2023 > 2024

Acronyme : **Network Information System**

NIS - Secteur Multiples

Sécurité et Cybersécurité

On parle de 8 secteurs 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** »*

« Exemple de Management de la Sécurité de l'information NIS 1 & 2

Présentation à diffusion restreinte - usage interne pour les participants.
Comité des Utilisateurs BCED 2024

Auteur : *David Blampain*
Conseiller en Sécurité de l'Information
Banque Carrefour D'échange de Données

* Chief Information Security Officer

Intervention(s)

Intervenant : David Blampain linkedin/davidblampain

Conseiller en Sécurité de l'Information (CISO)

22 ans d'expérience au service du Web, de l'IT et de l'ICT > 12 ans en sécurité de l'information.

Certifié SENIOR Lead Implementer & Risks Manager > ISO:IEC 27001 (ISMS) ; 27005 (RISKS) et 27032 (CyberSecurity) / CDPO

Intervenant invité : Valery Vander Geeten linkedin/valery-vander-geeten

Head of Legal & DPO du CCB Centre pour la Cyber Sécurité Belge

16 années d'expérience au service, avocat, juriste, assistant universitaire.

Certifié Risks Manager (ISO 27005) ; CDPO ; Sans Sec 301

Cyber Sécurité – Sommaire 1/1

1. **Etat des lieux**
2. **Les menaces Cyber** (CyberSécurité)
3. **NIS 1 à 2 : Belgique et Europe**
    1. NIS : Les 5W
    2. NIS : Légal
    3. NIS : Décodage sécuritaire
    4. NIS : Dream Team
    5. Organisation de la Cybersécurité dans le cadre du NIS
        1. Objectifs
        2. Management du risque informationnel
        3. Se protéger des cybers attaques
        4. Détecter les incidents de Sécurité
        5. Minimiser l'impact des incidents
        6. Méthodes complémentaires
4. **Conclusions**
5. **Annexes du ministère**
6. **Ressources pour aller plus loin**
7. **Le mot de la fin : un grand personnage**

1. Etat des Lieux NIS 1 et NIS 2

De nombreux éléments de cette présentation ont été retiré car ils sont identiques à ceux du CCB
Pour les aspects juridiques et légaux veuillez vous référer à la présentation :

NIS directive from Central States to Regional Challenges and Opportunities 2022.pdf

Seuls les éléments liés à la sécurité seront abordés dans cette présentation, il se peut que certaines diapositives ou rubriques soient fortement simplifiées (voir le sommaire).

2. Etat des menaces : les données …

Une étude démontre que les sites web et les applications des aéroports sont très mal protégés. Sur 100 aéroports testés, 97 d'entre eux ne sécurisent pas les données des passagers, mais aussi leurs propres documents comme des mots de passe et des registres comptables. Un conseil : ne jamais utiliser d'application mobile.

Les chercheurs ont aussi utilisé l'intelligence artificielle pour parcourir l'internet « underground », en analysant le contenu des forums et marchés du *dark web* à la recherche de données confidentielles qui

Les sites web des aéroports sont particulièrement problématiques, puisque 97 % s'appuient sur du code obsolète, dont 24 % d'entre eux contiennent des failles connues et graves. Les trois quarts des sites ne respectent ni le règlement général sur la protection des données (RGPD) ni la norme de sécurité des données pour les cartes de paiement (PCI DSS). Près d'un quart n'utilise aucun chiffrement pour la transmission des données, ou alors utilise la version 3 du protocole SSL qui est obsolète.

https://namex.co/hack-of-water-supply-in-small-florida-town-similar-to-israeli-attack-blamed-on-iran/

2. Etat des menaces : Livraisons de secret

Pourtant, brûlant de curiosité, notre passant ouvre cette clé USB non chiffrée dans une bibliothèque publique et y découvre des éléments troublants, selon une enquête du **Sunday Mirror**: 76 fichiers avec 174 documents, incluant des vidéos et des cartes associées... à la sécurité de l'aéroport londonien d'Heathrow, le principal hub européen (76 millions de passagers en 2016).

"Un porte-parole du hub aéroportuaire commente : « La priorité numéro un de Heathrow est d'assurer la sécurité des passagers et du personnel (…) Nous avons révisé tous nos plans de sécurité et nous sommes confiants sur le fait que l'aéroport demeure une zone protégée. »

Un particulier a ramassé une clé USB dans une rue de Londres. Ce qu'il découvre à l'intérieur révèle une faille béante de sécurité nationale.

https://namex.co/hack-of-water-supply-in-small-florida-town-similar-to-israeli-attack-blamed-on-iran/

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

WATER CYBER SECURITY ATTACK

Tous Images Vidéos Actualité Carte Préférences

Belgique (fr) Filtre parental : modéré À tout moment

Probe Into Florida Water Plant Hack Led to Discovery of ...
https://www.securityweek.com/probe-florida-water-plant-hack-led-discovery-watering...
An investigation conducted by industrial **cybersecurity** firm Dragos into the recent cyberattack on the **water** treatment plant in Oldsmar, Florida, led to the discovery of a watering hole **attack** that initially appeared to be aimed at **water** utilities. Law enforcement revealed in early February that a ...

Florida Water Treatment Plant Hit With Cyber Attack ...
https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/
On Friday, February 5, 2021, a hacker initiated an **attack** on an Oldsmar, Florida **water** treatment facility which briefly adjusted the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million. This **attack** occurred about 15 miles from the location of, and two days before the Super Bowl. If successful, the **attack** would have increased the amount of sodium hydroxide to an ...

US Water Plant Suffers Cyber Attack Through the Front Door
https://rusi.org/commentary/us-water-plant-suffers-cyber-attack-through-front-door
An attempted **cyber attack** against a **water** treatment plant in Florida highlights endemic failures in the **cyber security** of the US **water** sector. On 5 February, an unidentified attacker accessed the systems at a US **water** treatment plant in Oldsmar, Florida, and briefly altered the chemical levels in the drinking **water**.

Two more cyber-attacks hit Israel's water system | ZDNet
https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/
Two more **cyber-attacks** have hit Israel's **water** management facilities, officials from the **Water** Authority said last week. Officials said the **attacks** took place last month, in June, and didn't cause...

U.S. probes cyber attack on water system | Reuters
https://www.reuters.com/article/us-cybersecurity-attack-idUSTRE7AH2C320111121
(Reuters) - Federal investigators are looking into a report that hackers managed to remotely shut down a utility's **water** pump in central Illinois last week, in what could be the first known foreign...

Cyber Security 101 for Drinking Water - Water Quality and ...
https://waterandhealth.org/safe-drinking-water/drinking-water/cyber-security-101-for-...
Cyber Security Breaches of **Water** Systems **Cyber**-aggressors like cyberthieves can compromise the ability of **water** utilities to provide clean and safe **water**, harm the environment, erode customer confidence, and result in financial and legal liabilities for the utility and, ultimately, customers.

Recherches associées

- cyber security attacks
- recent cyber security attacks
- florida water cyber attack
- types of cyber security attacks
- examples of cyber security attacks
- preventing cyber security attacks
- cyber attack on water supply
- water plant cyber attack

PDF Water Sector Cybersecurity Brief for States
https://www.epa.gov/sites/production/files/2018-06/documents/cybersecurity_guide...
Many **water** and wastewater utilities, particularly small systems, lack the resources for information technology (IT) and **security** specialists to assist them with starting a **cybersecurity** program. Utility personnel may believe that **cyber-attacks** do not present a risk to their systems or feel that they lack the technical capability to improve their

SECURITY: Hackers force water utilities to sink or swim ...
https://www.eenews.net/stories/1060131769
News of a few **water**-sector **cyber** intrusions has trickled out publicly, including an **attack** on a North Carolina **water** utility in the aftermath of Hurricane Florence last year.

Hackers try to contaminate Florida town's water supply ...
https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV
(Reuters) - Hackers broke into the computer system of a facility that treats **water** for about 15,000 people near Tampa, Florida and sought to add a dangerous level of additive to the **water** supply,...

Cybersecurity & Guidance | American Water Works Association
https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecuri...
All **water** systems should act to examine **cybersecurity** vulnerabilities and develop a **cybersecurity** risk management program. AWWA is offering free **Cybersecurity** workshops specifically targeted towards small systems attendees.

