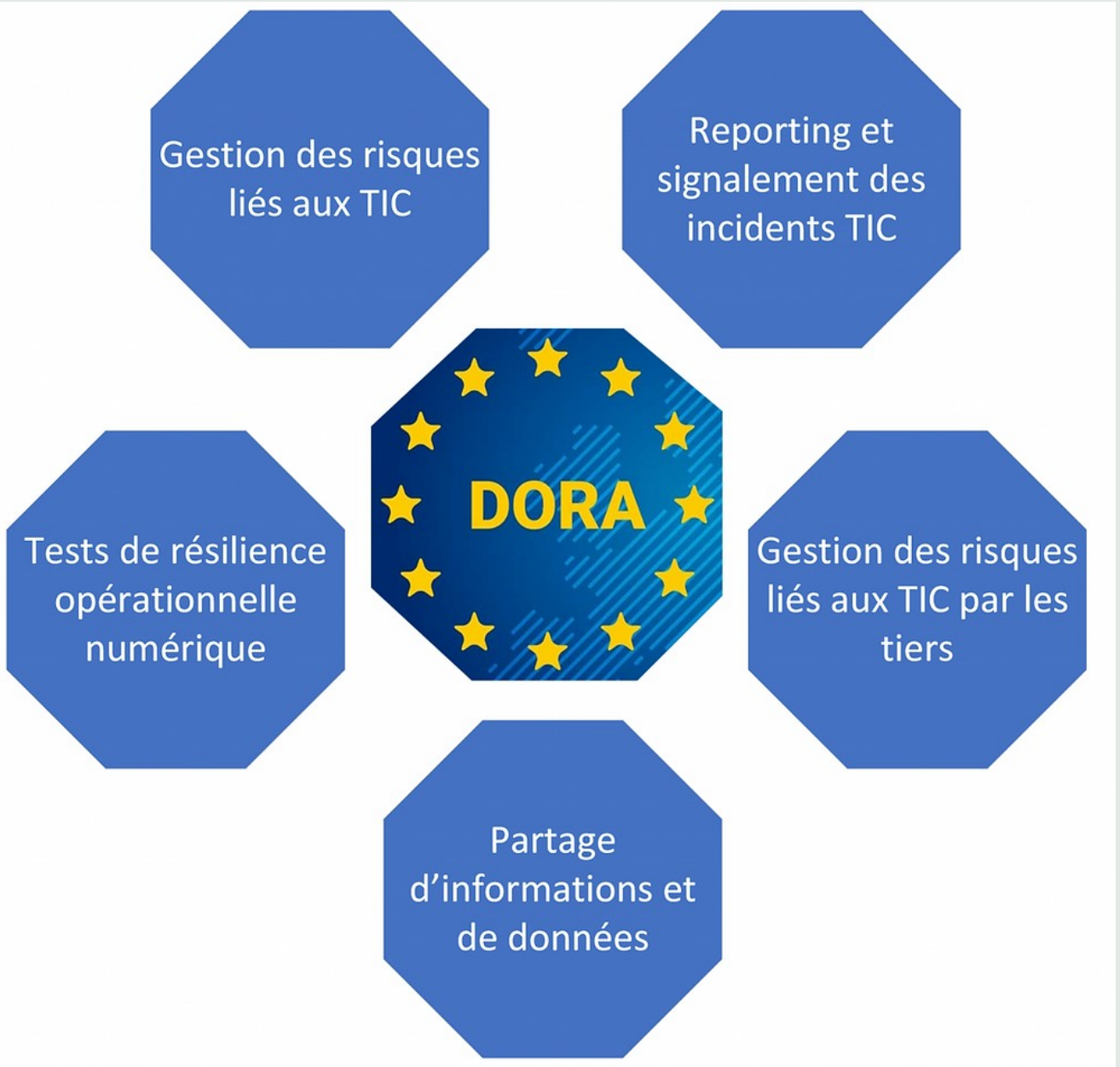
Entrée en application : Janvier 2025

Objectif principal : Garantir que le secteur financier européen peut maintenir des opérations résilientes lors de perturbations informatiques graves

Applicable à la quasi-totalité des entités financières opérant dans l'UE

S'étend aux fournisseurs tiers critiques de services TIC (technologies de l'information et de la communication)

Les cinq piliers



Piliers 1 & 2

1. Gestion des risques liés aux TIC

- Cadre solide de gouvernance des risques
- Identification, classification et cartographie des fonctions critiques
- Évaluations régulières des risques

2. Gestion des incidents

- Détection rapide des incidents
- Processus de réponse et de récupération
- Obligation de signalement des incidents majeurs aux autorités compétentes

Piliers 3, 4 & 5

3. Tests de résilience numérique

- Tests avancés obligatoires (comme les tests d'intrusion basés sur la menace)
- Fréquence des tests déterminée selon le profil de risque

4. Gestion des risques liés aux tiers

- Due diligence précontractuelle (processus d'investigation et de vérification approfondie)
- Surveillance continue des prestataires
- Stratégies de sortie documentées

5. Partage d'informations

- Partage des menaces et vulnérabilités entre entités financières
- Analyse des cybermenaces

Impact

Désignation obligatoire d'une fonction dédiée à la résilience opérationnelle numérique

Reporting normalisé des incidents majeurs liés aux TIC

Supervision directe des fournisseurs critiques de services TIC par les autorités européennes

Amendes administratives pouvant atteindre 2% du chiffre d'affaires annuel mondial de l'entité concernée

Pour les fournisseurs critiques de services TIC, les amendes peuvent aller jusqu'à 1% de leur revenu annuel mondial

Suspension temporaire ou permanente de la fourniture de services aux entités financières

RGPD

Le fameux...

RGPD

Titre complet : Règlement Général sur la Protection des Données (RGPD)

Adoption : Adopté en 2016 par l'Union Européenne

Entrée en application : 25 mai 2018

Objectif principal : Harmoniser les règles relatives à la protection des données personnelles dans l'UE

Applicable à TOUS !

Principes fondamentaux

1. Licéité, loyauté et transparence
•Traitement licite, loyal et transparent des données
•Information claire des personnes concernées

2. Limitation des finalités
•Finalités déterminées, explicites et légitimes
•Pas d'utilisation ultérieure incompatible

3. Minimisation des données
•Données adéquates, pertinentes et limitées à ce qui est nécessaire

4. Exactitude
•Données exactes et tenues à jour
•Suppression ou rectification des données inexactes

5. Limitation de la conservation
•Conservation limitée à la durée nécessaire

6. Intégrité et confidentialité
•Sécurité appropriée des données

7. Responsabilité (Accountability)
•Documentation de la conformité
•Capacité à démontrer le respect du règlement
•Traçage de la collecte et des traitements (qui, quoi et quand)

Mesures de sécurité

1. Mesures techniques

- Pseudonymisation et chiffrement des données
- Garantie de confidentialité, d'intégrité et de disponibilité
- Restauration et accès aux données en cas d'incident

2. Mesures organisationnelles

- Tests et évaluations réguliers
- Procédures de notification des violations
- Désignation d'un Délégué à la Protection des Données (DPO) dans certains cas

Obligations et sanctions

- Analyse d'impact (DPIA) pour les traitements à risque élevé
- Notification des violations de données à l'autorité de contrôle sous 72h
- Information des personnes concernées en cas de risque élevé
- Privacy by Design & by Default : protection des données dès la conception et par défaut
- Jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial