PROJETS INFORMATIQUES

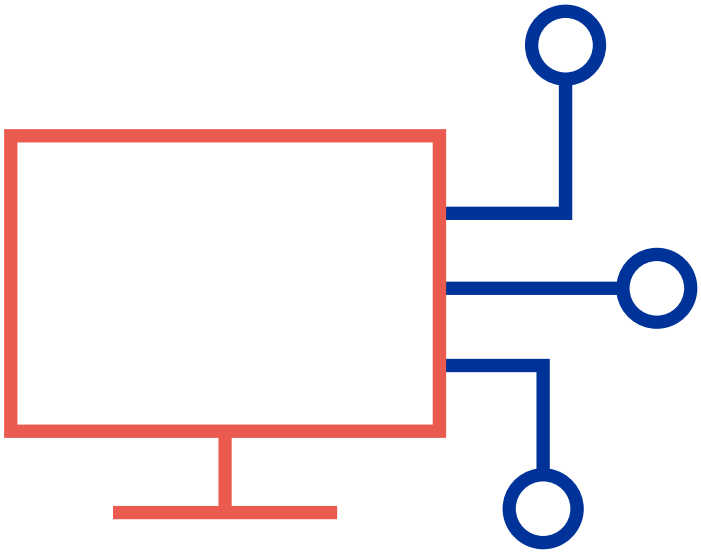
Audit de la mise en production d'applications dans un environnement agile

Office fédéral de l'informatique et de la télécommunication

23701

VERSION PRISES DE POSITION INCLUSES

11 JUIN 2024



EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS
SWISS FEDERAL AUDIT OFFICE

INFORMATIONS SUR LE DOCUMENT

ADRESSE DE COMMANDE
BESTELLADRESSE
INDIRIZZO DI ORDINAZIONE
ORDERING ADDRESS

Contrôle fédéral des finances (CDF)
Monbijoustrasse 45
3003 Berne
Suisse

NUMÉRO DE COMMANDE
BESTELLNUMMER
NUMERO DI ORDINAZIONE
ORDERING NUMBER

609.23701

COMPLÉMENT D'INFORMATIONS
ZUSÄTZLICHE INFORMATIONEN
INFORMAZIONI COMPLEMENTARI
ADDITIONAL INFORMATION

www.efk.admin.ch/fr
info@efk.admin.ch
+ 41 58 463 11 11

PRIORITÉS DES RECOMMANDATIONS

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis : 1 = élevés, 2 = moyens, 3 = faibles.
Sont par exemple considérés comme risques les projets non rentables, les infractions à la légalité ou à la régularité, les cas de responsabilité ou les atteintes à la réputation. Les effets et la probabilité de survenance sont ainsi évalués. Cette appréciation se fonde sur l'objet concret de l'audit (relatif) et non sur la pertinence pour l'administration fédérale dans son ensemble (absolu).

TABLE DES MATIÈRES

L'essentiel en bref **4**
Das Wesentliche in Kürze **6**
L'essenziale in breve **9**
Key points **11**

1 Mission et déroulement **14**
1.1 Contexte 14
1.2 Objectifs et questions d'audit 15
1.3 Étendue de l'audit et principe 15
1.4 Documentation et entretiens 15
1.5 Discussion finale 15

2 Constatations et appréciations **16**
2.1 Une première version des pipelines CNCICD est opérationnelle, quelques points ouverts doivent être finalisés 16
2.2 Le respect des exigences n'est que partiellement testé dans les pipelines CNCICD standard 17
2.3 Des conditions suffisantes sont réunies pour que les développeurs internes et externes mettent les exigences en œuvre 18
2.4 Des possibilités licites existent pour contourner les tests prévus dans les pipelines 19
2.5 L'intégrité des pipelines ne peut pas encore être complètement assurée 19
2.6 Des travaux sont en cours pour les activités d'ordre supérieur mais la perspective du SCI doit être renforcée 20

Annexe 1 – Directives et stratégies 22
Annexe 2 – Abréviations 23
Annexe 3 – Glossaire 24

AUDIT

Audit de la mise en production d'applications dans un environnement agile

Office fédéral de l'informatique et de la télécommunication

L'ESSENTIEL EN BREF

L'Office fédéral de l'informatique et de la télécommunication (OFIT) a récemment mis à jour son infrastructure informatique en nuage privé Atlantica. Il a notamment mis en œuvre une nouvelle plateforme de gestion des conteneurs logiciels. Cette technologie permet de regrouper le code d'une application avec les fichiers de configuration et les composantes nécessaires à son exécution. Réalisés dans le cadre du programme Amboss, les travaux se sont achevés à fin décembre 2023 et ont coûté quelque 13,2 millions de francs. Ils ont aussi porté sur la réalisation de nouvelles chaînes de processus et d'outils pour la mise en production automatisée des applications nommées « pipelines CNCICD ». Ces chaînes ont une importance particulière en termes de système de contrôle interne (SCI). Elles doivent en effet assurer que les tests du respect des exigences posées à une solution applicative ont été réussis avant que celle-ci passe en mode productif.

Dans cet audit, le Contrôle fédéral des finances (CDF) examine si les prescriptions et les processus de l'OFIT garantissent que les exigences – et particulièrement les exigences non-fonctionnelles telles que la sécurité, la conformité architecturale, l'incorporation des besoins du SCI, etc. – sont remplies dans toutes les mises en production d'applications. Le CDF a constaté qu'une première version des pipelines CNCICD est opérationnelle et déjà utilisée. Cependant, seule une partie des exigences non-fonctionnelles sont couvertes par les tests automatiques dans les mises en production. Les autres catégories d'exigences peuvent être testées au travers d'étapes manuelles de validation. Plusieurs points sont encore en suspens, l'OFIT y travaille. Le CDF a par ailleurs recommandé de renforcer la perspective du SCI dans ces travaux.

