Tester R 66

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | valider le respect des exigences de sécurité de l’information lorsque des applications ou le code sont déployés dans l'environnement de production |
| pilote | responsable sécurité de l’information |
| risques | * ne pas tester les nouveaux systèmes, mises à jour et nouvelles versions pendant le développement * ne pas tester par rapport aux exigences fonctionnelles et non fonctionnelles * ne pas tester les fonctions de sécurité, les restrictions d’accès, l’utilisation de la cryptographie, le codage sécurisé et les configurations sécurisées * ne pas utiliser un ensemble de critères pour le plan de test * ne pas inclure dans le plan de test les éléments nécessaires * ne pas utiliser des outils automatiques de vérification (analyseurs de code et de vulnérabilité) * ne pas valider le développement interne par des tests indépendants * ne pas utiliser des critères d’acquisition pour les logiciels externes |
| processus amont | * apprécier les risques * traiter les risques * développer * gérer les vulnérabilités |
| processus aval | * satisfaire aux exigences de la sécurité * appliquer la sécurité * utiliser la cryptographie |
| éléments d'entrée | * inventaire des actifs * plan de traitement des risques * clés cryptographiques |
| activités  (sous-processus) | * tester les nouveaux systèmes, mises à jour et nouvelles versions pendant le développement * tester par rapport aux exigences fonctionnelles et non fonctionnelles * tester :   + les fonctions de sécurité   + les restrictions d’accès   + l’utilisation de la cryptographie   + le codage sécurisé   + les configurations sécurisées * utiliser un ensemble de critères pour le plan de test * inclure dans le plan de test :   + un calendrier détaillé des activités et des tests   + les entrées et les sorties attendues   + les critères d'évaluation des résultats   + les décisions d'actions ultérieures possibles * utiliser des outils automatiques de vérification (analyseurs de code et de vulnérabilité) * valider le développement interne par des tests indépendants :   + activités de revue du code   + analyse de vulnérabilité   + test d’intrusion * utiliser des critères d’acquisition pour les logiciels externes |
| éléments de sortie | * principes d’ingénierie * plan de test |
| ressources | moyens techniques et informatiques |
| indicateurs | * taux de tests passés du premier coup * plans de tests réalisés sans retard * clés cryptographiques utilisées |
| procédures / documents | accès au code source, gestion des vulnérabilités, codage, utilisation de la cryptographie, traitement de l’information, relations avec les fournisseurs / plan de traitement des risques, plan de test, vulnérabilités techniques, résultats des revues de sécurité, clés cryptographiques, principes d’ingénierie, sécurité de l’information avec les fournisseurs |
| clients | ensemble du personnel |

responsable sécurité de l’information

valider le respect des exigences de sécurité de l’information lorsque des applications ou le code sont déployés dans l'environnement de production

tester / R 66

risques

processus aval

processus amont

* satisfaire aux exigences de la sécurité
* appliquer la sécurité
* utiliser la cryptographie
* apprécier les risques
* traiter les risques
* développer
* gérer les vulnérabilités
* ne pas tester les nouveaux systèmes, mises à jour et nouvelles versions pendant le développement
* ne pas tester par rapport aux exigences fonctionnelles et non fonctionnelles
* ne pas tester les fonctions de sécurité, les restrictions d’accès, l’utilisation de la cryptographie, le codage sécurisé et les configurations sécurisées
* ne pas utiliser un ensemble de critères pour le plan de test
* ne pas inclure dans le plan de test les éléments nécessaires
* ne pas utiliser des outils automatiques de vérification (analyseurs de code et de vulnérabilité)
* ne pas valider le développement interne par des tests indépendants
* ne pas utiliser des critères d’acquisition pour les logiciels externes

activités

éléments de sortie

éléments d'entrée

* tester les nouveaux systèmes, mises à jour et nouvelles versions pendant le développement
* tester par rapport aux exigences fonctionnelles et non fonctionnelles
* tester :
  + les fonctions de sécurité
  + les restrictions d’accès
  + l’utilisation de la cryptographie
  + le codage sécurisé
  + les configurations sécurisées
* utiliser un ensemble de critères pour le plan de test
* inclure dans le plan de test :
  + un calendrier détaillé des activités et des tests
  + les entrées et les sorties attendues
  + les critères d'évaluation des résultats
  + les décisions d'actions ultérieures possibles
* utiliser des outils automatiques de vérification (analyseurs de code et de vulnérabilité)
* valider le développement interne par des tests indépendants :
  + activités de revue du code
  + analyse de vulnérabilité
  + test d’intrusion
* utiliser des critères d’acquisition pour les logiciels externes
* principes d’ingénieries
* plan de test
* inventaire des actifs
* plan de traitement des risques
* clés crypto-graphiques

indicateurs

procédures / documents

clients

ressources

taux de tests passés du premier coup, plans de tests réalisés sans retard, clés cryptographiques utilisées

accès au code source, gestion des vulnérabilités, codage, utilisation de la cryptographie, traitement de l’information, relations avec les fournisseurs / plan de traitement des risques, plan de test, vulnérabilités techniques, résultats des revues de sécurité, clés cryptographiques, principes d’ingénierie, sécurité de l’information avec les fournisseurs

moyens techniques et informatiques

ensemble du personnel