BCED
Banque Carrefour d'Échange de Données

25/04/2024

Acronyme : **Network Information System**

NIS - Secteur Multiples

Sécurité et Cybersécurité

On parle de 6 secteurs en NIS 1 puis 17secteurs en NIS 2 supervisés par différentes autorités sectorielles avec comme coordinateur national et international le Centre pour la Cybersécurité Belgique (CCB).

*Cybernétique > vient du grec kubernao qui signifie **piloter**… **gouverner**.*
… Puis utilisé en mode Cyber avec sécurité > Eléments de sécurité à l'espace Cyber.

*La **sécurité** vient du latin securitas, « **tranquillité de l'âme** »*

« Management et conformité légale NIS 2 (Secteur Public)»

Présentation à diffusion restreinte - usage interne pour les participants.
Merci à Valéry Vander Geeten du CCB.

Auteur : *David Blampain*
CISO as A Service*
Conseiller en Sécurité de l'Information

* Chief Information Security Officer

Avant-propos Cet atelier est composé de :

1. La présentation en PDF
    1. Nom du fichier : NIS-Secteur-Administration-Présentation-BCED-DBlampain-V001.pdf
    2. Crée et produite par **David Blampain**
    3. Sources : CCB (Valery V) ; ENISA ; ANSSI ; ISO 27001 ; Expérience de terrain ; Outil de veille Professionnel ; Recherches OSINT ; CALLS divers ;

2. De la demande et proposition de **la BCED**

3. De la présence **des organismes suivants** :
    - Administration générale de la Culture
    - Administration générale de l'Aide à la jeunesse
    - Administration générale de l'Enseignement
    - Administration générale des Sports
    - ARES ; AVIQ ; BCSS ; SWDE (Digit'Eaux)
    - DPO du Ministère de la Communauté germanophone
    - ETNIC ; FOREM ; ONE
    - slsp Öffentlicher Wohnungsbau Ostbelgien
    - SPF Finances
    - SPW Agriculture, Ressources naturelles et Environnement
    - SPW Économie, Emploi, Recherche
    - SPW Mobilité et Infrastructures
    - SPW Secrétariat général
    - SPW Territoire, Logement, Patrimoine, Énergie
    - SWCS
    - … ?

eConférencier : David Blampain linkedin/davidblampain.com

23 ans d'expérience au service du Web, de l'IT et de l'ICT > 14 ans en sécurité de l'information !

Champs d'expertises :
1. **ISO 27001 & 27k**
2. **Directives/LOIS NIS 1 & 2**
3. LOI RGPD

Chief Information Security Officer (CISO) et/ou Conseiller en Sécurité de l'information ;

> MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION ET PROTECTION DES DONNÉES ;
> GESTION DES RISQUES et « COMPLIANCE » ;
> CONFÉRENCIER ET FORMATEUR ;
> CHERCHEUR & surtout TROUVEUR ☺ ;
> EXPERT SBS-SME ISO 27k Commission Européenne.

Expérience : **23 années d'expérience en ICT et 14 ans en sécurité de l'information** ;

Formations : Licence en Gestion et Management d'entreprise – Faculté Warocqué UMONS – Belgique (2001) ;
Ex-Master en Marketing & Advertising – SOLVAY– ULB - Bruxelles – Belgique (2003) ;
Ex-Master en Intelligence Stratégique – HEC - ULG - Liège – Belgique (2013) ;

Certifications : Certified ISO/IEC 27001 **Senior** Lead **Implementer** @ PECB Canada (2015) ;
Certified ISO/IEC 27032 **Senior** Lead **Cyber Security** Manager @ PECB Canada (2017) ;
Certified ISO/IEC 27005 **Senior Risk** Manager @ PECB Canada (2017) ;
Certified **Data Protection Officer** @ PECB Europe (2017) ;
Encours de formation puis certification : ISO 27002:2022 ; CISSP (ISC^2)

Passions : Sécurité, Informatique et Cyber Espace ; Arts Martiaux et Arts du mouvements ; Marche Nordique ; Lecture, Etude, Recherches et Ecriture ;

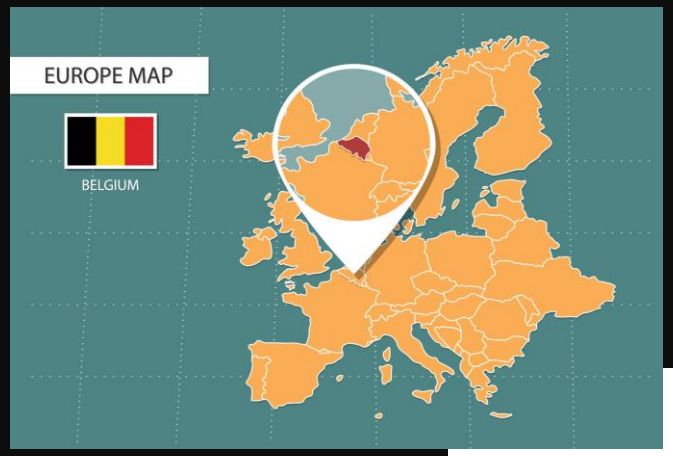
PLUS ? : Linkedin

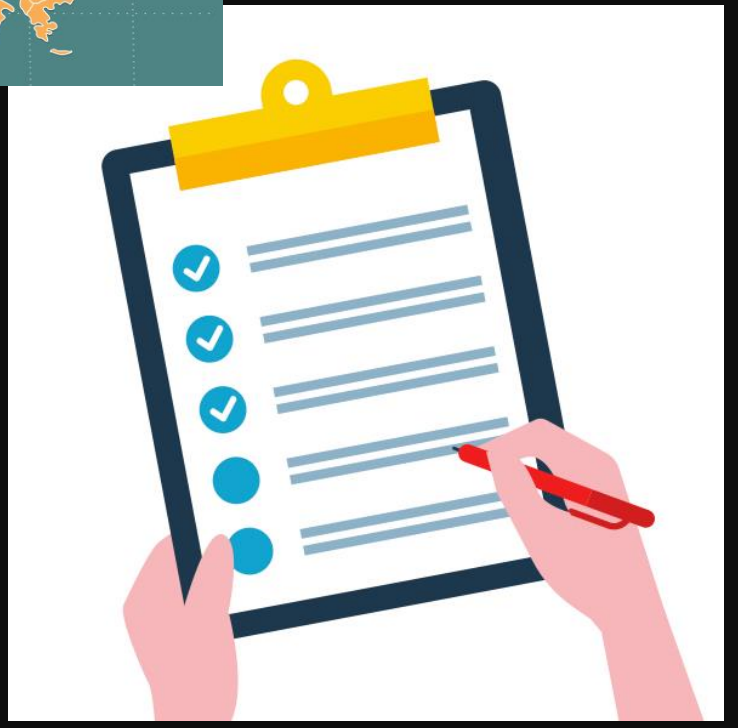
NIS 2 : Cyber Sécurité – Sommaire 1/1

1. **Etat des lieux : Belgique vs Europe**
2. **Les Menaces Cyber & Co**
3. **NIS 1 à 2 : Belgique vs Europe**
4. **Champs d'application**
5. **Autorité compétente**
6. **Gestion des risques / Frameworks de Cybersécurité / audit.**
7. **S'organiser ! Framework CCB**
8. **S'organiser ! Dans quelle cour on joue ?**
9. **S'organiser ! Management (Directeur)**
10. **S'organiser ! *"Boots on the ground" :* En Pratique avec ISO 27001**
11. **Notification des incidents**
12. **Supervision**
13. **Conformité**
14. **Agendas**
15. **Conclusions**

1. Etat des lieux

Belgique vs Europe





1 NIS : Ca veut dire quoi ? Et depuis quand ?

Network Information System : Système d'information en réseau.

Belgique : NIS 1
Loi du 7/04/2019
Entrée en vigueur le 03/05/2019
Pour 6 secteurs

Belgique : NIS 2
Entrée en vigueur potentielle Loi en octobre 2024
Pour 11 secteurs supplémentaires

Avec chacun(e) des Autorités sectorielles…

"La directive touche principalement et plus largement des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union Européenne."

Sources : www.CCB.gov.be et adaptation de www.ssi.gouv.fr

État d'avancement de la transposition de la directive NIS

NIS 1 : La directive (UE)2016/1148
Adoptée le 6 juillet 2016 (UE)
Adoptée en 2019 en Belgique
Implémentation : c'est NOW en Be

NIS 2 : La directive (EU) 2022/2555
Adoptée le 14/12/2022 (UE)
Adoptée en 10/2024 en Belgique
Implémentation effective 2025 en Be

Ce n'est PAS vraiment NOUVEAU …

- La directive NIS 1 est le premier texte législatif général de l'UE en matière de cybersécurité.
- Elle impose aux Etats members des obligations visant à renforcer le niveau général de cybersécurité dans l'UE.
- Transposé en Belgique par la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.
- Une directive NIS 2 est finalisée niveau Européen (2022)
- PQ ? Les menaces évoluent vites, sont complexes et adaptables. Une réforme s'imposait pour augmenter notre cyber resilience autant privée que publique ! (M. Schinas. – EC)

BCED
Banque Carrefour d'Échange de Données

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden

?

Source : https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

Le processus de transposition du NIS2 n'est pas encore achevé en Belgique. Le contenu de cette présentation est partiellement basé sur le projet de loi NIS2 et le projet d'arrêté royal et fournit, le cas échéant, un résumé simplifié de ces dispositions. Par conséquent, les éléments peuvent encore faire l'objet de modifications.

1. Etat des Lieux : Réflexions passées : La Belgique

Les choses ont pris du temps : La Directive NIS passée en Loi date du **7/04/2019**

Les OSE / FSN de NIS 1 n'ont pas tous été désignées mais certains le sont ;

Les OSE / OSI de NIS 2 en cours !

Les OSE / OSI sont confidentiels ! On ne doit en aucun cas fournir des listes dans la presse ou ailleurs ! Même si on peut se faire une idée…

Il est possible aussi de contacter le CCB « centre de la cyber sécurité » pour en savoir plus d'un point de vue légal : nis@ccb.belgium.be ET le ministère adéquat.

Opérateur De **S**ervice **E**ssentiel

Source : https://aroon-bourse.blogspot.com/2012/03/tendance-cac-40-du-07032012.html
Dessin non original remodifié avec humour > non utilisable commercialement > a titre de présentation privée.

Question ?

Faut-il attendre d'être désigné pour se Cybersécuriser ?

- LA DIRECTIVE NIS 1 (On y est) et NIS 2 (ça arrive)
- NON ! ET VOUS AVEZ DÉJÀ AVANCÉ ??? ☺

- Vos EXPERIENCES
- Le RGPD vs NIS : Même combat > augmenter la Sécurité et Cyber Sécurité (Données & IT) !
  = FRAMEWORKS : Harmoniser le "cadre de travail" et le niveau de sécurité européen.
- La loi NIS met en avant l'ISO 27001 uniquement en BELGIQUE
- BONUS : CCB
  - 4 Framework (PDF en ligne)
  - 3 Fichiers Excel de COMPLIANCE NIS (depuis mi-juin 2023)

L'EUROPE veut augmenter la Cybersécurité – NIS 2

Améliorer la directive NIS 1

1. Champ d'application plus large (nouveaux secteurs) ;
2. Nouvelles notions : **entités essentielles** et **importantes** – en fonction de la taille de l'entité (nombre de travailleurs et chiffre d'affaires) et de son secteur d'activité ;
3. Une identification formelle ne sera plus nécessaire (sauf exception) ;
4. Renforcement des exigences de sécurité et des méthodes d'analyse de risques >
    1. Sécurité des chaines d'approvisionnement et relations avec les fournisseurs ;
5. Renforcement et harmonisation des sanctions ;

Source : https://ec.europa.eu

1. Etat des lieux : l'EUROPE ne lâchera rien !
NIS 2 : le RETOUR

NIS 1 :
Les États membres de l'UE améliorent leurs capacités en matière de cybersécurité

NIS 2 : *Augmentation des capacités*
Des mesures de contrôle et d'exécution plus strictes seront introduites.

Une liste de sanctions administratives, y compris des amendes pour violation des obligations en matière de gestion des risques de cybersécurité et de notification, est établie.

NIS 1 :
Une coopération accrue au niveau de l'UE

NIS 2 : *Coopération*
Création de EU-CyCLONe (Incidents)
Renforcement du partage
Partage des vulnérabilités

Source : https://ec.europa.eu

1. Etat des lieux : NIS 1 > l'EUROPE ne lâchera rien ! NIS 2

NIS 1 :
Utilisation de pratique de gestion des risques

NIS 2 : *Gestion des risques en matière de cybersécurité*
Renforcement des exigences de sécurité
Renforcement de la Cyber Sécu des chaines d'approvisionnements
Responsabilité de la direction de l'entreprise
Obligations de signalement des incidents

Sanctions:

NIS 1 (en Belgique)
De 500 € à 200.000 € d'amende et des peines d'emprisonnement jusque 2 ans.

NIS 2 : jusque 10.000.000 € ou 2 % du chiffre d'affaires annuel d'amende administration comprise et sanction pour les managers …

1. Etat des lieux : l'EUROPE ne lâchera rien ! NIS 2 : le RETOUR : BELGIQUE

Actuellement en BELGIQUE

1. ACTUELLEMENT > ACTIF et sous le coup de la loi et de la désignation si vous avez reçu une lettre ?
   - Si pas vous renseigner.

2. La nouvelle directive complémentaire et plus contraignantes est passée : NIS 2 qui ensuite va être transposée dans une LOI.

Source : https://ec.europa.eu

1. Etat des lieux : NIS 2 : Europe

Rappel > Combler les lacunes de la NIS 1

1. NIS 1 = 6 Secteurs > NIS 2 = 17 Secteurs ;
2. Plafond clair entre TPE ; PME et grands comptes ;
3. Souplesse dans l'identification pour des petites structures à risques élevés ;
4. Distinction entre FSE et OSE éliminée > système de surveillance en fonction Important & Essentiel ;
5. Renforcement des exigences de sécurité et des méthodes d'analyse de risques ;
6. Sécurité des chaines d'approvisionnement et relations avec les fournisseurs ;
7. Formation des employés / directeurs / CEO … ☺
8. Inspiration sur la note 5G de la commission ;

« La proposition introduit des mesures de surveillance plus strictes pour les autorités nationales, des exigences d'application plus strictes et vise à harmoniser les régimes de sanctions dans les États membres. »

Source : https://ec.europa.eu

Les secteurs concernés par le NIS 1 & 2 (Hors sous-secteurs)

Secteurs NIS1 (opérateurs de services essentiels - OSE)

- Energie
- Transport
- Finances (banques et établissements financiers)*
- Fournisseurs de service numériques (FSN)
- Eau potable
- Infrastructures Numériques + Telecom and Co
- Santé

Nouveaux secteurs NIS2 (entités essentielles)

- Eau usée
- Autorités publiques publique
- Espace
- Fournisseurs de services TIC

Nouveaux secteurs NIS 2 (entités importantes)

- Services postaux
- Alimentation
- Chimie
- Fournisseurs numériques
- Recherche
- Gestion des déchets

2. Les Menaces Cyber & Co

2. Etat des menaces : ETAT contre ETAT : exemple IRAN vs ISRAEL

Iran 'opened a Pandora's box' in cyber attack on Israeli water system

The reported Israeli retaliation will give the Islamic Republic reason to think twice before launching a new cyber attack on Israeli civilian targets, according to Israeli defense experts.

BY YAAKOV LAPPIN

Israel's Sorek Desalination Plant on Nov. 22, 2018. Photo by Isaac Harari/Flash90.

Selon un ancien responsable de la défense israélienne, la cyberattaque iranienne de début avril 2020 contre une installation israélienne de traitement de l'eau, destinée à faire en sorte que les ordinateurs ajoutent trop de chlore à l'approvisionnement en eau d'Israël, représente une nouvelle phase de l'agression iranienne.

BUT : Nuire au infrastructure Civile
Impact : Assoiffer la population si l'attaque fonctionne en pleine canicule

Solutions de base avant attaque :

1. Upgrade des OS
2. Sécurité des comptes ADMIN
3. Monitoring d'alerte
4. Analyse heuristique des actions Malveillantes

Contre - attaque > paralysie du principal port maritime de l'Iran, le port Shahid Rajaee dans la ville de Bandar Abbas, qui est une plaque tournante stratégique pour les importations et exportations maritimes iraniennes et le trafic d'armes illicites.

Sources : https://www.jns.org/iran-opened-a-pandoras-box-in-cyber-attack-on-israeli-water-system

Principales Menaces - 2020

- L'argent est le vecteur principal de la motivation ;
- Attaque des fournisseurs (chaine d'approvisionnement) ;
- Attaque sur les infrastructures critiques ;
- Cyber espionnage ;
- Attaques > phishing email > brute force > RDP > Ransomware ;
- Erreurs humaines (Télétravail) ;
- Pic d'incidents cloud non malveillant ;
- Mauvaise configuration ;

… RasS ; PhaaS ; BeC ; RDoS ???

