9ème édition
de la

JOURNÉE FRANCAISE DE L'INGÉNIERIE DES EXIGENCES

3 Jours

6 Webconférences

Inscription gratuite

Du 15 au 17 Novembre 2022

De 11h30 à 14h30

IREB International Requirements Engineering Board

GASQ

CYBERSÉCURITÉ - L'IMPORTANCE DE BIEN CHOISIR LE BON RÉFÉRENTIEL D'EXIGENCES DE SÉCURITÉ

BERTRAND HELFRE

onepoint.
beyond the obvious

Polarsoft
The ALM Expert

ARCAD SOFTWARE

AGENDA

1) ONEPOINT

2) SECURITY & PRIVACY BY DESIGN

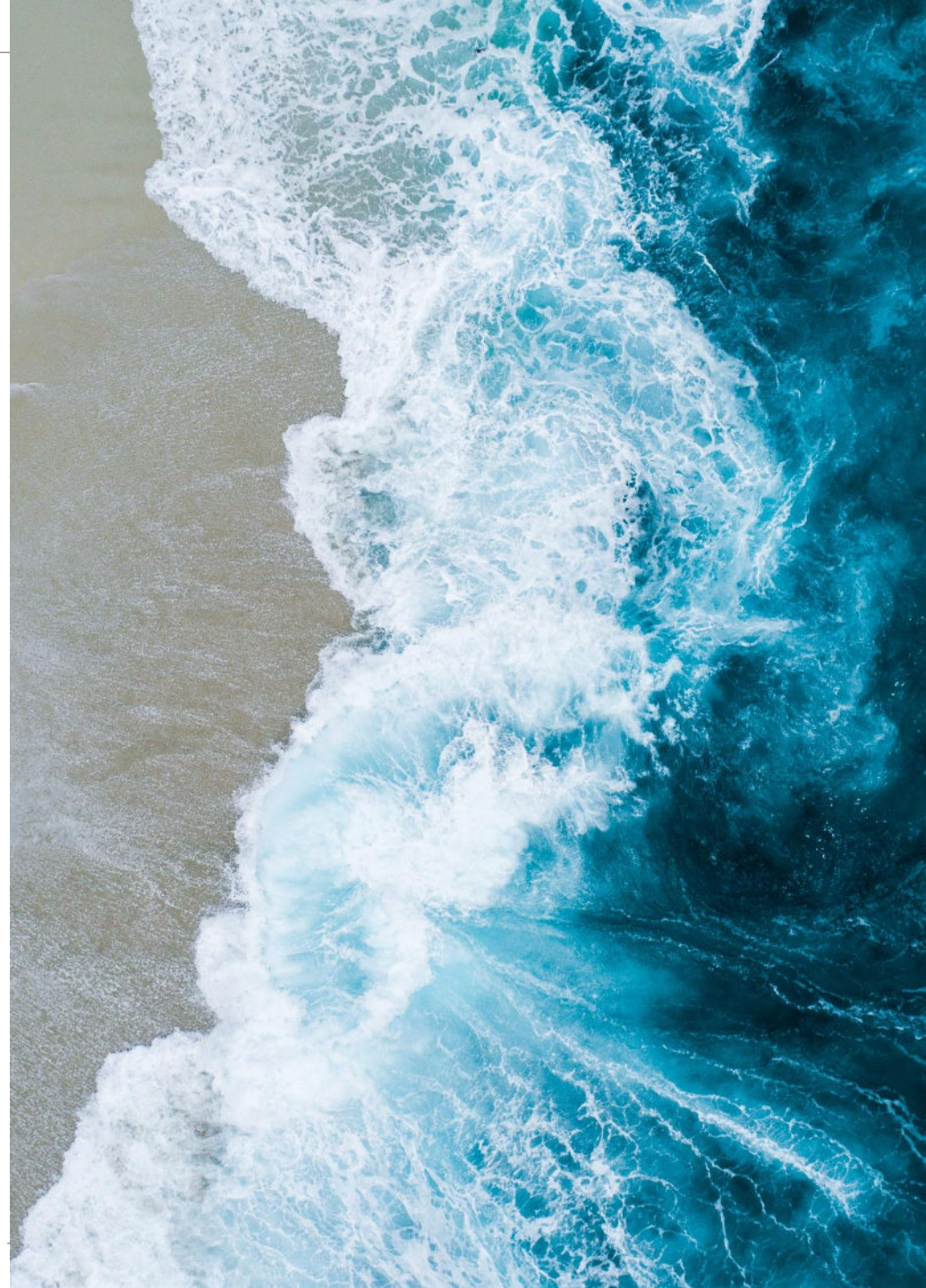
3) LES RÉFÉRENTIELS D'EXIGENCES DE SÉCURITÉ

4) LE(S)QUEL(S) CHOISIR ?

5) POUR CONCLURE

1

ONEPOINT



onepoint.
beyond the obvious

La transformation, de la vision stratégique à sa mise en œuvre opérationnelle

Né en 2002 à Paris, onepoint est un cabinet mondial pilote de conseil en gestion et en technologie qui a réinventé le modèle du conseil.

PLUS D'EXPERTISE, MOINS DE GESTION
PLUS DE COLLABORATION, MOINS DE HIÉRARCHIE
PLUS D'AUTONOMIE, MOINS DE CONTRÔLE

NOUS EMBAUCHONS DES TALENTS QUI CROIENT EN L'ARTISANAT
NOUS DÉVELOPPONS LES TALENTS PAR L'APPRENTISSAGE CONTINU

3000 employés

19 implantations dans le monde

400 million euros chiffre d'affaire

10 communautés d'expertise

Montréal, New-York, Paris, Bordeaux, Toulouse, Nantes, Rennes, Lyon, Aix en Provence, Amsterdam, Bruxelles, Zele, Luxembourg, Tel Aviv, Tunis, Melbourne, Singapour, Sydney

onepoint.
beyond the obvious

NOTRE IDENTITÉ

Onepoint a pour vocation d'architecturer de nouveaux modèles avec ses clients.
Nous co-construisons des solutions favorisant les opérations intelligentes, l'innovation, la résilience et la croissance verte.
En tirant parti de l'utilisation des technologies numériques et des données, tout en gardant à l'esprit les interactions humaines.