2

Water treatment plant hacked, chemical mix changed for tap ...
https://www.theregister.com/2016/03/24/water_utility_hacked/
John Leyden Thu 24 Mar 2016 // 12:19 UTC Hackers infiltrated a **water** utility's control system and changed the levels of chemicals being used to treat tap **water**, we're told. The **cyber-attack** is documented in this month's IT **security** breach report (available here, registration required) from Verizon **Security** Solutions.

Attempted cyberattack highlights vulnerability of global ...
https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnera...
Water facility **attacks** low profile, high impact Although cyberattacks on the electric grid grab the lion's share of attention, **attacks** on **water** facilities typically generate little press coverage...

Water Supply Cyber Breach Thwarted | IndustryWeek
https://www.industryweek.com/technology-and-iiot/article/21154622/water-supply-cy...
The **attack** against the City of Oldsmar's **water** treatment system is what OT nightmares are made of, explains Marty Edward, vice president of OT at **cybersecurity** firm Tenable and the DHS CERT director under the Obama administration, in a statement. "If successful, the damages of the **attack** would have been catastrophic.

Principales Menaces en 2023

ENISA THREAT LANDSCAPE

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

… RasS ; PhaaS ; BEC ; DaaS ; RDoS ???

2. Cyber Sécurité – TOP 15 des menaces par l'ENISA – 116 pages

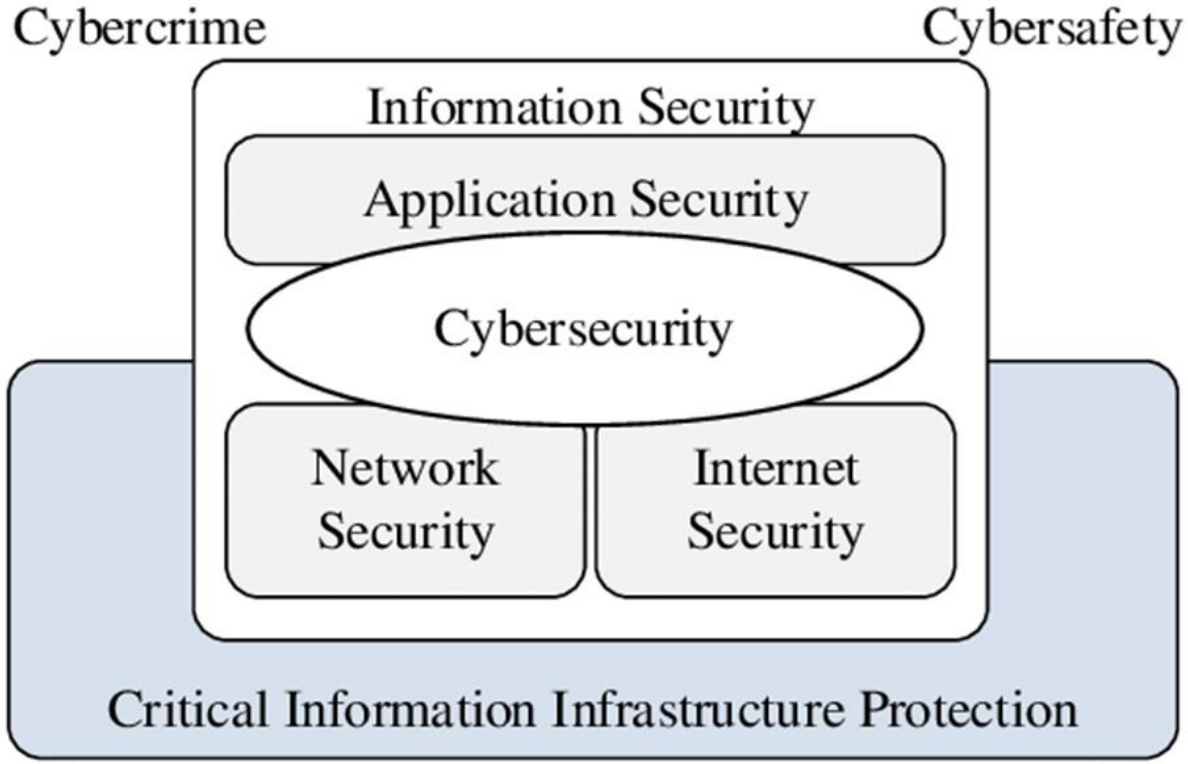
Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking	2020
1. Malware	↑	1. Malware	↑	1. Malware	→	1. Malware	→	→	1
2. Web based attacks	↑	2. Web based attacks	↑	2. Web based attacks	↑	2. Web Based Attacks	↑	→	2
3. Web application attacks	↑	3. Web application attacks	↑	3. Web application attacks	↑	3. Web Application Attacks	→	→	4
4. Botnets	↓	4. Denial of service	↑	4. Phishing	↑	4. Phishing	↑	→	3
5. Denial of service	↑	5. Botnets	↑	5. Spam	↑	5. Denial of Service	↑	↑	6
6. Physical damage/theft/loss	→	6. Phishing	→	6. Denial of service	↑	6. Spam	→	↓	5
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	7. Ransomware	↑	7. Botnets	↑	↑	10
8. Phishing	→	8. Ransomware	→	8. Botnets	↑	8. Data Breaches	↑	↑	8
9. Spam	↓	9. Insider threat (malicious, accidental)	→	9. Insider threat	→	9. Insider Threat	↓	→	9
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	10. Physical manipulation/ damage/ theft/loss	→	→	11
11. Data breaches	→	11. Exploit kits	↑	11. Data breaches	↑	11. Information Leakage	↑	↑	12
12. Identity theft	→	12. Data breaches	↑	12. Identity theft	↑	12. Identity Theft	↑	→	7
13. Information leakage	↑	13. Identity theft	↓	13. Information leakage	↑	13. Cryptojacking	↑	NEW	15
14. Ransomware	↑	14. Information leakage	↑	14. Exploit kits	↓	14. Ransomware	↓	↓	13
15. Cyber espionage	↑	15. Cyber espionage	↓	15. Cyber espionage	↑	15. Cyber Espionage	↓	→	14

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2016 with the one of 2015[1].

(Agence européenne pour de la Cybersécurité)
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

C’est quoi la CyberSécurité ?



Sources : PECB ISO 27032 > Petite copie non avouée du NIST américain ☺ ?

2. Cybersécurité : objectifs ANSSI en mode « Check-List »

Mise en oeuvre des règles NIS 6 à 16 - Liste de vérifications

Objectif de ce document : outiller la mise en oeuvre des recommandations du guide ANSSI

Ce document constitue un complément au guide ANSSI
Recommandations pour la protection des systèmes d'information essentiels
(réf. ANSSI-PA-085 version 1.0 du 18/02/2020)

Attention

Ce document rédigé par l'ANSSI présente les « Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte - Liste de vérifications ». Il est téléchargeable sur le site www.ssi.gouv.fr.
Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab*.
Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.
Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

** Licence ouverte / Open Licence v2.0.*
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

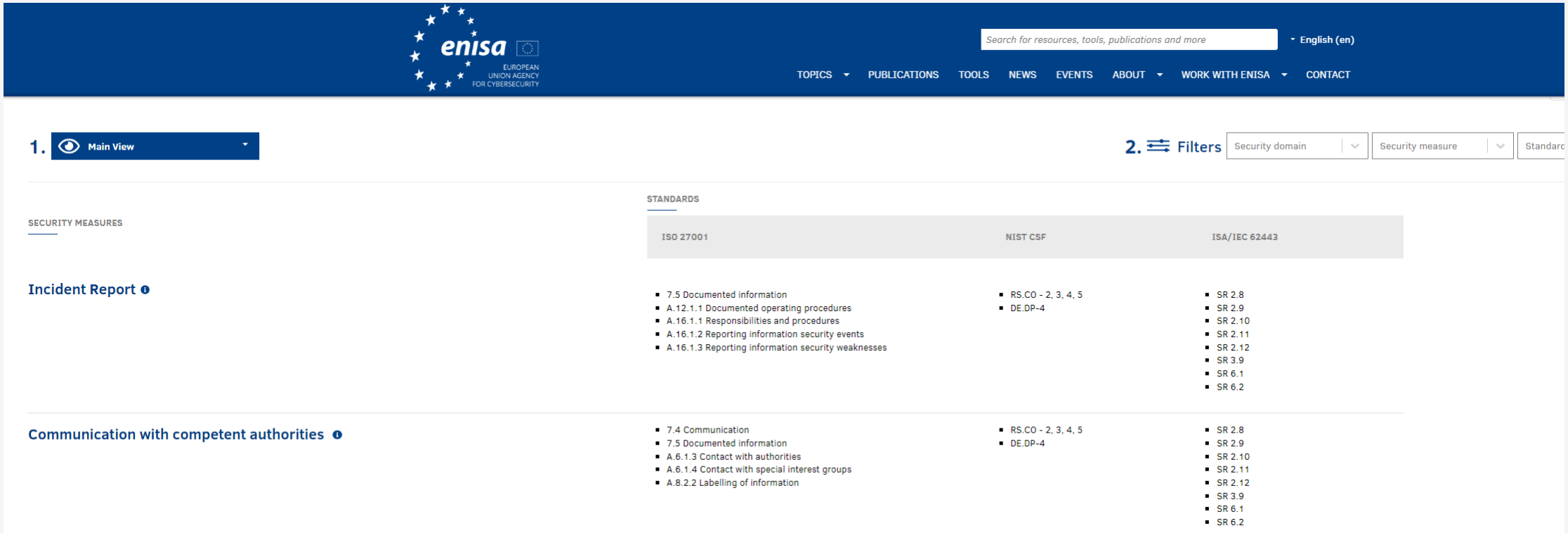
VERSION	DATE	NATURE DES MODIFICATIONS
1.0	18-12-20	Version initiale