Une première version des pipelines est en place, mais la couverture des exigences par les tests automatiques est limitée

Une approche structurée a présidé à la mise en œuvre des pipelines CNCICD. Selon le cahier des charges, les possibilités offertes par les environnements en nuage devaient être exploitées au maximum, tout en garantissant la sécurité. Ces travaux ont débouché sur une combinaison complexe d'outils et de processus, qui couvrent les étapes du développement applicatif et du déploiement des solutions en mode continu. Ainsi, les pipelines guident les développeurs et les exploitants durant la gestion des versions des objets de code et les activités de test et de validation (intégration). Dans un deuxième temps, ils les accompagnent en vue de la préparation des paquets logiciels et leur distribution sur les infrastructures productives (déploiement). Diverses fonctions annexes, telles que la journalisation des événements et le stockage d'informations sensibles, sont aussi mises à disposition. Certains points ouverts subsistent, mais cette première version a pu faire la preuve de son fonctionnement : quatre solutions applicatives ont déjà pu être mises en production au travers des pipelines, plus d'une centaine d'entre elles sont en cours de travail. Le processus d'adoption suit son cours, l'OFIT et les bénéficiaires de prestations gagnent en expérience. Des ajustements restent possibles.

La mise en production des applications ne peut se faire que par le biais d'un pipeline. Pour faciliter l'adoption de ce principe par les développeurs internes et externes, l'OFIT a mis en place une abondante documentation sous forme de descriptions, de guides, de standards, de vidéos et de listes de contrôle. Pour les applications en conteneurs livrées clés en main par des fournisseurs externes, un type spécifique de pipeline a été mis en œuvre.

Ces applications doivent donc aussi passer par les tests définis dans les chaînes d'outils pour être déployées sur l'infrastructure productive cible. Ainsi, les conditions sont réunies pour que les développeurs internes aussi bien qu'externes puissent utiliser judicieusement les pipelines CNCICD et s'assurer que les exigences définies soient respectées.

Les tests automatiques incorporés dans les pipelines CNCICD ne couvrent que des exigences relatives à la protection informatique de base. Ces tests, qui ne sont pas tous obligatoires, se concentrent sur la recherche de vulnérabilités, d'identifiants apparents dans les lignes de programmes et de qualité du code des applications. Par contre, pour les autres types d'exigences, fonctionnelles ou non, des tests automatiques n'ont pas été utilisés. En effet, dans ces cas, des définitions fastidieuses et spécifiques à chaque application seraient nécessaires. L'OFIT a plutôt privilégié la possibilité de définir des étapes de validation manuelle ou d'incorporer une boucle de test dans un outil ad hoc. Pour favoriser l'acceptation par les bénéficiaires de prestations, une voie médiane entre automatisation et intégration d'étapes manuelles a donc été choisie. Elle laisse toutefois encore une grande partie de la responsabilité de la mise en œuvre correcte des exigences aux équipes de développement. Le CDF estime que cette première version des pipelines CNCICD offre un point de départ raisonnable en termes d'incorporation du contrôle des exigences. Il part du principe que l'OFIT continuera de suivre l'évolution technologique en matière d'outils de test et de pousser l'automatisation dans la mesure du possible.

Des possibilités de contournement temporaire des tests existent

Parce que les tests automatiques retournent parfois des résultats faux-positifs ou qu'ils ne sont pas toujours pertinents pour un environnement donné, une possibilité de les désactiver a été mise en place (« whitelisting »). Selon le processus défini, cette exception doit être dûment documentée et validée par le bénéficiaire et le fournisseur de prestations. La validité de l'exception est limitée dans le temps. Pour le CDF, cette entorse contrôlée à l'obligation de tester les applications est acceptable.

D'autres possibilités de contournement existent. D'une part, les développeurs peuvent copier un pipeline existant et modifier la copie pour en retirer les étapes de tests obligatoires. Ils peuvent alors théoriquement l'utiliser pour mettre en production des applications sans les tester. Des mécanismes de protection des définitions de pipelines par signature cryptographique étaient prévus dans le programme Amboss. Ils n'ont toutefois pas encore pu être mis en place, faute d'un produit compatible sur le marché. La protection des pipelines est donc insuffisante pour l'instant, mais l'OFIT garde cette lacune sur sa liste de points en suspens. D'autre part, la détection a posteriori de tels cas reste possible au travers de l'analyse des journaux d'exécution des pipelines. Pour ces raisons, le CDF renonce à une recommandation sur ce point.

Le CDF précise qu'il n'a pas pu évaluer l'efficacité des contrôles mis en œuvre dans le cadre des pipelines CNCICD. L'OFIT a pu montrer que les données à cet effet sont disponibles, mais leur analyse pour un échantillon représentatif de mises en production n'est pas encore industrialisée.

Opérationnalisation en cours, la perspective du SCI doit être mieux prise en compte

Un comité est en charge du pilotage de la plateforme CNCICD, de la définition de sa gouvernance et des priorités de son futur développement. Des représentants des domaines Business Solutions et Plattform Services de l'OFIT, ainsi que des spécialistes de la sécurité y siègent. Par contre, la perspective du SCI n'est pas explicitement représentée au sein du comité.

Un cadre de référence décrivant les principales fonctions liées aux pipelines est en passe d'être adopté. Parmi ces fonctions, des activités d'ordre supérieur sont d'ailleurs déjà menées. Elles portent notamment sur la surveillance du fonctionnement et les contrôles de la sécurité et de la bonne santé des pipelines et des applications. Un audit de sécurité des pipelines a ainsi été réalisé fin décembre 2023. Les processus et les responsabilités découlant des fonctions décrites dans le cadre de référence ne sont toutefois pas encore tous définis et institutionnalisés, mais leur opérationnalisation est à l'agenda du comité. Par conséquent, le CDF renonce à une recommandation sur ce point. En revanche, il a recommandé de renforcer la perspective du SCI au sein du comité et de son agenda.