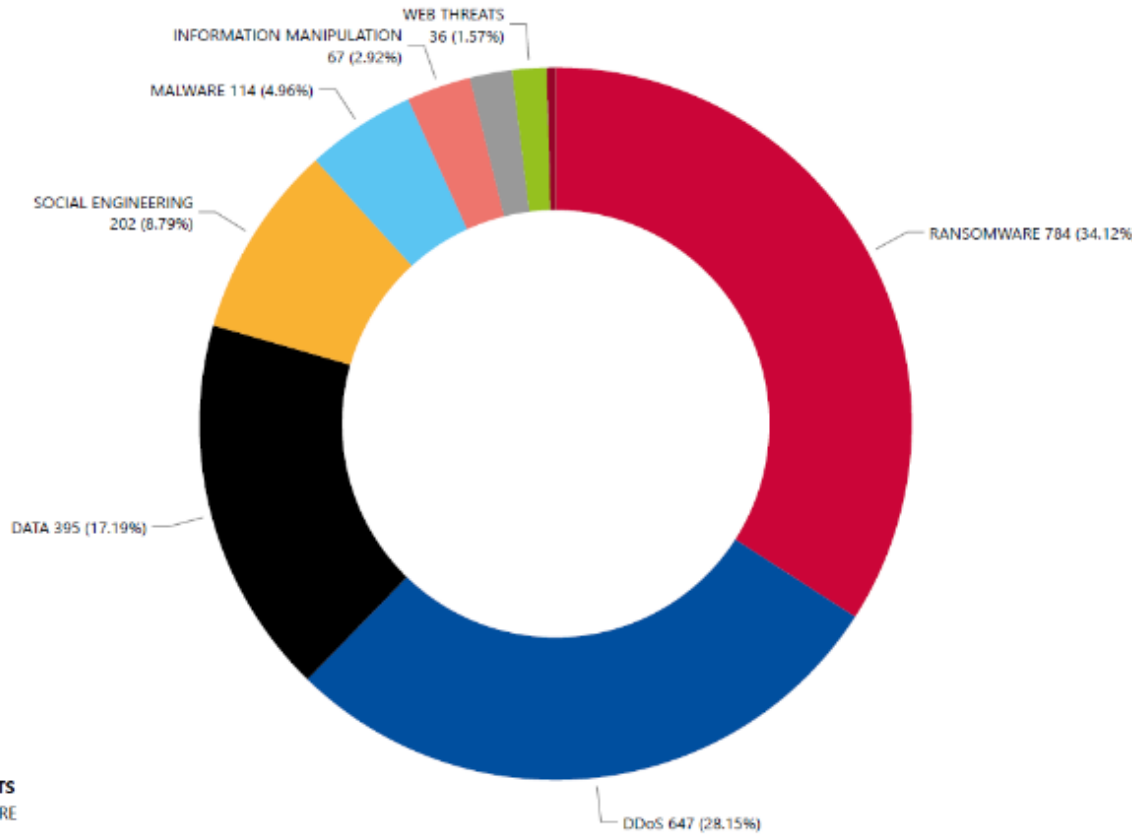
file:///C:/Users/AL5133/Downloads/ENISA%20Threat%20Landscape%202023.pdf

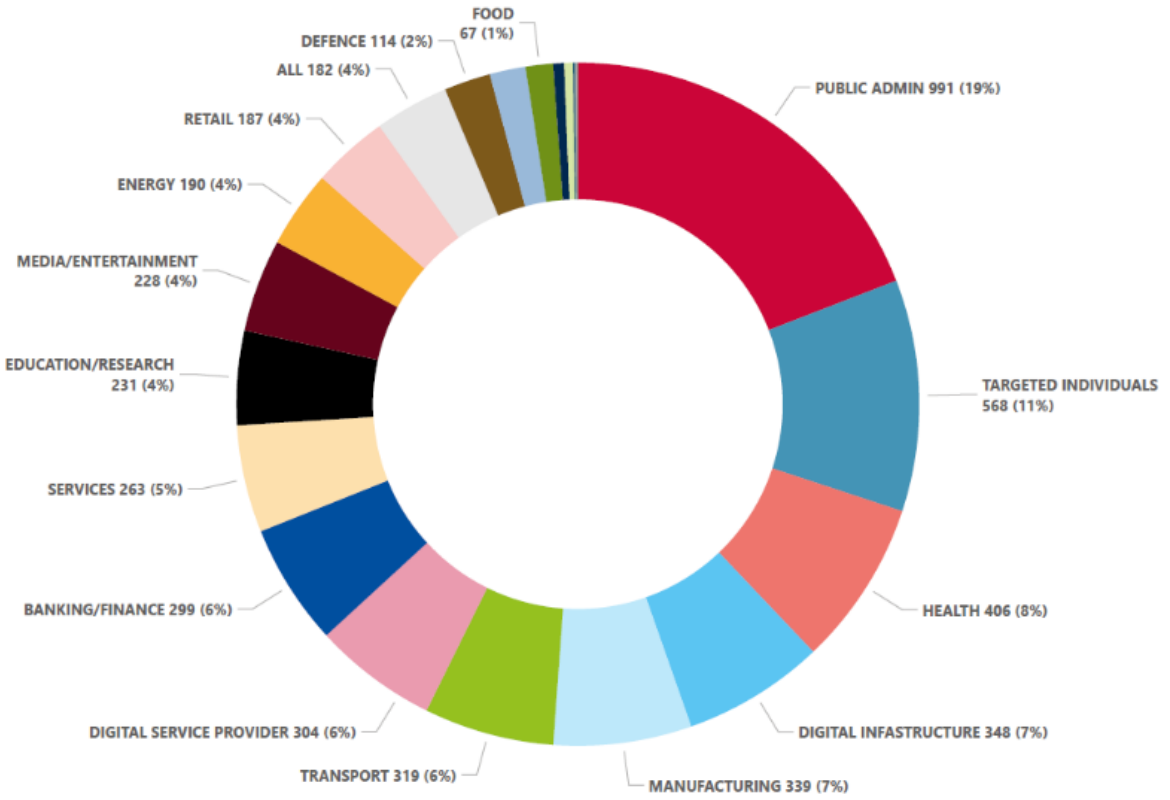
Principales Menaces - 2023

- Les ransomwares et les menaces de de disponibilité se classent 1er ;
- Les acteurs des menaces détournent des outils légitimes pour limiter le risque de se faire identifier.
- La géopolitique continue d'avoir une forte incidence sur les cybers ops.
- Hackeur As A Service explose !
- L'extorsion de fond s'est professionnalisée.
- Intensification d'opération de répression et le démentellement de groupe.
- Augmentation des zéro days.
- Menaces la plus répandue sont les téléphones mobiles est le SPYWARE.
- Les hacktivistes se surestiment… mais attaques…
- Compromission des mails business
- Attaque via les technologies Microsoft.
- Compromission de données …
- Chatbot est un risque avec IA (Information)
- Attaques DDOs de plus en plus importantes & complexes
- Menace de fermeture d'internet !
- Augmentation des cas Manipulation de la Russie sur Internet/Web 2.0 (Pas uniquement l'Ukraine)
- Manipulation de l'information par l'IA
- Attaque sur les chaines d'approvisionnement … passage par les employés (Privilèges élevés)

file:///C:/Users/AL5133/Downloads/ENISA%20Threat%20Landscape%202023.pdf

Exemples de menaces / secteurs touchés

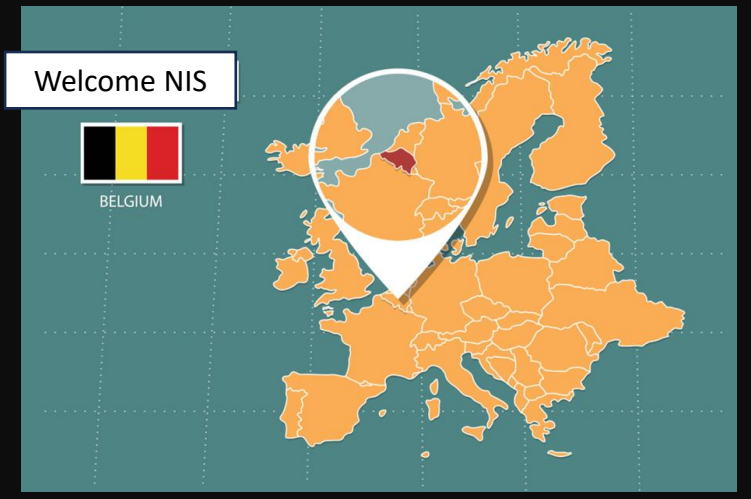




file:///C:/Users/AL5133/Downloads/ENISA%20Threat%20Landscape%202023.pdf

3. NIS 1 et NIS 2

Europe vs Belgique



3.1 NIS : Qui dirige ?

EUROPE : Point de contact est **l'ENISA**
European Union Agency For CyberSecurity

BELGIQUE: Point de contact et référent est le **CCB :**
Centre pour la Cyber Sécurité

Autorité sectorielle :
Une commission avec des présidents :
on ne peut pas savoir qui sait …
on ne peut pas avoir les mails si on n'est pas un OSE. (Essentiel & Important pour NIS 2)

Contacter nis@ccb.belgium.be

On ne peut pas en parler ! Rien dans la presse …

Stratégies Nationales

Groupement des CIRST

Groupe de coopération européenne

Sources : www.enisa.eu

3.1 NIS : Ça sert à quoi ?

Une directive devenue loi qui oblige surtout à :

- **Améliorer les capacités nationales** en matière de cybersécurité ;
- **Renforcer la coopération** au niveau de l'Union européenne ;
- Promouvoir une culture de la **gestion des risques** et du **signalement des incidents** ;
- Utiliser des **Framework de sécurité** ;
- Être dans **les règles de l'art** en la matière ;

} Europe

*Center for Security and Response Team

Sources : www.CCB.gov.be & www.ssi.gouv.fr

3.2 NIS 1 : Legal : Qui fait quoi ?

Entité fédérée, région,…

Service de certification et d'inspection

NIS COOPERATION GROUP

CENTRE FOR CYBER SECURITY BELGIUM

ibz Centre de crise Intérieur

Sectoral authority

National Bank

FSMA

BIPT

Sectoral authorities
Identification OES, Control/sanctions OES

CENTRE FOR CYBER SECURITY BELGIUM

Sources : www.CCB.gov.be

3.2 NIS 1 : Legal : vous êtes quoi ?

***En Belgique** : VOUS ETES UN « SERVICE ESSENTIEL » dit « opérateur de service essentiel » ?*

L'OSE visé par la loi NIS est une entité **publique ou privée** qui exerce effectivement une activité en Belgique :

- liée à la fourniture d'un service essentiel dans l'un des secteurs repris à l'annexe I de cette loi,
- dispose d'au moins un établissement sur le territoire belge,
- et qui est reconnue, par décision administrative de l'autorité sectorielle compétente
    - (Voir ci-dessous question n°4), comme fournissant un service essentiel.

VOICI les CRITERES CUMULATIFS :

- ✓ 1. Appartenir à l'un des secteurs ou sous-secteurs visés à l'annexe I de la loi NIS ;
- ✓ 2. Fournir un service qui est qualifié de « service essentiel » par l'autorité sectorielle compétente ;
- ✓ 3. La fourniture du service est tributaire des réseaux et des systèmes d'information (ce qui est présumé être le cas par la loi NIS) ;
- ✓ 4. La survenance d'un « incident » lié à la « sécurité des réseaux et des systèmes d'information » de l'opérateur serait susceptible d'avoir un « effet perturbateur important » sur la fourniture du service essentiel (suivant les critères déterminés par l'autorité sectorielle compétente ;

Un service essentiel est un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques.

L'autorité sectorielle compétente détermine au sein de son secteur les services qualifiés de « services essentiels » en tenant compte notamment des services essentiels repris à l'annexe I de la loi NIS.

Sources : www.CCB.gov.be

3.2 NIS 1 : Légal : Cadre général légal

***BELGIQUE**: Point de contact est le **CCB** :*
Centre pour la Cyber Sécurité

Site Web : *https://ccb.belgium.be/ = le CSIRT*

**Exemple : https://www.cert.be/fr est devenu service opérationnel du CCB concernant les incidents ;*
https://ccb.belgium.be/fr/cert/signaler-un-incident
https://cert.europa.eu/

La Belgique dispose de 7 CSIRT (Organisation commerciale, ICT, financier, agence du gouvernement, …)

L'autorité sectorielle « Commission spéciale» il faut contacter le CCB : nis@ccb.belgium.be

En vigueur : Arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (entré en vigueur le 18 juillet 2019).

***Exemple d'échéance BELGE** : La PSI doit être faite dans l'année de l'identification > L'implémentation l'année d'après > Les audits et analyse de risques ensuite sur Maximum 3 ans. Des analyses internes chaque année et une externe (sur 3 ans).*

Rmq : Adoptée par les institutions européennes le 6 juillet 2016

*Computer Emergency Response Team

Sources : www.CCB.gov.be

3.3 NIS : Obligations générales : **Décodages Sécuritaires**


Enigma

Obligation légale

Management avec objectifs et mesures de sécurité, formation, PSI vraiment appliquées,…

1. La loi NIS entend garantir que les opérateurs de services dits essentiels prennent des **mesures de sécurité techniques** et **organisationnelles** afin de prévenir tout incident ou d'en **limiter l'impact** et, ce faisant, d'assurer la sécurité et la **continuité** de la vie des citoyens et entreprises européennes.

Antimalwares, IDS, IPS, Firewall, Sandboxing, logs… (>Forensics)

Plan de continuité d'activité général (Et plan informatique/cyber compris)

Analyse de risques pas uniquement sur les données ! (Hors DPIA)

2. Les OSE qui sont victimes d'une cyberattaque doivent le signaler à un organisme central. Le signalement des incidents permettra une meilleure coopération et une meilleure identification des menaces.

Gestion des incidents de sécurité EST différents de la gestion des BUGs ou Incident normaux.

Traçabilité et échange d'information

Outils de veille et suivi.

Sources : www.CCB.gov.be

NIS2 Piliers principaux :

CENTRE FOR CYBERSECURITY BELGIUM

Capacités des états membres

Autorités nationales

Stratégies nationales

Cadres pour la divulgation coordonnée de la vulnérabilité (DCV)

Cadres de gestion de crise

Management

Responsabilité du Management/direction en cas de non-conformité.

Les organisations essentielles et importantes **doivent** prendre des mesures de sécurité (Cyber compris).

Les organisations essentielles et importantes doivent notifier les incidents et les menaces.

Coopération et Echange d'information

enisa

NIS COOPERATION GROUP

Registre européen des vulnérabilités

Examens par les pairs entre États membres

Rapport annuel sur l'état de la cybersécurité dans l'UE

Registre des entités fournissant des services transfrontaliers

3.1 NIS ScreenShot de LOI NIS 1

Titre

7 AVRIL 2019. - Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Source : CHANCELLERIE DU PREMIER MINISTRE
Publication : 03-05-2019 numéro : 2019011507 page : 42857 **PDF : version originale**
Dossier numéro : 2019-04-07/15
Entrée en vigueur : 03-05-2019

Ce texte modifie les textes suivants :2003014009 2017014203 2011000399 1998003158 2002003392 1994025189

3. Quel est l'objet principal de la directive NIS2 ?

CENTRE FOR CYBERSECURITY BELGIUM

La directive du NIS est une matière principalement liée à la sécurité publique qui est une compétence fédérale

(Avis du Conseil d'Etat)

Champ d'application limité des entités

Taille maximale/type d'entité dans les annexes +. identification nationale

(//NIS1 : entités fournissant des services essentiels et/ou des infrastructures critiques)

Obligations communes en matière de cybersécurité (Trans-sectorielles)

menace cybernétique" : toute circonstance, tout événement ou toute action susceptible d'endommager, de perturber ou de compromettre de toute autre manière les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et d'autres personnes - article 6, paragraphe 10, de la directive. 6 (10)

Essential entities (art. 2 and 3)

Entités essentielles (art. 2 et 3)

Grandes entités (> 50M ou 250 ETP) de l'annexe I " Secteurs de haute criticité " + Directive entités critiques CER + identification nationale basée sur la criticité - art. 2 (2).

Mesures de gestion des risques liés à la cybersécurité (art. 21)

Prévenir *ou minimiser l'impact des incidents sur les destinataires de leurs services et sur d'autres services* (y compris leur impact sociétal et économique).

Entités importantes (art. 2 et 3)

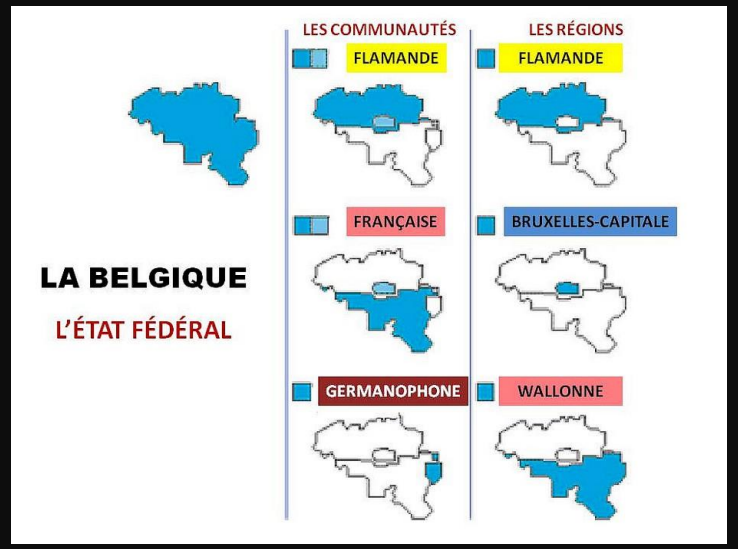
Entités moyennes (> 10M ou 50 ETP) de l'annexe I " Secteurs de haute criticité " + entités grandes ou moyennes de l'annexe II " Autres secteurs critiques " + identification nationale basée sur la criticité - art. 2 (2).

