Frameworks de cybersécurité pour PME

P.Leclercq
07/05/2024

Liste des frameworks de sécurité

- ISO 27001
- NIST Cybersecurity Framework (CSF)
- Cyber Essentials (UK NCSC)
- CyberFundamentals Framework (CCB)
- CIS Controls

ISO 27001

ISO 27001

- Standard international publié par l'International Standard Organization (ISO)
- Décrit les exigences pour établir, implémenter et maintenir un système de gestion de la **sécurité de l'information** (ISMS)
- Publication de la 1ère version: 2005, basé sur le standard BS 7799-2
- Version actuelle: ISO 27001:2022 (ces notes sont basées sur la version 2013)

ISO 27001 – Buts et moyens

- Protéger la confidentialité, l'intégrité et la disponibilité de l'information (CIA)
- Certification des individus et des entreprises possible
- Normatif et non prescriptif : ne dit pas comment implémenter les exigences, mais aucun point des sections 4 à 10 ne peut être ignoré

ISO 27001 - Structure

- Clause 4 : Contexte de l'organisation
- Clause 5 : Leadership
- Clause 6 : Planification
- Clause 7 : Support

PLAN

- Clause 8 : Fonctionnement

DO

- Clause 9 : Evaluation des performances

CHECK

- Clause 10 : Amélioration

ACT

- Annexe A : Objectifs et mesures de référence (14 sections, 114 contrôles)

ISO 27001 – Documents obligatoires

Domaine d'application (scope)	Politique d'utilisation correcte
Politique de sécurité de l'information	Politique de contrôle d'accès
Processus d'évaluation et de traitement des risques	Procédures opérationelles pour la gestion de l'IT
Déclaration d'applicabilité (justification de l'inclusion ou non des contrôles annexe A)	Principes d'ingénierie de la sécurité des systèmes
Plan de gestion des risques	Politique de sécurité pour les fournisseurs
Résultats de l'évaluation et du traitement des risques	Procédure de gestion des incidents de sécurité de l'information
Définition des rôles et responsabilités dans la sécurité	Procédure de gestion de la continuité
Inventaire des actifs	Exigences légales, statutaires, régulatoires et contractuelles

ISO 27001 – Enregistrements obligatoires

- Liste de compétences, formations, aptitudes et qualifications
- Résultats de la surveillance et mesures du système de sécurité
- Programme d’audit
- Résultats des audits
- Résultats des revues de la direction
- Non-conformités, actions correctives et résultats
- Journaux d’événements, administrateurs et opérateurs

ISO27001 – Annexe A

A.5: Politique de sécurité de l'information	A.5.1:Orientations de la direction
A.6: Organisation de la sécurité	A.6.1:Organisation interne
	A.6.2: Appareils mobiles et télétravail
A.7: Sécurité des ressources humaines	A.7.1: Avant l'embauche
	A.7.2: Pendant la durée du contrat
	A.7.3: Rupture, terme ou modif. du contrat
A.8: Gestion des actifs	A.8.1: Responsabilité des actifs
	A.8.2: Classification de l'information
	A.8.3: Manipulation des supports
A.9: Contrôle d'accès	A.9.1: Exigences métier des accès
	A.9.2: Gestion de l'accès des utilisateurs
	A.9.3: Responsabilité des utilisateurs
	A.9.4: Contrôle de l'accès