Identifiant	Intitulé de la recommandation	Associée à une exigence d'une règle	Mesure retenue, exclue ou non applicable ?	Niveau de mise en œuvre
R1	Modifier les éléments de configuration par défaut	Oui	Retenue	Pas commencé
R1-	Pallier l'impossibilité de changer un élément par défaut	Non	Retenue	Pas commencé
R2	Installer uniquement les services ou fonctionnalités indispensables	Oui	Retenue	Pas commencé
R2-	Pallier l'impossibilité de désinstaller un service non indispensable	Oui	Retenue	Pas commencé
R3	Définir et utiliser des configurations de référence	Non	Retenue	Pas commencé
R4	Établir un inventaire technique des éléments et des accès au SIE	Non	Retenue	Pas commencé
R5	Utiliser uniquement des équipements maîtrisés	Oui	Retenue	Pas commencé
R6	Dédier aux SIE des supports amovibles identifiés	Oui	Retenue	Pas commencé
R7	Décontaminer les supports amovibles avant leur utilisation	Oui	Retenue	Pas commencé
R7+	Utiliser un équipement dédié à l'analyse des supports amovibles	Non	Retenue	Pas commencé
R8	Mettre en œuvre une traçabilité de l'utilisation des supports amovibles	Non	Retenue	Pas commencé
R8+	Mettre en œuvre un outil de protection contre l'exfiltration de données	Non	Retenue	Pas commencé
R9	Segmenter le SI en systèmes et sous-systèmes	Oui	Retenue	Pas commencé
R10	Autoriser les interconnexions suivant le besoin de fonctionnement	Oui	Retenue	Pas commencé
R11	Mettre en place un cloisonnement physique	Oui	Retenue	Pas commencé
R11-	Mettre en place un cloisonnement logique par le chiffre	Oui	Retenue	Pas commencé
R11- -	Mettre en place un cloisonnement logique	Oui	Retenue	Pas commencé
R12	Chiffrer les données en amont du stockage avec des secrets distincts	Non	Retenue	Pas commencé
R13	Contrôler le cloisonnement mis en place en cas d'externalisation	Oui	Retenue	Pas commencé
R14	Infrastructures numériques : cloisonner les services internes	Oui	Retenue	Pas commencé
R15	Segmenter les SIE publics en au moins deux sous-systèmes	Oui	Retenue	Pas commencé
R16	Accès public : chiffrer et authentifier les flux au niveau applicatif	Oui	Retenue	Pas commencé
R17	Accès public : authentifier les utilisateurs	Non	Retenue	Pas commencé
R17+	Accès public : authentifier les utilisateurs avec deux facteurs	Non	Retenue	Pas commencé
R18	Accès nomade : mettre en place un tunnel chiffré et authentifié	Oui	Retenue	Pas commencé
R19	Accès nomade : authentifier les utilisateurs avec deux facteurs	Oui	Retenue	Pas commencé
R20	Accès nomade : chiffrer intégralement le disque du poste	Oui	Retenue	Pas commencé
R21	Accès nomade : utiliser des filtres de confidentialité	Non	Retenue	Pas commencé
R22	Accès interne : mettre en place un tunnel chiffré et authentifié	Oui	Retenue	Pas commencé
R23	Filtrer les flux aux interconnexions entre les systèmes et entre les sous-systèmes	Oui	Retenue	Pas commencé

2. Cybersécurité : recommandations NIS au niveau européen

NIS Cooperation Group - Reference document on security measures for Operators of Essential Services.
https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

ENISA - Interactive table of the NIS Cooperation Group minimum security measures for OES (mapping tool).
https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services



Check liste outil du CCB : Made in 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.

01/03/2023 · 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.

01/03/2023 · 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.

01/03/2023 · 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.

01/03/2023 · pdf

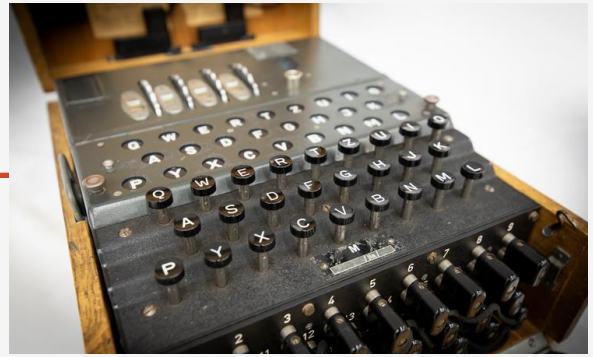
Download

3. NIS 1 : Belgique

techvisibility.com

* 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.

3.3 NIS 1 : 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 OSE 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 mais pas uniquement sur les données à caractère personnel ! (différent d'une DPIA)

2. Les OSE notifier les incidents liées à la sécurité de leur réseau et systèmes d'information. La notification des incidents permet une assistance, une 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

2° "autorité sectorielle" : l'autorité publique désignée par la loi ou par le Roi par arrêté délibéré en Conseil des ministres ;

5° "organisme d'évaluation de la conformité" : organisme visé à l'article I.9.7° du Code de droit économique ;

6° "audit de certification" : un audit réalisé dans le cadre d'une certification visée à l'article 22, § 2 ;

7° "autorité nationale d'accréditation" : organisme créé par le Roi en exécution de l'article VIII.30 du Code de droit économique ;

Art. 20. L'opérateur de services essentiels prend les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information dont sont tributaires ses services essentiels.

Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances techniques.

L'opérateur prend également les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.

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.

L'arrêté visé à l'alinéa 1er est pris après avis de l'autorité nationale d'accréditation, de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er.

§ 2. Le respect des exigences visées au paragraphe 1er est établi par un certificat délivré par un organisme d'évaluation de la conformité accrédité selon la norme ISO/IEC 17021 ou ISO/IEC 17065 par l'autorité nationale d'accréditation ou par une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation".

Le certificat délivré doit relever du domaine de certification pour lequel l'organisme d'évaluation de la conformité a été accrédité et porter sur l'ensemble du contenu de la P.S.I.

Art. 23. § 1er. L'opérateur de services essentiels désigne son point de contact pour la sécurité des systèmes et réseaux d'information et en communique les données à l'autorité sectorielle compétente dans un délai de trois mois à dater de la notification de la désignation comme opérateur de services essentiels, et, sans délai, après chaque mise à jour de ces données.

2. Art. 20 § 1 de la loi NIS : mesures de sécurité

- **1) Mesures techniques + organisationnelles**

- **2) Nécessaires et proportionnées**
  - Répondre utilement et de manière adaptée à un problème particulier dans une situation donnée.
  - **Individualiser les mesures**

- **3) Pour gérer les risques qui menacent la sécurité des réseaux et systèmes d'information**

  - **Risque** = notion centrale de la loi (art. 6, 15° de la loi NIS) *« toute circonstance ou évènement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ».*
  - ***A*nalyse de risques**

  - **Menace la sécurité des réseaux et systèmes d'information :**
    - Disponibilité : aptitude d'un système à être accessible et utilisable → garantir son fonctionnement
    - Authenticité : aptitude d'un système à confirmer qu'il est ce qu'il prétend être
    - Intégrité : aptitude d'un système à ne pas être altéré par des entités non autorisées
    - Confidentialité: aptitude d'un système à ne pas permettre l'accès à ses données à des personnes non autorisées.
    - … Traçabilité ? … cfr RGPD ?