Obligations de signalement(art. 23)

notifier tout incident ayant un impact significatif sur la fourniture de leurs services ;

communiquer aux destinataires de leurs services toute menace cybernétique significative ;

4. Champs application



4. NIS2 Directive entity of the public sector

- **Art. 2 (2).** Quelle que soit leur taille, la présente directive s'applique également aux entités d'un type visé à l'annexe I ou II, lorsque :

- (f) l'entité est une entité de l'administration publique :

- (i) de l'administration centrale telle que définie par un État membre conformément au droit national [niveau fédéral] ;

- (ii)au niveau régional tel que défini par un État membre conformément au droit national qui, à la suite d'une évaluation fondée sur les risques, fournit des services dont l'interruption pourrait avoir un impact significatif sur des activités sociétales ou économiques critiques. [niveau fédéré]

- **Art. 3 (1).** Aux fins de la présente directive, les entités suivantes sont considérées comme des entités essentielles:

- (d) les entités de l'administration publique visées à l'article 2, paragraphe 2, point (f) (i) du gouvernement central

- l'administration publique fédérale

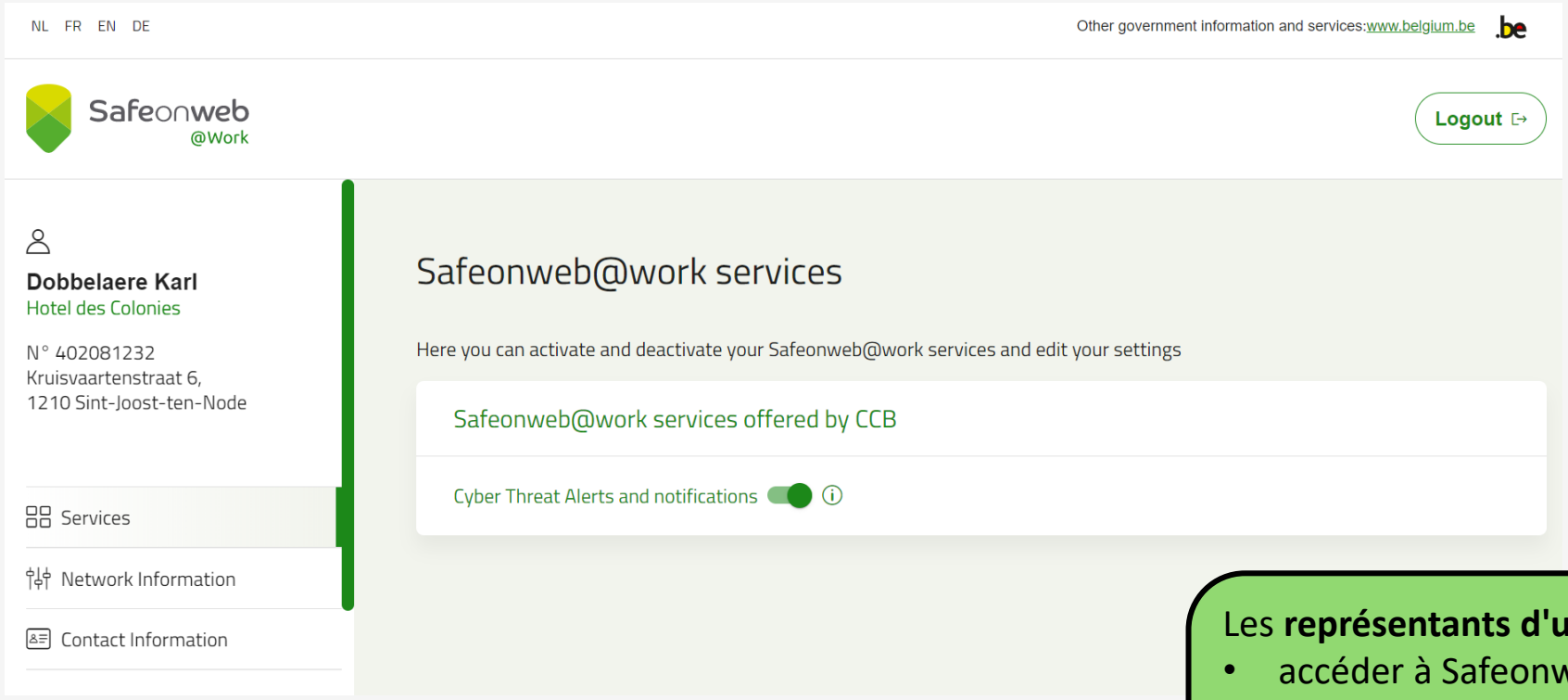
4. Définition d'une entité de l'administration publique :

Art. 8 34° « entité de l'administration publique » : une autorité administrative visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants :	Art. 8 34° "overheidsinstantie": een administratieve overheid als bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:
a) elle n'a pas de caractère industriel ou commercial;	a) zij is niet van industriële of commerciële aard;
b) elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi.	b) zij oefent niet hoofdzakelijk een activiteit opgesomd in de kolom soort entiteit van een van de andere sector of deelsector van een van de bijlagen.
c) elle n'est pas une personne morale de droit privé.	c) zij is geen privaatrechtelijke rechtspersoon.

Champs d'applications	En dehors du champ d'application
Entités de l'annexe I et de l'annexe II (+ voir size-cap*) **Administrations publiques dépendant de l'Etat fédéral :** **Dont :** - SPF Justice (avec une exclusion pour la base de données judiciaire) ; - SPF Intérieur (avec une exclusion partielle pour le NCCN) ; - SPF Affaires étrangères (avec une exclusion pour les réseaux et systèmes d'information des ambassades en dehors de l'UE). Zones d'urgence	Certaines **administrations fédérales** actives dans le domaine de la sécurité nationale et/ou publique (art. 5) (en partie) : SGRS/ADIV Sûreté de l'état / VSSE OCAM/OCAD Ministère de la Défense Police & Inspection Générale de la Police CCB / NCCN Comité P / Comité R **Autorités judiciaires et juridictions** **Parlements** **Banque nationale de Belgique.** **Installations nucléaires - classe I** (à l'exception des parties utilisées pour la production et la distribution d'électricité)
Les **administrations publiques fédérées identifiées** (régions et/ou communautés).	Les **administrations locales et le secteur de l'éducation s'attendent à ce qu'ils fournissent un service mentionné à l'annexe I ou II** (ou spécifiquement identifié).
	Systèmes d'information classifiés ou systèmes de documents nucléaires

4. Mécanisme d'enregistrement obligatoire

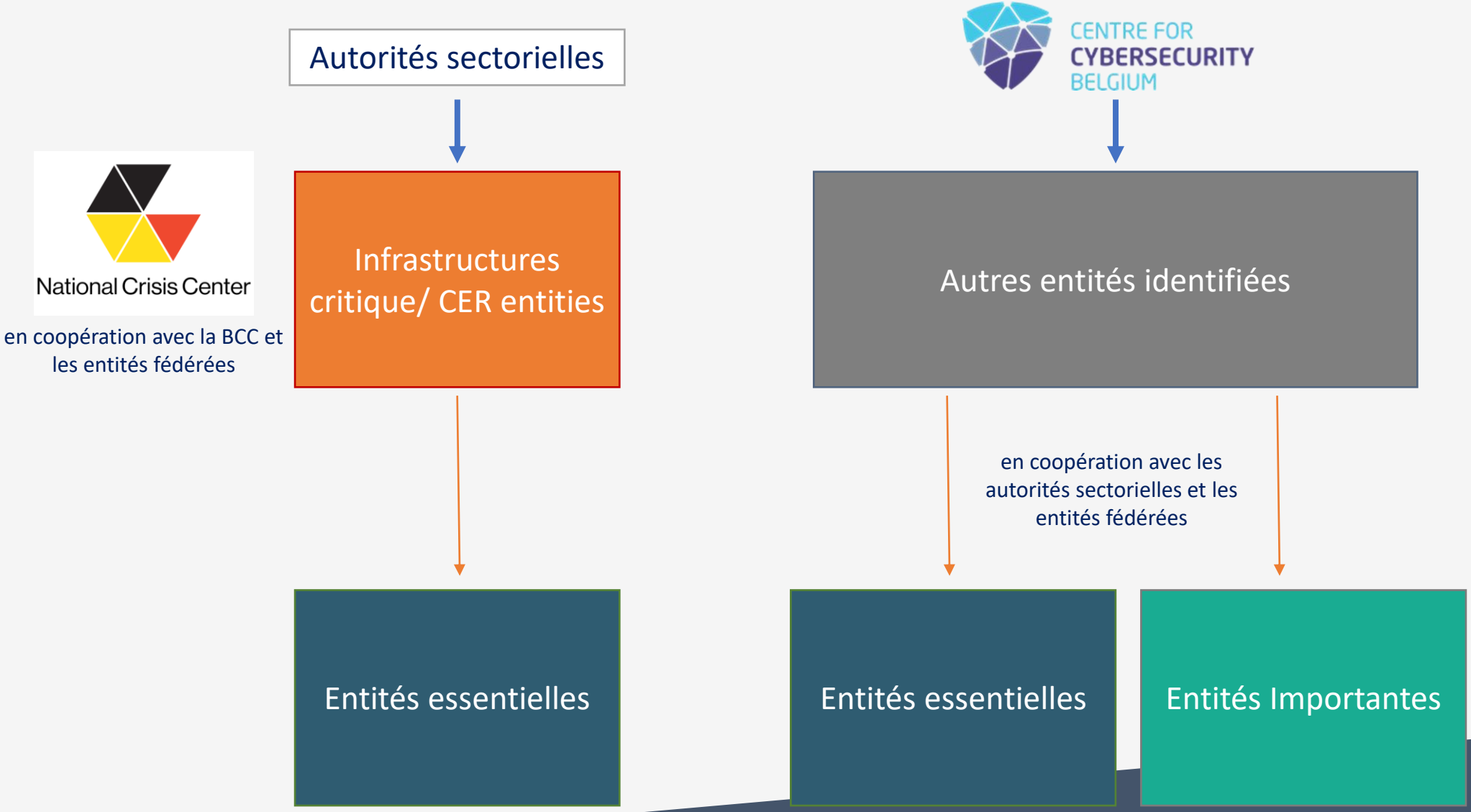
Réutilisation des données existantes détenues par les administrations publiques sur les entités du NIS2 (principe administratif du "only once")



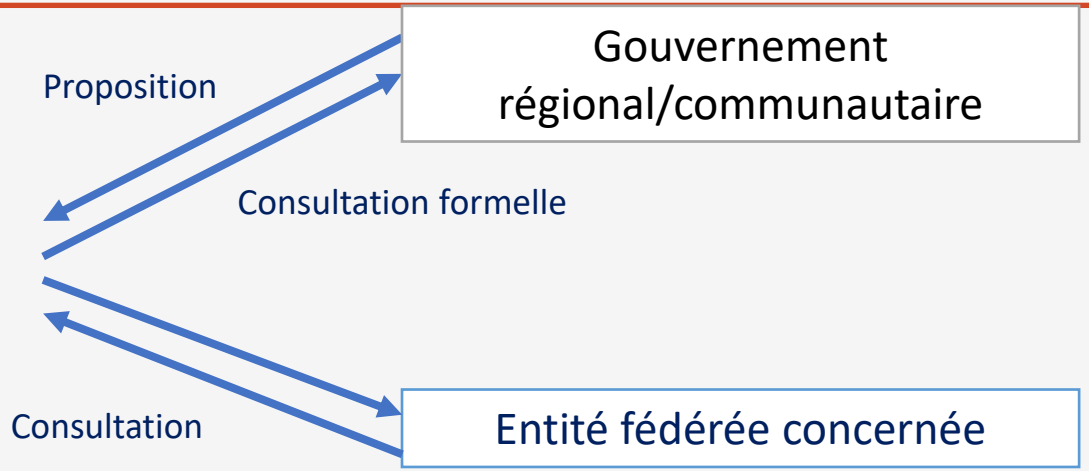
Les **représentants d'une organisation pourront :**

- accéder à Safeonweb@work
- enregistrer leurs coordonnées et les informations relatives au réseau
- s'enregistrer *en tant qu'entité NIS*
- *indiquer* le *secteur d'*activité

4. Identification nationale supplémentaire

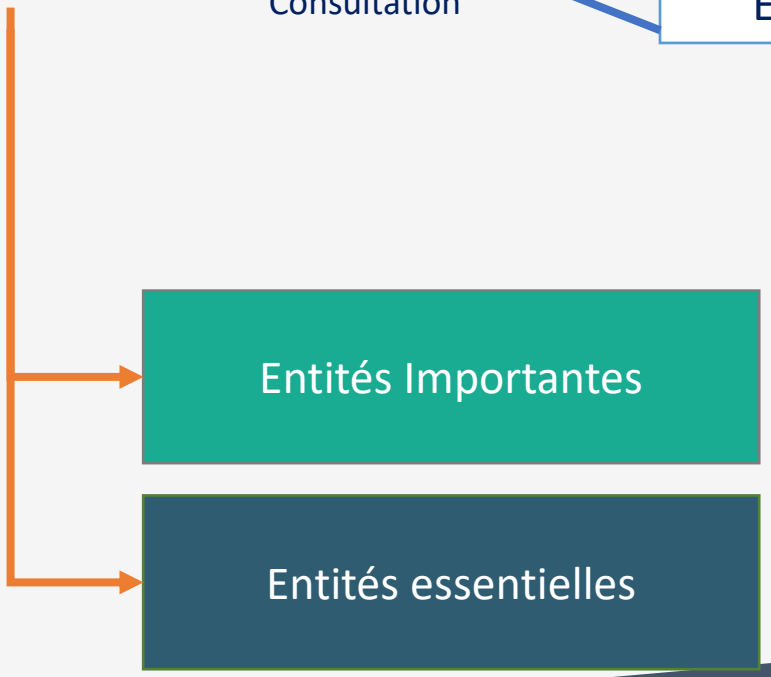


4. Processus spécifique pour l'administration publique fédérée



Identification basée sur l'évaluation des risques :

"Les autorités publiques [...] qui fournissent des services dont l'interruption pourrait avoir un impact significatif sur des activités sociétales ou économiques critiques." (art. 11, §2)



5. Autorités compétentes

CENTRE FOR CYBER SECURITY BELGIUM

5. Autorité nationale de cybersécurité

- Le Centre pour la cybersécurité en Belgique (CCB) est conçu comme l'autorité nationale CyberSec.
- L'autorité nationale de cybersécurité est chargée de :
  - contrôler et coordonner la mise en œuvre de la loi NIS2
  - contrôler sa mise en œuvre par les entités essentielles et importantes (QUID des Basic ?)
  - Gérer les crises et les incidents liés à la cybersécurité
- L'autorité nationale de cybersécurité est :
  - l'autorité compétente pour la supervision des entités essentielles et importantes (avec le soutien des autorités sectorielles/services d'inspection)
  - le CSIRT national
  - point de contact unique pour la mise en œuvre de la législation NIS2
  - Représentant de la Belgique dans le groupe de coopération
  - Représentant de la Belgique dans le réseau CSIRT
  - Représentant de la Belgique dans le réseau de l'organisation européenne de liaison en cas de crise cybernétique (EU-CyCLONe)

6. Gestion des risques / Frameworks de Cybersécurité / audit

6. Exigences générales en matière de cybersécurité (art. 20 et 21 de la directive)

CENTRE FOR CYBERSECURITY BELGIUM

Gouvernance

Mesures de gestion des risques liés à la cybersécurité

Obligation explicite d'effectuer une analyse des risques, d'adopter une politique formelle de sécurité de l'information (PSI/IBB) et une politique coordonnée en matière de vulnérabilité (CVD).

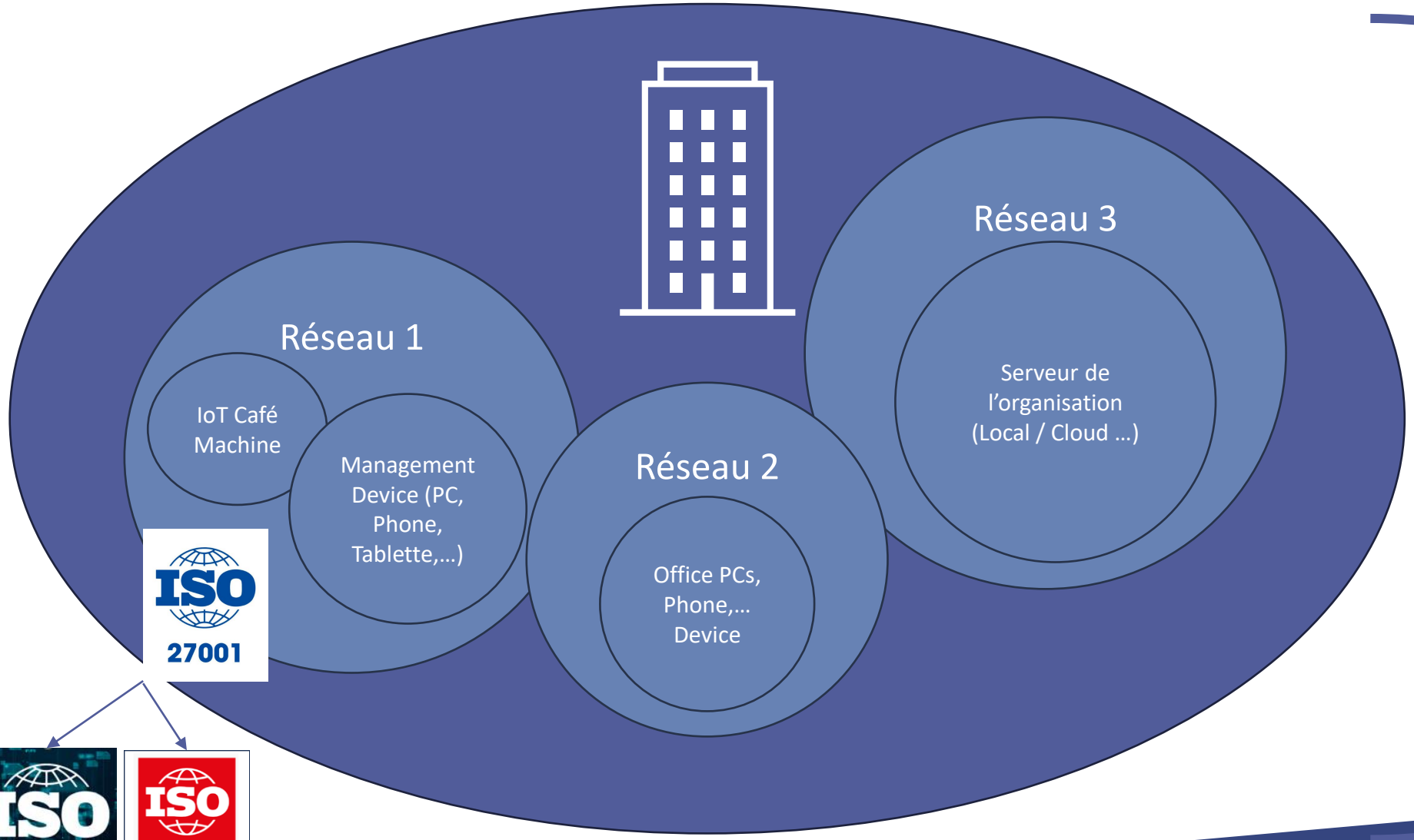
Présomption de conformité en cas de certification volontaire CCB Cyberfundamentals ou NBN ISO EN 27001 (avec le champ d'application correspondant)

ISO 27001

ISO 27002

ISO 27005

6. Mesures du champ d'application



Champ d'application du NIS 2 = entité entière

6. Mesures de gestion des risques (art. 21)

Appropriées **et proportionnées**

Gérer les **risques liés à la sécurité des réseaux et des systèmes d'information**

Utilisé pour nos activités ou pour la fourniture de nos services

Prévenir ou minimiser l'impact des incidents sur les destinataires de leurs services et sur d'autres services.