PRÜFUNG

Prüfung der Produktivsetzung von Anwendungen in einem agilen Umfeld

Bundesamt für Informatik und Telekommunikation

DAS WESENTLICHE IN KÜRZE

Das Bundesamt für Informatik und Telekommunikation (BIT) hat kürzlich seine IT-Infrastruktur in der Private Cloud Atlantica auf den neuesten Stand gebracht. Das BIT hat insbesondere eine neue Plattform zur Verwaltung von Software-Containern eingeführt. Diese Technologie ermöglicht es, den Anwendungscode mit den Konfigurationsdateien und den für die Ausführung der Anwendung erforderlichen Komponenten zu bündeln. Die Arbeiten, die im Rahmen des Programms «Amboss» durchgeführt wurden, wurden Ende Dezember 2023 abgeschlossen und kosteten rund 13,2 Millionen Franken. Sie umfassten auch die Realisierung neuer Prozess- und Toolketten für die automatisierte Produktivsetzung der als «CNCICD-Pipelines» bezeichneten Anwendungen. Diese Ketten haben eine besondere Bedeutung im Hinblick auf das interne Kontrollsystem (IKS). Sie sollen nämlich sicherstellen, dass die Tests der Anforderungen an eine Anwendung bestanden wurden, bevor diese produktiv gesetzt wird.

In dieser Prüfung untersucht die Eidgenössische Finanzkontrolle (EFK), ob die Vorgaben und Prozesse des BIT gewährleisten, dass die Anforderungen – und insbesondere die nicht-funktionalen Anforderungen wie die Sicherheit, die Architekturkonformität, die Einbeziehung der IKS-Erfordernisse usw. – bei sämtlichen Produktivsetzungen von Anwendungen erfüllt werden. Die EFK hat festgestellt, dass eine erste Version der CNCICD-Pipelines betriebsbereit ist und bereits verwendet wird. Bei den Produktivsetzungen decken die automatischen Tests jedoch nur einen Teil der nicht-funktionalen Anforderungen ab. Die übrigen Anforderungskategorien können über manuelle Validierungsschritte getestet werden. Mehrere Punkte sind noch offen, an welchen das BIT aber arbeitet. Die EFK hat zudem empfohlen, die Perspektive des IKS bei diesen Arbeiten stärker zu berücksichtigen.

Eine erste Version der Pipelines ist implementiert, die Tests decken jedoch nur einen Teil der Anforderungen ab

Bei der Umsetzung der CNCICD-Pipelines wurde ein strukturierter Ansatz verfolgt. Gemäss Pflichtenheft sollten die sich durch die Cloud-Umgebungen bietenden Möglichkeiten voll ausgeschöpft werden, dies bei gleichzeitiger Gewährleistung der Sicherheit. Das Ergebnis dieser Arbeiten war eine komplexe Kombination von Tools und Prozessen, welche die Phasen der Anwendungsentwicklung und der kontinuierlichen Bereitstellung von Lösungen abdecken. Die Pipelines führen die Entwicklungsteams und die Betreibenden demnach bei der Verwaltung der Versionen von Codeobjekten und bei den Test- und Validierungsaktivitäten (Integration). In einem zweiten Schritt begleiten die Pipelines sie bei der Vorbereitung der Software-Pakete und deren Verteilung auf die produktiven Infrastrukturen (Deployment). Verschiedene Nebenfunktionen, wie die Protokollierung von Ereignissen und die Speicherung sensibler Informationen, werden ebenfalls bereitgestellt. Zwar bleiben noch einige offene Punkte, doch hat diese erste Version ihre Funktionsfähigkeit unter Beweis gestellt: Vier Anwendungen konnten bereits über die Pipelines produktiv gesetzt werden, mehr als hundert sind noch in Arbeit. Der Übernahmeprozess schreitet voran und das BIT und die Leistungsempfängerinnen und -empfänger sammeln Erkenntnisse. Anpassungen sind nach wie vor möglich.

Die Produktivsetzung von Anwendungen muss über eine Pipeline erfolgen. Um den internen und externen Entwicklerinnen und Entwicklern die Anwendung dieses Grundsatzes zu erleichtern, hat das BIT eine umfangreiche Dokumentation in Form von Beschreibungen, Leitfäden, Standards, Videos und Checklisten zusammengestellt.

Für von externen Anbietern schlüsselfertig gelieferte Container-Anwendungen wurde eine spezielle Art von Pipeline eingerichtet. Diese Anwendungen müssen demnach ebenfalls die in den Toolketten festgelegten Tests durchlaufen, um in der produktiven Zielinfrastruktur bereitgestellt zu werden. Damit sind die Bedingungen erfüllt, dass sowohl interne als auch externe Entwicklerinnen und Entwickler die CNCICD-Pipelines sinnvoll nutzen und sicherstellen können, dass die festgelegten Anforderungen erfüllt sind.