- Les mesures de sécurité ne devraient pas être « une charge financière et administrative excessive » ou « impliquer la conception, le développement ou la fabrication d'un produit commercial particulier »

Art. 20 § 2 de la loi NIS

- **1) Garantir un niveau de sécurité**
  - Permettre à un système de résister, à un niveau de confiance donné, à des évènements susceptibles de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

- **2) Sécurité physique et logique**
  - **Physique :** mesures garantissant la capacité de résistance des éléments matériels des réseaux et systèmes d'information (accès physique aux équipements informatiques, salle des serveurs, etc.).
  - **Logique :** mesures garantissant la capacité de résistance des éléments logiques des réseaux et systèmes d'information (contrôle d'accès au logiciel, cryptage, surveillance, anti-virus, etc.).

- **3) Adapté aux risques existants**

- **4) Compte tenu de l'état des connaissances techniques actuelles**
  - Technique doit être présente sur le marché, comme un produit déjà commercialisé, et non encore à l'état de prototypes qui la rendrait difficilement disponible.
  - Veille technologique incontournable

Art. 20 § 3 de la loi NIS

- Mesures appropriées en vue de prévenir des incidents
  - **Appropriées:** dépend de l'objet sur lequel elles portent = prévenir les incidents
  - **Prévenir les incidents:** limiter leur impact, dans la perspective de permettre la continuité de la fourniture des services essentiels.

- **<u>Mesures spécifiques obligatoires (art. 21, § 3 et 4)</u>**

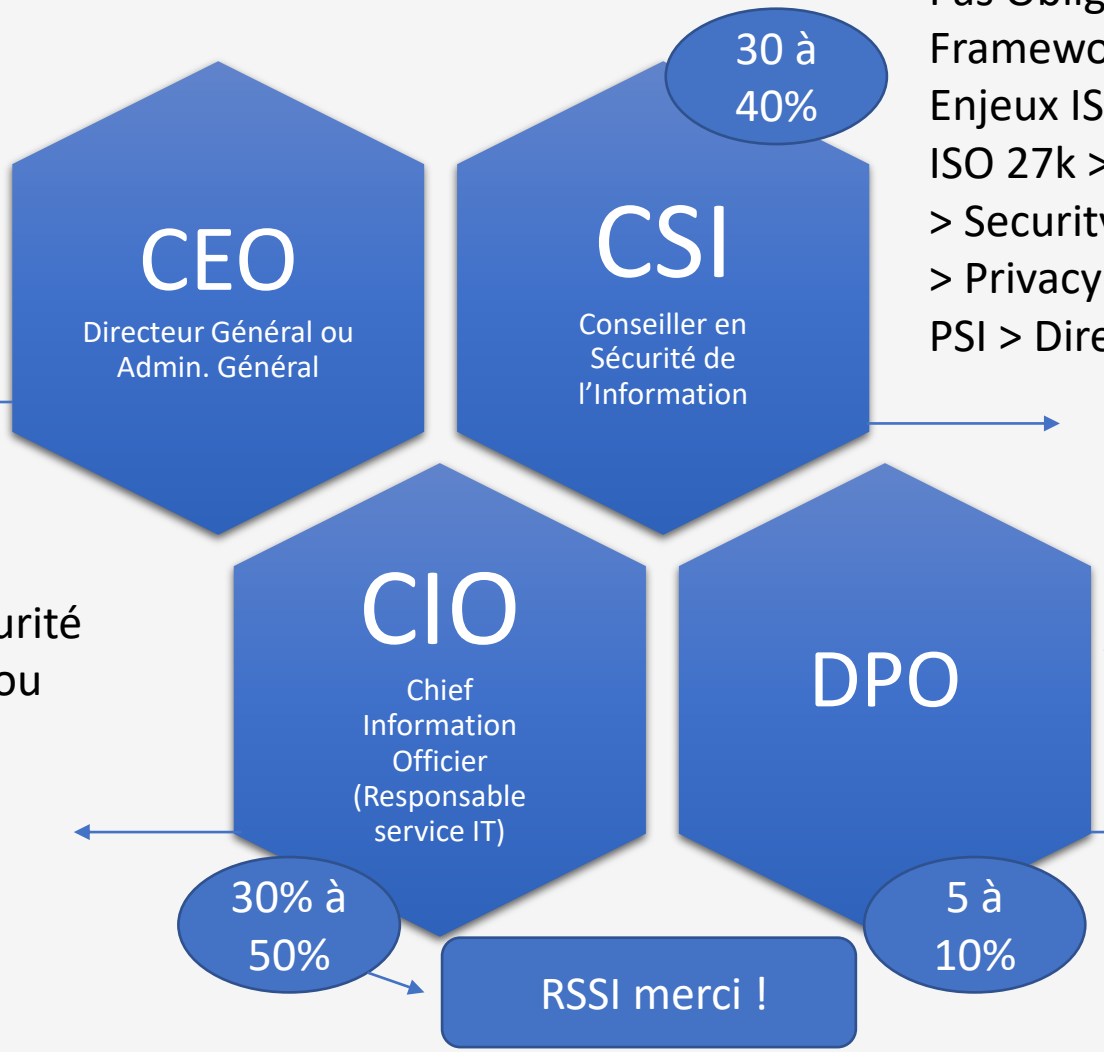
- *Le Roi peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels d'un ou plusieurs secteurs (par arrêté royal);*
- *L'autorité sectorielle peut imposer des mesures complémentaires de sécurité (par décision administrative individuelle).*

3.4 NIS 1 : Equipe NIS > Gouvernance (exemple simplifié)

Management: soutien et compréhension vis-à-vis de ses équipes des enjeux et obligations (généraux, sectoriels + ISO 27001 + RGPD)

Approuver une politique de sécurité de l'information (PSI) ! (avec une stratégie claire)

Nommer un Responsable de la Sécurité des Systèmes d'Information (**RSSI**) ou Chief Information Security Officier (CISO) qui décharge le CIO
Elévation du niveau de sécurité
Actions techniques et procédures tactiques



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

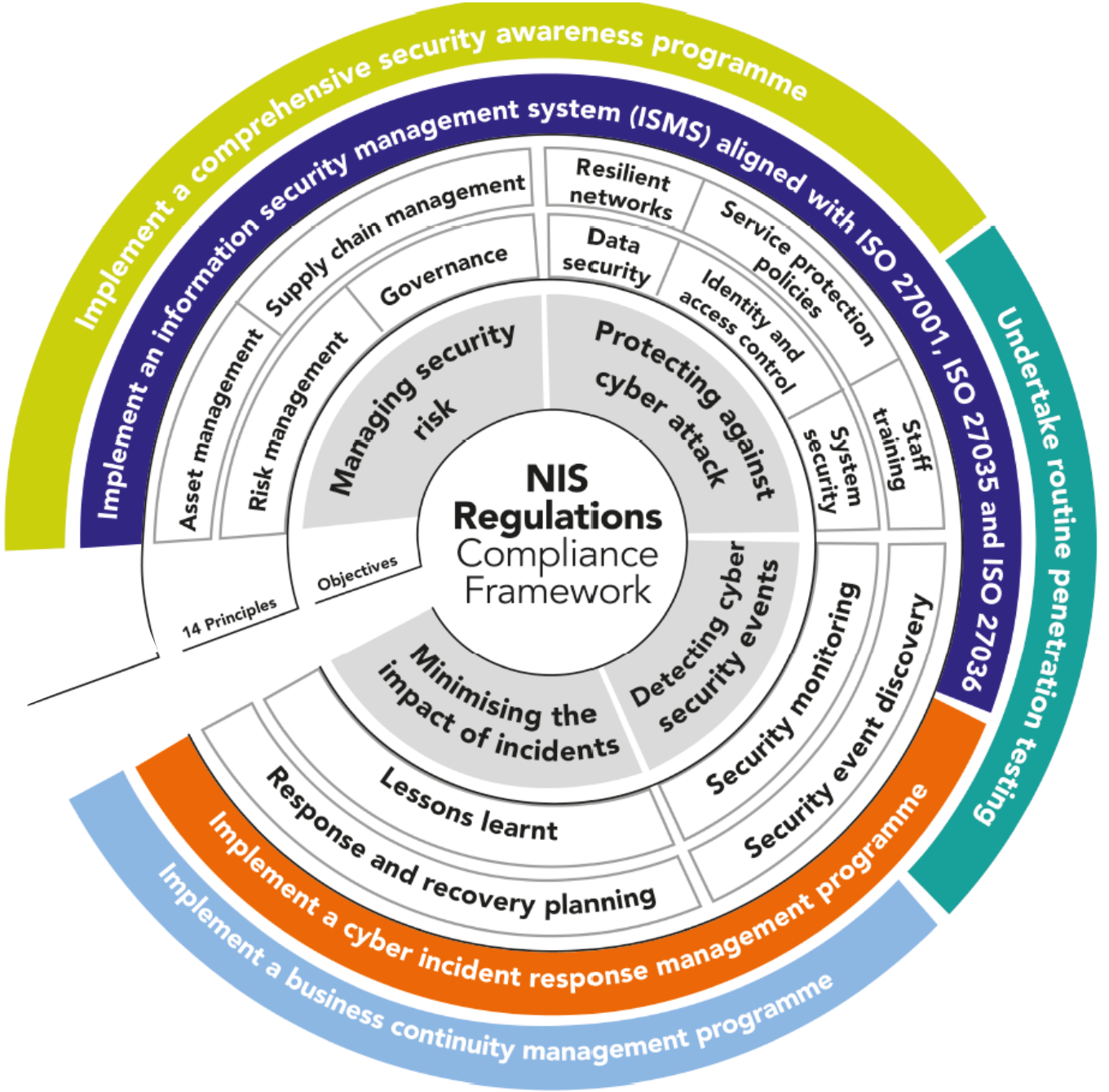
Privacy by design/by default
A18 de l'ISO 27001 > 27002
(parfois DPO et CSI sont exercés par la même personne)