CO-CONSTRUCTION

De la vision stratégique à sa mise en œuvre opérationnelle. En utilisant une approche d'intelligence collective, nous **co-architecturons** et co-réalisons la **transformation** avec les employés de nos clients au sein de leur écosystème, en façonnant un super-collectif axé sur la valeur.

COMMUNAUTÉS D'EXPERTISE

Croisant les regards d'experts de tous les domaines (**développeurs**, **architectes d'entreprise**, spécialistes **cyber**, de l'**IA et la donnée**, **designers**, **stratèges business**, **philosophes** et **sociologues**), onepoint définit et met en œuvre les outils numériques pertinents pour répondre aux enjeux transversaux et développer l'innovation et la compétitivité de ses clients.

ECOSYSTÈME INNOVANT

Elle développe un écosystème et un **modèle entrepreneurial innovants** dans une **organisation décloisonnée** qui lui permettent de révéler les talents, libérer la créativité et bénéficier de circuits de décision courts. **Entreprise pilote**, onepoint invente de nouveaux modèles, les expérimente sur elle-même et les déploie pour ses clients. (ex. Smart Building, RESET Scorecard, ...)

UNE VISION DU FUTUR

Nos convictions et savoir-faire sur les sujets en transformation.

- **Plateformisation des services**
- **Expérience employés**
- **Fabriques digitales**
- **Villes et bâtiments intelligents**

5 valeurs animent notre action : Authenticité. Ouverture. Élégance. Engagement. Courage.

L'EXPERTISE EN CYBERSECURITE CHEZ ONEPOINT

Mission

"INSCRIRE DANS L'ADN DE NOS CLIENTS LE « SECURITY/PRIVACY » BY DESIGN
DANS UNE DÉMARCHE PÉRENNE, ÉTHIQUE, RESPONSABLE

+200 Projets réalisés, références développées dans tous les secteurs

+30 Partenariats & labels (institutionnels et technologiques)

+100 Experts en Cybersécurité

ISO 27001 onepoint détient la certification ISO 27001

Stratégie et gouvernance de la cybersécurité

- Diagnostic 360° et stratégie de sécurité
- Gestion des cyber-risques
- Pilotage de programme de sécurité
- Résilience et gestion de crise
- Formation et communication face aux risques cyber

Protection des données Personnelles

- Accompagnement DPO
- Audit de maturité et conformité
- Mise en œuvre opérationnelle de la conformité
- Privacy & security by design
- Sensibilisation et formation

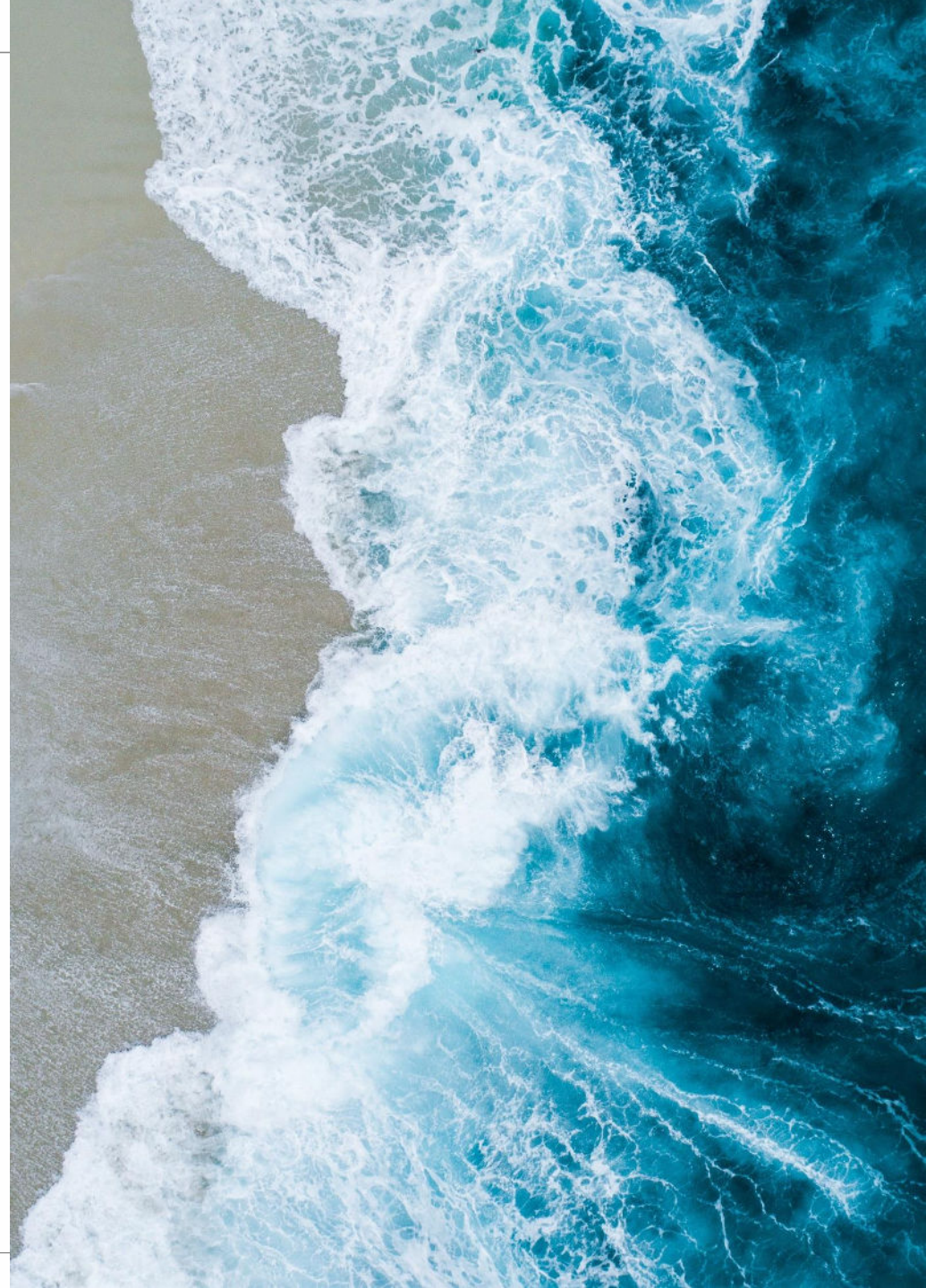
Cybersécurité & Technologies

- Identité Numérique
- Sécurité du Cloud
- Sécurité de l'Environnement de Travail
- Sécurité Applicative
- Opérations de Cybersécurité
- Audit et test de sécurité

5 valeurs animent notre action : Authenticité. Ouverture. Élégance. Engagement. Courage.

