LiveCampus

Apprentissage connecté

Sommaire

LiveCampus

Apprentissage connecté

Présentation de l'ISO/IEC 27001:2022

Brève histoire et contexte de l'ISO 27001.
Objectif : définir un Système de Management de la Sécurité de l'Information (SMSI).
Structure : politique, planification, amélioration continue (PDCA).

LiveCampus

Apprentissage connecté

93 mesures réparties

Organisationnel	Humain	Physique	Technologique

https://cyberupgrade.net/blog/compliance-regulations/iso-27001-controls-list-a-complete-guide-to-annex-a-and-control-objectives-in-2025/?utm_source=chatgpt.com

LiveCampus

Apprentissage connecté

Le **NIST (National Institute of Standards and Technology)** est une agence fédérale américaine dépendant du département du Commerce.

Il s'adresse à toutes les organisations, quel que soit leur secteur ou leur taille. Il est particulièrement apprécié dans les domaines critiques : santé, énergie, transport, finances…

LiveCampus

Apprentissage connecté

Structure du NIST CSF 2.0
Le framework repose sur trois piliers fondamentaux :

Fonctions clés (Core Functions)
Ce sont les **5 fonctions historiques** qui organisent tout le processus de cybersécurité :

LiveCampus

Apprentissage connecté

Fonction	Rôle
Identify	Comprendre l'environnement organisationnel, les actifs critiques, les risques.
Protect	Mettre en œuvre les protections (contrôles d'accès, formation, sécurité applicative…).
Detect	Surveiller et identifier rapidement les incidents.
Respond	Réagir de manière structurée aux incidents détectés.
Recover	Restaurer les capacités et services impactés.

LiveCampus

Apprentissage connecté

En version 2.0, une 6e fonction a été ajoutée :

Govern devient centrale : elle met l'accent sur la responsabilité de la direction et l'alignement stratégique.

LiveCampus

Apprentissage connecté

Catégories et sous-catégories

- Chaque fonction contient des **catégories** (par ex. : gestion des actifs, gestion des identités, formation, sécurité physique, sécurité des données…).
- Chaque catégorie est divisée en **sous-catégories** décrivant des objectifs spécifiques.
- En tout, le NIST CSF 2.0 contient **22 catégories** et **106 sous-catégories**.

LiveCampus

Apprentissage connecté

Tiers d'implémentation (Implementation Tiers)

Tier	Description
Tier 1 – Partial	Pratiques ad hoc, peu de coordination.
Tier 2 – Risk Informed	Compréhension des risques, mise en œuvre partielle.
Tier 3 – Repeatable	Processus définis, documentés et répétés.
Tier 4 – Adaptive	Adaptation continue, innovation en sécurité, retour d'expérience intégré.

LiveCampus

Apprentissage connecté

Les tiers ne sont pas des niveaux de certification, mais **des repères d'auto-évaluation**.

LiveCampus

Apprentissage connecté

Nouveautés de la version 2.0 (février 2024)

•**Ajout de la fonction "Govern"** pour mettre en avant la stratégie, la conformité, l'éthique numérique.

• **Réécriture inclusive et simplifiée du langage** pour faciliter la compréhension par les PME.

• Introduction de **profils sectoriels** pour adapter le framework aux besoins spécifiques (santé, énergie, supply chain…).

•Meilleure intégration avec d'autres normes (ISO 27001, COBIT, CIS Controls, etc.)

• Mise à jour des **ressources d'accompagnement** : guides pratiques, outils de mappage et autoévaluation.

LiveCampus

Apprentissage connecté

Référentiels OWASP

ASVS (Application Security Verification Standard)

ASVS est une **grille de vérification de la sécurité applicative**, élaborée par OWASP. Elle sert de **cadre de référence pour l'audit, le développement sécurisé** et l'élaboration de cahiers des charges techniques.

LiveCampus

Apprentissage connecté

L'ASVS est composé de **14 domaines** (V1 à V14), avec des dizaines de **critères de vérification** répartis sur **3 niveaux de rigueur**.

