Programme

1. Le cyber-espace et la sécurité de l'information
2. Les bases de la cryptologie et de l'authentification

3. La sécurité des logiciels et des développements

- **Les critères d'évaluations**
- **Les principales méthodes pour les développements sécurisés**

Critères d'évaluation

Common Criteria

1996 : harmonisation des critères d'évaluation de la sécurité des systèmes d'information par le projet des critères communs.

1999 : Common criteria V2.1 = norme ISO 15408

Niveau EAL : Evaluation Assurance Level		
EAL 1	=	Produit testé fonctionnellement
EAL 2	=	Produit testé structurellement
EAL 3	=	Produit testé et vérifié méthodiquement
EAL 4	=	Produit conçu, testé et vérifié méthodiquement
EAL 5	=	Produit conçu, testé de façon semi-formelle
EAL 6	=	Produit conçu, testé et vérifié de façon semi-formelle
EAL 7	=	Produit conçu, testé et vérifié de façon formelle

Pour aller plus loin : https://www.ssi.gouv.fr/uploads/2015/01/CCpart3v21-fr.pdf

Produits de sécurité certifiés ANSSI

Deux types d'évaluations :

- **Certification de sécurité de premier niveau (CSPN) :**
  - Tests en « boîte noire » effectués en temps et délais contraints
- **Produits qualifiés :**
  - Évaluations des critères communs

> Les produits logiciels et matériels ayant reçu une qualification sont regroupés par services de sécurité offerts sur le catalogue du site de l'Agence nationale de la sécurité des systèmes d'information, ils recouvrent les catégories de besoins suivantes :
>
> - Protection du poste de travail
> - Signature électronique et gestion de la preuve
> - Pare-feu
> - Chiffrement IP
> - Ressource cryptographique
> - Administration de la sécurité

https://www.ssi.gouv.fr/particulier/logiciels-preconises-par-lanssi-2/

3. La sécurité des logiciels et des développements

ISO 27034

- Modèle pour faciliter l'intégration de la **sécurité dans le cycle de vie des applications**
  - Concepts, principes
  - Composants et processus
- La norme s'applique autant aux **développements internes** qu'à l'**acquisition**
- Elle ne propose pas de règles de développement
- Périmètre : Personnes, processus, informations, logiciels, infrastructures

"Security is a requirement"

Requirements should be defined and analyzed for each and every stage of the application's life cycle and managed on a continuous basis.

"Application security is context-dependent"

The type and scope of application security requirements are influenced by the risks associated with the application which come in the form of (1) business; (2) regulatory; and (3) technological.

"Appropriate investment for application security"

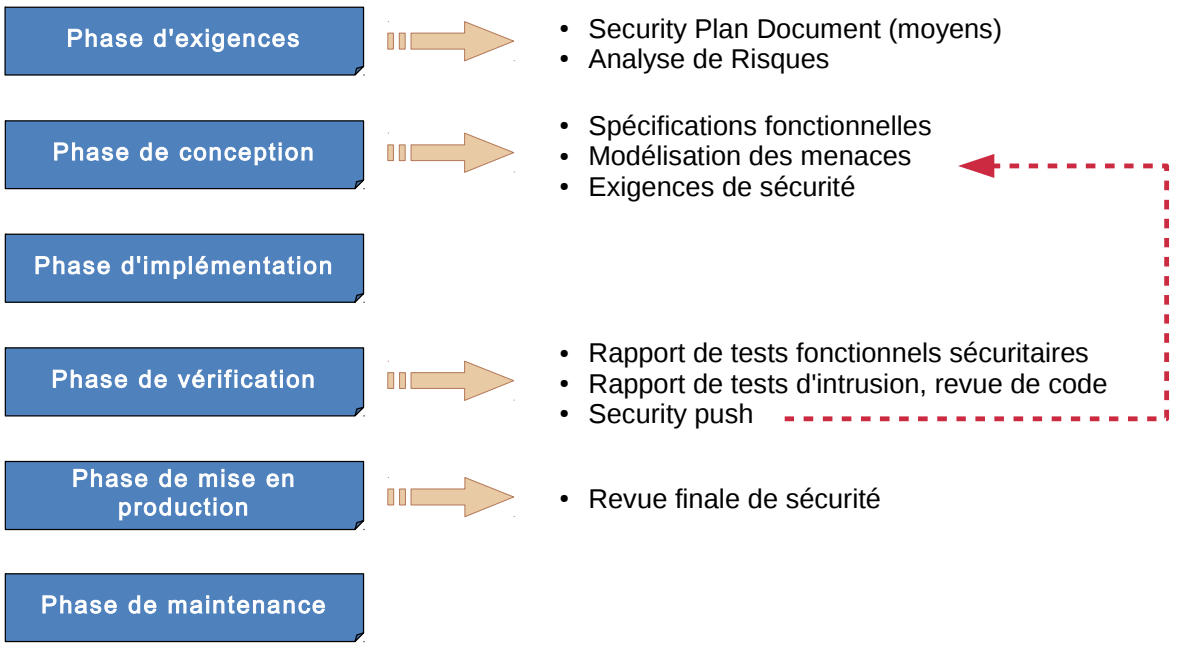
Costs for applying Application Security Controls and performing audit measurements should align with the Targeted Level of Trust.