Mesures :

techniques, opérationnelles et **organisationnelles.**

+ Mana + Hum + Phys + Tech (ISO 27001)

Coût de la mise en œuvre

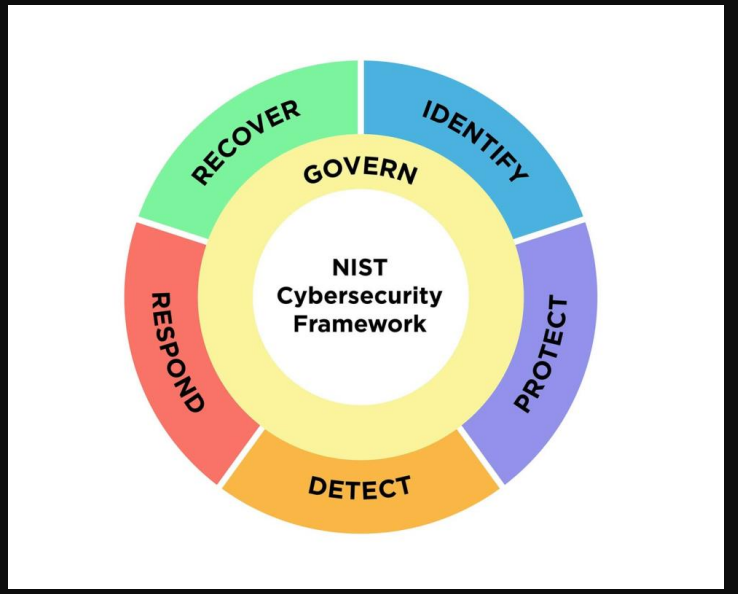
État de l'art et, le cas échéant, normes européennes et internationales pertinentes

Proportionnalité : degré d'exposition de l'entité aux risques, sa taille, la probabilité d'occurrence des incidents et leur gravité, y compris leur impact sociétal et économique.

6. NIS2: **Approche tous risques visant à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents**, et comprenant au moins les éléments suivants**(art. 21)** :

- (a) l'analyse des risques et les politiques de sécurité des systèmes d'information
- (b) le traitement des incidents
- (c) la continuité des activités, notamment la gestion des sauvegardes et la reprise après sinistre, ainsi que la gestion des crises
- (d) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité des relations entre chaque entité et ses fournisseurs directs ou ses prestataires de services
- (e) la sécurité dans l'acquisition, le développement et la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités (CVD)
- (f) les politiques et procédures permettant d'évaluer l'efficacité des mesures de gestion des risques liés à la cybersécurité
- (g) les pratiques d'hygiène informatique de base et la formation à la cybersécurité
- (h) les politiques et procédures relatives à l'utilisation de la cryptographie (Chiffrement) ;
- (i) la sécurité des ressources humaines, les politiques de contrôle d'accès et la gestion des actifs ;
- (j) l'utilisation de solutions d'authentification multifactorielle ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes de communication d'urgence sécurisés au sein de l'entité, le cas échéant.

7. S’organiser ! Framework CCB



7. NIST Framework / ISO & compagnie

- Les mesures de niveau d'assurance de base sont en mesure de couvrir 82% des attaques.
- Les mesures au niveau d'assurance Important sont en mesure de couvrir 94 % des attaques.
- Les mesures de niveau d'assurance Essential sont capables de couvrir 99,99% des attaques.

- NIST CSF
- ISO 27001:2022
- IEC 62443-1 & 3
- CIS Controls V8

Equivalence Certification ISO 27001 > NIS 1 & 2

7. Cyberfundamentals Framework | Centre for Cyber security Belgium

Small

Le niveau de départ Small permet à une organisation de procéder à une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées.

7

LEVEL SMALL
▼ DOWNLOAD

Basic

Le niveau d'assurance **Basic** contient les mesures de sécurité de l'information standard pour toutes les entreprises. Ceux-ci fournissent une valeur de sécurité efficace avec des technologies et des processus qui sont généralement déjà disponibles. Lorsque cela se justifie, les mesures sont adaptées affinées.

33

LEVEL BASIC
▼ DOWNLOAD

Important

Le niveau d'assurance Important est conçu pour minimiser les risques de cyberattaques ciblées par des acteurs disposant de compétences et de ressources communes, en plus des risques de cybersécurité connus.

94

LEVEL IMPORTANT
▼ DOWNLOAD

Essential

Le niveau d'assurance Essentiel va plus loin et est conçu pour faire face au risque de cyberattaques avancées par des acteurs disposant de compétences et de ressources étendues.

103

LEVEL ESSENTIAL
▼ DOWNLOAD

BONUS : conseils d'orientation « CO » 99 CO 127 CO +- 320 CO

Mesures progressives et cumulatives : Basic 12 mois > Important > Essentiel (36 mois)

Small

Le niveau de départ **Small** permet à une organisation de procéder à une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées.

pdf

Download

Basic

Le niveau d'assurance **Basic** contient les mesures de sécurité de l'information standard pour toutes les entreprises. Ceux-ci fournissent une valeur de sécurité efficace avec des technologies et des processus qui sont généralement déjà disponibles. Lorsque cela se justifie, les mesures sont adaptées et affinées.

pdf

Download

Important

Le niveau d'assurance **Important** est conçu pour minimiser les risques de cyberattaques ciblées par des acteurs disposant de compétences et de ressources communes, en plus des risques de cybersécurité connus.

pdf

Download

Essentiel

Le niveau d'assurance **Essentiel** va plus loin et est conçu pour faire face au risque de cyberattaques avancées par des acteurs disposant de compétences et de ressources étendues.

pdf

Download

https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework

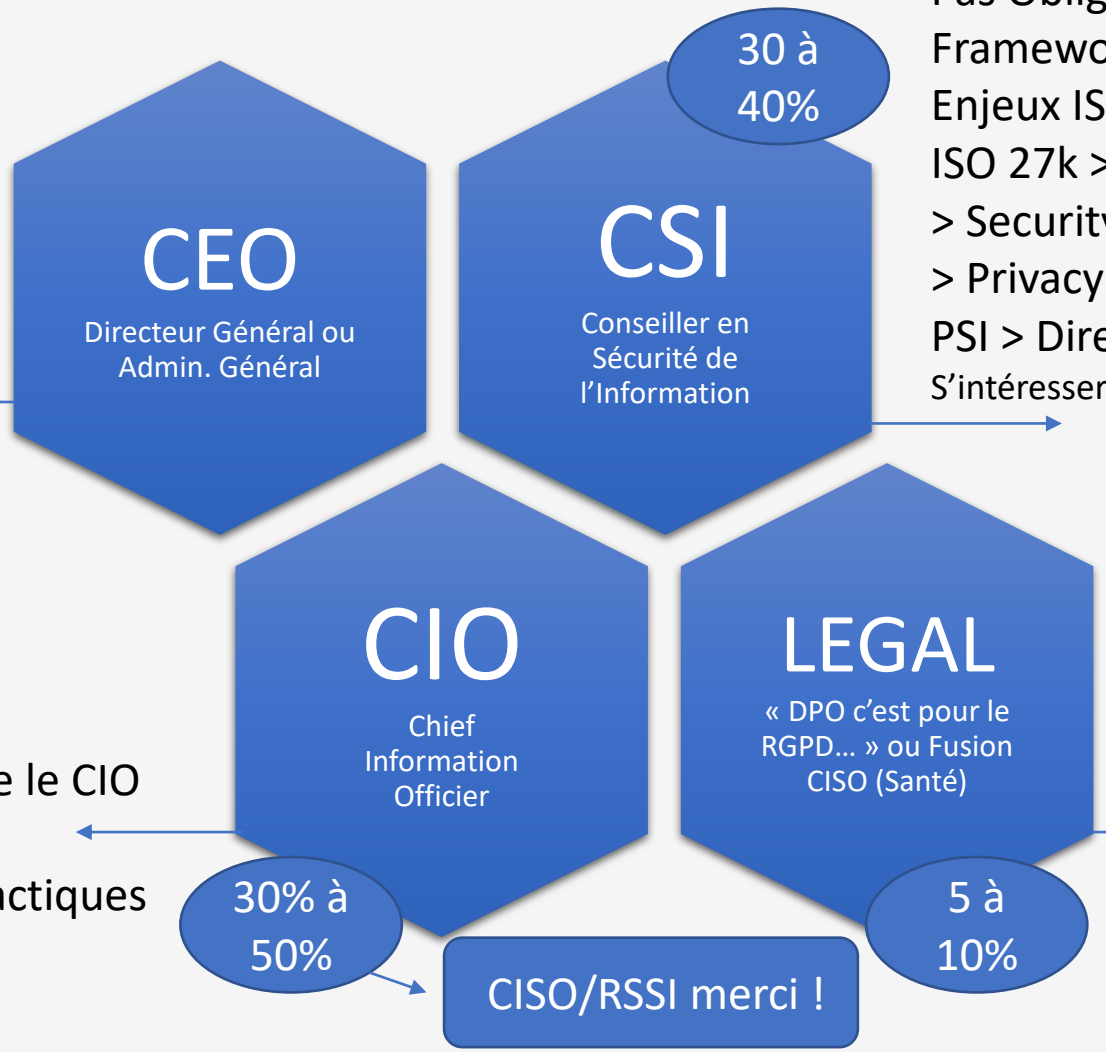
« Management Intégré avec le RGPD si possible ».

7 NIS : Team Exemple simplifié > Gouvernance NIS

Soutien et compréhension à ses équipes des enjeux des Framework sectoriels + ISO 27001 + OSE

Contact avec CCB et Autorité > Officialiser.

Une VRAI PSI ! (+Stratégie)



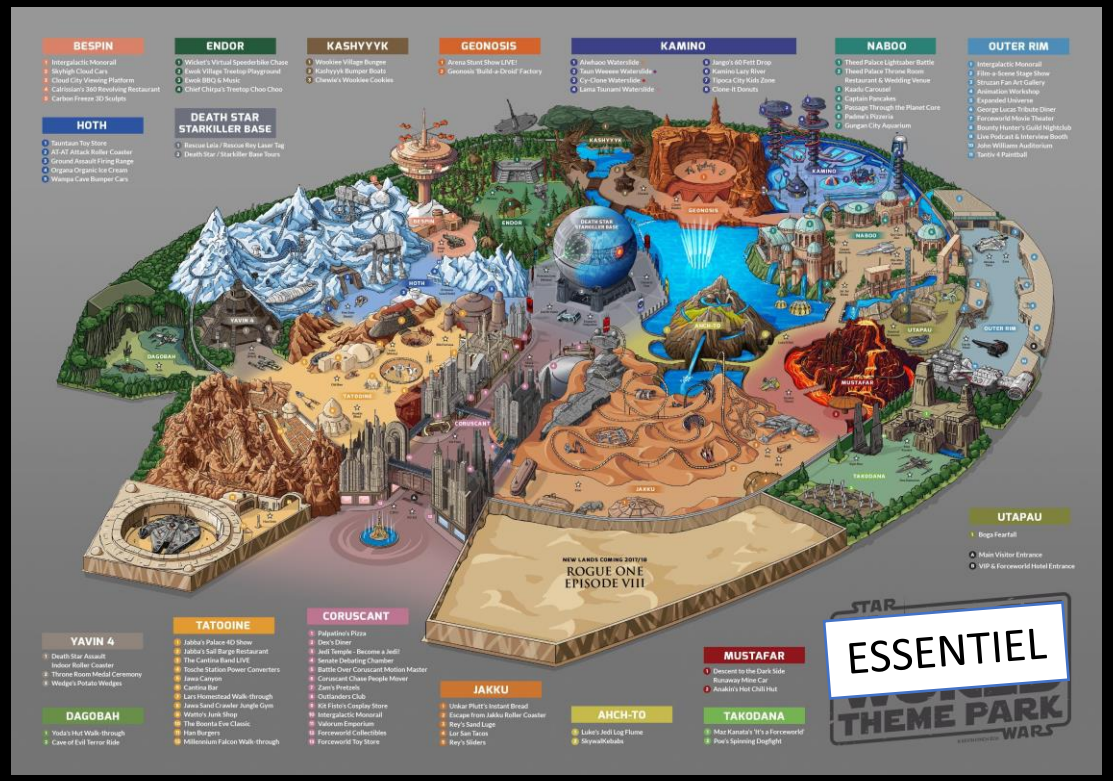
Pas Obligatoire > Car CISO MAIS !
Framework sur mesure
Enjeux ISO 27001 <> Comité de sécurité
ISO 27k > Normes de votre secteur
> Security By Design
> Privacy By Design
PSI > Directive Opérationnelle
S'intéresser au Cyber Security Act

Framework légal ou consigne
Privacy By Design
A18 de l'ISO 27001 > 27002

Nommer un **RSSI/CISO** qui décharge le CIO
Elévation du niveau de sécurité
Actions techniques et procédures tactiques
« La routine quoi ! ☺ »

+ RH
+ Autres services métier à écouter ;

8. S’organiser ! Dans quelle cour on joue ?



BASIC

IMPORTANT

8. Cadres de référence pour l'évaluation de la conformité

Les entités essentielles soumettent à une évaluation régulière de la conformité

- CyberFundamentals (CyFun®)
- ISO 27001
- Inspection par le CCB

↓

Obligatoire

Les entités importantes peuvent se soumettre à une évaluation régulière de la conformité

- CyberFundamentals (CyFun®)
- ISO 27001

↓

Volontaire

Évaluation de la conformité par un organisme d'évaluation de la conformité (OEC) accrédité et autorisé par le CCB

8. CCB Évaluation du risque de défaillance

Évaluation du risque de défaillance par secteur et par taille è niveau approprié de cyber fondamentaux

CENTRE FOR CYBERSECURITY BELGIUM

Version: 2023-08-03

Energy			*Common skills*		*Common skills*		*Common skills*		*Extended Skills*		*Extended Skills*	
Organization Size (L/M/S = 3/2/1)	**3**	*Threat Actor Type*	**Competitors**		**Ideologues Hactivists**		**Terrorist**		**Cyber Criminals**		**Nation State actor**	
Cyber Attack Category	*Global or Targetted*	*Impact*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0
	Total	Total		0		7,5		30		120		127,5

Score	CyFun Level
285	**ESSENTIAL**

https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/choosing-right-cyber-fundamentals-assurance-level-your-organisation

8. Évaluation des risques spécifiques

L'évaluation des risques est **obligatoire**.

L'évaluation des risques est au cœur du cadre des **cyber fondamentaux**

BASIC - ID.GV-4.1: Dans le cadre de la gestion globale des risques de l'entreprise, une stratégie globale de gestion des risques liés à la sécurité de l'information et à la cybersécurité doit être élaborée et mise à jour en cas de changement.

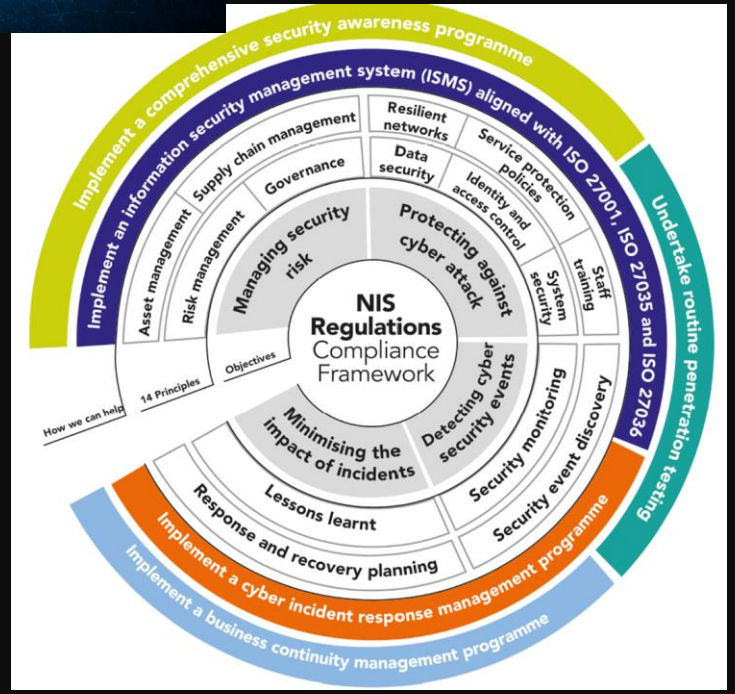
BASIC - ID.RA-5.1: L'organisme procède à des évaluations des risques dans lesquelles le risque est déterminé par les menaces, les vulnérabilités et l'impact sur les processus et les actifs de l'entreprise.

Aucune méthodologie spécifique n'est imposée pour l'évaluation des risques.
MAIS si vous devez suivre ISO 27001 … de manière « logique » c'est la « philo » ISO 27005.