Die in die CNCICD-Pipelines eingebetteten automatischen Tests decken nur Anforderungen im Zusammenhang mit dem IT-Grundschutz ab. Diese Tests, von denen nicht alle obligatorisch sind, konzentrieren sich auf die Ermittlung von Schwachstellen und von in Codezeilen sichtbaren Anmeldedaten sowie auf die Qualität des Anwendungscodes. Für die anderen Arten von Anforderungen – ob funktional oder nicht – wurden keine automatischen Tests verwendet. In diesen Fällen wären nämlich aufwändige, anwendungsspezifische Definitionen erforderlich. Das BIT zog es vor, manuelle Validierungsschritte festlegen zu können oder eine Testschleife in ein Ad-hoc-Tool einbauen zu können. Um die Akzeptanz seitens der Leistungsempfängerinnen und -empfänger zu fördern, wurde daher ein Mittelweg zwischen Automatisierung und der Integration manueller Schritte gewählt. Damit bleibt jedoch immer noch ein grosser Teil der Verantwortung für die korrekte Umsetzung der Anforderungen bei den Entwicklungsteams. Nach Ansicht der EFK stellt diese erste Version der CNCICD-Pipelines eine angemessene Ausgangsbasis hinsichtlich der Einbettung der Anforderungstests dar. Sie geht davon aus, dass das BIT die technologische Entwicklung der Testtools weiterverfolgen und die Automatisierung so weit wie möglich ausbauen wird.

Es bestehen Möglichkeiten für die vorübergehende Umgehung von Tests

In Anbetracht der Tatsache, dass automatische Tests manchmal fälschlicherweise positive Ergebnisse hervorbringen oder nicht immer für eine bestimmte Umgebung relevant sind, wurde eine Möglichkeit geschaffen, sie zu deaktivieren (Whitelisting). Gemäss dem dafür festgelegten Verfahren muss eine solche Ausnahme ordnungsgemäss dokumentiert und von der oder dem Leistungsempfangenden und der oder dem Leistungserbringenden bestätigt werden. Die Ausnahme gilt nur für eine begrenzte Zeit. Für die EFK ist diese kontrollierte Abweichung von der Pflicht, Anwendungen zu testen, vertretbar.

Es gibt weitere Möglichkeiten für eine Umgehung. Unter anderem können die Entwicklerinnen und Entwickler eine bestehende Pipeline kopieren und die Kopie abändern, indem sie obligatorische Testschritte entfernen. Sie können sie dann theoretisch dafür verwenden, Anwendungen produktiv zu setzen, ohne sie zu testen. Im Programm Amboss waren Mechanismen zum Schutz der Pipeline-Definitionen mittels kryptografischer Signatur vorgesehen. Sie konnten jedoch noch nicht implementiert werden, da es kein kompatibles Produkt auf dem Markt gibt. Momentan sind die Pipelines also unzureichend geschützt, was jedoch einer der noch offenen Punkte auf der Liste des BIT ist. Eine nachträgliche Erkennung solcher Umgehungsfälle ist aber nach wie vor durch eine Analyse der Ausführungsprotokolle der Pipelines möglich. Aus diesen Gründen verzichtet die EFK auf eine Empfehlung zu diesem Punkt.

Die EFK weist darauf hin, dass sie die Wirksamkeit der im Zusammenhang mit den CNCICD-Pipelines implementierten Kontrollen nicht beurteilen konnte. Das BIT konnte zeigen, dass die Daten hierfür vorhanden sind, deren Analyse ist für eine repräsentative Stichprobe von Produktivsetzungen aber noch nicht ausreichend industrialisiert.

Operationalisierung läuft, Perspektive des IKS muss stärker berücksichtigt werden

Für die Steuerung der CNCICD-Plattform, die Festlegung der Plattform-Governance und die Schwerpunkte für deren zukünftige Entwicklung ist ein Komitee zuständig. Darin sitzen Vertreterinnen und Vertreter der Bereiche Business Solutions und Plattform Services des BIT sowie Sicherheitsexpertinnen und-experten. Die Perspektive des IKS ist in dem Komitee jedoch nicht speziell vertreten.

Ein Referenzrahmen, der die wichtigsten Tätigkeiten im Zusammenhang mit den Pipelines beschreibt, steht kurz vor der Verabschiedung. Von diesen Tätigkeiten werden bereits einige übergeordnete ausgeführt. Diese umfassen insbesondere die Überwachung der Funktionsfähigkeit und die Kontrolle der Sicherheit und des ordnungsgemässen Zustands der Pipelines und Anwendungen. Ende Dezember 2023 wurde dementsprechend ein Sicherheitsaudit der Pipelines durchgeführt.

Die Prozesse und Verantwortlichkeiten, die sich aus den im Referenzrahmen beschriebenen Tätigkeiten ergeben, sind jedoch noch nicht alle definiert und institutionalisiert, ihre Operationalisierung steht jedoch auf der Agenda des Komitees. Die EFK verzichtet daher diesbezüglich auf eine Empfehlung. Sie hat aber empfohlen, die Perspektive des IKS innerhalb des Komitees und auf dessen Agenda stärker zu berücksichtigen.

Originaltext auf Französisch

VERIFICA

Verifica della messa in produzione di applicazioni in un ambiente agile

Ufficio federale dell'informatica e della telecomunicazione

L'ESSENZIALE IN BREVE

Recentemente l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) ha aggiornato la sua infrastruttura di cloud privato Atlantica. Nello specifico ha introdotto una nuova piattaforma di gestione dei container. Questi ultimi consentono di raggruppare il codice di un'applicazione, i relativi file di configurazione e le componenti necessarie alla sua esecuzione. I lavori di realizzazione della nuova piattaforma sono stati eseguiti nel quadro del programma AMBOSS e completati alla fine di dicembre 2023 per un costo di circa 13,2 milioni di franchi. In questo contesto sono state sviluppate anche nuove catene di processi e strumenti per la messa in produzione automatizzata delle applicazioni, denominate «pipeline CNCICD» (integrazione, distribuzione e deployment continui in base agli standard del cloud nativo). Tali catene di processi e strumenti ricoprono particolare importanza nell'ambito del sistema di controllo interno (SCI). Servono infatti a garantire che i test di verifica della conformità dei requisiti imposti a una soluzione applicativa siano stati superati prima che questa entri in funzione nell'ambiente produttivo.