"Application security should be demonstrated"

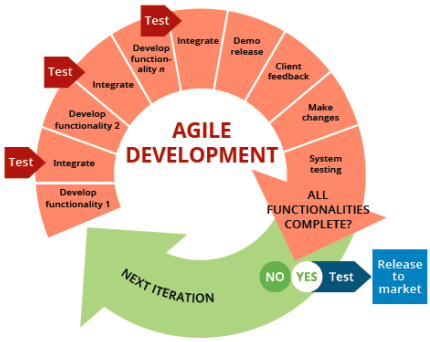
Auditing process leverage the verifiable evidence provided by Application Security Controls to confirm if it has reached management's Targeted Level of Trust.

Processus de développement sécurisé
« Security Development Lifecycle », ou « SDL »

Microsoft® Security Development Lifecycle Process Template



Et dans un environnement agile ?

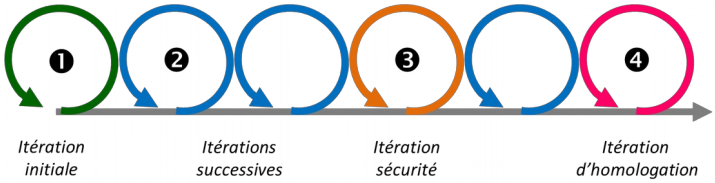


Un triste constat ...

⇒ La sécurité est généralement étudiée après la recette fonctionnelle :

- Budget très limité (ou inexistant...)
- Actions possibles restreintes

⇒ La sécurité est parfois prise en compte dans une **itération « Sécurité »** à la fin des itérations successives :

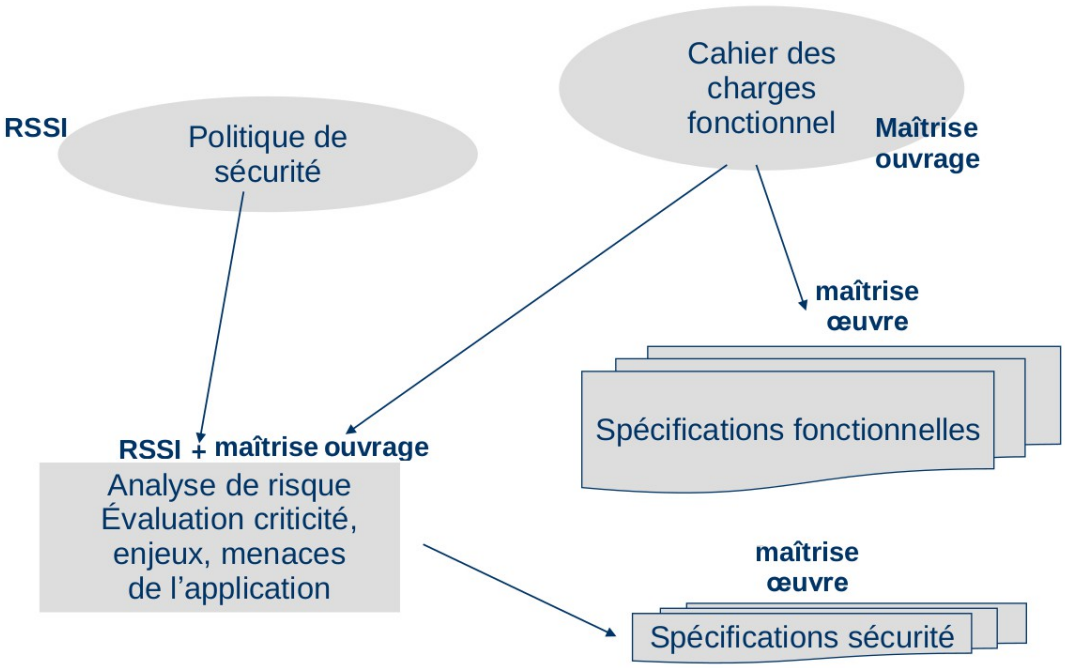


Guide de l'ANSSI – 2017

Intégrer la sécurité numérique en démarche Agile

⇒ Intégration d'une **Analyse de risque** à chaque itération

Les acteurs de l'Intégration de la Sécurité dans les Projets (ISP)