2

SECURITY & PRIVACY BY DESIGN



source Linkedin, Jeremy Renard, Comment transposer l'ISP (Intégration de la Sécurité dans les Projets) dans un contexte AGILE ?

En prenant en compte les exigences de sécurité, de protection des données, et <u>les référentiels associés</u> dès le début, puis à chaque étape du projet.

REFERENTIELS DE SÉCURITÉ… IL EN EXISTE UNE MULTITUDE

Citons quelques exemples …

Dans l'industrie automobile, la certification **ISO 21434** contribue à la satisfaction des exigences en vue d'obtenir l'homologation des véhicules.

La certification **ISO 27001** n'est pas une obligation.

Toutefois, par exigence du marché ou avantage concurrentiel, elle peut être requise.

La Réglementation Générale sur la Protection des Données

RGPD

La certification **HDS** est obligatoire pour les hébergeurs de données de santé à caractère personnel.

Les guides de l'**ANSSI**, du **NIST**, de l'**ENISA** proposent des démarches et bonnes pratiques qu'il faut connaitre et exploiter en fonction des besoins.

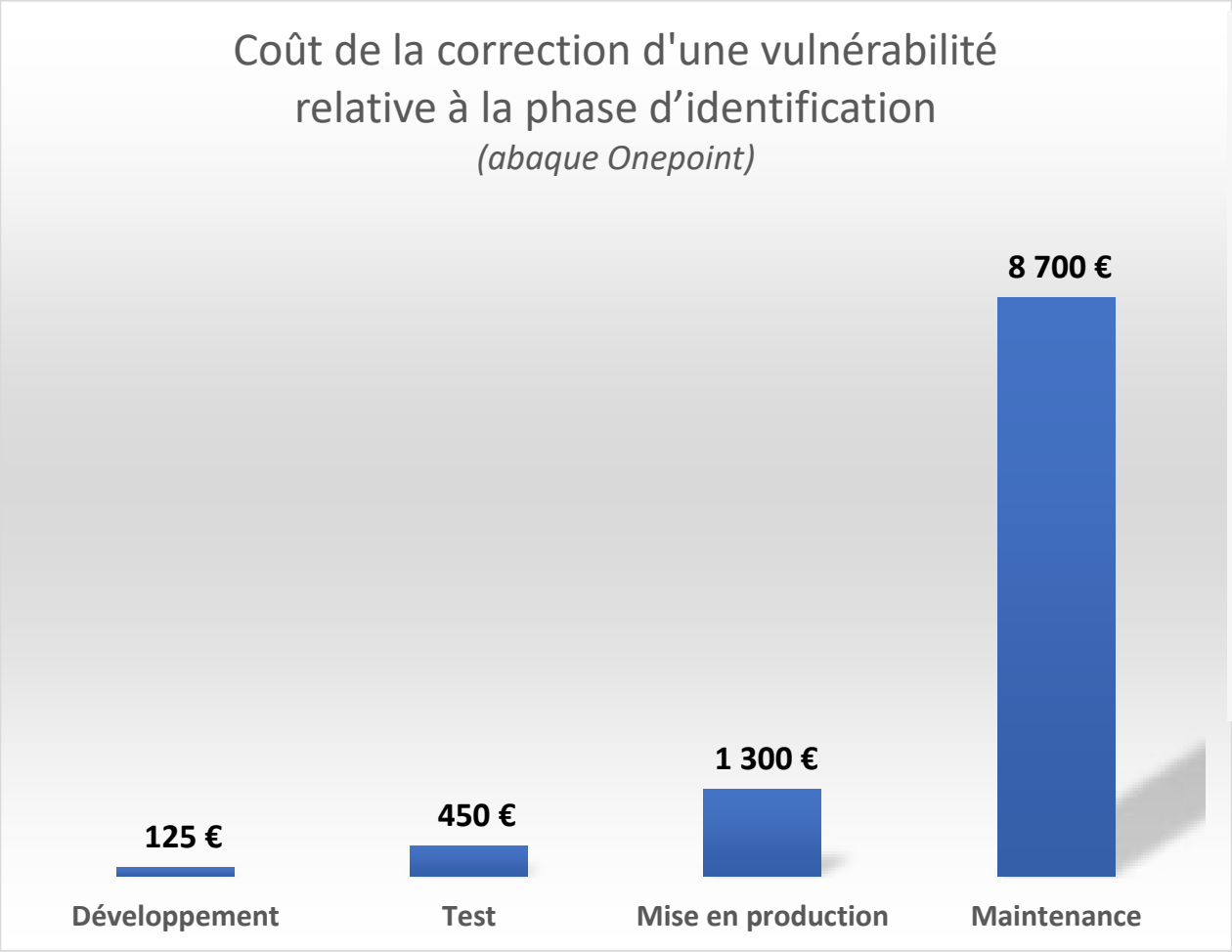
La norme **PCI DSS**, n'est pas obligatoire au regard de la loi aux Etats-Unis.