+ RH
+ Autres services métier à écouter ;

3.5 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.

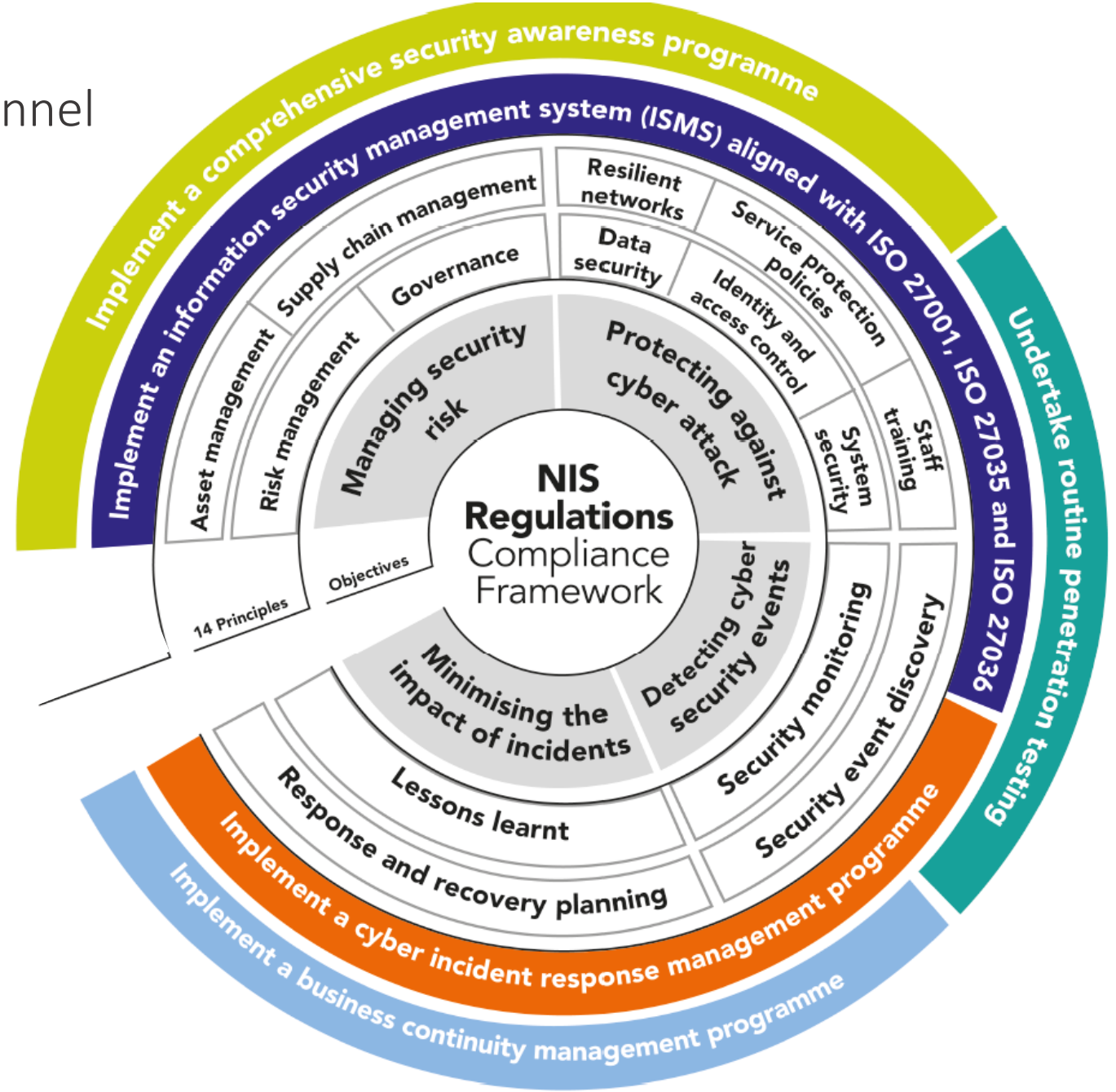
Art. 22. § 1er. La P.S.I. visée à l'article 21, § 1er, est, jusqu'à preuve du contraire, présumée conforme aux exigences de sécurité, visées à l'article 20, lorsque les mesures de sécurité qu'elle comporte répondent aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale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



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

3.5 Organisation de la Cybersécurité
2. Management du risque informationnel

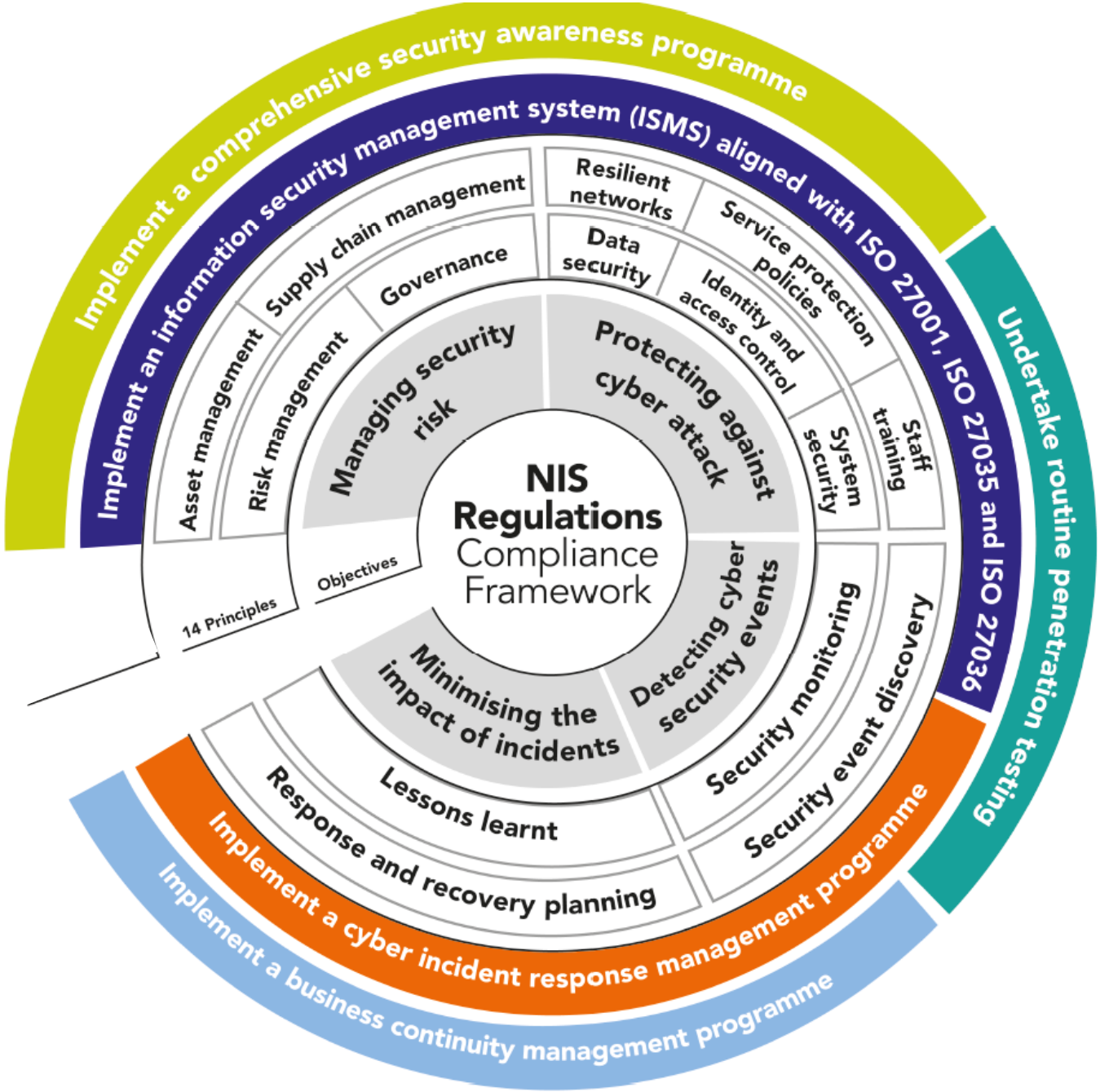
1. Mettre en place une **gouvernance NIS** (projet).
2. Mettre en place un **management des actifs.**
3. Mettre en place un **programme d'analyse de risques** (Idéal pas uniquement Cyber) : ISO 31000 + ISO 27005.
    1. **Manager le risques** avec ARTEMIS (MFWB & SPW), MONARC/EBIOS ou OCTAVE, …
4. Gérer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