9. S’organiser !

Inspecteur/Inspectrice
Directrice/Directeur

Management de base



9 Organisation de la CyberSécurité
1. Objectifs

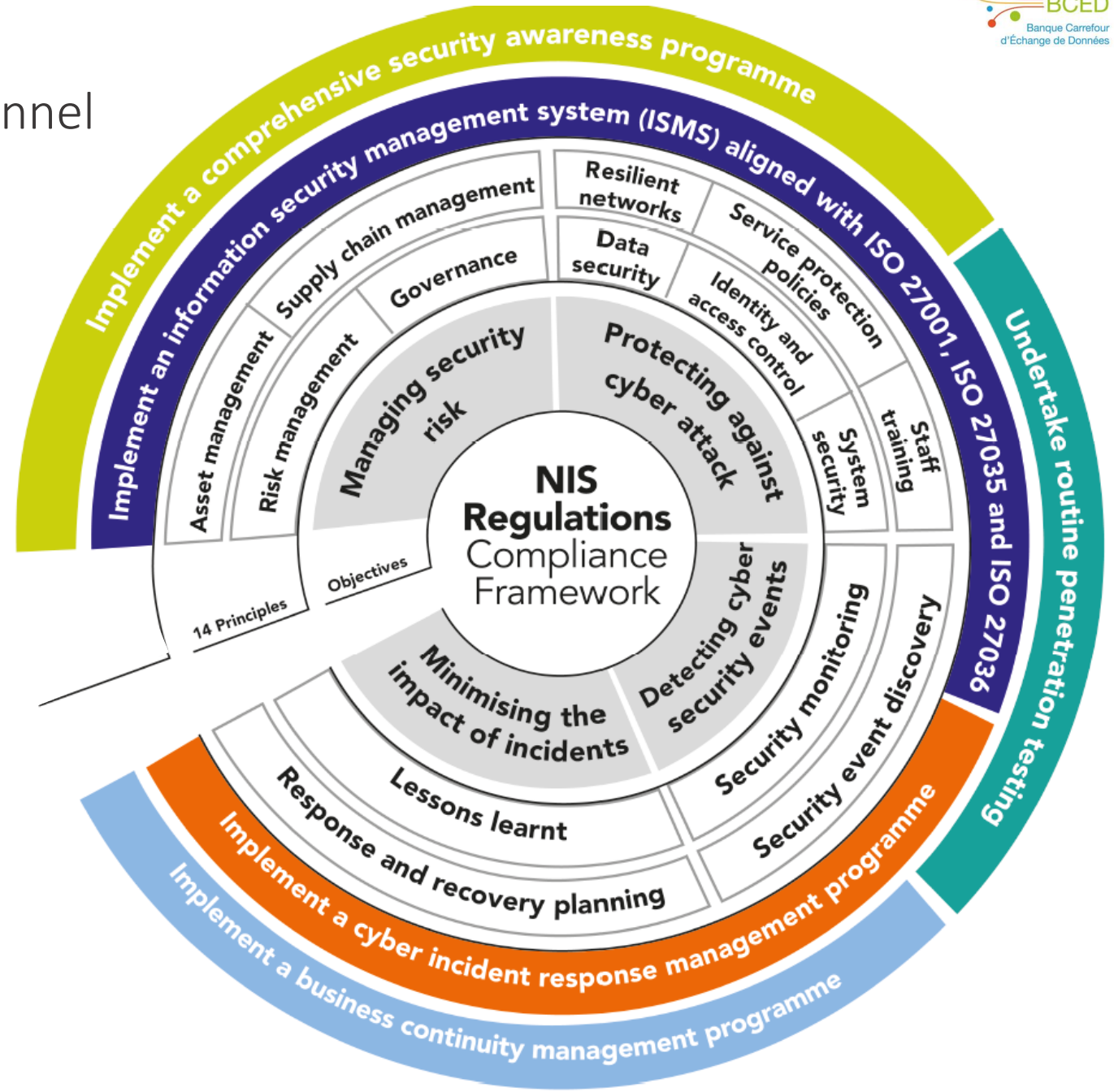
1. Manager le risque de l'information.
2. Se protéger des Cyber Attaques.
3. Détecter les incidents.
4. Minimiser l'impact des incidents.
5. +La direction :
    1. Approuve la gestion des risques ;
    2. Manage la vue d'implémentation des mesures ;
    3. Est responsable en cas de non-conformité ;
    4. Doit se former à la Cyber ;
    5. Adopte une procédure de formation pour l'équipe ;

Art. 22. § 1er. La P.S.I. visée à l'article 21, § 1er, est, jusqu'à preuve du contraire, présumée conforme aux exigences de sécurité, visées à l'article 20, lorsque les mesures de sécurité qu'elle comporte répondent aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi, par arrêté délibéré en Conseil des ministres.

Sources : https://www.itgovernance.co.uk

9 Organisation de la CyberSécurité
2. Management du risque informationnel

1. Mettre en place une **gouvernance NIS** (projet).
2. Mettre en place un **management des actifs.**
3. Mettre en place un **programme d'analyse de risques** (Idéal pas uniquement Cyber) : ISO 31000 + ISO 27005.
    1. **Manager le risques** avec **ARTEMIS** ou MONARQUE en **Belgique**.
    2. Ou EBIOS, OCTAVE, …
4. Gérer votre **chaîne d'approvisionnement :** Processus de la création à la destruction**.**



Sources : https://www.itgovernance.co.uk

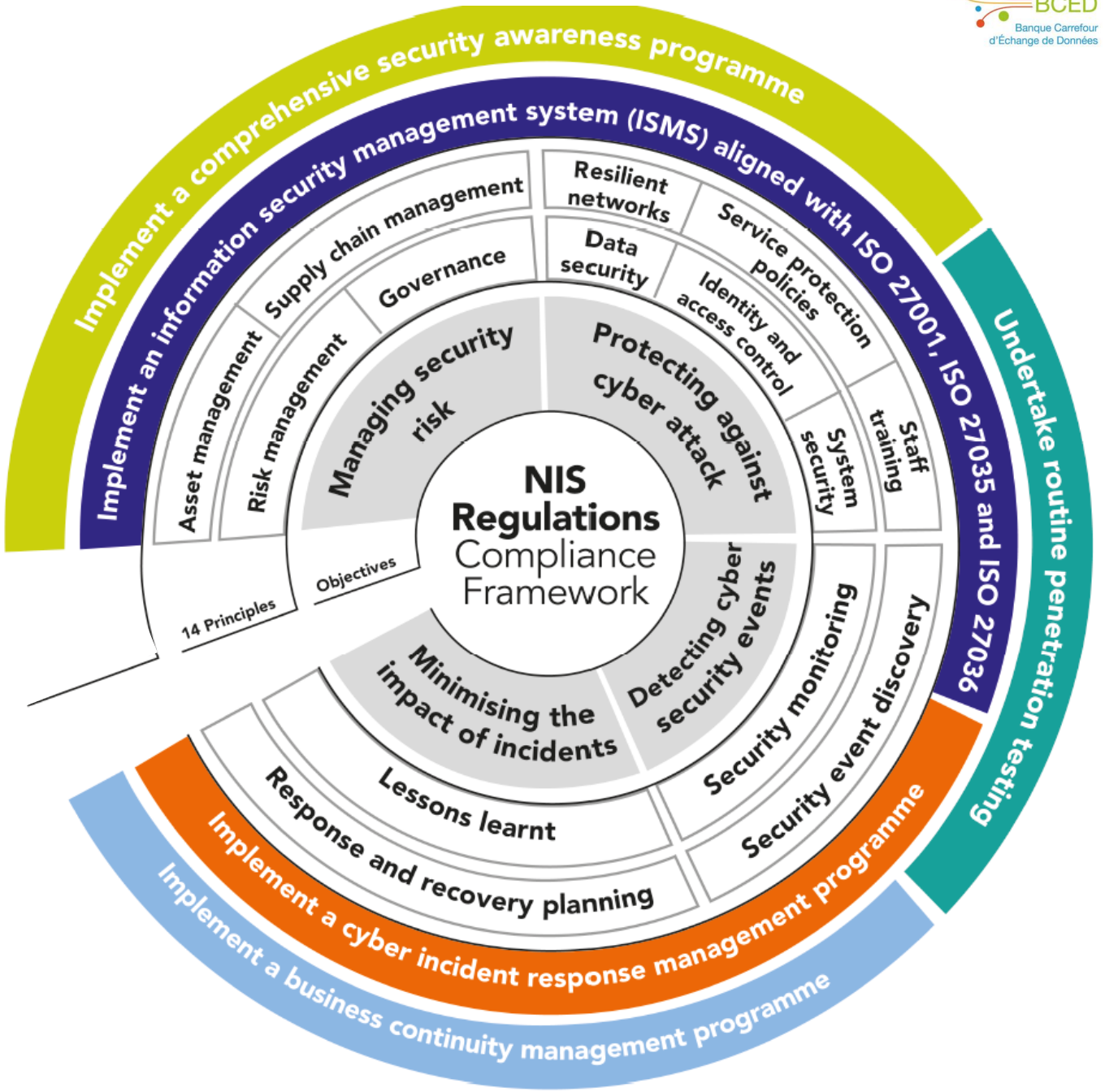
9 Organisation de la Cybersécurité
3. Se protéger des Cyberattaques

1. **Sécuriser vos données :** de la création de la donnée à sa destruction, de l'ouverture du flux à sa fermeture.
2. **Disposer de réseaux résilients :** avoir des réseaux redondants par exemple.
3. **Disposer de procédures de sécurité :** Une politique générale, des directives par annexe ISO et des procédures pour le terrain.
4. **Contrôle des identités et de la gestion des accès :** De la création à la destruction des comptes tout doit être tracé.
5. **Sécuriser vos systèmes :** en fonction des technologies chaque système est spécifique.
6. **Former votre personnel à la sécurité.**

Sources : https://www.itgovernance.co.uk

9 Organisation de la CyberSécurité
4. Détecter les incidents de sécurité

1. **Mettre en place un monitoring de sécurité** : disposer de logiciels détectant les anomalies, les menaces ou les attaques ;
    1. On parle *« d'Intrusions Detection System »* (IDS) avec une segmentation NIDS pour les réseaux (Network) et HIDS (Host bases) pour des machines) ; Un détecteur pour l'ensemble et des détecteurs par machines.
    2. Les IDPS : « *Intrusion detection and prevention systems* » permet d'identifier des comportements suspects et garantisse au besoin l'application des procédures de sécurité. C'est un complément devenu obligatoire au IDS et HIDS.
2. **Découvrir les évènements de sécurité et les tracer** : la directive NIS impose le traçage de tous les incidents de sécurité via un outil de gestion des incidents : de l'identification à sa résolution. Il est demandé également de communiquer vos incidents graves au CSIRT. Cette base de données d'incidents est une obligation légale.



Sources : https://www.itgovernance.co.uk

9 Organisation de la CyberSécurité
5. Minimiser l'impact des incidents

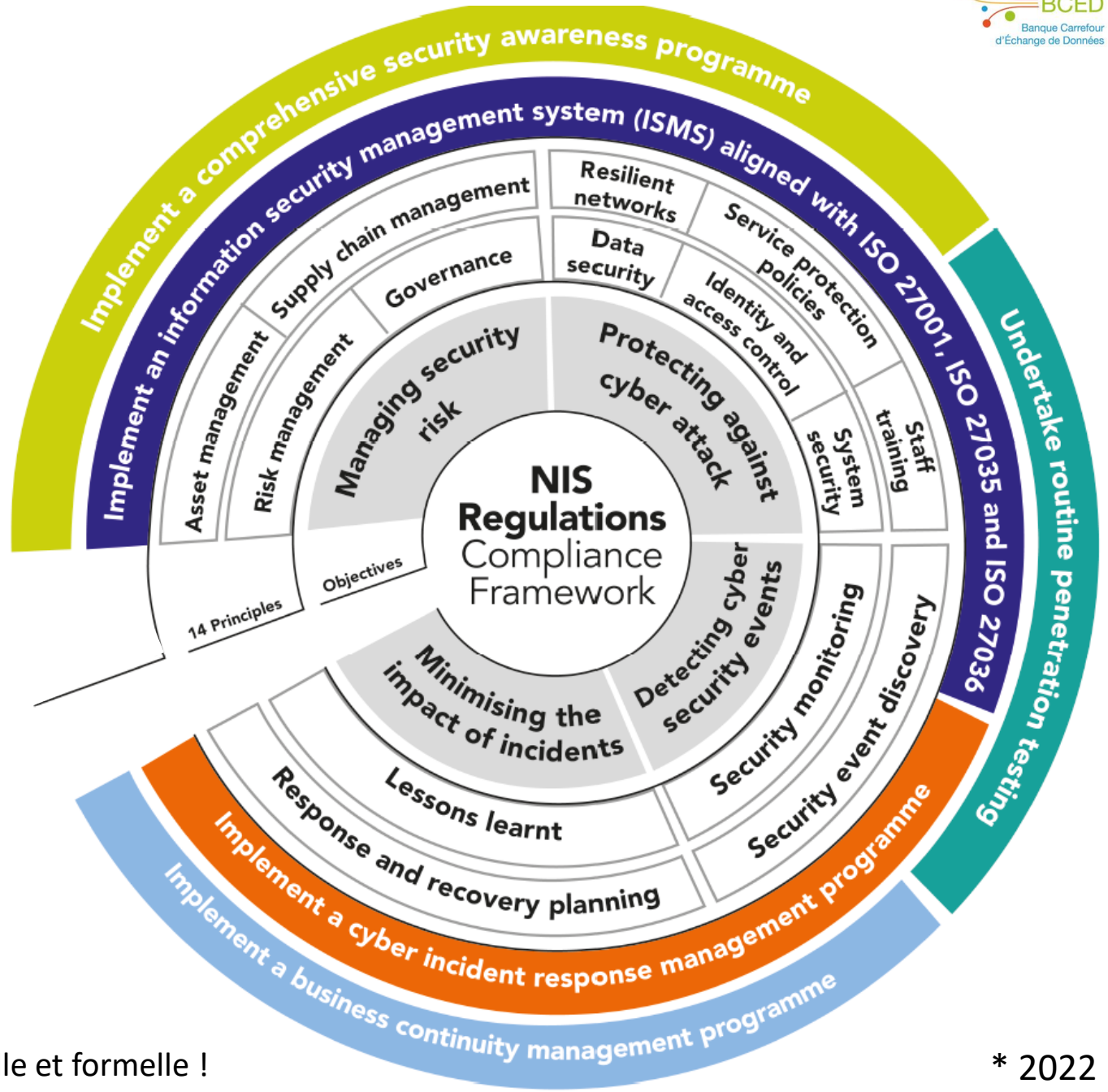
1. Disposer de rapports d'incidents qui permettent de comprendre comment a été résolu l'incident et quelles sont les actions de prévention, de détection ou de correction qui ont été mise en place ;

2. Disposer d'un planning qui permet de connaître le temps moyen des incidents. Ce planning va de pair avec le plan de continuité des incidents et la gestion des risques. L'idée est de permettre de savoir en combien de temps les services peuvent être opérationnels après un incident (Attaque de site, coupure de service,…)

Sources : https://www.itgovernance.co.uk

9 Organisation de la CyberSécurité
6. Méthodes complémentaires

1. Mise en place d'un management de la sécurité de l'information via les normes ISO 27k est recommandé* ;
   1. Ecriture d'une politique de sécurité, directives et procédures ;
   2. **Exigences** de sécurité ;
   3. Implication des employés et de la direction ;
2. Être « Alerte » et réagir aux attaques informatiques. (en relation avec le CERT)
3. Mise en place de 3 Programmes :
   1. Formation et sensibilisation à la sécurité ;
   2. Pen-test récurrent (Applications ; Réseaux ; …)
   3. Ecriture et test d'un plan de continuité d'activité en ce compris un plan de sécurité informatique ;



RAPPEL : Gestion des incidents de sécurité de manière officielle et formelle !

* 2022

Sources : https://www.itgovernance.co.uk

10. S’organiser !

Boots on the ground

En Pratique avec ISO 27001

10. ISO c’est quoi ?

- Norme internationale : « Organisation internationale de normalisation »
- Guidelines de bonnes pratiques
- Elle peut mener à une certification
- Multi Secteur et thématique
- Sortes de bibliothèque standardisée gigantesque
- Plus de 20000 normes depuis 1947
- Avec l’ISO on fait des audits… (entre autres) donc on peut détecter des mauvaises habitudes !
- … comme un « PCMN » finalement au niveau structure ☺

Search

I'm looking for 27000

Filter

- All results
- Standards [50]
- Pages [10]
- News [69]
- Publications [1]
- Documents [196]

Looking for the finer details?

Customize your search by combining multiple criteria

326 results found (1 ms)

ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

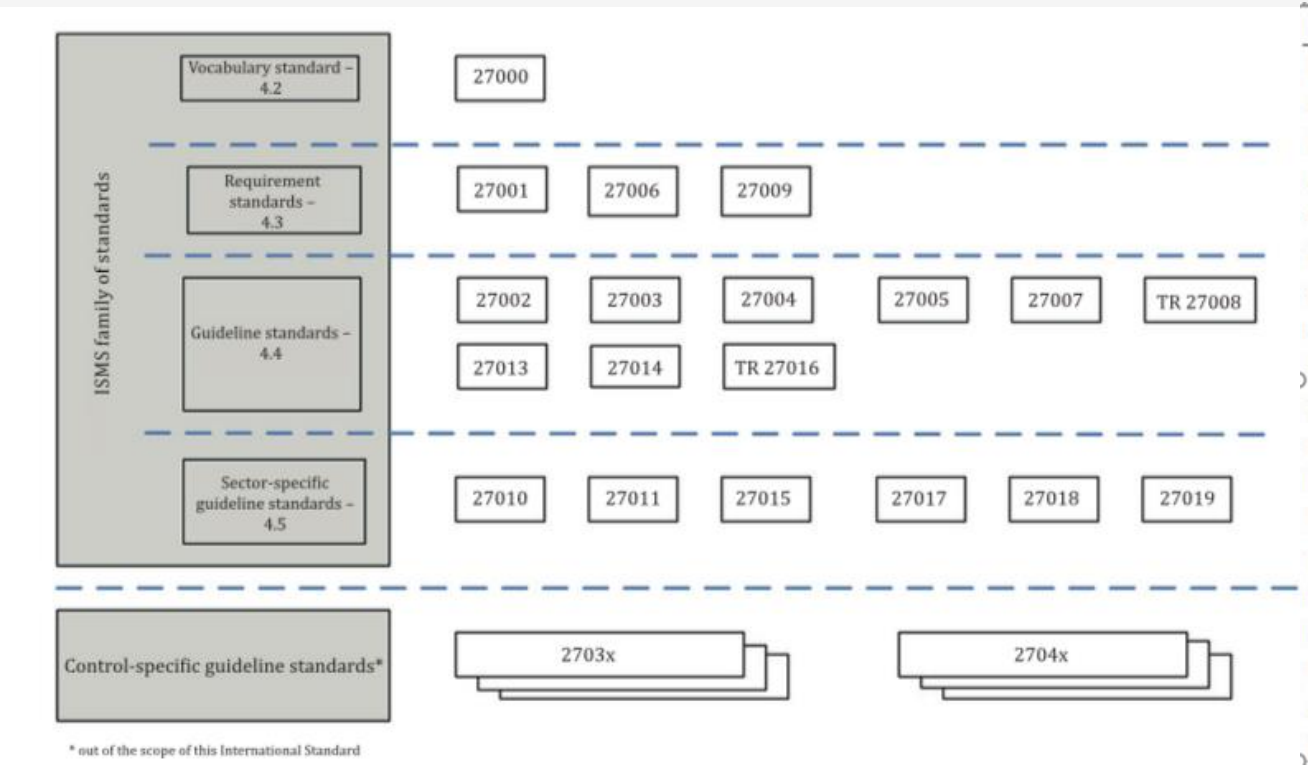
ISO/IEC **27000**:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, ...