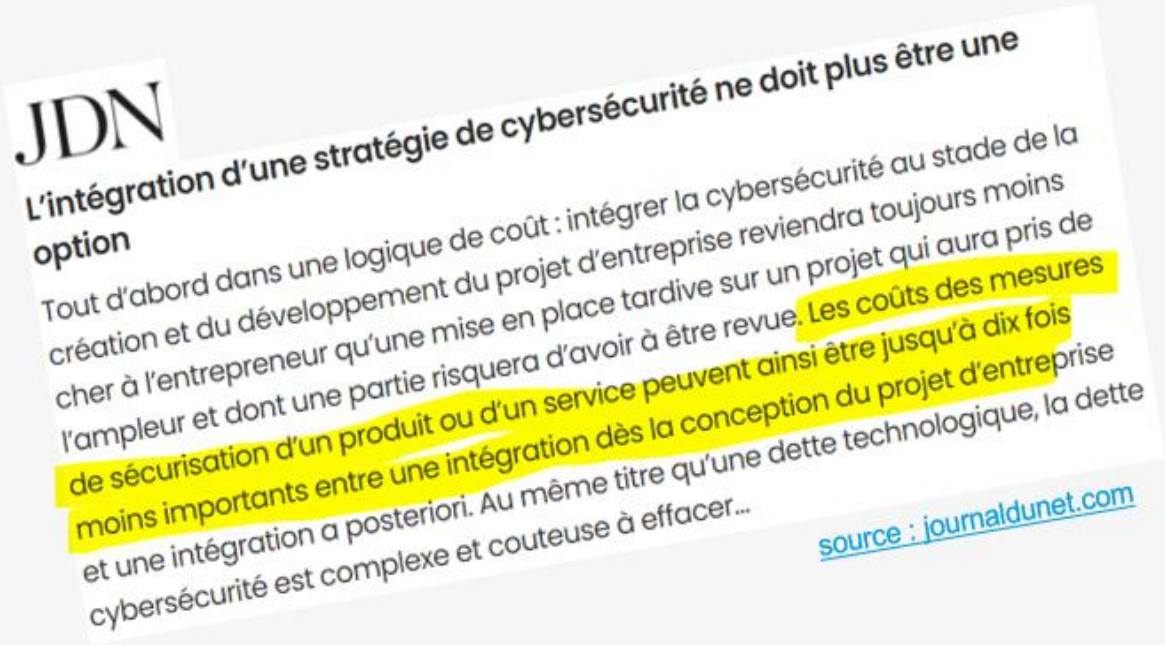
Elle est toutefois vivement recommandée, voire incontournable.

obligatoire

SECURITY BY DESIGN: UN R.O.I. TRÈS FAVORABLE

Des coûts de sécurisation beaucoup plus faibles s'ils sont intégrés au plus tôt





JDN

L'intégration d'une stratégie de cybersécurité ne doit plus être une option

Tout d'abord dans une logique de coût : intégrer la cybersécurité au stade de la création et du développement du projet d'entreprise reviendra toujours moins cher à l'entrepreneur qu'une mise en place tardive sur un projet qui aura pris de l'ampleur et dont une partie risquera d'avoir à être revue. Les coûts des mesures de sécurisation d'un produit ou d'un service peuvent ainsi être jusqu'à dix fois moins importants entre une intégration dès la conception du projet d'entreprise et une intégration a posteriori. Au même titre qu'une dette technologique, la dette cybersécurité est complexe et couteuse à effacer...

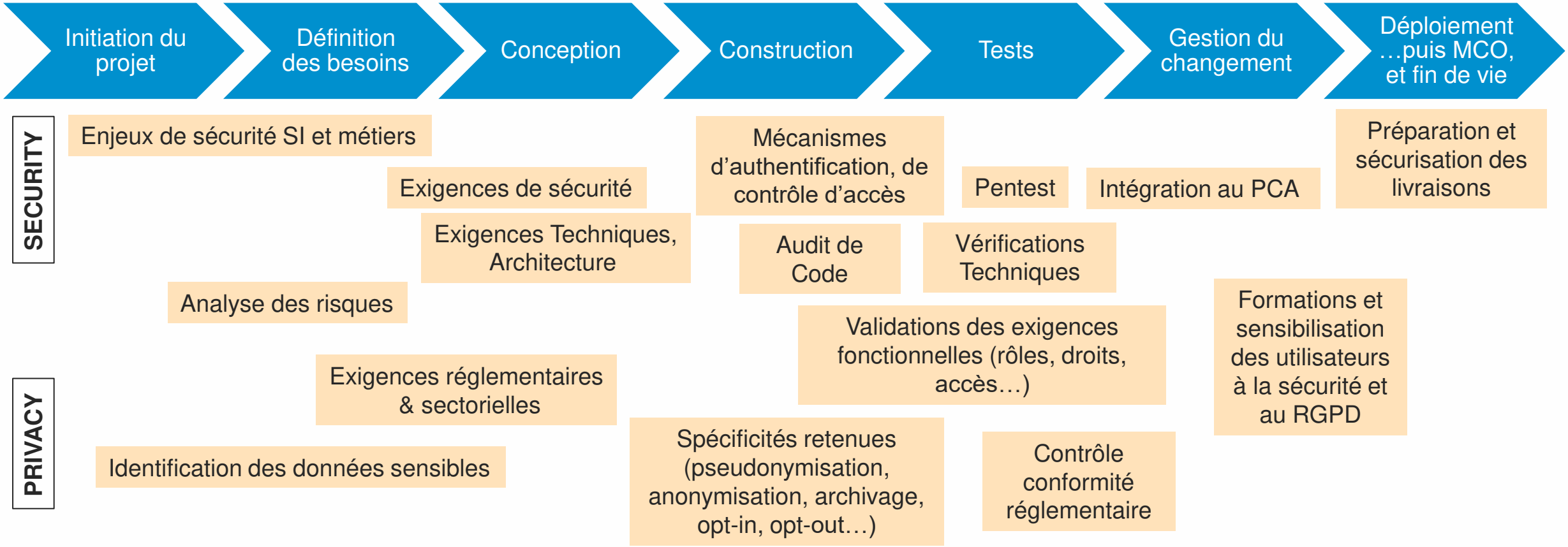
source : journaldunet.com

- **Tout le monde**

Chacun - tech ou pas - doit contribuer à l'implémentation de la sécurité dans le projet.