Nell'ambito della presente verifica, il Controllo federale delle finanze (CDF) ha esaminato il rispetto da parte dell'UFIT delle sue prescrizioni e dei suoi processi che garantiscono l'osservanza dei requisiti per quanto riguarda la messa in produzione di tutte le applicazioni, in particolare dei requisiti non funzionali, ad esempio in materia di sicurezza, conformità architetturale e osservanza delle necessità del SCI. Il CDF ha potuto constatare che una prima versione delle pipeline CNCICD è già operativa. Tuttavia i test automatici nell'ambito della messa in esercizio soddisfano solo una parte delle esigenze non funzionali. Le altre categorie di esigenze possono essere testate tramite processi manuali di validazione. L'UFIT è impegnato a risolvere numerose questioni ancora in sospeso in questo ambito. Al riguardo, il CDF ha inoltre raccomandato di riservare maggiore attenzione al SCI.

Prima versione delle pipeline già in funzione, limitato tuttavia il rispetto delle esigenze da parte dei test automatici

Per implementare le pipeline CNCICD è stato adottato un approccio strutturato. Il capitolato d'oneri imponeva di sfruttare al massimo le possibilità offerte dagli ambienti cloud, garantendo al contempo la sicurezza. Da questi lavori è risultata una complessa combinazione di strumenti e processi che assicurano lo svolgimento continuativo delle fasi di sviluppo delle applicazioni e di distribuzione delle soluzioni. Le pipeline guidano dunque gli sviluppatori e i gestori nell'esercizio delle versioni dei codici oggetto e nelle attività di test e validazione (integrazione). Successivamente li supportano nella preparazione dei pacchetti software e nella loro distribuzione sulle infrastrutture produttive (deployment). Inoltre vengono messe a disposizione diverse funzioni aggiuntive, come la registrazione degli eventi e l'archiviazione di informazioni sensibili. Nonostante alcuni aspetti in sospeso, questa prima versione delle pipeline si è dimostrata efficace: quattro soluzioni applicative sono già in funzione nell'ambiente produttivo e oltre un centinaio sono in fase di elaborazione. Il processo di adozione delle pipeline sta seguendo il suo corso e l'UFIT, così come i beneficiari delle prestazioni, stanno acquisendo sempre più dimestichezza nel loro impiego. Ciononostante è possibile attuare alcuni miglioramenti.

La messa in produzione delle applicazioni è realizzabile unicamente sulla base di una pipeline. Per sostenere gli sviluppatori interni ed esterni nel rispetto di questo principio, l'UFIT ha elaborato una ricca documentazione composta di descrizioni, guide, standard, video e liste di controllo. Per le applicazioni in container consegnate, pronte per l'uso, da fornitori esterni è stata attuata una pipeline specifica.

Anche queste applicazioni devono quindi superare i test stabiliti nelle catene di strumenti prima di essere distribuite sull'infrastruttura produttiva di destinazione. Così facendo gli sviluppatori interni ed esterni possono utilizzare le pipeline correttamente e assicurarsi che le esigenze prestabilite siano rispettate.

I test automatici previsti dalle pipeline CNCICD soddisfano solo i requisiti relativi alla protezione informatica di base. Questi test, non tutti obbligatori, si focalizzano sulla ricerca delle vulnerabilità, di identificativi figuranti nelle linee di codice nonché della qualità del codice delle applicazione.

Per contro non sono stati effettuati test automatici su altre categorie di esigenze, né funzionali né d'altro genere. In questi casi occorrerebbe elaborare complicate definizioni specifiche in riferimento a ogni singola applicazione. L'UFIT ha preferito la possibilità di definire tappe di validazione manuale o di integrare un ciclo di test in uno strumento ad hoc. Per agevolare l'accettazione da parte dei beneficiari delle prestazioni, l'UFIT ha dunque scelto una via di mezzo tra l'automazione e l'integrazione di tappe manuali. Tuttavia questo approccio attribuisce ancora una grande responsabilità in merito all'attuazione corretta delle esigenze ai team di sviluppo. Il CDF ritiene che la prima versione delle pipeline CNCICD rappresenti un buon punto di partenza per l'integrazione del controllo delle esigenze, ma presuppone che l'UFIT continui a seguire lo sviluppo tecnologico in materia di strumenti di test e a favorire, per quanto possibile, l'automazione.

Possibilità di disattivare temporaneamente i test

Dato che, talvolta, i test automatici forniscono risultati falsamente positivi o non pertinenti nel rispettivo ambiente, è stata prevista la possibilità di disattivarli («whitelisting»). In base alla procedura stabilita, si tratta di una deroga che deve essere debitamente documentata e convalidata dal beneficiario e dal fornitore delle prestazioni. La validità di tale deroga deve essere limitata nel tempo. Il CDF considera accettabile questa eccezione controllata all'obbligo di testare le applicazioni.

Esistono inoltre altre possibilità per evitare i test. Gli sviluppatori possono innanzitutto copiare una pipeline esistente e modificarne la copia per rimuovere le tappe di test obbligatorie. In tal modo riescono, in teoria, a mettere in funzione le applicazioni in ambiente produttivo senza prima testarle. Il programma AMBOSS prevede meccanismi di protezione delle definizioni di pipeline tramite firma crittografata. Tuttavia, a causa della mancanza di un prodotto compatibile sul mercato, tali meccanismi non sono ancora operativi. Al momento la protezione delle pipeline risulta quindi insufficiente, ma l'UFIT ha inserito questa lacuna tra i punti in sospeso da risolvere. Inoltre le analisi dei protocolli di esecuzione delle pipeline consentono di rilevare a posteriori i casi in cui è avvenuta una messa in esercizio non conforme. Per queste ragioni il CDF ha deciso di non formulare alcuna raccomandazione al riguardo.