Code	Domaine	Description	Exemple de contrôle
V1	Architecture, Design & Threat Modeling	Validation des choix d'architecture, modélisation des menaces, séparation logique des composants.	Le système doit documenter les modèles de menaces et avoir une séparation claire des rôles.
V2	Authentication	Mécanismes d'authentification sécurisés : mots de passe, MFA, gestion des sessions d'authentification.	L'application doit intégrer une authentification à 2 facteurs (2FA) pour les comptes administrateurs.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V3	Session Management	Gestion sécurisée du cycle de vie des sessions (création, expiration, invalidation).	L'ID de session doit être réinitialisé après l'authentification.
V4	Access Control	Mise en œuvre des autorisations selon les rôles, logique côté serveur, et contrôle d'accès granulaire.	Les utilisateurs ne doivent pas pouvoir accéder à des fonctions administratives s'ils ne sont pas autorisés.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V5	Validation, Sanitization, Encoding	Traitement des entrées utilisateurs pour éviter injections, XSS, etc.	Toutes les entrées doivent être validées côté serveur selon des règles strictes.
V6	Stored Cryptography	Chiffrement des données sensibles stockées avec des algorithmes éprouvés.	Les mots de passe doivent être hashés avec un algorithme de type bcrypt ou Argon2.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V5	Validation, Sanitization, Encoding	Traitement des entrées utilisateurs pour éviter injections, XSS, etc.	Toutes les entrées doivent être validées côté serveur selon des règles strictes.
V6	Stored Cryptography	Chiffrement des données sensibles stockées avec des algorithmes éprouvés.	Les mots de passe doivent être hashés avec un algorithme de type bcrypt ou Argon2.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V7	Error Handling and Logging	Gestion des erreurs et journalisation sécurisée sans fuite d'informations.	Les logs ne doivent jamais contenir de mots de passe ou jetons d'accès.
V8	Data Protection	Confidentialité, intégrité et minimisation des données personnelles.	Les données sensibles doivent être masquées lors de l'affichage et transmises sur HTTPS.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V9	Communications	Sécurisation des communications réseau (TLS, HTTPS, sécurité des certificats).	Le protocole TLS 1.2 ou supérieur doit être utilisé pour toutes les communications.
V10	Malicious Code	Protection contre les injections de code malveillant ou bibliothèques compromises.	L'application doit scanner automatiquement les dépendances logicielles.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V11	Business Logic	Sécurisation de la logique métier : prévention des abus, contournements.	L'utilisateur ne peut pas valider un paiement sans avoir passé l'étape de facturation.
V12	File and Resources	Contrôle sur la gestion des fichiers et ressources (uploads, accès, permissions).	Les fichiers uploadés doivent être vérifiés, limités en type et taille.

LiveCampus

Apprentissage connecté

Code	Domaine	Description	Exemple de contrôle
V13	API and Web Services	Sécurisation des interfaces API (REST, SOAP, GraphQL), authentification, validation, throttling.	Les appels API doivent nécessiter un jeton d'authentification et un contrôle d'origine.
V14	Configuration	Contrôle de la configuration sécurisée (frameworks, environnements, modules).	Les erreurs détaillées ne doivent pas s'afficher en production.

LiveCampus

Apprentissage connecté

Ces 14 domaines sont ensuite évalués à **trois niveaux de rigueur** :

- **Niveau 1 (Basic)** : exigences minimales pour les applications à faible risque.
- **Niveau 2 (Standard)** : recommandé pour la majorité des applications professionnelles.
- **Niveau 3 (Advanced)** : pour les systèmes critiques (finance, santé, défense…).

LiveCampus

Apprentissage connecté

- Comprendre et visualiser la relation entre les grands référentiels de cybersécurité (ISO 27001, NIST CSF, OWASP…).
- Favoriser la mémorisation active à travers une approche visuelle et collaborative.
- Développer l'esprit de synthèse et la capacité à faire des liens entre normes, frameworks, et bonnes pratiques.

LiveCampus

Apprentissage connecté

Rôles et responsabilités

Responsable de la Sécurité des Systèmes d'Information (RSSI)

- Définit la stratégie de sécurité.
- Pilote les audits, les plans de remédiation et les exercices de gestion de crise.
- Interagit avec la direction générale pour aligner sécurité et stratégie métier.
- Met en place un **SMSI** selon ISO 27001

LiveCampus

Apprentissage connecté

Outils au choix (selon configuration de la salle) :

- **Numérique** : XMind, Freeplane, Miro, Klaxoon (version gratuite en ligne).
- **Papier / Post-it** : Paperboard + feutres + fiches couleurs.