SECURITY & PRIVACY BY DESIGN - ETAT DE L'ART

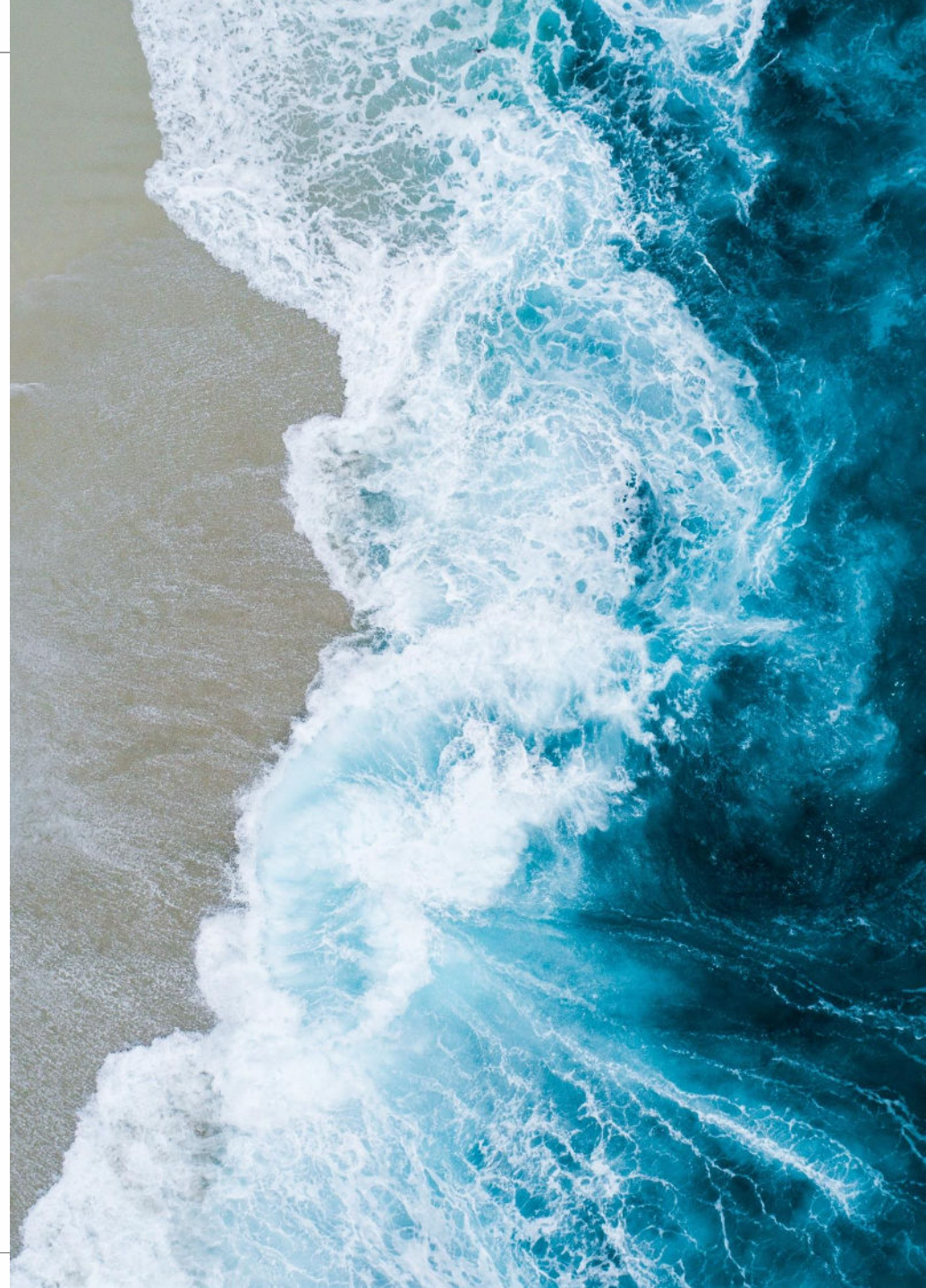
Prendre en compte les exigences de sécurité, et de protection des données tout au long du cycle de vie d'un projet ou d'une application



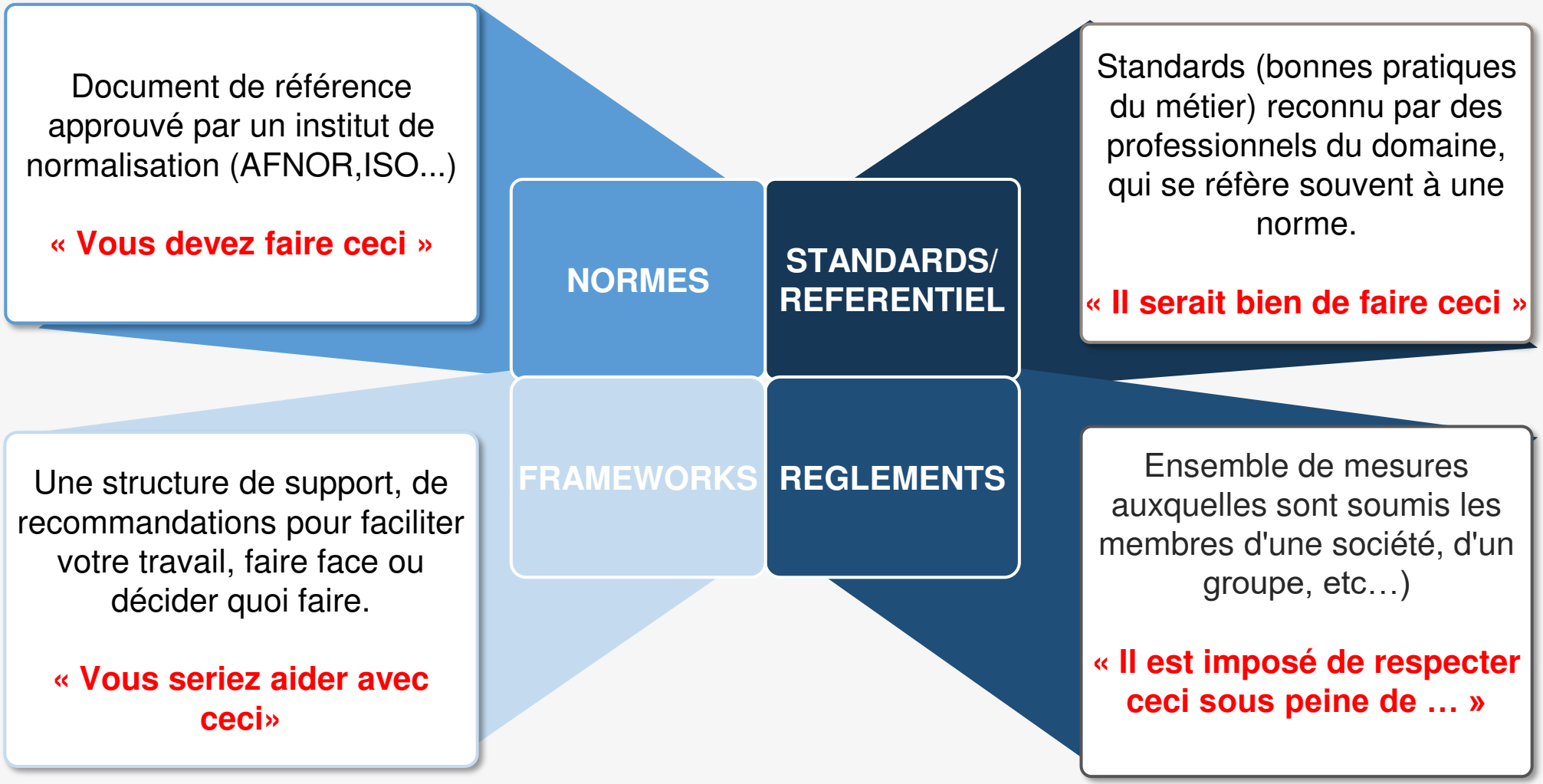
Pour nous accompagner, de nombreux des référentiels, normes, guides et règlements existent…

3

LES REFERENTIELS D'EXIGENCES DE SECURITE



STANDARDS, RÉFÉRENTIELS, NORMES, RÈGLEMENTS, OU CADRE DE TRAVAIL ?