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

3.6 Organisation de la Cybersécurité
3. Se protéger des Cyberattaques

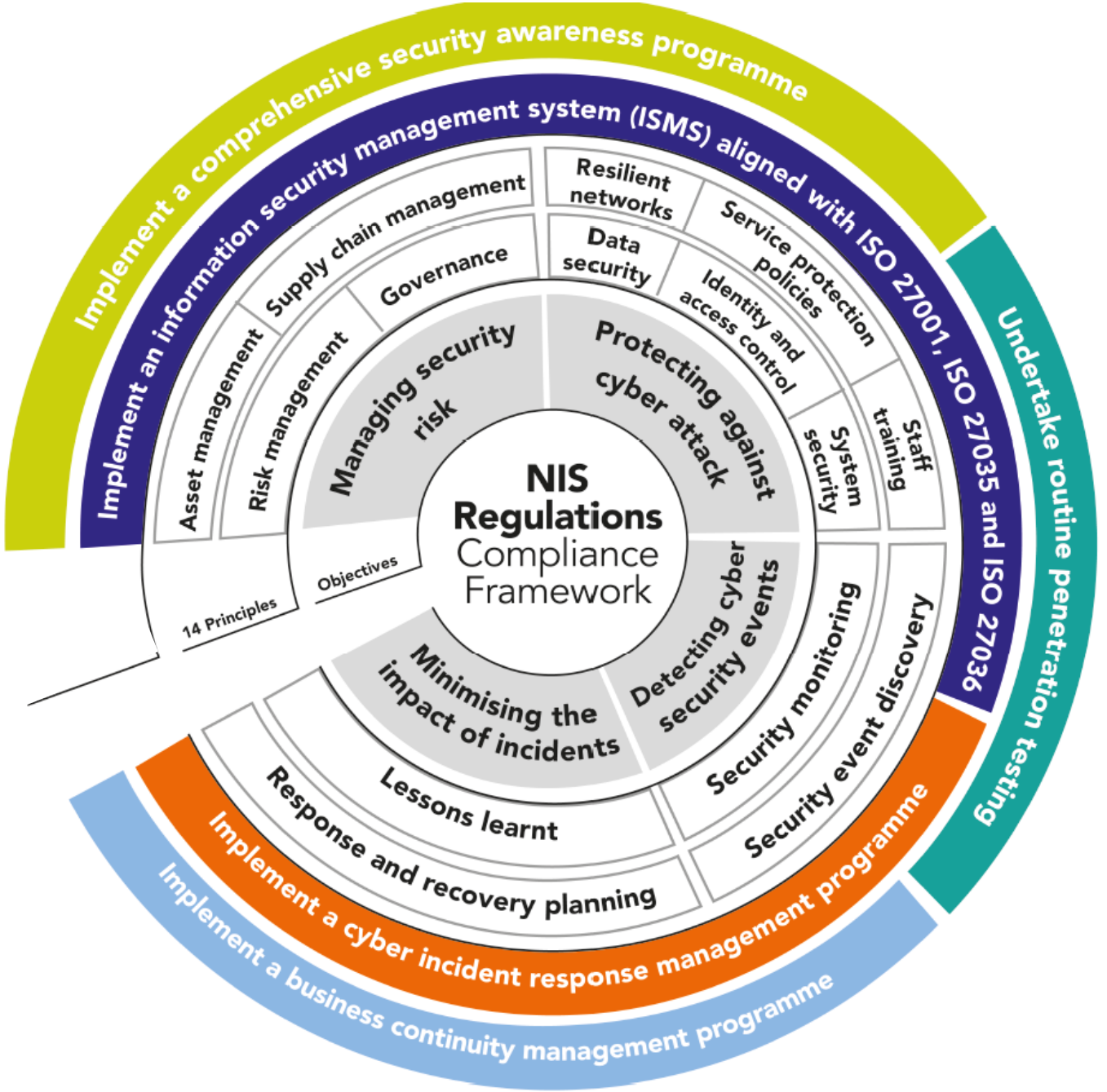
1. **Sécuriser vos données :** de la création de la donnée à sa destruction, de l'ouverture du flux à sa fermeture.
2. **Disposer de réseaux résilients :** avoir des réseaux redondants par exemple.
3. **Disposer de procédures de sécurité :** Une politique générale, des directives par annexe ISO et des 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 systèmes est spécifique.
6. **Former votre personnel à la sécurité.**



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

3.6 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* » permettent eux 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 bases de données d'incidents est une obligation légale.