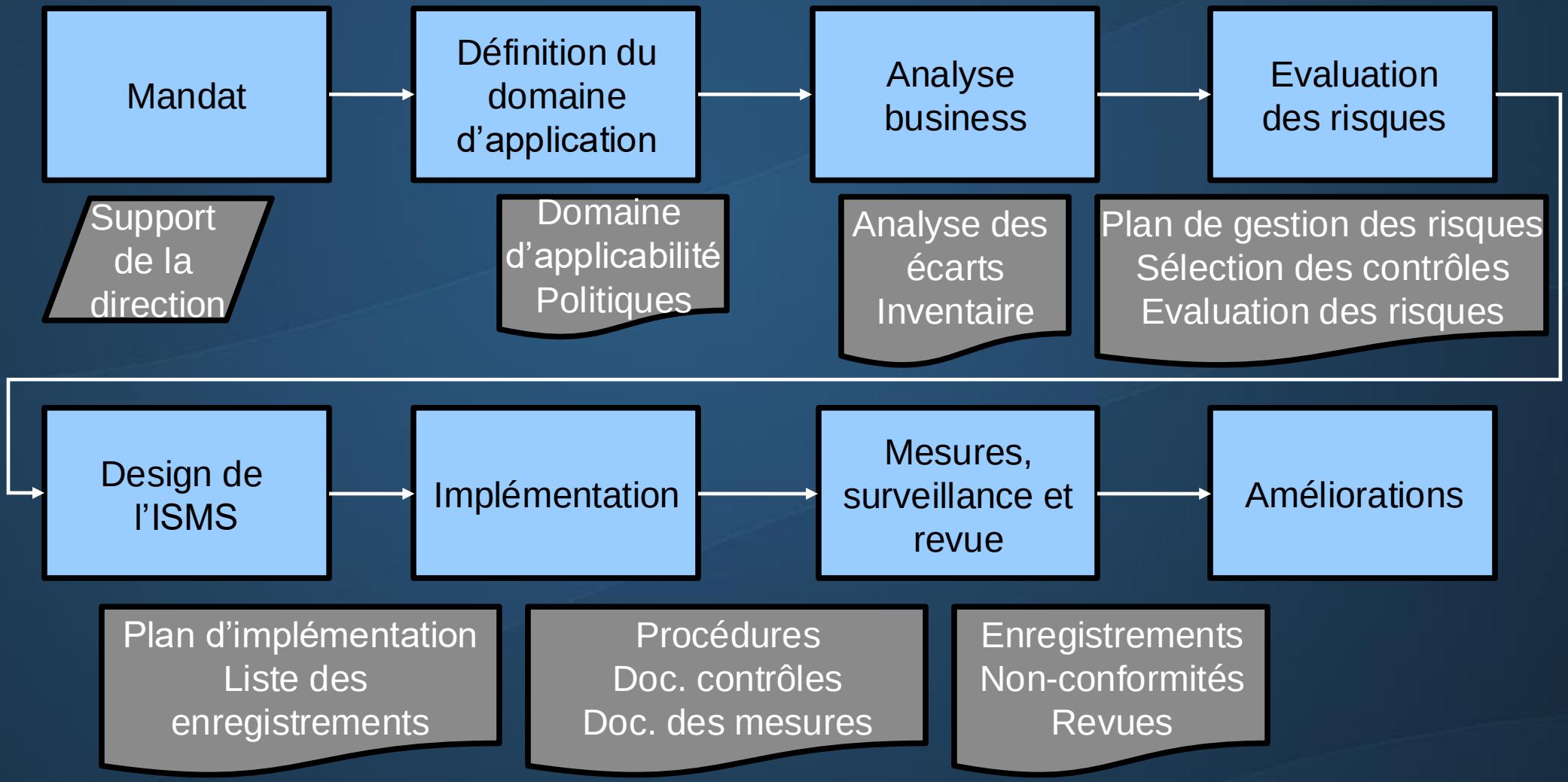
ISO27001 – Annexe A

A.10: Cryptographie	A.10.1:Mesures cryptographiques
A.11: Sécurité physique et environnementale	A.11.1:Zones sécurisées
	A.11.2: Matériels
A.12: Sécurité liée à l'exploitation	A.12.1: Procédures liées à l'exploitation
	A.12.2: Protection contre les malwares
	A.12.3: Sauvegardes
	A.12.4: Journalisation et surveillance
	A.12.5: Maîtrise des logiciels en exploit.
	A.12.6: Gestion des vulnérabilités
	A.12.7: Audit des S.I.
A.13: Sécurité des communications	A.13.1: Gestion de la sécurité des réseaux
	A.13.2: Transfert de l'information

ISO27001 – Annexe A

A.14: Acquisition, développement et maintenance des systèmes d'information	A.14.1: Exigences de securité pour S.I.
	A.14.2: Sécurité des processus de dév.
	A.14.3: Données de test
A.15: Relations avec les fournisseurs	A.15.1: Sécurité dans les relations
	A.15.2: Gestion de la prestation du service
A.16: Gestion des incidents de sécurité	A.16.1: Gestion des incidents et amélioration
A.17: Sécurité dans la gestion de continuité de l'activité	A.17.1: Continuité de la sécurité
	A.17.2: Redondance
A.18: Conformité	A.18.1: Conformité légale et réglementaire
	A.18.2: Revue de la sécurité

ISO 27001 – Plan de projet (ISO 27003)



ISO 27001 – PME ?