Il CDF precisa di non aver potuto valutare l'efficacia dei controlli impiegati nel quadro delle pipeline CNCICD. L'UFIT ha dimostrato di disporre di dati che attestano l'efficacia dei controlli, ma non vi è ancora una soluzione industrializzata per un'analisi rappresentativa delle procedure di messa in produzione.

Messa in funzione in corso: necessaria una maggiore considerazione dell'approccio del SCI

Un comitato, composto da rappresentanti delle divisioni Business Solutions e Platform Services dell'UFIT nonché da esperti di sicurezza, è stato incaricato di gestire la piattaforma CNCICD, di definirne la governance e stabilire le priorità del suo futuro sviluppo. Tuttavia l'approccio del SCI non è rappresentato esplicitamente all'interno del comitato.

Attualmente è in fase di approvazione un quadro di riferimento che descrive le principali funzioni relative alle pipeline. Tra queste funzioni, alcune attività prioritarie sono d'altronde già operative. Si tratta, in particolare, di attività incentrate sulla sorveglianza dell'esercizio e sui controlli della sicurezza e del buon funzionamento delle pipeline e delle applicazioni. A fine dicembre è stato eseguito un controllo sulla sicurezza delle pipeline. Non sono ancora stati definiti né consolidati tutti i processi e le responsabilità inerenti alle funzioni descritte nel quadro di riferimento, tuttavia la loro messa in esercizio rientra tra le priorità del comitato. Di conseguenza, il CDF ha deciso di non formulare una relativa raccomandazione. Ha invece raccomandato di rafforzare l'approccio del SCI all'interno del comitato e della sua agenda.

Testo originale in francese

AUDIT

Audit of application releases in an agile environment

Federal Office of Information Technology, Systems and Telecommunication

KEY POINTS

The Federal Office of Information Technology, Systems and Telecommunication (FOITT) recently upgraded its Atlantica private cloud IT infrastructure. In particular, it implemented a new software container management platform. This technology enables an application's code to be grouped together with the configuration files and components needed to run it. The work, carried out as part of the Amboss programme, was completed by the end of December 2023 at a cost of some CHF 13.2 million. It also involved the creation of new process chains and tools for the automated release of applications known as CNCICD pipelines. These pipelines are of particular importance in terms of the internal control system (ICS). They must ensure that tests to check compliance with the requirements placed on an application solution have been successfully completed before it goes into production mode.

In this audit, the Swiss Federal Audit Office (SFAO) examined whether the FOITT's specifications and processes ensure that requirements – particularly non-functional requirements such as security, architectural conformity, incorporation of ICS needs, etc. – are met in all application releases. The SFAO found that an initial version of the CNCICD pipelines is operational and already in use. However, only some of the non-functional requirements are covered by automatic tests in the releases. The other requirement categories can be tested through manual validation steps. Several issues are still pending, and the FOITT is working on them. The SFAO also recommended that the ICS perspective be strengthened in this work.

A first version of the pipelines is in place, but the coverage of requirements through automatic tests is limited

A structured approach was used to implement the CNCICD pipelines. The specifications stipulated that the possibilities offered by cloud environments had to be exploited to the full, while ensuring security. This work resulted in a complex combination of tools and processes, covering the stages of application development and deployment of solutions in continuous mode. The pipelines guide developers and operators through the version management of code objects and the testing and validation (integration) activities. They then support them in preparing software packages and distributing them to production infrastructures (deployment). Various ancillary functions, such as event logging and the storage of sensitive information, are also made available. Although some issues are still pending, this first version has proved its worth: four application solutions have already been released through the pipelines, and more than a hundred are currently being worked on. The adoption process is progressing, and the FOITT and service recipients are acquiring experience. Adjustments remain possible.

Applications can only be released through a pipeline. In order to facilitate the adoption of this principle by internal and external developers, the FOITT has created a wealth of documentation in the form of descriptions, guides, standards, videos and checklists. A specific type of pipeline has been implemented for containerised applications delivered on a turnkey basis by external suppliers. This means that these applications also have to pass the tests defined in the tool chains before they can be deployed on the target production infrastructure. This ensures that both internal and external developers can make appropriate use of the CNCICD pipelines and ensure that the defined requirements are met.

The automatic tests incorporated in the CNCICD pipelines only cover requirements relating to basic IT protection. These tests, which are not all mandatory, focus on looking for vulnerabilities, apparent identifiers in program lines and the quality of application code. However, for other types of requirements, whether functional or not, automatic tests were not used. In these cases, lengthy definitions specific to each application would be necessary.

Instead, the FOITT favoured the possibility of defining manual validation steps or incorporating a test loop into an ad hoc tool. In order to encourage service recipients to accept the system, a middle way between automation and the incorporation of manual steps was therefore chosen. However, this still leaves a large share of the responsibility for the correct implementation of the requirements to the development teams.

The SFAO believes that this first version of the CNCICD pipelines offers a reasonable starting point in terms of incorporating requirements control. It assumes that the FOITT will continue to keep pace with technological developments in testing tools and push for automation wherever possible.

Options exist for temporarily bypassing tests

Since automatic tests sometimes return false-positive results or are not always relevant to a given environment, an option to deactivate them ("whitelisting") was introduced. According to the defined process, this exception must be duly documented and validated by the beneficiary and the service provider. The exception is valid for a limited period of time. For the SFAO, this controlled deviation from the obligation to test applications is acceptable.