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the ...

ISO/IEC 27001 Standard – Information Security Management Systems

10. Aie mon œil



ISO-Norm	Title
ISO 27000	Information security management systems—Overview and vocabulary
ISO 27001	Information security management systems—Requirements
ISO 27002	Code of practice for information security management
ISO 27003	Information security management system implementation guidance
ISO 27004	Information security management—Measurement
ISO 27005	Information security risk management
ISO 27006	Requirements for bodies providing audit and certification of ISMSs
ISO 27007	Guidelines for ISMS auditing
ISO 27008	Guidelines for auditors on ISMS controls
ISO 27010	ISMSs for inter-sector and inter-organizational communications
ISO 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO 27013	Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
ISO 27014	Proposal on an information security governance (ISG) framework
ISO 27016	Information security management—Organizational economics
ISO 27017	Guidelines on information security controls for use of cloud computing
ISO 27018	Code of practice for data protection controls for public cloud computing
ISO 27031	Guidelines for ICT readiness for business continuity
ISO 27032	Guidelines for cyber security
ISO 27033-1	Network security—Part 1: Overview and concepts

Mais aussi 27701 (RGPD)

10.Les Clauses de base :

- Contexte de l'organisation : SWOT + BMC + PESTEL + …
- Leadership : Direction + Politique + Rôle (+Responsabilités,…)
- Planification : Risques + Objectifs + Plan
- Support = Ressources * Compétences * Sensibilisation * Communication * Doc
- Fonctionnement : Planifications + Analyse de Risques + Traitement
- Evaluations et performances : Surveillance + Audit Interne + Direction
- Amélioration : non conformités + actions correctives + Kaizën

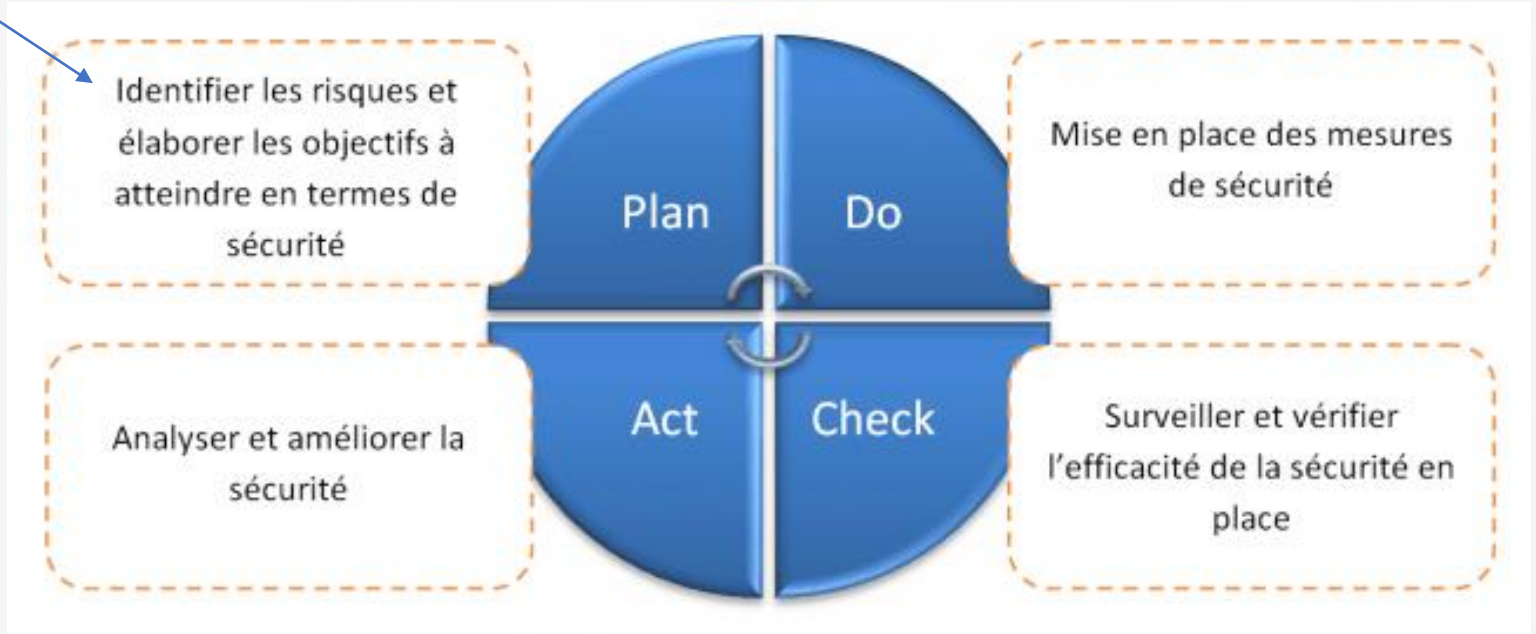
PSSI
PCA
PTR

Mitiger les risques

Comment détecter les failles dans le système d'information (informatique ou non) dans son entreprise / conseil pour procéder à un audit de sécurité ?

10. PDCA : PLAN DO CHECK ACT

« ANALYSE de RISQUES »



Sources PECB ISO 27001

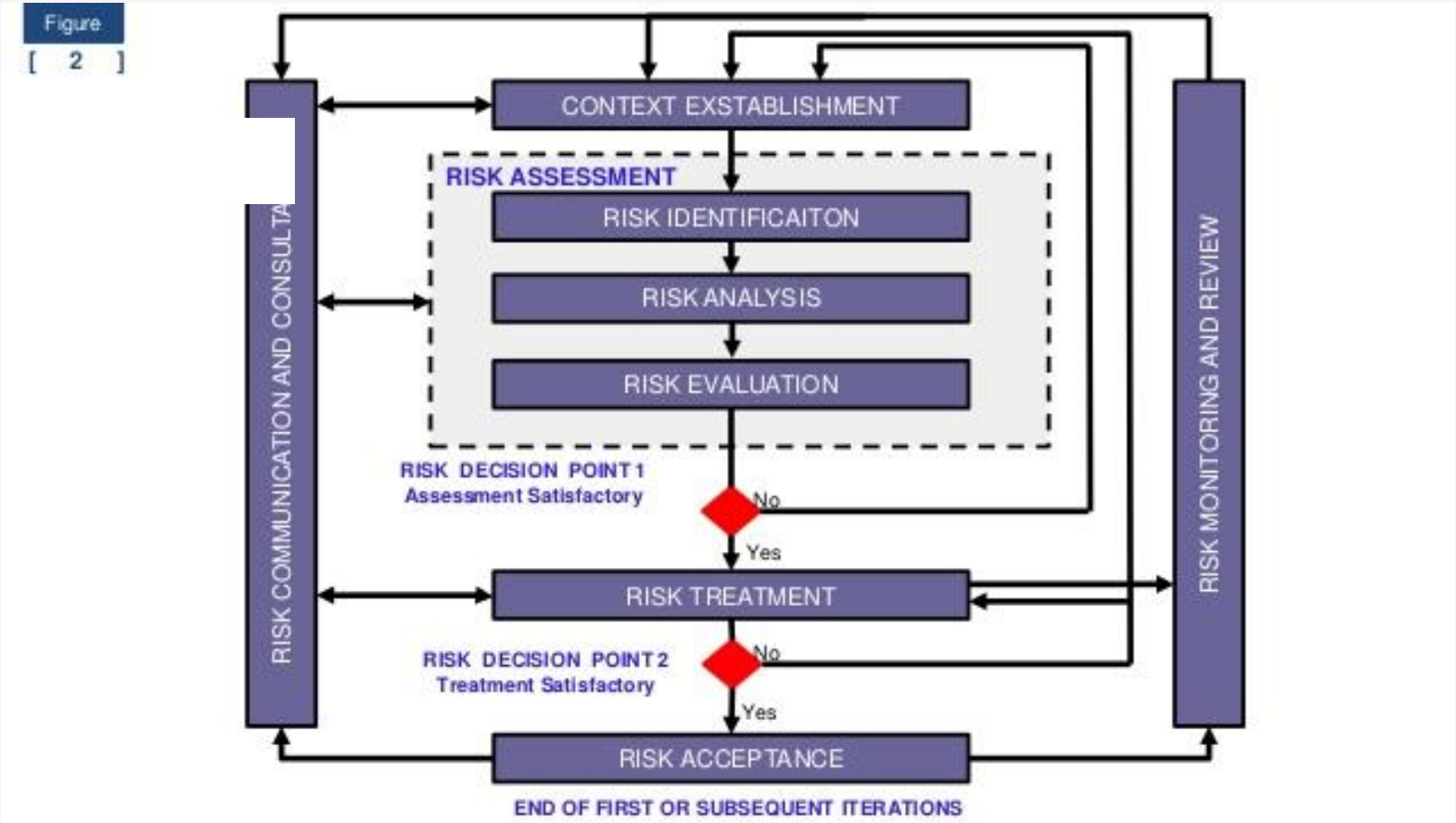
10. PDCA : THE FULL MÉTHODE

Plan	Do	Check	Act
Stratégie du SMSI	Structure organisationnelle		
Contexte de l'organisation	Informations documentées	Suivi, mesure, analyse et évaluation	
Analyse du système existant	Conception des contrôles et processus		Traitement des non-conformité
Leadership et gestion de projet	Communication	Audit Interne	
Périmètre	Sensibilisation et formation		Amélioration continue
Politique de sécurité	Mise en œuvre des contrôles	Revue de direction	
Appréciation des risques	Gestion des incidents		
Déclarations d'applicabilités	Gestion des opérations		

4 PHASES : 21 ETAPES : 101 SUBCATEGORIES : XXX SUBSUBCAT

Sources PECB ISO 27001

10. Iso 27005 : Risk



Sources Norme ISO 27005

10. Les nouvelles mesures ISO 27001:2023 + Attributs ISO 27002:2022

1. Renseignements sur les menaces
2. Sécurité des informations pour l'utilisation des services cloud
3. Préparation des TIC pour la continuité des activités
4. Surveillance de la sécurité physique
5. Gestion de la configuration
6. Suppression d'informations
7. Masquage des données
8. Prévention des fuites de données
9. Activités de suivi
10. Filtrage Web
11. Codage sécurisé

10. ISO 27002:2022 : ATTRIBUTS

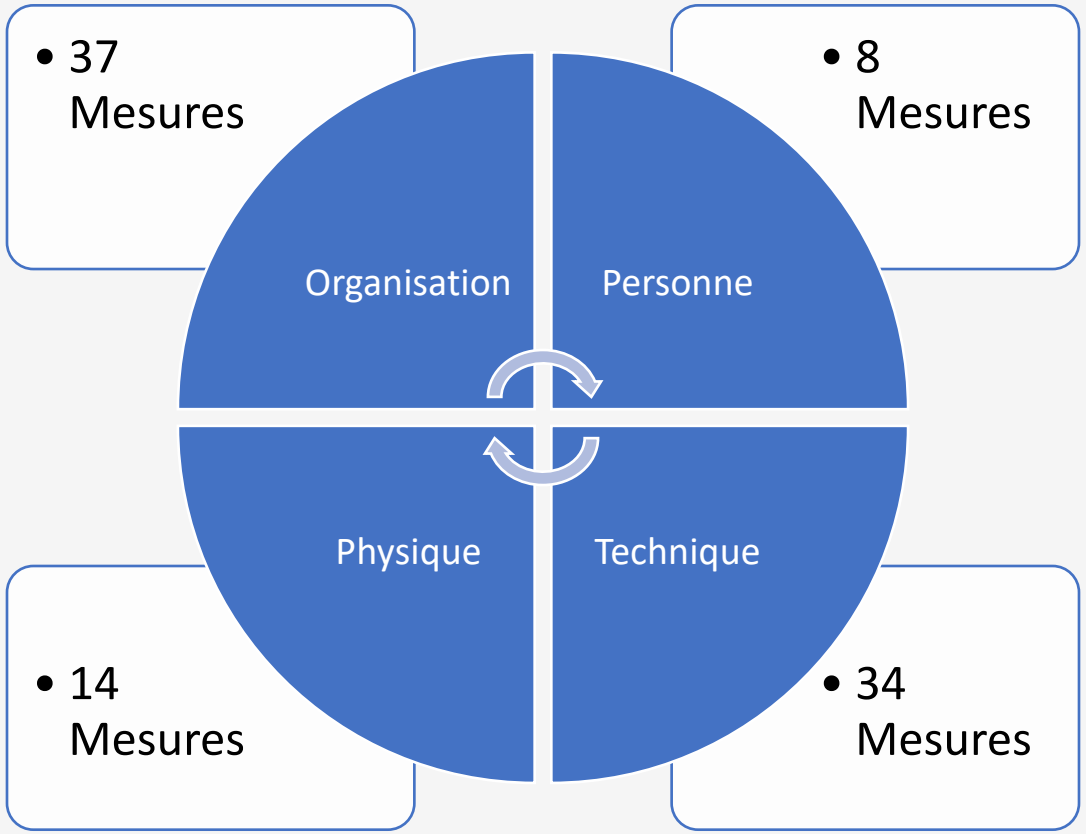
- La description des mesures de sécurité comprend également des préconisations et quatre attributs :
  - Types de mesures :
    - Prévention
    - Détection
    - Correction
  - Propriétés de la sécurité de l'information :
    - Confidentialité
    - Intégrité
    - Disponibilité
    - BONUS : Traçabilité + Authenticité
  - Concepts « NIST » :
    - Identification
    - Protection
    - Détection
    - Traitement
    - Récupération

10. ISO 27002:2022 : Attributs : Capacité opérationnelles

- La description des mesures de sécurité comprend également des préconisations et quatre attributs :
  1. Gouvernance
  2. Management des actifs
  3. Protection de l'information
  4. Sécurité des ressources humaines
  5. Sécurité Physique
  6. Sécurité des réseaux et systèmes
  7. Sécurité des applications
  8. Configuration sécurisée
  9. Management des accès et des identités
  10. Management des menaces et des vulnérabilités
  11. Continuité
  12. Sécurité des relations fournisseurs
  13. Conformité et aspects légaux
  14. Management de la sécurité des incidents
  15. S'assurer de la sécurité de l'information

10. ISO 27001:2013 (114) VS ISO 27001:2023 (93)

- DOMAINES (La mise en place)
- ANNEXES (Les mesures ET pas les contrôles ☺ !)



10. Organisation (37)

- 5.1 **Politiques de sécurité de l'information**
- 5.2 Rôles et responsabilités en matière de sécurité de l'information
- 5.3 Séparation des tâches
- 5.4 Responsabilités du management
- 5.5 Contact avec les autorités
- 5.6 **Contact avec les groupes d'intérêts spéciaux**
- 5.7 Renseignements sur les menaces
- 5.8 Sécurité de l'information dans la gestion de projet
- 5.9 **Inventaire des informations et autres actifs associés**
- 5.10 Utilisation acceptable des informations et autres biens associés
- 5.11 Retour des actifs
- 5.12 Classification des informations
- 5.13 Étiquetage de l'information
- 5.14 Transfert d'informations
- 5.15 **Contrôle d'accès**
- 5.16 Gestion de l'identité
- 5.17 Informations d'authentification
- 5.18 Droits d'accès
- 5.19 Sécurité de l'information dans les relations avec les fournisseurs
- 5.20 Prise en compte de la sécurité des informations dans les accords avec les fournisseurs
- 5.21 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement des TIC
- 5.22 Suivi, révision et gestion du changement des services des fournisseurs
- 5.23 Sécurité de l'information pour l'utilisation des services cloud
- 5.24 Planification et préparation de la gestion des incidents de sécurité de l'information
- 5.25 Évaluation et décision concernant les événements liés à la sécurité de l'information
- 5.26 Réponse aux incidents de sécurité de l'information
- 5.27 Tirer les leçons des incidents de sécurité de l'information
- 5.28 **Collecte de preuves**
- 5.29 Sécurité de l'information pendant les perturbations
- 5.30 Préparation aux TIC pour la continuité des activités
- 5.31 Exigences légales, statutaires, réglementaires et contractuelles
- 5.32 Droits de la propriété intellectuelle
- 5.33 Protection des dossiers
- 5.34 Vie privée et protection des PII (Personally Identifiable Information)
- 5.35 **Examen indépendant de la sécurité des informations**
- 5.36 Respect des politiques, règles et normes en matière de sécurité de l'information
- 5.37 Procédures d'exploitation documentées

10. Personne (8)

- 6.1 Screening
- 6.2 Modalités et conditions d'emploi
- 6.3 **Sensibilisation, éducation et formation à la sécurité de l'information**
- 6.4 Procédure disciplinaire
- 6.5 Responsabilités après la cessation ou le changement d'emploi
- 6.6 Accords de confidentialité ou de non-divulgation
- 6.7 **Travail à distance**
- 6.8 Rapport sur les événements liés à la sécurité de l'information

