Meeting Chapitre OWASP-Cotonou

Les normes et standards d'audit de la fonction informatique au sein d'une organisation: Valeurs pratiques.

Dr. Ing Emery Kouassi Assogba

APDP, Octobre 2023

Plan

- Normes, standards et réglementations
- Les décisions stratégiques d’une entreprise
- Quelques normes et standard en sécurité des SI
- Réglementation au Bénin

Différence entre norme et standard

- Dans l'industrie, l'économie ou les services, une norme est un ensemble de règles de conformité ou de fonctionnement légiféré par un organisme de normalisation mandaté, comme l'ISO au niveau international, l'UIT, l'AFNOR,
- Un standard est un ensemble de recommandations ou de préférences préconisées par un groupe d'utilisateurs caractéristiques et avisés.

Qu’est ce qu’une norme (1)?

D’après AFNOR une **norme** est un **cadre de référence** qui vise à fournir **des lignes directrices, des prescriptions techniques ou qualitatives pour des produits, services ou pratiques au service de l’intérêt général**. Elle est le fruit d’une **co-production** consensuelle entre **les professionnels** et **les utilisateurs** qui se sont engagés dans son élaboration. Toute organisation peut ou non s’y référer. **C’est pourquoi la norme est dite volontaire.**

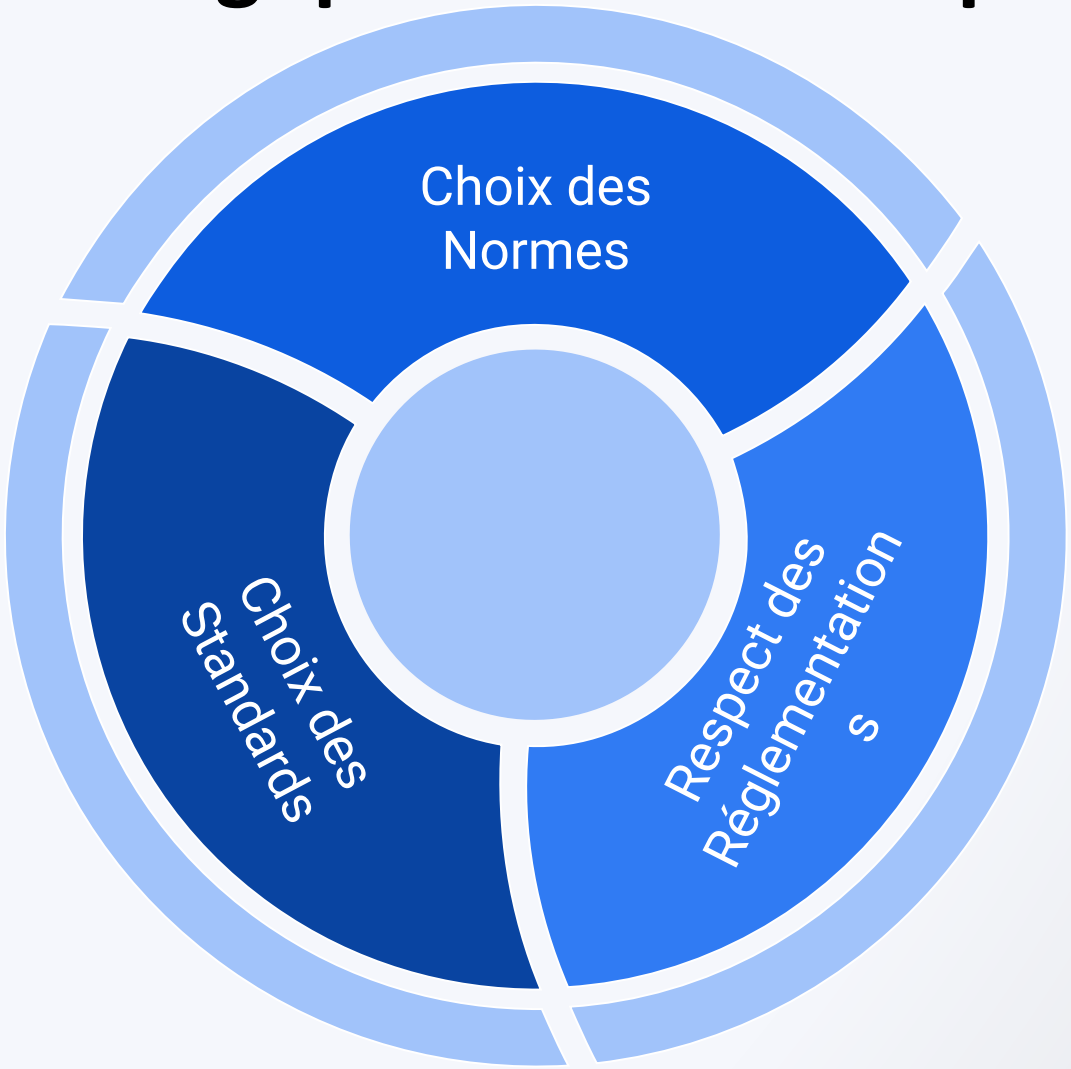
Qu’est ce qu’une norme (2)?