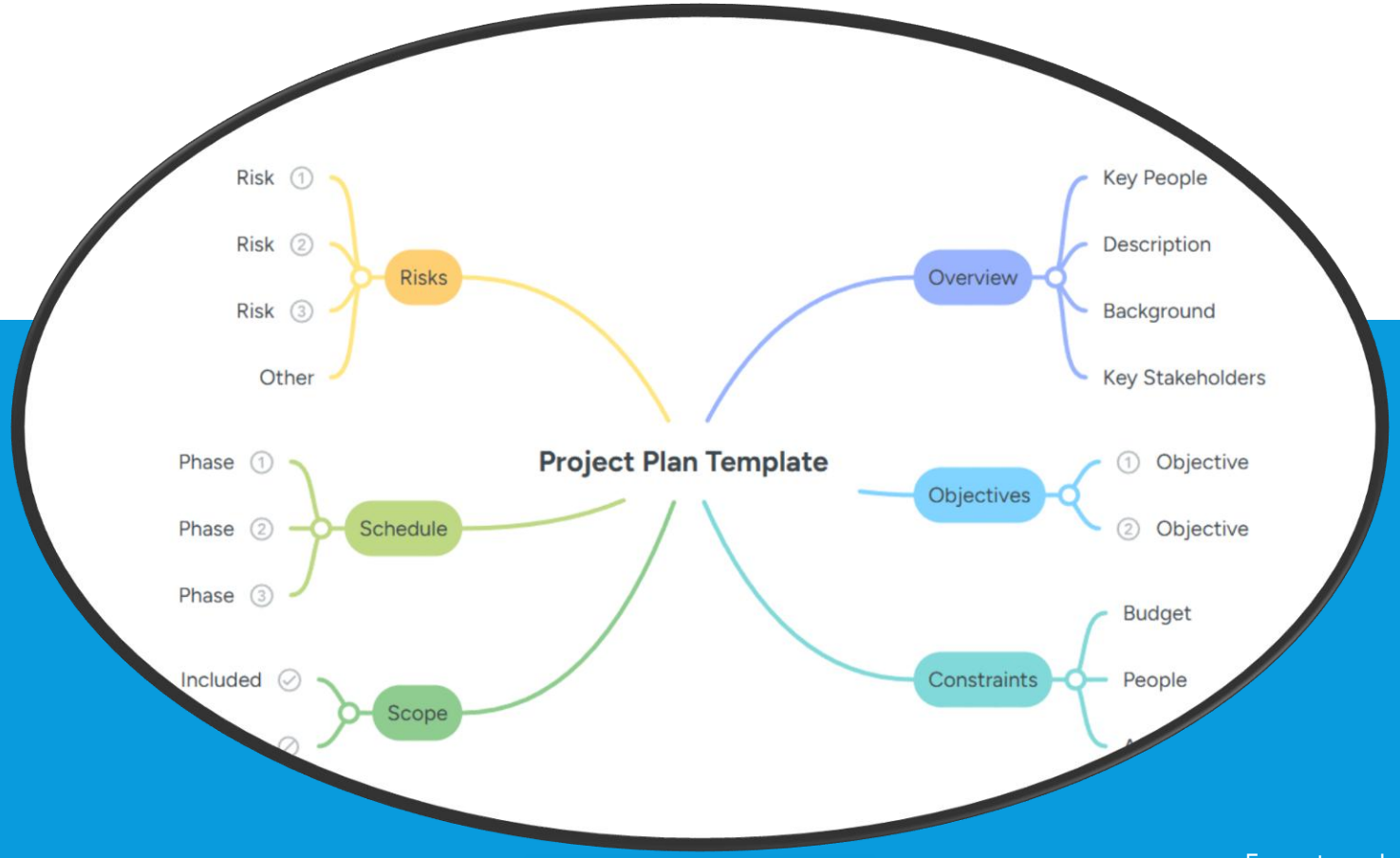
LiveCampus

Apprentissage connecté

Référentiel	Type	Objectif principal	Périmètre
ISO 27001	Norme internationale	Mettre en place un SMSI (Système de management de la sécurité de l'information)	Organisationnel
NIST CSF 2.0	Cadre américain	Réduire les risques cybersécurité avec 6 fonctions	Opérationnel
OWASP Top 10	Liste de risques	Identifier les principales failles applicatives	Technique
OWASP ASVS	Grille de vérification	Valider les niveaux de sécurité dans le développement	Technique

LiveCampus

Apprentissage connecté



LiveCampus

Apprentissage connecté

Glossaire

A

- **ASVS** : *Application Security Verification Standard* – Norme OWASP pour vérifier la sécurité des applications à plusieurs niveaux.
- **Asset** : Ressource ayant de la valeur pour une organisation (ex. : données, équipements, logiciels).
- **Availability (Disponibilité)** : Principe de la **triade CIA** ; garantit que l'information est accessible quand elle est nécessaire.