- ISO publie ISO/IEC 27001:2022 - Information Security Management Systems - A practical guide for SMEs (CHF 42)
- Expériences montrent qu'une PME de ~50 personnes peut être certifiée au bout de 8 à 12 mois dans des secteurs avec forte présence de l'IT
- Coût min. d'implémentation : > 1 année/homme
- ! coûts de maintenance de la certification : 1 audit externe/an + un audit approfondi de recertification tous les 3 ans
- En Belgique : NIS/NIS 2 = ISO 27001 (bientôt CyFun)

ISO 27001 – Références

- https://www.iso.org/standard/27001
- https://advisera.com/iso-27001/
- https://www.itgovernance.co.uk/iso27001

NIST Cybersecurity Framework

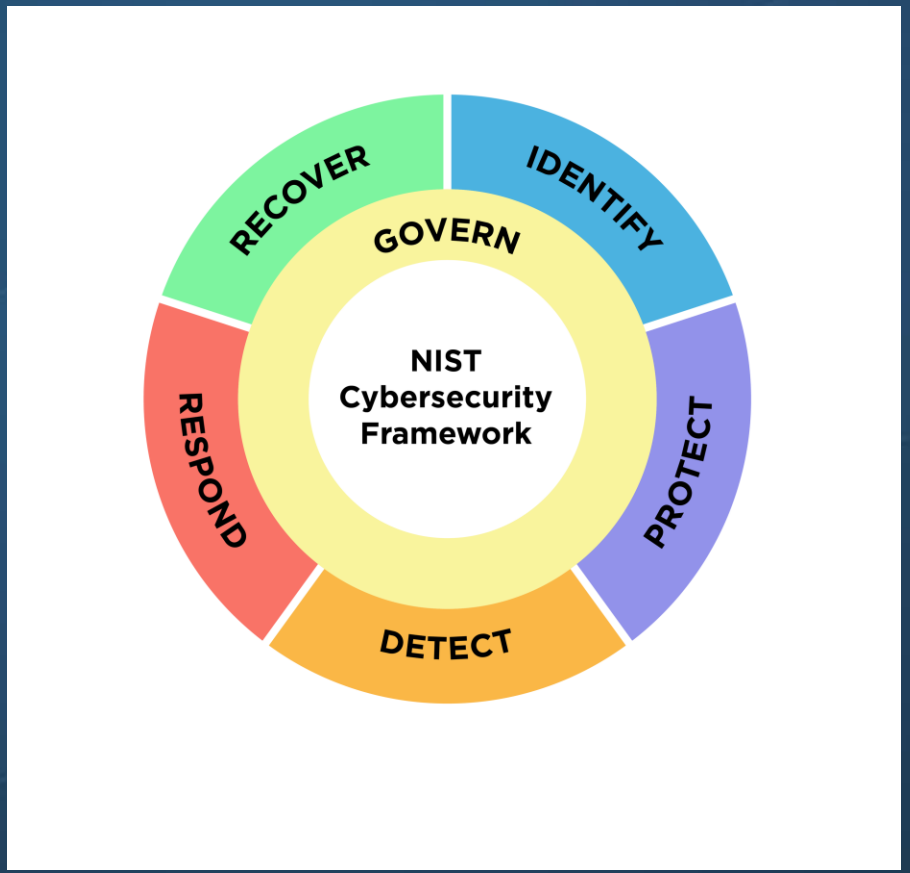
NIST Cybersecurity Framework

- NIST = National Institute of Standards and Technology, agence du département du Commerce des Etats-Unis
- NIST CSF publié en 2014, version actuelle: CSF 2.0, publiée le 26/2/2024
- Non prescriptif : décrit les résultats désirés, pas comment ils sont réalisés