Other ways of getting around it exist. Firstly, developers can copy an existing pipeline and modify the copy to remove the mandatory test steps. They can then theoretically use it to release applications without testing them. Mechanisms for protecting pipeline definitions by means of cryptographic signature were included in the Amboss programme. However, it has not yet been possible to implement them, due to the lack of a compatible product on the market. Pipeline protection is therefore inadequate for the time being, but the FOITT is keeping this shortcoming on its list of pending issues. Secondly, it is still possible to detect such cases a posteriori by analysing pipeline execution logs. For these reasons, the SFAO decided not to issue a recommendation on this point.

The SFAO stated that it had not been able to assess the effectiveness of the controls implemented for CNCICD pipelines. The FOITT was able to show that the relevant data is available, but it has not yet been formally analysed for a representative sample of releases.

Operationalisation is under way, but the ICS perspective needs to be better integrated

A committee is in charge of steering the CNCICD platform, defining its governance and the priorities for its future development. Representatives of the FOITT's Business Solutions and Platform Services domains, as well as security specialists, sit on this committee. However, the ICS perspective is not explicitly represented on the committee.

A reference framework describing the main pipeline-related functions is in the process of being adopted. Among these functions, higher-level activities are already being conducted. These include monitoring operations and checking the security and fitness of pipelines and applications. A pipeline security audit was carried out at the end of December 2023. However, the processes and responsibilities stemming from the functions described in the terms of reference have not yet all been defined and institutionalised, but the committee is working on their operationalisation. The SFAO has therefore decided not to make a recommendation on this point. However, it has recommended that the ICS perspective be strengthened within the committee and its work agenda.

Original text in French

PRISE DE POSITION GÉNÉRALE DE L'OFFICE FÉDÉRAL DE L'INFORMATIQUE ET DE LA TÉLÉCOMMUNICATION

Danke für die Erarbeitung des ausführlichen Berichts. Das Audit mit den Beteiligten verlief sehr gut. Die vorgeschlagene Empfehlung werden wir umsetzen.

1 MISSION ET DÉROULEMENT

1.1 Contexte

Dans le cadre de ses services d'informatique en nuage (en anglais « cloud computing »), l'Office fédéral de l'informatique et de la télécommunication (OFIT) propose aux unités administratives de la Confédération l'environnement sécurisé de son propre centre de calcul ainsi que l'accès aux services des fournisseurs de nuages publics. Depuis 2016 déjà, la plateforme en nuage centrale Atlantica est à la disposition des bénéficiaires de prestations qui optent pour la variante des serveurs sur site de l'OFIT pour y établir leurs solutions applicatives. Cette offre de services matérialise ainsi un des modèles d'approvisionnement prévus par la stratégie d'informatique en nuage de l'administration fédérale (« nuages privés »). Le Contrôle fédéral des finances (CDF) a examiné dans un audit précédent la mise en œuvre de cette stratégie[1].

Une des caractéristiques de la mise en œuvre d'applications sur des plateformes de type cloud est l'utilisation de la technologie des « conteneurs ». Les conteneurs sont des paquets logiciels regroupant le code, les fichiers de configuration, les bibliothèques et toutes les dépendances requises pour qu'une solution applicative puisse s'exécuter. Ces paquets peuvent être facilement et rapidement répliqués, et être utilisés dans de multiples environnements. Avec l'usage de conteneurs, les équipes de développeurs bénéficient d'une meilleure portabilité, d'une flexibilité et d'une évolutivité accrues de leurs développements.

L'environnement de containerisation de la plateforme Atlantica arrivant en fin de vie, l'OFIT lance en juillet 2022 le programme Amboss en vue de son remplacement. Le programme a visé notamment les buts suivants :

- Mettre en place une nouvelle infrastructure de conteneurs basée sur Red Hat Open Shift (RHOS).
- Poser les bases de la migration des solutions applicatives développées sous l'ancien environnement.
- Mettre en place une chaîne d'outils et de processus pour faciliter et automatiser la gestion des versions et la mise en production de solutions applicatives containerisées.
- Assurer la mise en œuvre des normes de sécurité.
- Faciliter les aspects humains et organisationnels liés à ce changement.

Le programme Amboss a coûté quelque 13,2 millions de francs (total des coûts des projets et de l'avant-projet, mais sans participation aux dépenses d'exploitation, de migration et de licences après l'introduction de la première version), dont 9,1 millions de francs avec incidence sur le frein à l'endettement. Il a été clôturé avec succès à fin décembre 2023, quelques points ouverts sont en cours de finalisation dans le cadre des activités d'exploitation. Les clients peuvent accéder à la nouvelle offre via la prestation de marché CAE (« container application environment » en français « environnement d'application de conteneur), qui leur permet de commander l'environnement RHOS pour y établir une application.

La mise en œuvre de solutions applicatives dans un environnement cloud repose sur des cadres méthodologiques et technologiques particuliers, par exemple :

- L'agilité et la démarche SAFe[2], prônant la collaboration entre équipes auto-organisées et leurs clients, la fixation autonome des objectifs et des cycles de développement itératifs et courts.
- L'approche « cloud natif » (exploitation d'un maximum des nouvelles possibilités offertes par les architectures de type cloud).
- L'intégration, la livraison et le déploiement continus (en anglais « continuous integration, distribution and/or deployment », abrévié en CI/CD), selon lesquels les versions des développements sont stockées, testées et mises en production à l'aide d'une chaîne d'outils largement automatisée.

---

1 « Audit de la mise en œuvre de la stratégie cloud » (n° d'audit 23766), disponible sur le site internet du CDF.

2 Scaled Agile Framework, modèle d'organisation et de processus destiné à déployer la méthode agile à grande échelle.

Dans un contexte agile, l'automatisation des mises en production joue un rôle particulièrement important. Les chaînes d'outils doivent en effet permettre les itérations rapides de développement, les tests automatisés et des déploiements en continu.