10. Physique (14)

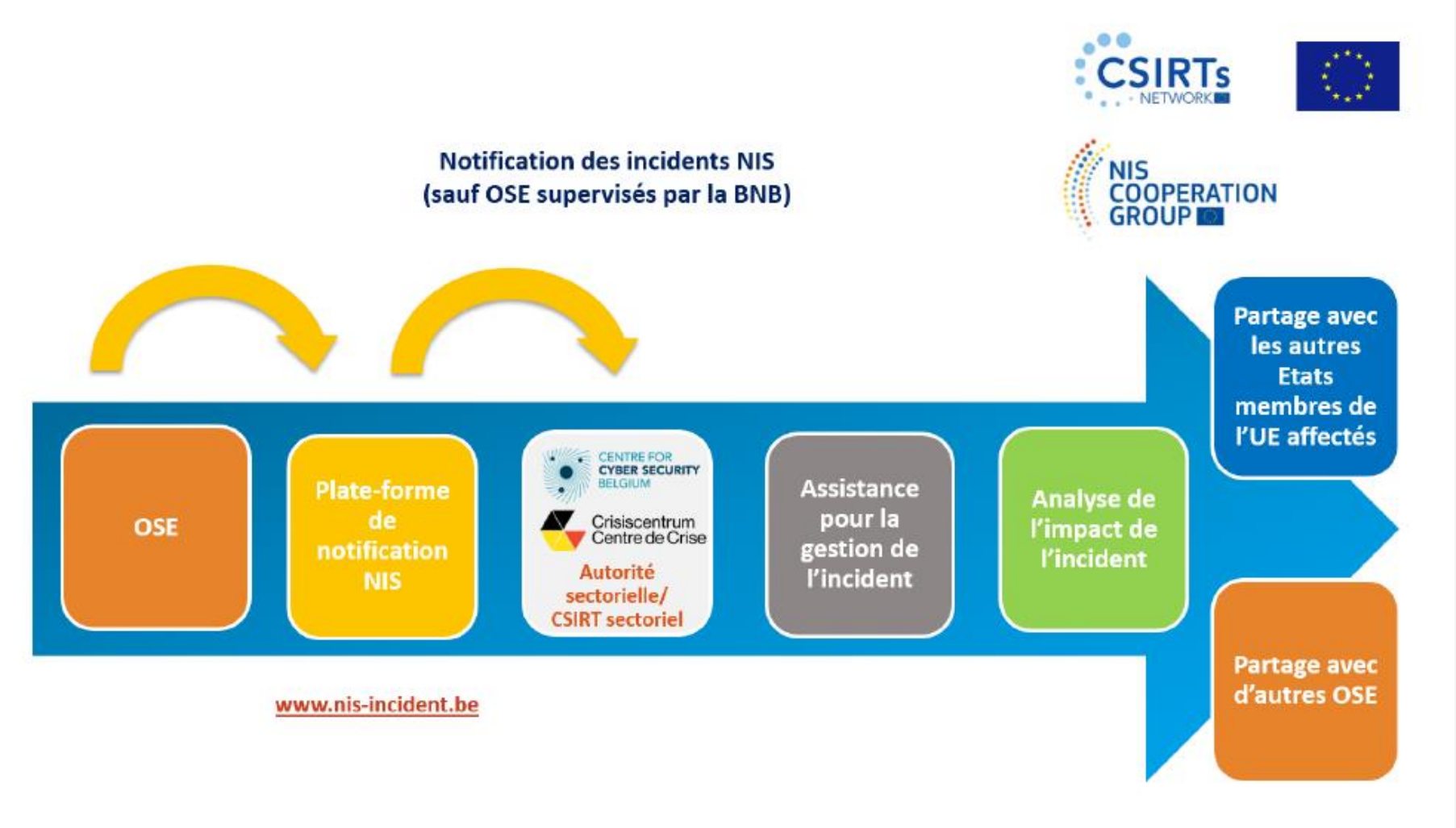
- 7.1 Périmètres de sécurité physique
- 7.2 **Entrée physique**
- 7.3 Sécurisation des bureaux, des salles et des installations
- 7.4 Surveillance de la sécurité physique
- 7.5 Protection contre les menaces physiques et environnementales
- 7.6 Travailler dans des zones sécurisées
- 7.7 Bureau et écran dégagés
- 7.8 Emplacement et protection des équipements
- 7.9 Sécurité des actifs hors site
- 7.10 **Supports de stockage**
- 7.11 Services d'appui
- 7.12 Sécurité du câblage
- 7.13 Entretien des équipements
- 7.14 **Elimination sécurisée ou réutilisation des équipements**

10. Technique (34)

- 8.1 **Périphériques d'extrémité des utilisateurs**
- 8.2 Droits d'accès privilégiés
- 8.3 Restriction de l'accès aux informations
- 8.4 Accès au code source
- 8.5 Authentification sécurisée
- 8.6 Gestion des capacités
- 8.7 **Protection contre les logiciels malveillants**
- 8.8 Gestion des vulnérabilités techniques
- 8.9 Gestion de la configuration
- 8.10 **Suppression d'informations**
- 8.11 Masquage de données
- 8.12 Prévention des fuites de données
- 8.13 Sauvegarde de l'information
- 8.14 Redondance des installations de traitement de l'information
- 8.15 Journalisation
- 8.16 Activités de suivi
- 8.17 Synchronisation d'horloge
- 8.18 Utilisation de programmes utilitaires privilégiés
- 8.19 Installation de logiciels sur des systèmes opérationnels
- 8.20 Sécurité des réseaux
- 8.21 Sécurité des services réseau
- 8.22 **Ségrégation des réseaux**
- 8.23 Filtrage Web
- 8.24 Utilisation de la cryptographie
- 8.25 Cycle de vie du développement sécurisé
- 8.26 Exigences de sécurité des applications
- 8.27 Architecture de système sécurisée et principes d'ingénierie
- 8.28 **Codage sécurisé**
- 8.29 Test de sécurité en développement et acceptation
- 8.30 Développement externalisé
- 8.31 Séparation des environnements de développement, de test et de production
- 8.32 Gestion des modifications
- 8.33 Informations sur les tests
- 8.34 Protection des systèmes d'information pendant les tests d'audit

11. Notification des incidents

11. Notification des incidents > souhaitable



Sources : www.CCB.gov.be

11. Notification d'incidents NIS 2

https://www.Nis-incident.be

24h

- Alerte rapide (téléphone, courrier) + vraisemblablement causée par une action illégale ou malveillante ou pouvant avoir un impact transfrontalier.

CENTRE FOR CYBERSECURITY BELGIUM

National Crisis Center

72h

- Notification officielle de l'incident : évaluation de l'incident, de sa gravité et de son impact + indicateurs de compromission.
- Mise à jour des informations

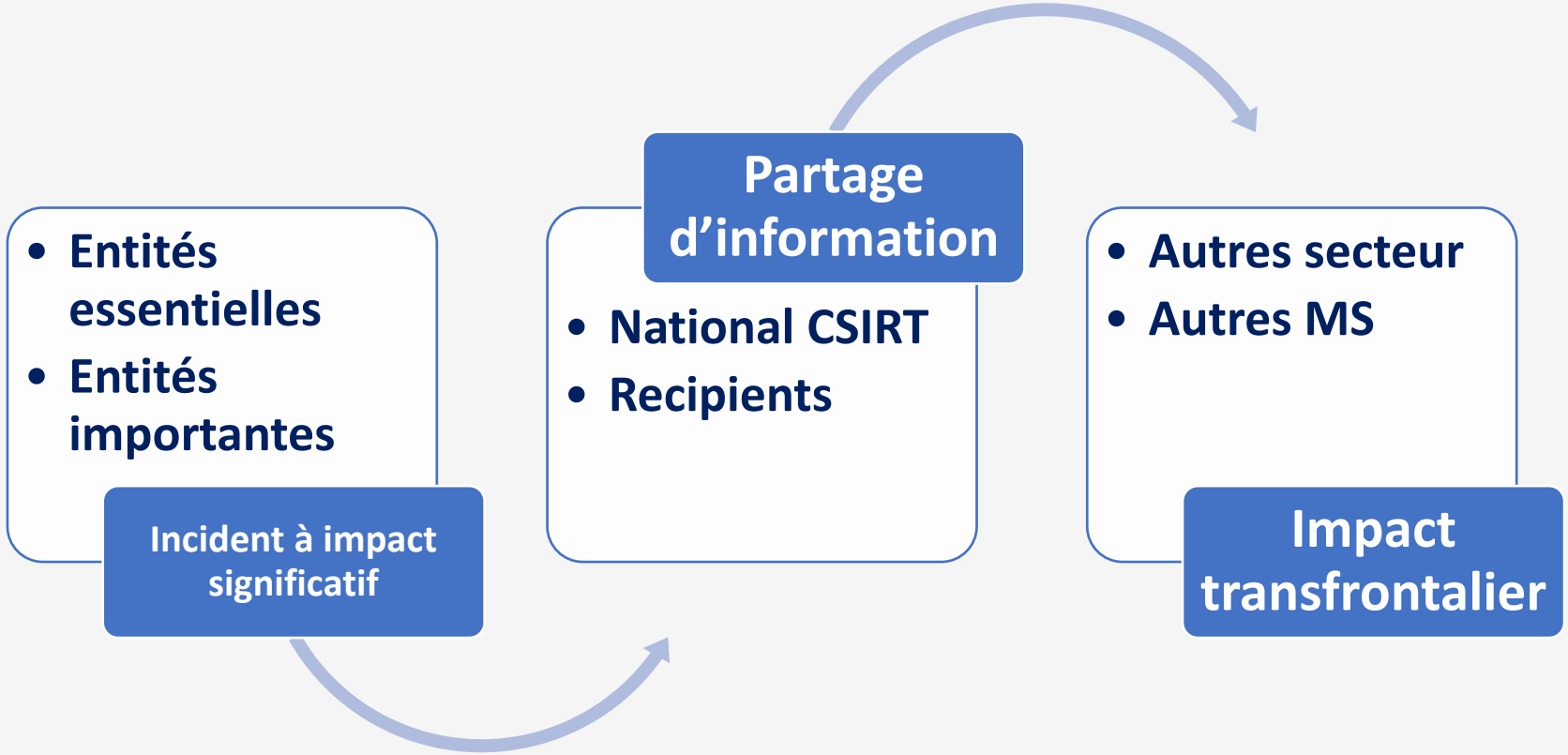
Mise à jour si demande

1 month

- Rapport :
  - Description détaillée de l'incident, de sa gravité et de son impact ;
  - type de menace ou la cause fondamentale qui a probablement déclenché l'incident:
  - les mesures d'atténuation appliquées et en cours

11. Notification

- tout incident ayant un impact significatif sur la fourniture des services mentionnés dans les annexes.
- Le cas échéant, ces entités notifient, sans retard injustifié, aux destinataires de leurs services les incidents susceptibles de nuire à la fourniture de ce service.



11. Incident Significatif

"incident" : tout événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des services connexes offerts par les réseaux et les systèmes d'information ou accessibles par leur intermédiaire ;

Un incident est considéré comme significatif si

(a) l'incident a causé ou est susceptible de causer une perturbation opérationnelle grave et substantielle ou des pertes financières pour l'entité concernée ;
(b) l'incident a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des pertes matérielles ou immatérielles considérables.

NIS COOPERATION GROUP

Guidance from the NIS CG & CCB

12. Supervision

12. Important vs essentiel

Entités importantes	Entités essentielles
Ex-post *(supervision après un incident, preuve d'infractions)*	*Ex-ante et Ex-post*
Inspections sur site et supervision hors site	
Audits de sécurité ciblés basés sur des évaluations des risques	
Analyses de sécurité	
Demande d'informations	
	Évaluation régulière de la conformité effectuée par un organisme d'évaluation de la conformité (CAB) ou par le service d'inspection (CCB ou sectoriel)
Demander des preuves sur la mise en œuvre des politiques de cybersécurité	

12. Évaluation régulière obligatoire de la conformité pour les entités essentielles avec 3 options différentes

Federale Audit Fédéral

Privé/publicCAB

CyFun®

CCB Certification/Label Cyber Fundamentals par un CAB autorisé (avec le champ d'application approprié)

OR

Certification ISO 27001

par un CAB autorisé (avec le champ d'application et la déclaration d'applicabilité pertinents)

ISO 27001

OR

CENTRE FOR CYBERSECURITY BELGIUM

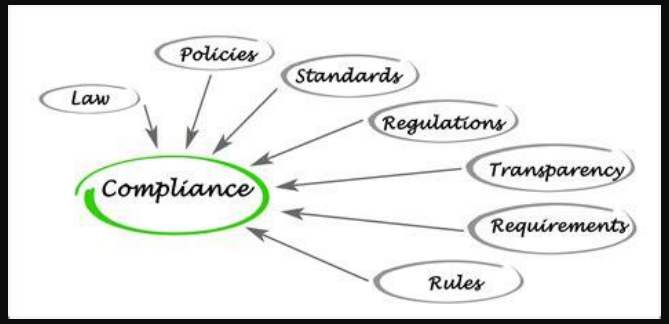
Inspection obligatoire par le CCB

(redevances pour les entités publiques – à l'exception des administrations fédérales qui ne sont pas soumises aux audits de la FIA)

L'entité doit effectuer un mappage avec les exigences de CyFun ou de ISO27001

Présomption de conformité

13. Conformité



13. Système d'évaluation de la conformité de CyberFundamentals

➔ (en collaboration avec)

- Le CCB a mis au point un système d'évaluation de la conformité de CyberFundamentals qui est officiellement accepté par BELAC.
- L'évaluation de la conformité doit être effectuée par un organisme d'évaluation de la conformité (CAB) accrédité et autorisé.

  ➢ Accréditation selon le règlement UE 765/2008 (exigences d'accréditation et de surveillance du marché par l'organisme national d'accréditation)

  Sauf disposition contraire de la législation belge

  Les demandes d'accréditation peuvent être adressées à BELAC selon la procédure applicable. Une fois accréditée, l'autorisation peut être demandée à l'autorité de certification CCB (NCCA).

Système d'évaluation de la conformité CyberFundamentals (CyFun® CAS) www.cyfun.be
Public cible : Organisme national d'accréditation et organismes d'évaluation de la conformité (candidats).

13. Vue d’ensemble de l’évaluation CyberFundamentals

	BASIC	IMPORTANT	ESSENTIAL
Type d’évaluation	Vérification	Vérification	Certification
Comment se déroule l’évaluation ?	Vérification de l’auto-évaluation	Vérification de l’auto-évaluation	Audit de certification basé sur l’auto-évaluation
Évaluation réalisée par	**CAB accrédité et autorisé**	**CAB accrédité et autorisé**	**Accrédité et autorisé**CAB
Résultat de l’assurance	Affirmation vérifiée	Affirmation vérifiée	Certificat
Label (délivré par l’autorité de certification CCB)			

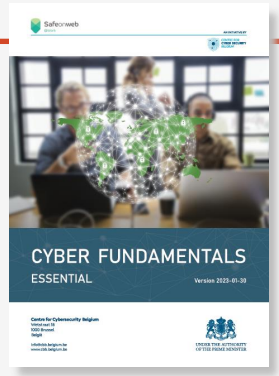
Le rapport d’auto-évaluation CyberFundamentals (Toolbox CyFun®) est la clé (d’entrée) du processus d’évaluation de la conformité.

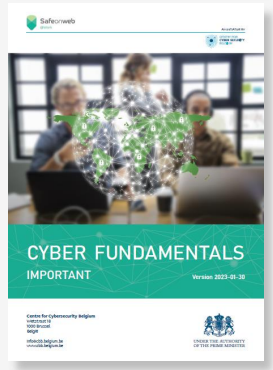
13. Impact de l'évaluation des risques (RA) Cyberfundamentals

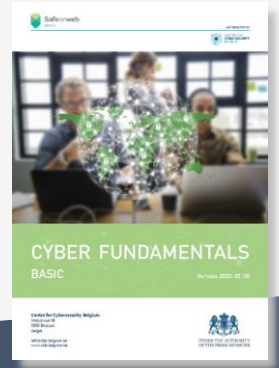
Entités essentielles

Entités importantes

RA







13. Portée des évaluations de la conformité

Scope Organisation dans son ensemble

➔ À moins que les environnements IT/OT ne soient physiquement et/ou techniquement séparés

➔ Dois être exécuté de manière à ce que les environnements hors du champ d'application n'influencent pas les risques de l'environnement visé

➔ À clarifier dans le cadre de l'évaluation de la conformité

<u>Motivated</u> Exclusions

BASIC ➔ Maximum 1 mesure CyberFundamentals

IMPORTANT ➔ Maximum 3 mesures CyberFundamentals

ESSENTIAL ➔ Maximum 5 mesures CyberFundamentals

Les mesures clés ne peuvent pas être exclues

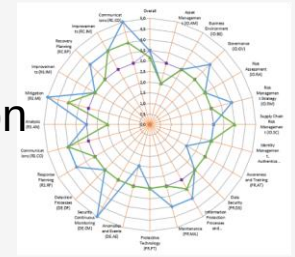
Les mesures liées aux aspects de gestion ne peuvent être exclues

13. CyberFundamentals toolbox

CyFun Selection tool
(Évaluation du risque)

Energy			Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category	Global or Targeted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score		
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total		0		7,5		30		120		127,5	285	ESSENTIAL

CyFun Outil d'auto-évaluation



CyberFundamentals
Évaluation de la conformité
Régime pour les CAB

CyberFundamentals
Framework mapping

CyberFundamentals La boîte à outils est accessible au public➔ **www.cyfun.eu**

13. Mesures administratives et sanctions

CENTRE FOR CYBERSECURITY BELGIUM

Avertissements

Instructions à fixer

Recommandations de surveillance

Commander des déclarations publiques et des informations à l'intention des utilisateurs

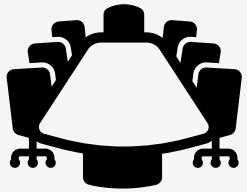
Inspections ciblées et ponctuelles

13. Mesures administratives spécifiques

Si les mesures correctives demandées ne sont pas prises par une entité essentielle dans le délai imparti, le service d'inspection peut :

a) demander la suspension temporaire d'une certification ou d'une autorisation concernant tout ou partie des services ou activités concernés fournis par l'entité essentielle ;

b) demander d'interdire temporairement à toute personne physique chargée d'exercer des responsabilités de direction au niveau de directeur général ou de représentant légal dans l'entité essentielle d'exercer des fonctions de direction dans cette entité.



sans préjudice des règles de responsabilité applicables aux établissements publics, ainsi que de la responsabilité des fonctionnaires et des agents élus ou nommés.