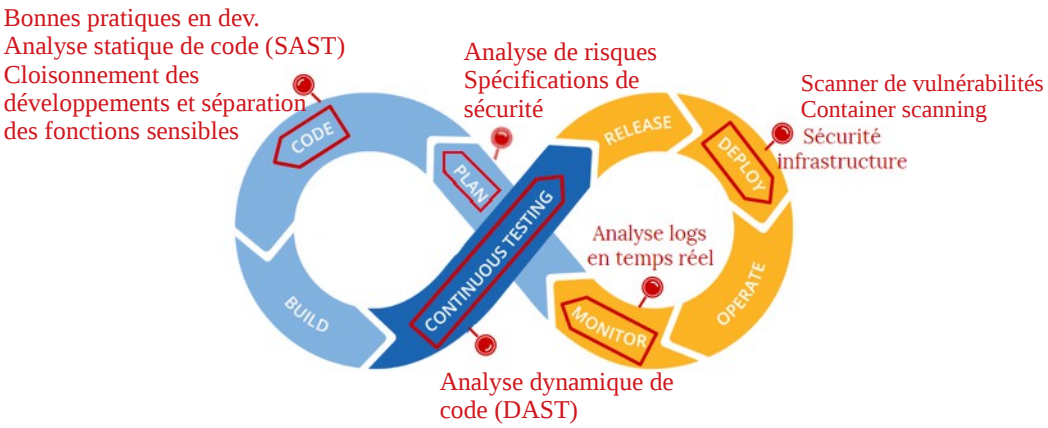


3. La sécurité des logiciels et des développements

Du devOps au devSecOps

Objectifs :

- Intégrer la sécurité aux projets DevOps
- Une sécurité intégrée et non sur un périmètre de sécurité qui protège les applications et les données



- Permet d'appliquer les piliers de l'approche **C.A.L.M.S :**
  - Culture, Automatisation, Lean, Mesure et Solidarité

SAST : Static Application Security Testing ou White box testing
DAST : Dynamic Application Security Testing

Culture – Y-a-t-il un pilote dans DevOps ?
C'est une démarche qui requiert sensibilisation et pédagogie pour espérer une adoption réussie, et des outils de serious gaming sont de plus en plus employés.

Automatisation – DevOps & OpsDev
L'automatisation est une des clés de la réussite pour DevOps. Pour autant on ne peut pas se borner à considérer DevOps comme une simple chaîne automatisée allant du Développement vers les Opérations. En pratique, dans une approche DevOps réussie, le Développement se positionne en tant que consommateur d'infrastructures clé en main. Les Opérations s'installent alors dans une démarche OpsDev, et fournissent des infrastructures à la demande pour toutes les phases d'intégration continue depuis la compilation jusqu'à la qualification, en passant par les tests unitaires.

Lean
La philosophie du Lean trouve ses sources dans les méthodes de production de Toyota, où la recherche de la performance se fait grâce à l'élimination des gaspillages appelés « muda » en Japonais. Les types de gaspillage sont au nombre de 7 : surproduction, attentes, transport, étapes inutiles, stocks, mouvements inutiles, corrections/retouches. Ils peuvent être appliqués à bon nombre d'activités industrielles, et résonnent désormais fortement aux oreilles des professionnels l'informatique avec le Lean IT.

Mesure : permet une Amélioration Continue en mettant en place des indicateurs de performances.

Solidarité – « C'est pas moi, c'est nous »
Avec la solidarité c'est encore la culture qui est en avant, ou plutôt le changement de culture autour d'un conflit d'intérêt séculaire datant des origines de l'informatique. Les équipes Opérations ont en effet pour objectif de garantir la stabilité des systèmes, avec comme principal moyen le contrôle strict et la limitation des changements. A l'inverse, les équipes Développement ont pour mission d'apporter les changements nécessaires le plus vite possible, au risque d'impacter la stabilité.

Intégration de la sécurité dans les contrats (ISC)

- Inclure **des clauses** dans les **contrats** :
  - des clauses sur les contrôles et audits
  - des clauses sur la correction des vulnérabilités détectées
  - des clauses sur l'analyse de code
  - des clauses sur les scans de vulnérabilités
  - des pénalités financières en cas de nos respects des clauses
- Demander les **PAS** (Plan d'Assurance Sécurité) et les **PSSI** aux prestataires
- S'assurer de la conformité **RGPD** du prestataire
- Bien valider le niveau de sécurité à imposer au sous-traitant !

Avantages du test d'intrusion

Point de vue offensif, qui **complète le point de vue défensif** de l'audit
Minimisation des faux positifs d'un scanner de vulnérabilités
Révélation d'**effets de bord non identifiés**
Un test confidentiel permet de **tester les détections et réactions**

Inconvénients du test d'intrusion

Même si proche d'attaques réelles, elles n'en sont pas : le vrai attaquant a l'avantage du moment et du tempo
Compétences plus rares
Intrusion non réussie ne veut pas dire sécurité parfaite
Peut faire de vrais dégâts