LES RÉFÉRENTIELS D'EXIGENCES DE SÉCURITÉ & DE DONNEES

Des référentiels existent pour définir les exigences relatives à la sécurité & aux données. Il est également essentiel de tenir compte des référentiels internes (chartes, politiques, directives).

SECURITY

- **ISO 2700x**: Normes de sécurité de l'information
- **EBIOS-RM** & **MEHARI**: Gestion des risques basés sur la norme ISO 27005
- **ISO 20000**: TI – Gestion des services
- **OWASP**: Référentiel pour le développement d'application WEB
- **ISO 27034:** Validation de la sécurité des applications
- **ANSSI:** Nombreux guides et recommandations sur les mesures de sécurité techniques et organisationnelles
- **NIST:** Référentiel cybersécurité américain

PRIVACY

- **ISO 27018:** Protection des données personnelles identifiables (PII) dans le cloud
- **PCI DSS :** Cartes de paiement
- **ENISA :** Agence de l'union européenne pour la cybersécurité (guides, mesures de sécurité)
- **CNIL**: Guides sur le Règlement Général sur la Protection des Données (**RGPD**), bonnes pratiques et outils (exemple : AIPD)
- **HDS :** Hébergement Données de Santé
- **ISO 27701:** mesures de sécurité des données personnelles et droits associés

INDUSTRY & BUSINESS

- **AIEA et IEC 62859 :** Domaine Nucléaire
- **IEC 62443 :** Exigences de sécurité relatives aux systèmes d'automatisation et de commandes Industrielles
- **EBA:** Guideline Autorité Bancaire Européenne
- **ANSSI:** Guides métiers (ex: Cybersécurité des systèmes industriels)
- **ISO 21434** / **UNR 155:** Véhicules routiers - Cybersécurité
- **Cloud Security Alliance** CCM (Cloud Control Matrix) contrôle cybersécurité Cloud
- **DORA:** Résilience opérationnelle en finance

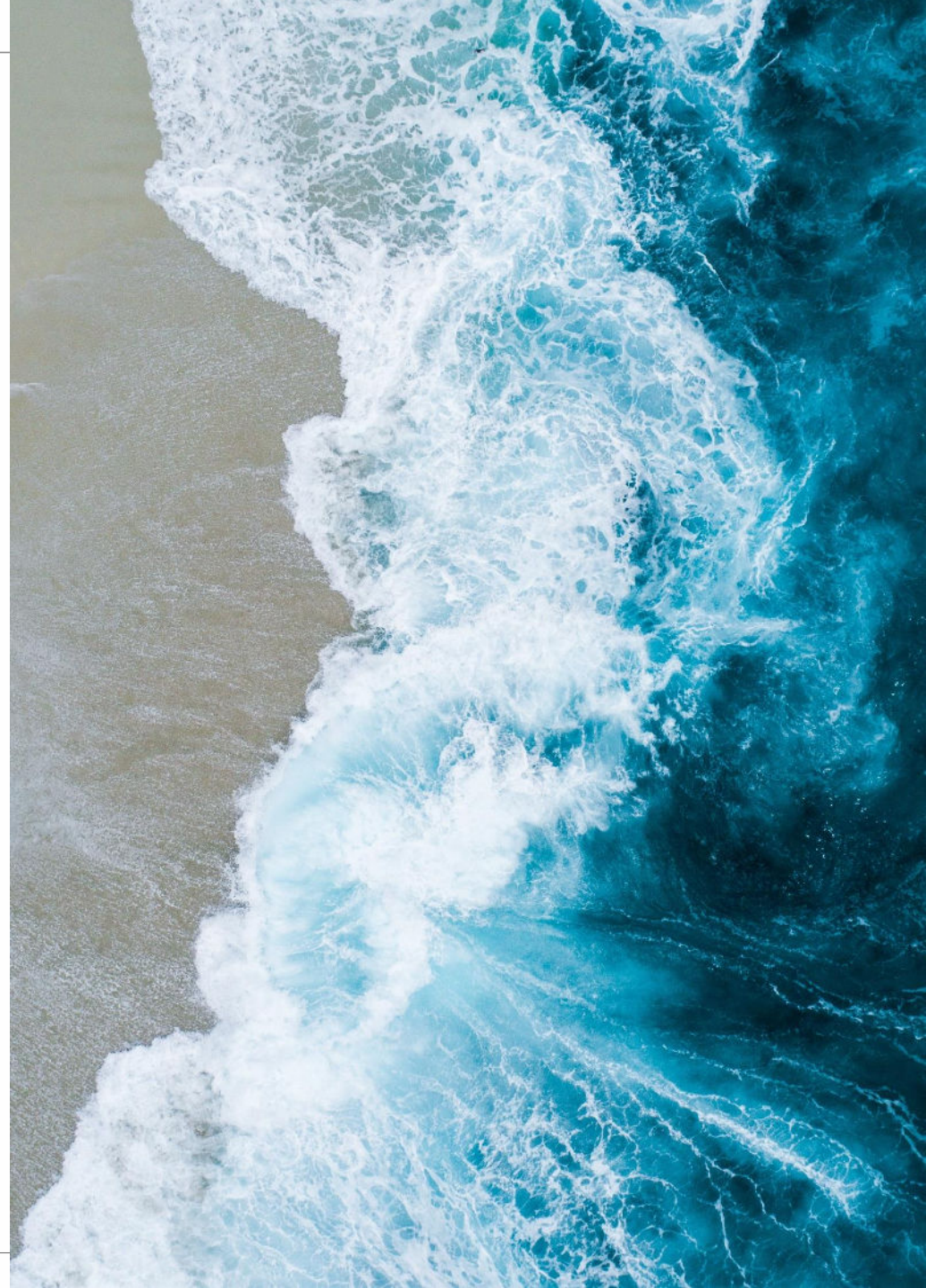
⚠ **Liste non exhaustive**

Normes | Standards / Référentiels | Framework | Règlements

.../...