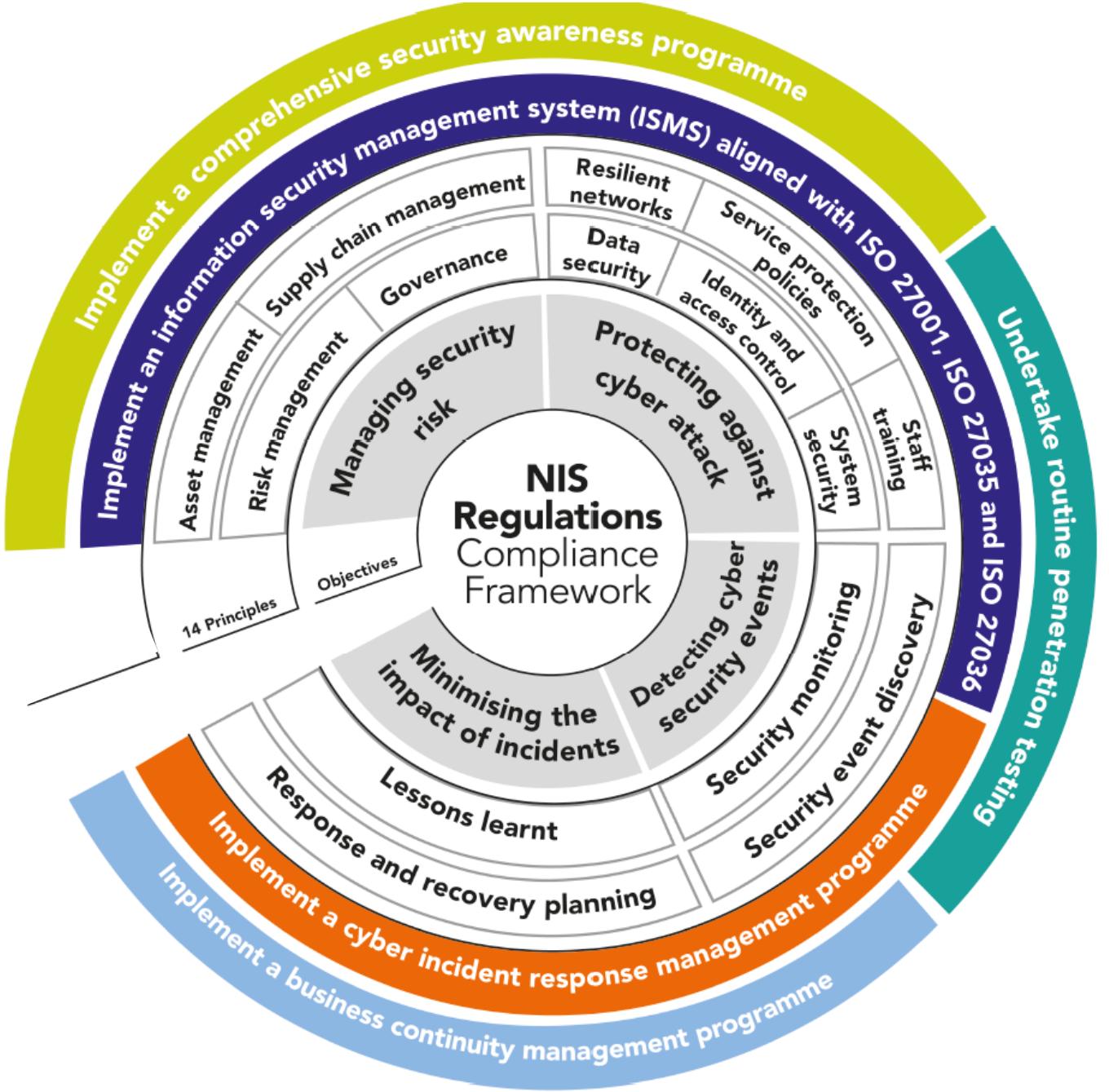


Sources : https://www.itgovernance.co.uk

3.6 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 moyens 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

Notification des incidents NIS1 & NIS 2

- De nombreux éléments de cette présentation ont été retiré car ils sont identiques à ceux du CCB ! Valery Vander Geeten.
- Pour les aspects juridiques et légaux veuillez vous référer à la présentation :

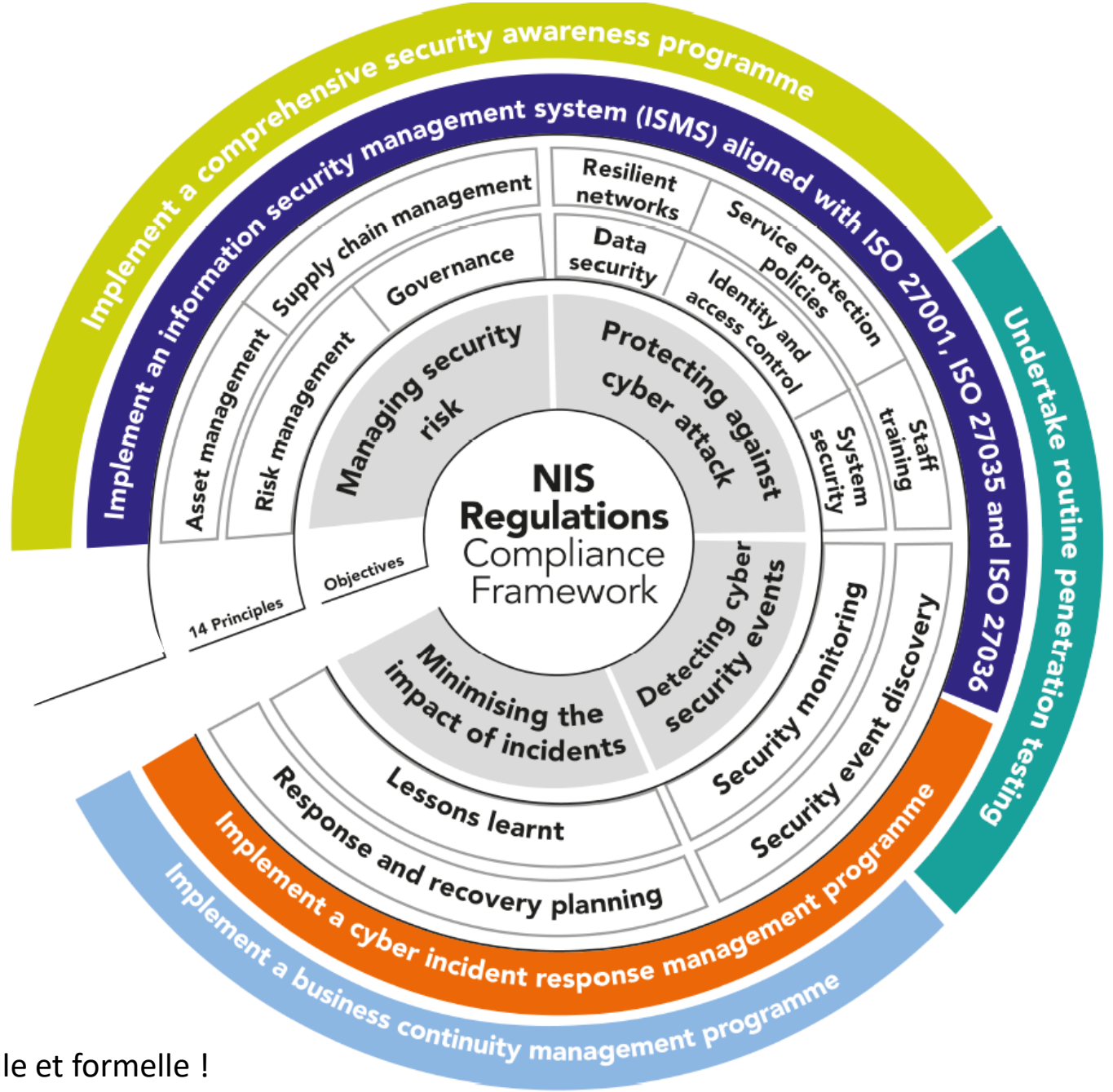
  - NIS directive from Central States to Regional Challenges and Opportunities 2022.pdf

  - Seuls les éléments liés à la sécurité seront abordés dans cette présentation, il se peut que certaines diapositives ou rubriques soient fortement simplifiées (voir le sommaire).

Sources : www.CCB.gov.be

3.6 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 ;