13. Amendes administratives

Ne s’applique pas aux entités actives dans le secteur de l’administration publique de l’annexe I.

14. Agenda

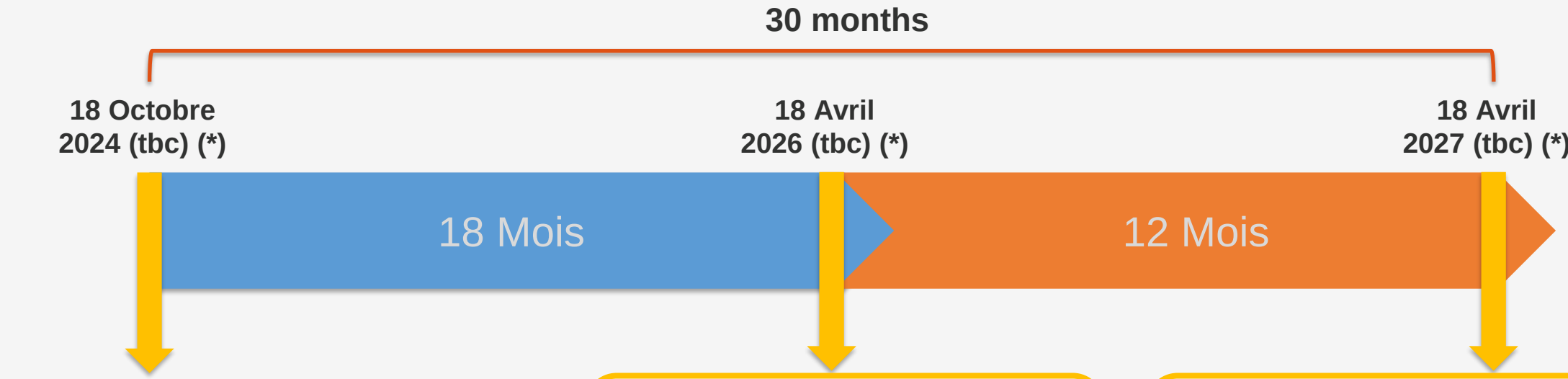
14. Entrée en vigueur des obligations NIS2 pour les entités importantes et essentielles

Toutes les obligations NIS2 (loi et arrêté royal) commenceraient à s'appliquer à partir du 18 octobre 2024* :
… Mesures de cybersécurité
… Notification d'incident

Supervision éventuelle (avec un calendrier spécifique pour les premières évaluations régulières de la conformité pour les entités essentielles – voir diapositive suivante).
Etc.

* à confirmer (en cas d'identification formelle, le délai court à compter de la notification de la décision administrative)

13. Calendrier précis pour l'évaluation régulière de la conformité des entités essentielles



Entrée en vigueur
Loi NIS2 (à confirmer)

Objective: AL Basic or Important (*)
- Date limite de vérification parCAB **ou** ISO 27001 Scope & Statement of Applicability

Objective: AL Essential (*)
- Date limite pour laCyFun certification by CAB **or**
- ISO 27001 certification Scope & Déclaration d'applicabilité

Alternative (CCB Inspection):
Vérifier l'état du processus de conformité NIS2:
- CyFun Self-Assessment **or**
- ISO 27001 Scope & SoA (+I.B.B./P.S.I.)

*(en cas d'identification formelle, le délai court à compter de la notification de la décision administrative)

13. Étapes suivantes


DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Adoption de la directive NIS2 14/12/2022

Projet de loi approuvé par le Conseil des ministres 10/11/2023

Janvier/Février 2024 Examen/deuxième lecture

Loi adoptée par le Parlement 25/04/2024 ?

June 2024 (Elections)

Entrée en vigueur Loi NIS 2 18/10/2024

Groupes de travail

Consultation publique/avis formels

Discussion/adoption de la loi au Parlement

Préparation

Droit de l'exécution forcée

Arrêté royal approuvé par le Conseil des ministres10/11/2023

Conseils formelsRD

Adoption RD

Préparation

RD d'exécution

Entry into force NIS 2 RD 18/10/2024 (tbc)

14. Conclusions

14. Conclusions

14. Conclusions : Obligations Minimales Belges si OSE

1. GRANDES Mesures générales de sécurité liées aux services essentiels

Rappel : Be : AR du 12 /07/2019 art 20 de la loi NIS ; et article 21 de la directive NIS 2

- Mesures :
  - Techniques (ex. sécurité réseaux) ;
  - Système d'information (données,…) ;
  - Organisationnelles (Management) ;
- Gestion des risques
  - Analyse des Besoins de sécurité (CIA+A) ;
  - Garantie d'applicabilité ;
- Sécurité Physique et logique :
  - En fonction de l'état des connaissances techniques actuelles ;
  - Veille technologique incontournable ;
- Contrôler la sécurité des réseaux et systèmes d'information liés à la fourniture de leur(s) service(s) essentiel(s) : PSSI (1 an) ; audit interne (1 an) et audit externe (3 ans) ;
- Collaborer et échanger des informations avec les différentes autorités NIS compétentes
- Notifier et gérer les incidents ;

Sources : www.CCB.gov.be

14. Conclusions : Obligations Minimales Belges avec un peu de NIS 2

2. **Des Mesures Spécifiques de sécurité en fonction des autorités**
   Voir votre lettre et autorité
   Mon conseil > Security By Design (Organisation > Humain > Physique > Informatique)
3. **Disposer d'une politique de sécurité des systèmes** et réseaux d'information (PSI et/ou PSSI) reprenant au moins les objectifs et les mesures de sécurité concrètes ; Budget …
4. **Pouvoir prouver lui-même en documentant** de manière adéquate son analyse de risques, le niveau de sécurité de ses mesures techniques/organisationnelles, le caractère approprié des mesures en vue de prévenir des incidents, etc.

   OU **mais non obligatoire** disposer de la **certification ISO 27001** délivrée par un organisme d'évaluation de la conformité accrédité par BELAC (ou par une institution européenne équivalente) et couvrant les mesures de sécurité des réseaux et systèmes d'information nécessaires à la fourniture du ou des services essentiels ;
5. **Désigner un point de contact** pour la sécurité des systèmes et réseaux d'information (exemple RSSI) et en communiquer les données à l'autorité sectorielle compétente dans un délai de trois mois (pour la Belgique) à dater de la notification de la désignation comme opérateur de services essentiels ;
6. **Formation** de toutes les équipes et des directions.
7. **State of arts**, … relevant European and international standards

Art 21. use MFA ; Secure voice, video and text communications …
TikTok … Messenger ?

Sources : www.CCB.gov.be

14. Exemple courrier a été envoyé à un OSE (Exemple pour l'EAU)

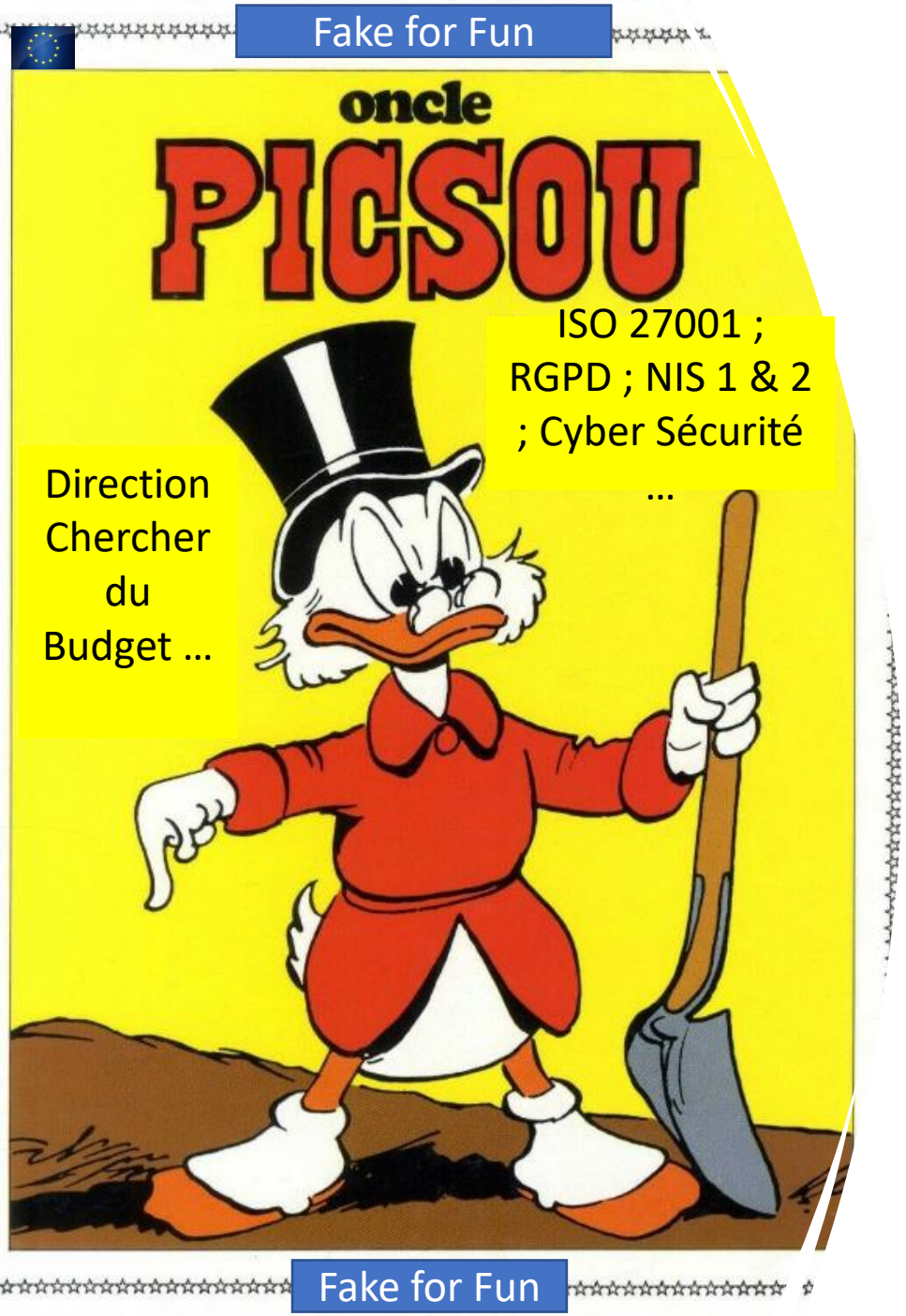
- Art. 23 § 1er de la loi NIS : désigner un point de contact pour la sécurité des syst. et réseaux d'information et d'en communiquer les coordonnées au Comité ;
- Art. 16 : transmettre un descriptif des réseaux et syst. d'information ;
- Art. 24 §3 : notifier tous les incidents ;
- Art.20 : prendre les mesures techniques et organisationnelles pour gérer les risques et prendre les mesures appropriées en vue de prévenir les incidents ;
- Art 21 § 1er : élaborer une politique de sécurité des syst. et réseaux d'information ;
- Art 21 §2 : mettre en œuvre toutes les mesures de votre P.S.I. ;
- Art. 38 §§ 1 & 3 : réaliser un audit interne ;
- Art. 38 §§ 2 & 3 : faire réaliser un audit externe ;

100% Classique

AVEZ-VOUS RECU UN COURRIER ?

Point de vue :

RIEN de NOUVEAU en Cybersécurité MAIS ! **Il faut le faire pour de vrai…**



Idéalement pour des économies d'échelles, temps et compétences

- **Réaliser UN MANAGEMENT Intégré**
  - **(1) ISO 27001** ;
  - **(2) Compliance RGPD** ;
  - **(3) Compliance NIS** ;
  - (4) De Facto > **Cyber-Sécurité** ! ;
  - **Management Intégré** (1) + (2) + (3) + (4)

6. Ressources pour aller plus loin

ISO 27K

https://www.iso.org/fr/isoiec-27001-information-security.html (ISO 27001)
https://www.iso.org/standard/44375.html (27032 CyberSecurity)
https://www.iso.org/standard/63461.html (27033 Réseaux)
https://www.iso.org/standard/44378.html (27034 Applications)
https://www.iso.org/standard/60803.html (27035 Gestion des Incidents)
https://www.iso.org/standard/59648.html (27036 Supplier Relationships)
https://www.iso.org/standard/72435.html (27110 CyberSecurity & Privacy)
https://www.iso.org/standard/62777.html (27799 Secteur de la Santé)

Check : 22301 (Continuité) ; 31000 (Risques Globaux)

Sécurité des systèmes industriel : https://www.exera.com/
Sécurité et Cyber Sécurité : https://canso.org/ (Onglet Recherche > Cyber Sécurité)

Incidents : Avis de la Presse et d'Experts :

Allez sur DuckDuckGo ; Qwant et Google

ISO 27002 : Guides de bonnes pratiques
ISO 27005 : Gestion des risques de l'information
ISO 31000 : Gestion des risques
ISO 22301 : Continuité d'activité

EUROPE NIS

https://www.enisa.europa.eu/topics/nis-directive
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada
BONUS : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Contacts :

https://ccb.belgium.be/fr
https://www.cert.be/fr
CERT > Spécial NIS
En cas d'incident : https://nis-incident.be/fr/

HELP ? : le CCB ! nis@ccb.belgium.be

La BCED : support@labced.be
Gouvernance et Management > Https://www.linkedin/davidblampain.com

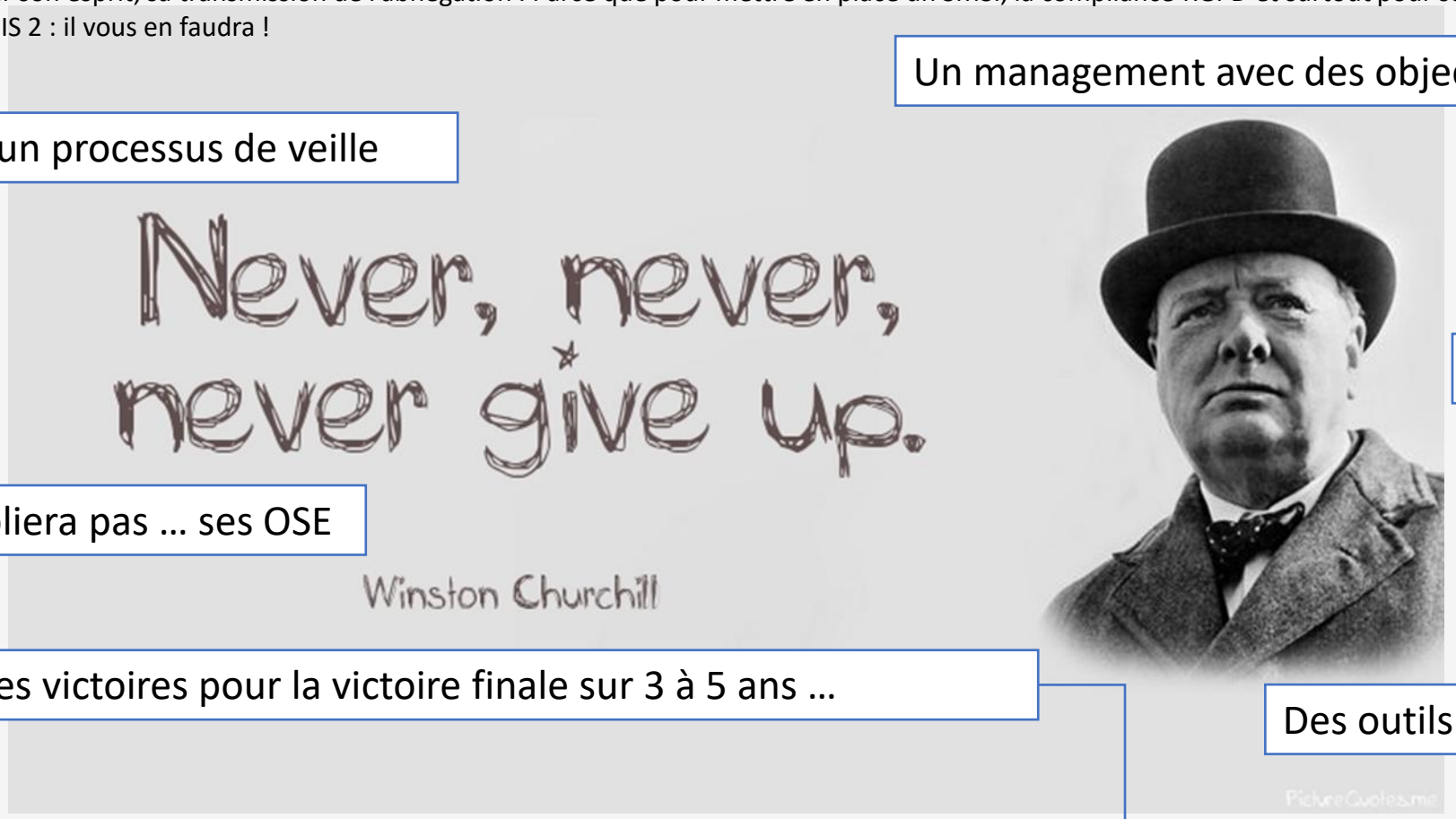
Rester humble et discret pour éviter d'attirer les hackers… IT dire la vérité à la direction. La direction dire la vérité à l'état et aux citoyens.

7. Fin : La sécurité de l'information c'est :

Rmq : Merci à Churchill pour son esprit, sa transmission de l'abnégation : Parce que pour mettre en place un SMSI, la compliance RGPD et surtout pour sécuriser en fonction de la Loi NIS 1 et NIS 2 : il vous en faudra !

Un management avec des objectifs.

Mettre en place un processus de veille



State Of Art

ET Que l'Europe n'oubliera pas … ses OSE

Une stratégie de petites victoires pour la victoire finale sur 3 à 5 ans …

Des outils professionnels

Bref : Patience

Gouvernance et Management >
capitaine.cyber@protonmail.com (David Blampain)
David.blampain@labced.be