4

LE(S)QUEL(S) CHOISIR ?



UN CHOIX POSSIBLE PAR L'APPROCHE

	Approche par conformité	Approche par la maîtrise des risques
Enjeux & contexte	• Volonté ou maintien de labélisation Certification requise • Normes métiers exigées	• Maîtrise des risques • Identification des actifs & savoir-faire à protéger référentiels
Avantages / Opportunités	• Avantage concurrentiel • Gage de confiance	• Exhaustivité et priorisation des risques à traiter • Coûts / délais adaptés
Inconvénients	• Coûts / délais / Orga.	• Pas de labélisation

NON EXCLUSIF

En marge des ces deux approches, le choix de référentiels va également dépendre de l'expertise et du savoir-faire du ou des intervenants, des habitudes du client, de la zone géographique…

UN RETOUR D'EXPERIENCE ONEPOINT ? PRENONS UN EXEMPLE

Contexte

- **scale-up de la fintech** en hyper-croissance,
- sur le **marché français** et à l'international,
- envisage de **conquérir le marché nord-américain**.
- enjeux de **sécurisation de son SI, et de la protection des données** personnelles.

Mission

Sollicitation de Onepoint afin d'évaluer :

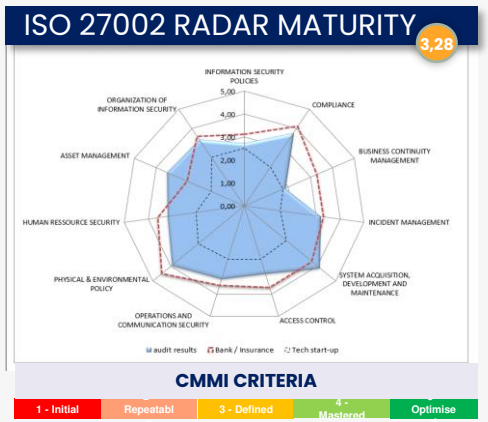
- L'état de la **sécurité de son SI**,
- De la **maturité** de son SI,
- Et de sa conformité avec la norme **ISO 27002**.

Référentiels exploités

ISO/CEI 27002

Bonnes pratiques pour le management de la sécurité d'information (SMSI)

CMMI



Opportunités

ISO/CEI 27001

Système de management de la sécurité d'information (SMSI)

AICPA SOC 2 Formerly SAS 70 Reports

Restitutions

PROJECT PRIORITIZATION LEVEL 2: 1 YEAR TO 3 YEARS

ISO THEME	DESCRIPTION
ISO 27001 Certification	Target an ISO 27001 certification to enforce customer confidence and illustrate definitely the good maturity of the company

Choix du référentiel, mise en pratique par scenario

PERSONA 1 – Mathilde - Chef de projet Marketing WEB

Mathilde travaille pour une entreprise de distribution électronique. Sa direction lui a confié la responsabilité du projet de refonte du site web e-commerce qui est hébergé en dehors de l'UE mais qui vend à l'international. Elle est accompagnée par un consultant en cybersécurité pour aborder la démarche et identifier les référentiels utiles. Une PSSI existe.

PERSONA 2 – Rémy – Chef de produit d'un logiciel automobile embarqué

Rémy est en charge du développement d'un nouveau logiciel embarqué pour automobile. Le logiciel sera réalisé en langage C. Une partie des données sera traitée et stockées sur le Cloud. Aucune donnée personnelle ne sera stockée. Des référentiels internes (politique, gestion des processus et assurance qualité) existent.

PERSONA 3 – Nicolas – Consultant / Auditeur Sécurité

Pour le compte d'une collectivité territoriale, Nicolas est chargé de faire un audit de sécurité afin de vérifier la conformité sécuritaire et réglementaire de l'architecture et des applications en place. Une attention particulière doit être accordée à la confidentialité et à la disponibilité du SI. Des données de santé peuvent être stockées pour les besoins d'assistance, de livraisons de repas et d'accompagnement sanitaire.

ADAPTER LE CHOIX DES RÉFÉRENTIELS SELON LE CONTEXTE

Initiation du projet	Définition des besoins	Conception	Construction	Tests	Gestion du changement	Déploiement …puis MCO, et fin de vie

Mathilde

Refonte d'un site web

ISO 27001 / 27002: Exigences de mise en œuvre d'un SMSI et bonnes pratiques

Formations et sensibilisations avec supports **CNIL** et **ANSSI**

EBIOS-Risk Manager: Analyse et traitement des risques

Prise en compte de la **PSSI**

PCI DSS

OWASP: Réf. pour le dév. d'appli. WEB

Mise à jour de la **PSSI**

CNIL: pour la conformité au **RGPD** et l'Analyse d'Impact (AIPD)

Rémy

Logiciel auto. embarqué

ISO 21434: Véhicules routiers - Cybersécurité

ANSSI: Règles de développement sécurisé de logiciels en langage C.

Prise en compte des **Référentiels Internes**

MEHARI: Analyse et traitements des risques

Cloud Security Alliance CCM (Cloud Control Matrix) contrôle cybersécurité Cloud

Mise à jour des **Référentiels Internes**

ANSSI: Guides Cybersécurité des systèmes industriels

Nicolas

Audit Sécurité Collectivité

ISO 27001 / 27002: Exigences de mise en œuvre d'un SMSI et bonnes pratiques

ISO 22301:2019 Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences

ANSSI : Sécurité Numérique des collectivité Territoriales : L'essentiel de la règlementation

EBIOS-RM: Analyse et traitement des risques

HDS : Hébergement Données de Santé

CNIL: pour la conformité au **RGPD** et l'Analyse d'Impact (AIPD)

COMMENT GÉRER CES RÉFÉRENTIELS (EVOLUTIONS, VEILLE, ACTUALITÉS…) ?