LiveCampus

Apprentissage connecté

B

•**Broken Access Control** : Type de vulnérabilité OWASP où les contrôles d'accès sont mal implémentés.

LiveCampus

Apprentissage connecté

C

- **CIA** : Acronyme pour **Confidentialité, Intégrité, Disponibilité** – les trois piliers de la sécurité de l'information.
- **Confidentiality (Confidentialité)** : Limitation de l'accès à l'information aux seules personnes autorisées.
- **Cryptographic Failures** : Défauts dans l'utilisation ou l'implémentation de mécanismes cryptographiques (anciennement "Sensitive Data Exposure").
- **Cheat Sheet** : Fiche pratique OWASP pour appliquer rapidement des bonnes pratiques de sécurité.

LiveCampus

Apprentissage connecté

D

- **Defense in Depth** : Stratégie de sécurité consistant à déployer plusieurs couches de défenses (pare-feu, authentification, chiffrement…).
- **Detect (NIST)** : Fonction visant à identifier les événements de cybersécurité (logs, alertes, surveillance…).

LiveCampus

Apprentissage connecté

G

•**Govern (NIST v2.0)** : Nouvelle fonction du NIST CSF 2.0 dédiée à la gouvernance de la cybersécurité.

LiveCampus

Apprentissage connecté

I

- **Identify (NIST)** : Fonction qui vise à comprendre le contexte, les ressources et les risques (inventaires, cartographie, classification...).
- **Implementation Tier** : Niveau de maturité du NIST CSF (de Tier 1 = partiel à Tier 4 = adaptatif).
- **Integrity (Intégrité)** : Assurance que les données n'ont pas été altérées ou modifiées sans autorisation.
- **Injection** : Type d'attaque OWASP (ex : SQL Injection) où du code malveillant est inséré dans une requête.
- **ISO/IEC 27001** : Norme internationale de gestion de la sécurité de l'information.

LiveCampus

Apprentissage connecté

L

•**Least Privilege (Principe du Moindre Privilège)** : Accorder aux utilisateurs les droits strictement nécessaires.

M

•**Monitoring** : Suivi et enregistrement des événements pour détecter les incidents.
•**MITRE ATT&CK** : Base de connaissances sur les tactiques et techniques utilisées par des cyberattaquants.

LiveCampus

Apprentissage connecté

N

- **NIST** : *National Institute of Standards and Technology* – organisme américain éditeur du Cybersecurity Framework.
- **NIST CSF** : Cadre de cybersécurité structuré autour de fonctions, catégories et sous-catégories.

LiveCampus

Apprentissage connecté

P

•**Protect (NIST)** : Fonction axée sur les mesures de prévention (contrôles d'accès, sensibilisation, sécurité des données…).

•**Privacy by Design** : Intégration de la protection de la vie privée dès la conception d'un système.

LiveCampus

Apprentissage connecté

R

- **Recover (NIST)** : Fonction qui vise à restaurer les services suite à un incident.
- **Respond (NIST)** : Fonction de réponse aux incidents pour limiter les impacts.
- **Risk** : Possibilité qu'une menace exploite une vulnérabilité et cause un dommage.

LiveCampus

Apprentissage connecté

S

- **SAMM** : *Software Assurance Maturity Model* – modèle de maturité OWASP en 5 domaines.
- **Security Misconfiguration** : Failles dues à des erreurs de configuration (ex. : ports ouverts, erreurs par défaut…).
- **Security Logging** : Journalisation des événements de sécurité.
- **SSRF** : *Server-Side Request Forgery* – attaque OWASP où le serveur est forcé de faire des requêtes internes.

LiveCampus

Apprentissage connecté

T

- **Threat** : Menace – événement ou entité susceptible de porter atteinte à la sécurité d'un actif.
- **Top 10 (OWASP)** : Liste des 10 vulnérabilités applicatives les plus critiques.
- **Tier (NIST)** : Niveau de maturité d'une organisation selon le NIST CSF (Tier 1 à 4).

LiveCampus

Apprentissage connecté

Cas pratique