NIST CSF - Contenu

- CSF Core: liste des résultats désirés
- CSF Organizational Profiles: description des états actuel et cible
- CSF Tiers: description de la rigueur des moyens de gestion de la sécurité

NIST CSF – Fonctions



NIST CSF – Fonctions

Fonction	Catégorie
Gouverner	Contexte organisationnel
	Stratégie de la gestion des risques
	Rôles, responsabilités et autorités
	Politique
	Surveillance
	Gestion des risques de la chaîne d'approvisionnement
Identifier	Gestion des actifs
	Evaluation des risques
	Amélioration

NIST CSF – Fonctions

Fonction	Catégorie
Protéger	Gestion des identités, authentification et contrôle d'accès
	Sensibilisation et formation
	Sécurité des données
	Sécurité de la plateforme
	Résilience des infrastructures technologiques
Détecter	Surveillance continue
	Analyse des événements indésirables

NIST CSF – Fonctions

Fonction	Catégorie
Répondre	Gestion des incidents
	Analyse des incidents
	Rapports et communications en matière de réponse aux incidents
	Atténuation des incidents
Récupérer	Exécution du plan de récupération après incident
	Communication de récupération après incident

Toutes les fonctions doivent être développées en parallèle. Gouverner, Identifier, Protéger et Détecter doivent fonctionner en continu, Répondre et Récupérer doivent être prêts à tout moment si un incident de sécurité survient.

NIST – Liste des contrôles techniques

- Voir NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)
- 1189 contrôles

NIST CSF - Niveaux

Niveau	Dénomination	Caractéristiques
Niveau 1	Partiel	Application de la stratégie de cybersécurité ad hoc
Niveau 2	Informé du risque	Pratiques de gestion des risques approuvées par le management, mais pas implémentées en totalité, et de manière non uniforme
Niveau 3	Répétable	Pratiques de gestion des risques approuvées, exprimées sous forme de politiques, appliquées par des processus et procédures régulièrement mis à jour; personnel formé; cybersécurité surveillée à tous les niveaux de l'entreprise.
Niveau 4	Adaptatif	Gestion des risques de cybersécurité fait partie de la culture d'entreprise, au même niveau que les risques financiers ou organisationnels; l'organisation adapte ses pratiques basées sur l'évolution des risques, les retours d'expérience et des indicateurs prédictifs.

NIST CSF – Adaptation aux PME

- Voir smallbusinesscyber et NIST.SP.1300.pdf
- Liste d'actions, de questions et de documents types par fonction
  - Comprendre
  - Evaluer
  - Prioritiser
  - Communiquer

NIST CSF - PME

- Documents types

Notre mission:	
Quels risques de cybersécurité pourraient nous empêcher de remplir notre mission?	

Exigences légales:	
Exigences régulatoires:	
Exigences contractuelles:	

Actif	Usage	Propriétaire	Données sensibles	MFA?	Risque en cas de perte d'accès

NIST CSF – Références

- https://www.nist.gov/cyberframework
- Voir smallbusinesscyber et NIST.SP.1300.pdf

Cyber Essentials

Cyber Essentials

- Développé par le National Cyber Security Centre (NCSC) du Royaume-Uni spécifiquement pour les PME, soutenu par le gouvernement GB
- Certifiant pour les entreprises en GB
- Normatif et prescriptif
  - Actifs dans le domaine d'application bien définis, y compris le cloud
  - Actions claires et précises
- 2 niveaux
  - Cyber Essentials : certification par auto-évaluation (119 questions) et vérification des réponses
  - Cyber Essentials Plus : certification par audit (IASME consortium)

Cyber Essentials - Coût

Taille	Nombre d'employés	Prix (€)
Micro	0-9	380
Petite	10-49	520
Moyenne	50-249	590
Grande	250+	710

- La certification comprend une assurance contre le risque cyber
- Renouvellement annuel