- D’après ISO une norme est comparable à une formule qui décrirait la meilleure façon de faire.
  - Que ce soit pour la fabrication d’un produit, la gestion d’un processus, la prestation d’un service ou la fourniture de matériel, les normes couvrent un large éventail d’activités.
  - Les normes reposent sur les connaissances des experts dans leur domaine de prédilection, conscients des besoins des organisations qu’ils représentent – qu’il s’agisse des fabricants, des distributeurs, des acheteurs, des utilisateurs, des associations professionnelles, des consommateurs ou des organismes de réglementation.

Qu’est ce qu’une réglementation?

- La réglementation est l'ensemble des règlements, c'est-à-dire des mesures légales, des règles, des prescriptions, des indications et autres textes juridiques qui régissent une activité sociale ou qui concernent un domaine particulier. Elle est rédigée par les administrations compétentes ou les personnes mandatées.

Les décisions stratégiques d’une entreprise



Quelques normes en sécurité des SI

- Sécurité de l'information, cybersécurité et protection de la vie privée
  - ISO/IEC 27001:2022 Exigences
  - ISO/IEC 27002:2022 - Mesures de sécurité de l'information
  - ISO/IEC 27004:2016 - Management de la sécurité de l'information

Quelques standard en sécurité des SI

- PCI DSS : Le standard PCI DSS est un standard pour les industries de paiement par carte
- OWASP WSTG: est un standard pour les tests des applications web
- OWASP ASVS : est un standard pour la vérification de la sécurité des applications

Les réglementations au Bénin

- Loi portant code du numérique en république du Bénin:
  - Livre Premier : Des Réseaux Et Services De Communications Électroniques
  - Livre Troisième Des Prestataires De Services De Confiance
  - Livre Quatrième Du Commerce Électronique
  - Livre Cinquième De La Protection Des Donnees A Caractere Personnel
  - Livre Sixième De La Cybercriminalité Et De La Cybersécurité
  - Livre Septième Des Dispositions Transitoires Et Finales

Les réglementations au Bénin

- Politique de sécurité des systèmes d'information de l'Etat (PSSIE)
  - La PSSIE est un document de référence et stratégique qui définit les règles, les procédures et les bonnes pratiques de sécurité à respecter pour garantir la sécurité des systèmes d'information de l'administration publique.
  - C'est un pilier de la protection des infrastructures et systèmes d'information de l'Etat.
  - La PSSIE est élaborée par l'ex Agence nationale de la sécurité des systèmes d'information (exANSSI) actuelle ASIN et est applicable à tous les organismes de l'Etat.

Les réglementations au Bénin

- L'Autorité de Protection des Données à caractère Personnel (APDP)
  - L'Autorité de Protection des Données à caractère Personnel (APDP) est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte à l'identité humaine, aux droits de l'Homme, à la vie privée, aux libertés individuelles ou publiques.
  - Autorité administrative indépendante, elle exerce ses missions conformément aux dispositions de la loi n° 2017-20 portant code du numérique en République du Bénin.
  - https://apdp.bj/procedures/

En pratique comment auditer la fonction informatique

1. Identifier les normes, standards et les réglementations applicables à l'entreprise
   - PCI DSS, ISO 2700x,
     - Présent dans la documentation stratégique SDSI, PSSI
2. Identifier les manuels de procédures et les plans d'action de la documentation stratégique
   - Vérifier Conformité avec le principes, les exigences, les règles et les recommandations
   - Vérifier la mise en oeuvre à travers la documentation fonctionnelle
     - Log, piste d'audit, configuration etc

En pratique comment auditer la fonction informatique

3. Évaluer le progrès de l'organisation par rapport à l'audit précédent
    - Mise en oeuvre des recommandations