Gérer la veille, les évolutions

onepoint. beyond the obvious

- Référentiels internes actualisés
- Sensibilisation et partage entre consultants via workplace (réseau interne)
- Cellule de veille et réseau interne qui réalise une synthèse sur la base de sources hebdomadaires:
  - https://veillecyberland.wordpress.com/
  - Revue de presse de l'ANSSI
  - Et autres actualités …

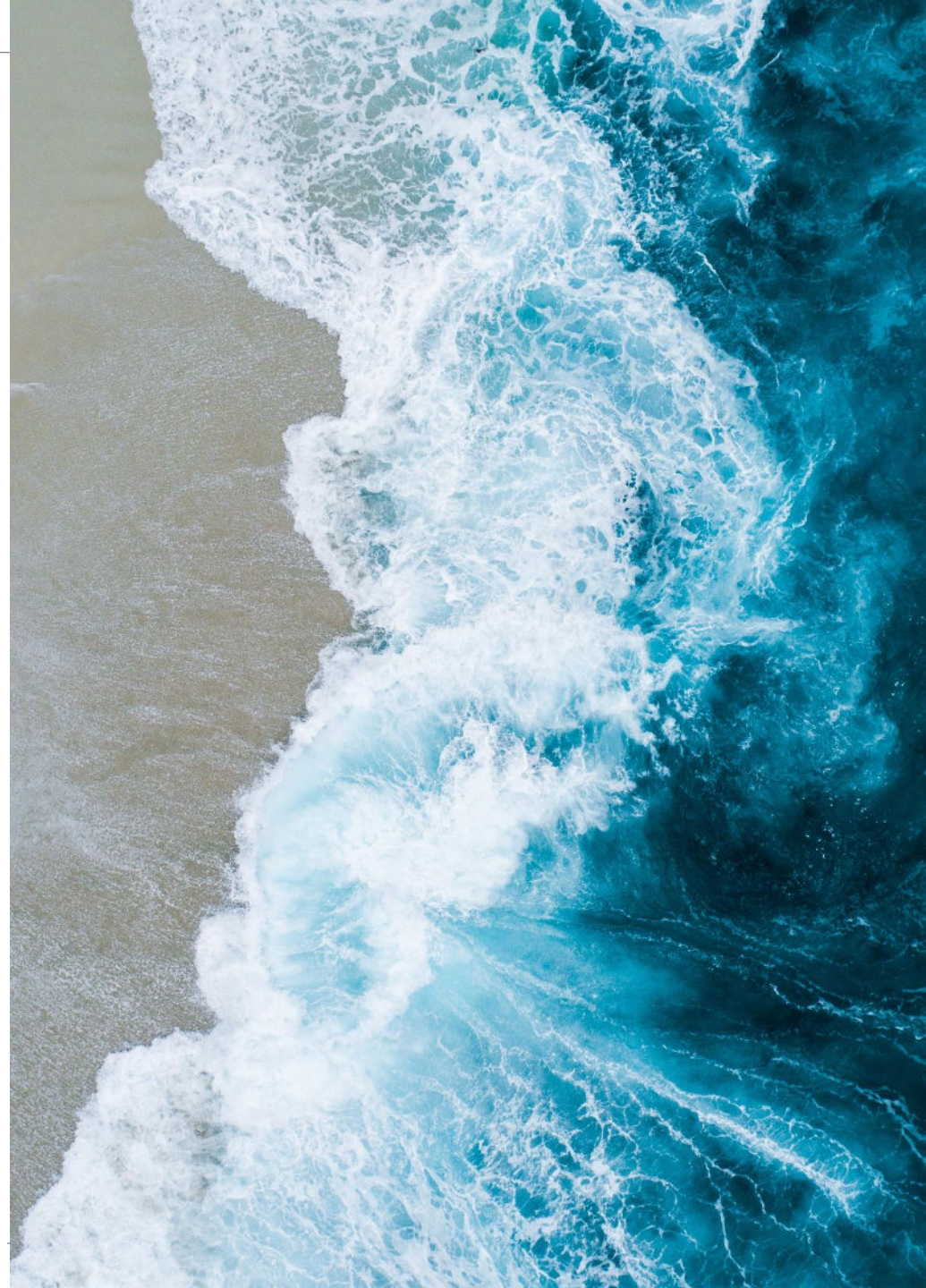
COMMENT GERER CES EXIGENCES ? OUTILS ? TRAÇABILITÉS ?

Des outils ?

- Espaces documentaires internes issues des expériences et missions précédentes onepoint. beyond the obvious
- Solutions exploitées par les clients pour documenter et gérer les exigences (ReqSuite, Visure Req., suite Atlassian, Xebrio…)
- Il existe aussi des logiciels de Gouvernance, Risque et Conformité qui permettent de gérer les politiques et référentiels associés.

5

POUR CONCLURE



POUR CONCLURE

Une multitude de référentiels et de réglementations…

pour encadrer les domaines de la sécurité de l'information et de la protection des données.

Certains sont incontournables, voire obligatoires…

par besoin d'homologation ou de certification. Il est indispensable de tenir compte des référentiels internes existants (chartes, politiques, directives).

A considérer comme des « référentiels d'objectifs », des bases de travail

A exploiter en fonction des objectifs visés, avec l'expertise et la connaissance des différents interlocuteurs (responsables projets, experts métiers et SI, experts en cybersécurité et en protection des données)

Un choix dépendant du contexte sectoriel et des besoins

Il est donc essentiel que les organisations puissent définir leurs besoins en termes de sécurité au plus tôt afin de déterminer les référentiels utiles.
Pensez à intégrer le « Security & Privacy By Design » dés le début du projet.

9ème édition
de la

JOURNÉE FRANCAISE DE L'INGÉNIERIE DES EXIGENCES

3 Jours

6 Webconférences

Inscription gratuite

Du 15 au 17 Novembre 2022
De 11h30 à 14h30

Le rendez-vous incontournable des experts du domaine

CFTL
Comité Français des Tests Logiciels

Merci de votre écoute !

Bertrand Helfre
Partner Cyber
Stratégie et Gouvernance

b.helfre@groupeonepoint.com
+33 (6) 11 43 01 54

onepoint.
beyond the obvious

IREB International® Requirements Engineering Board

GASQ

Polarsoft
The ALM Expert

ARCAD SOFTWARE