Cyber Essentials - Contrôles

Thème	Contrôle
Firewalls	Changer le mot de passe par défaut ou bloquer l'accès administrateur
	Bloquer l'accès à l'interface d'administration à partir d'internet (ou imposer MFA ou liste d'adresses IP permises)
	Bloquer les connections entrantes non authentifiées
	S'assurer que les règles entrantes des firewalls sont approuvées et documentées
	Rapidement désactiver les règles non nécessaires
Configuration sécurisée	Désactiver les comptes utilisateurs non nécessaires
	Changer les mots de passe par défaut ou faibles
	Supprimer les logiciels non nécessaires
	Désactiver l'exécution automatique sans autorisation
	Imposer l'authentification des utilisateurs
	Activer le verrouillage automatique

Cyber Essentials - Contrôles

Gestion des mises à jour de sécurité	Les logiciels doivent avoir des licences valables et être supportés
	Supprimer les logiciels quand ils ne sont plus supportés
	Activer les mises à jour automatiques dans la mesure du possible
	Appliquer les mises à jour dans les 14 jours quand elles corrigent des vulnérabilités critiques ou à risque élevé
Contrôle d'accès	Avoir un processus pour créer et activer les comptes d'utilisateurs
	Authentifier les utilisateurs avec des identifiants uniques
	Désactiver les comptes utilisateurs non nécessaires
	Implémenter un accès multifacteur quand c'est possible (l'authentification pour les services cloud doivent être MF)
	Utiliser des comptes séparés pour les actions d'administrateur
	Désactiver les privilèges quand ils ne sont plus nécessaires

Cyber Essentials - Contrôles

Protection contre les malwares	Actifs avec anti-malware	Mettre à jour les logiciels anti-malware suivant les recommandations du fournisseur
		Configurer les logiciels pour bloquer les malwares
		Configurer les logiciels pour bloquer les codes mal intentionnés
		Bloquer les connexions aux sites web malicieux
	Actifs avec liste d'applications autorisées	Approver activement les applications autorisées avant de les déployer
		Maintenir une liste d'applications autorisées; les utilisateurs ne peuvent pas être capable d'installer une application non signée

Cyber Essentials - Recommandations

- La sauvegarde des données est mentionnée dans les recommandations annexes

Cyber Essentials - Références

- https://www.ncsc.gov.uk/cyberessentials/
- https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf

CyberFundamentals Framework

CyberFundamentals Framework

- Ensemble de mesures concrètes visant à :
  - protéger les données
  - réduire de manière significative le risque des cyber-attaques les plus courantes,
  - accroître la cyber-résilience d'une organisation.
- Basé sur: NIST CSF, ISO 27001 / ISO 27002, CIS Controls et IEC 62443
- Organisation de la certification en cours

CyberFundamentals - Niveaux

- Choix du niveau facilité par un tableur d'évaluation des risques
- Contrôles basés sur NIST CSF (sauf Small)

Niveau	Cible	% attaques couvertes	Contrôles
Small	Micro-organisations ou connaissances techniques limitées	-	7
Basic	Toutes les entreprises standard	82	31
Important	Attaquant à compétences communes	94	95
Essentiel	Attaquant à compétences avancées	100	101

CyFun – Contrôles - Small

- Small
  1) Protéger toutes les connexions avec l'authentification multifactorielle
  2) Installer immédiatement toutes les mises à jour de sécurité
  3) Installer un antivirus
  4) Sécuriser votre réseau
  5) Sauvegarder vos données
  6) Droits d'administration
  7) Recommandations finales
     1) Protégez physiquement vos actifs, savoir qui contacter en cas d'incident

CyFun – (future) Certification

	Basic	Important	Essentiel
Type de vérification	Vérification	Vérification	Certification
Méthode de vérification	Vérification d'auto-évaluation	Vérification d'auto-évaluation	Audit de certification
Standard d'accréditation	ISO/IEC 17029	ISO/IEC 17029	ISO/IEC 17021-1
Fréquence	-	-	Surveillance annuelle, recertification tous les 3 ans
Evidence de conformité	Déclaration vérifiée	Déclaration vérifiée	Certificat
NIS2		X	X

CCB – Cybersécurité pour les PME

- En-dehors de CyFun, le CCB a publié un guide de cybersécurité pour les PME (plus basé sur ISO 27001)