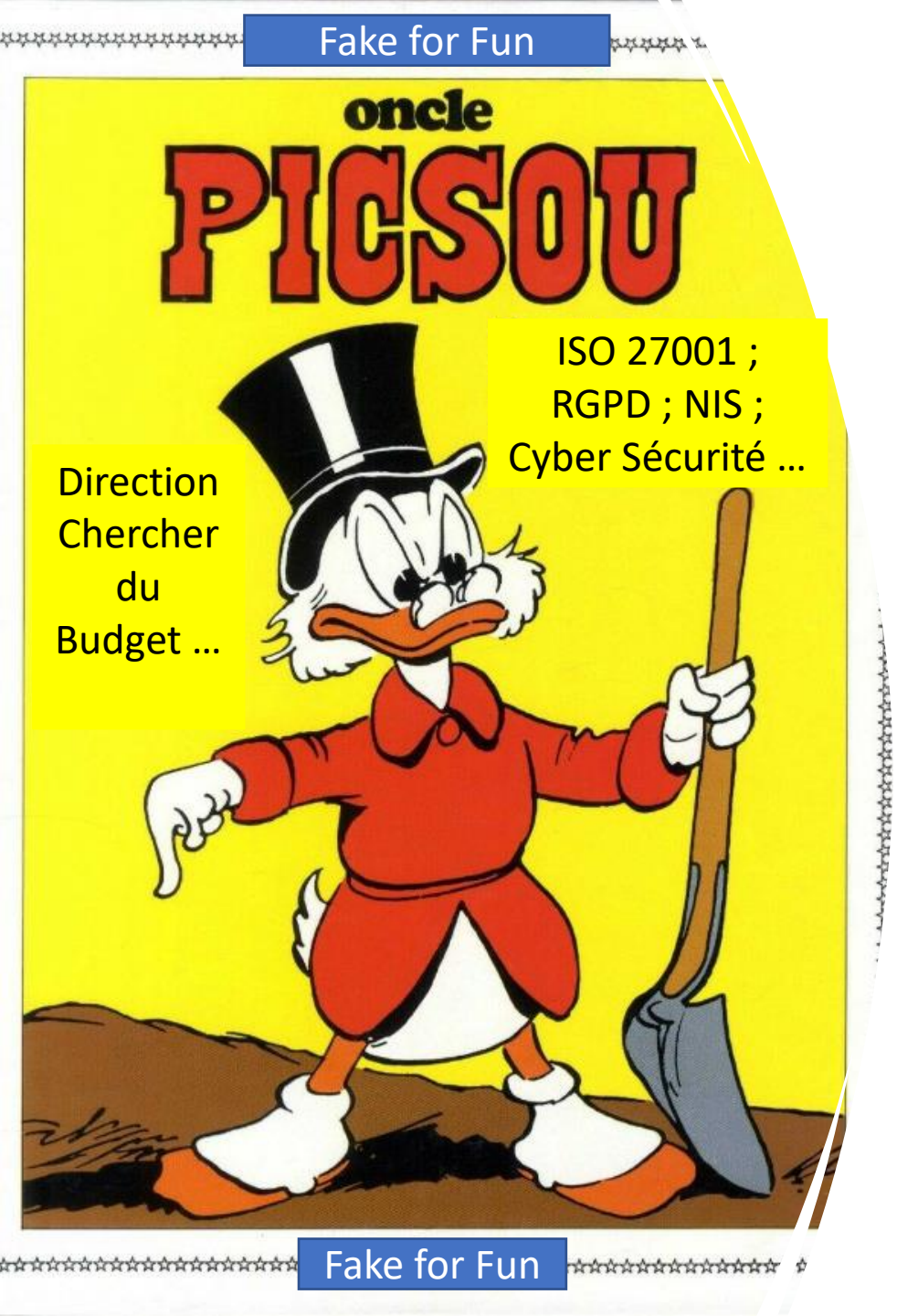


RAPPEL : Gestion des incidents de sécurité de manière officielle et formelle !

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

Point de vue :

RIEN de NOUVEAU en sécurité et cybersécurité SAUF QUE ! Il faut le faire pour de VRAI…



Idéalement pour des économies d'échelles, temps et compétences

- **Réaliser UN MANAGEMENT Intégré – Belgique ?**
  - **(1) ISO 27001** ;
  - **(2) Compliance RGPD** ;
  - **(3) Compliance NIS** ;
  - (4) De Facto > **Cybersécurité** ! ;
    - Actions techniques importantes
  - **> Management Intégré** (1) + (2) + (3)

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)

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
https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
BONUS : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

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

DevSecOps : OWASP : https://owasp.org

CyberSécurité : CSC20 & CSC 18 : https://www.cisecurity.org

Contacts :

Pour en savoir plus, vous pouvez consulter le site et FAQ du CCB (lien) /
ou contacter directement le CCB (nis@ccb.belgium.be).

En cas d'incident (non NIS) : https://www.cert.be/fr/signaler-un-incident
En cas d'incident NIS : https://nis-incident.be/fr/
(voir les guides du CCB pour le notification des incidents)

Banque Carrefour d'échange de données : david.blampain@ewbs.be

Idées complémentaires :
Discussion de groupe des eConferences NIS 1 et NIS 2 (14 eConferences)

- Travailler à faire avancer votre Management ! > Management Intégré : « RGPD + NIS + ISO 27001 (32>33>34>… Cyber Sécurité)»
- Budget pour la sécurité de l'information hors budget IT svp ;
- Se driller sur des attaques ; Planifier des attaques avec MITRE ;
- Rapports des autres hôpitaux suite aux attaques (Mise à jour des OS) ; (Protection des comptes Admin) ;
- Future certification de cybersécurité des produits et services (Cyber Security Act - CSA);
- FortiSandBox ;
- IAM ;
- Retour d'expérience du CHU Charleroi (ISO 27001) ;

- **A LIRE** :
- https://www.cyberveille-sante.gouv.fr/index.php/accueil
- https://www.lexalert.be/fr/article/votre-organisation-est-elle-pr-te-faire-face-aux-nouvelles-obligations-en-mati-re-de-cybers-curit

- **A TESTER** :
- https://www.isaca.org/-/media/info/conquest/index.html

- **Se FORMER** > SANS ; ISC² (CISSP) ; ISACA (CISM ; CISA) ; ISO 27001 Lead Implémenter ;

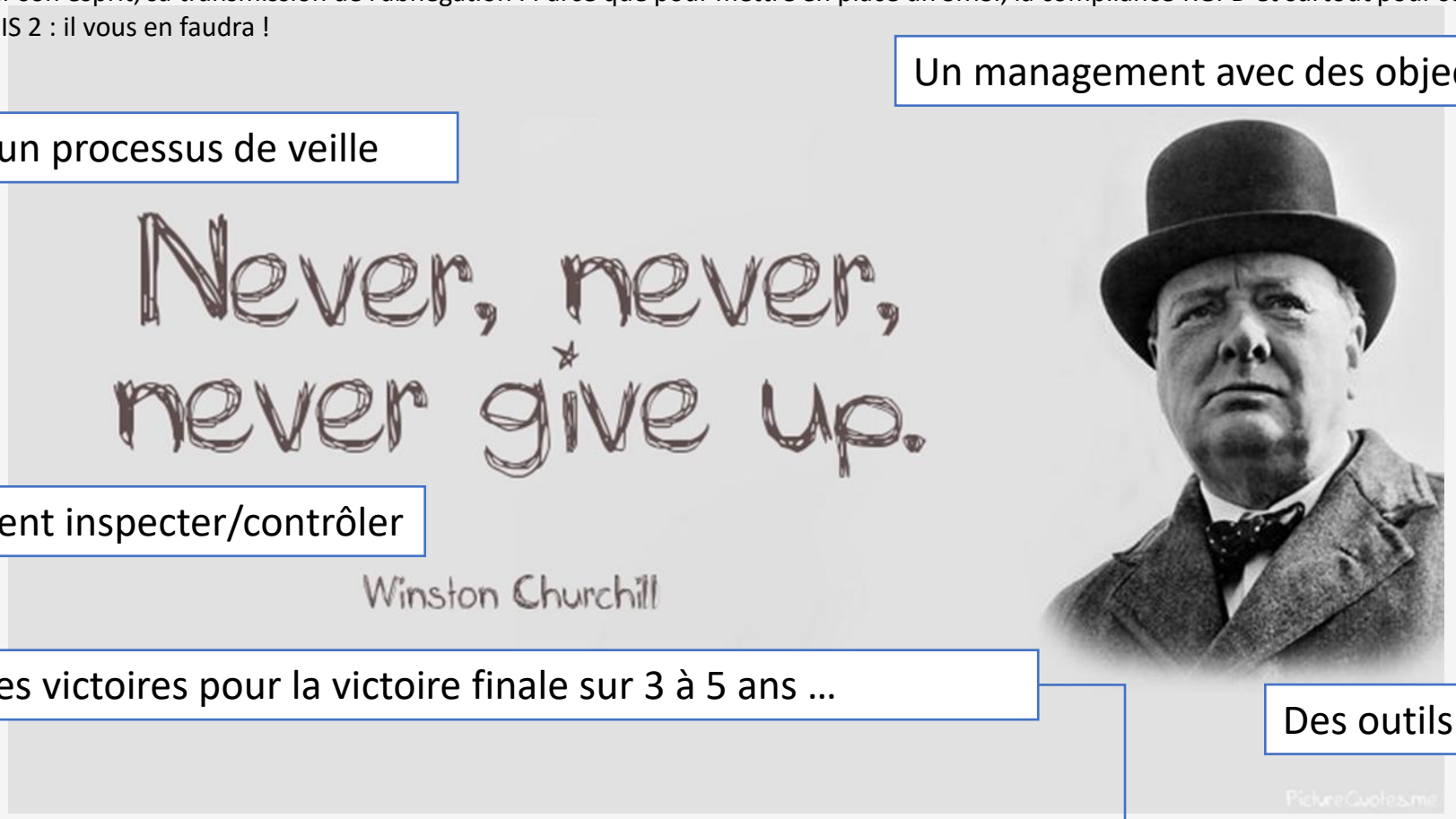
Rester humble et discret pour éviter d'attirer les hackers… IT dire la vérité à la direction. La direction dire la vérité à l'état et aux citoyens.

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



Les autorités NIS peuvent inspecter/contrôler

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

Des outils professionnels

Bref : Patience