01 – Impliquez le top management	07 – Sauvegardez toutes les informations
02 – Elaborez une politique de sécurité et un code de conduite	08 – Gérez l'accès à vos ordinateurs et réseaux
03 – Sensibilisez vos travailleurs aux risques cyber	09 – Sécurisez les postes de travail et les appareils mobiles
04 – Gérez vos ressources informatiques importantes	10 – Sécurisez les serveurs et composants réseaux
05 – Mettez à jour tous les programmes	11 – Sécurisez les accès à distance
06 – Installez une protection anti-virus	12 – Disposez d'un plan de la continuité et de gestion des incidents

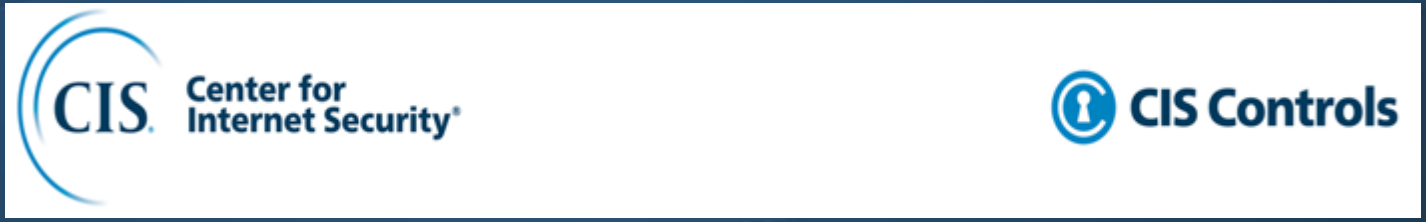
CCB – Cybersécurité pour les PME

- 2 niveaux
  - Protection de base : 51 contrôles
  - Protection avancée : 113 contrôles

CynFun et CCB - Références

- https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework
- https://ccb.belgium.be/fr/document/guide-pour-les-pme

CIS Controls



CIS Controls

- Projet initié en 2008 par le SANS Institute (SANS Top 20) en réponse aux attaques subies par les entreprises de défense américaines, puis transféré au Center for Internet Security (CIS) en 2015
- Basées sur observation d'attaques réelles
- Version actuelle: v8 (20 -> 18 actions clés)
- Structure basée sur NIST CSF
- Pas de notion de gouvernance, axés sur organisation et solutions techniques

CIS Controls

- 3 niveaux (« Implementation Groups »)
  - IG1: PME avec expertise IT limitée, contrôles disponibles avec des solutions grand public – 56 contrôles
  - IG2: Entreprise avec personnel dédié à la gestion de l'IT et de la sécurité, contrôles disponibles avec des solutions d'entreprise et de l'aide d'experts pour l'implémentation – 130 contrôles
  - IG3: Entreprise avec plusieurs experts spécialisés dans des branches différentes de sécurité – 153 contrôles

CIS Controls

Contrôle	IG1	IG2	IG3
01 – Inventaire et contrôle des actifs matériels	2	4	5
02 – Inventaire et contrôle des actifs logiciels	3	6	7
03 – Protection des données	6	12	14
04 – Configuration sécurisée des actifs	7	11	12
05 – Gestion des comptes	4	6	6
06 – Contrôle d'accès	5	7	8
07 – Gestion continue des vulnérabilités	4	7	7
08 – Gestion des journaux d'audit	3	11	12
09 – Protection des emails et des browsers	2	6	7
10 – Défense contre les malwares	3	7	7
11 – Récupération des données	4	5	5
12 – Gestion de l'infrastructure réseau	1	7	8

CIS Controls

Contrôle	IG1	IG2	IG3
13 – Surveillance et défense du réseau	0	6	11
14 – Sensibilisation à la sécurité et formation	8	9	9
15 – Gestion des prestataires de services	1	4	7
16 – Sécurité des applications	0	11	14
17 – Gestion de la réponse aux incidents	3	8	9
18 – Tests de pénétration	0	3	5

CIS Benchmarks

- Parallèlement, CIS publie des recommandations de configuration sécurisées (CIS Benchmarks) pour de nombreux produits:
  - OS
  - Middlewares (bases de données, serveurs Web, Office...)
  - Composants réseaux (firewalls...)
  - Solutions cloud.....

CIS - Références

- https://www.cisecurity.org/controls
- https://www.cisecurity.org/cis-benchmarks