Pour répondre à ces tendances et au troisième objectif du programme mentionné ci-dessus, une plateforme dite « CNCICD » (intégration, livraison et déploiement continus dans une perspective « cloud natif ») a été mise en place. Ces travaux dans le périmètre du programme Amboss ont généré des coûts d'environ 3,2 millions de francs, ils ont abouti. Une première mouture d'un ensemble de chaînes d'outils et de processus (« pipelines CNCICD ») facilitant et automatisant la gestion des versions des applications et leur mise en production est opérationnelle depuis janvier 2024. Les clients peuvent accéder à cette nouvelle offre via la prestation de marché CI/CD, étroitement liée à la prestation de marché CAE.

1.2 Objectifs et questions d'audit

Sous l'angle du système de contrôle interne (SCI), les processus et systèmes de mise en production de solutions applicatives doivent assurer qu'elles ont été dûment testées au préalable, spécialement celles traitant de données financières. Leur intégrité doit aussi être assurée. Or, dans les approches les plus poussées du développement en mode CI/CD, les tests sont automatisés et en cas de réussite, les nouvelles versions des applications sont déployées sans autre intervention dans les environnements productifs.
Conséquence de cette automatisation, le point focal des contrôles change : Les tests doivent être définis pour couvrir la totalité des exigences fonctionnelles et non-fonctionnelles – sécurité, performance, conformité architecturale, incorporation des besoins du SCI, droits d'accès, etc. La chaîne d'outils et sa configuration doivent être fiables. Les modalités de la séparation des tâches, notamment entre développeurs et exploitants, doivent être réexaminées. Le monitorage des activités des pipelines devient critique et les contrôles automatiques doivent être traçables.
Le CDF a déjà émis des recommandations en relation avec cette thématique dans des audits précédents. Il veut maintenant juger si les prescriptions et les processus de l'OFIT garantissent que les exigences, et particulièrement les exigences non-fonctionnelles, sont satisfaites dans toutes les mises en production d'applications. Il a traité notamment les questions suivantes :

- Les exigences non-fonctionnelles sont-elles prises en compte dans les chaînes d'outils CI/CD ?
- Les processus garantissent-ils que tant les développeurs internes que les externes mettent en œuvre les exigences ?
- Des contrôles suffisants sont-ils en place dans les processus pour garantir le respect des exigences, et celles-ci sont-elles effectivement respectées ?
- Des activités de contrôle d'ordre supérieur existent-elles pour découvrir rapidement les éventuelles lacunes dans la mise en œuvre des applications ?

1.3 Étendue de l'audit et principe

L'audit a été mené du 26 février au 12 avril 2024 par André Stauffer (responsable de révision) et un spécialiste externe. Il a été conduit sous la responsabilité de Bernhard Hamberger. Le présent rapport ne prend pas en compte les développements ultérieurs à l'audit.

1.4 Documentation et entretiens

L'OFIT a fourni toutes les informations nécessaires au CDF de manière exhaustive et compétente. Les documents et l'infrastructure requis ont été mis à disposition de l'équipe d'audit sans restriction.

1.5 Discussion finale

La discussion finale a eu lieu le 14 mai 2024. L'OFIT était représenté par les responsables des domaines Platform Services et Révision interne. Du côté du CDF, les participants étaient le responsable de mandat, le chef du centre de compétence et le responsable de révision.
Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux directions d'office, respectivement aux secrétariats généraux, de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 CONSTATATIONS ET APPRÉCIATIONS

2.1 Une première version des pipelines CNCICD est opérationnelle, quelques points ouverts doivent être finalisés

La conception des pipelines CNCICD, effectuée dans le cadre du programme Amboss, a suivi une démarche méthodologique structurée. Un premier fondement est constitué par le modèle de phases du cycle CI/CD représentant les étapes de mise en œuvre des solutions applicatives. Des cadres normatifs ont par ailleurs guidé la réalisation de ces pipelines : les principes de gestion de la technologie de l'OFIT, du cloud natif, du GitOps – une approche systématique de contrôle des versions pour le développement d'infrastructures et d'applications – ont été appliqués. En matière de sécurité, la stratégie « Zero Trust » – aucun appareil connecté ne doit recevoir des accès par défaut – et un standard de sécurité informatique pour le DevOps – une philosophie de l'ingénierie informatique pour l'intégration des rôles du développement et de l'administration des infrastructures – ont dicté l'agenda. Enfin, cinq objectifs ont été définis pour ces travaux : les pipelines CNCICD devaient être construits sur la base de standards cloud natifs, pouvoir s'appliquer à n'importe quelle architecture cible, être extensibles dynamiquement, être configurables sous forme de code et être traçables et observables. En toile de fond, la méthode de gestion de projet HERMES garde sa validité pour les activités de développement.

Les étapes du cycle CI/CD ne sont que partiellement couvertes par les pipelines CNCICD. Dans le cycle d'intégration continue (CI), les activités de planification et de codage (« Plan » et « Code ») restent dans le giron des analystes d'affaires et des développeurs. Ces intervenants doivent continuer de formaliser les exigences, de concevoir et d'écrire les programmes à l'aide de leurs environnements dédiés. Les fonctions des pipelines entrent en jeu dès le moment où les changements de code sont prêts pour être intégrés dans la gestion des versions et compilés (phase « Build »). La phase suivante « Test » contient des contrôles automatiques et manuels. En cas de réussite, une opération manuelle doit être effectuée pour mettre à disposition les artefacts pour le cycle de déploiement continu, notamment avant le passage en production. Cette séparation entre les deux parties du cycle CI/CD est voulue, les pipelines ne sont ainsi pas entièrement automatisés.

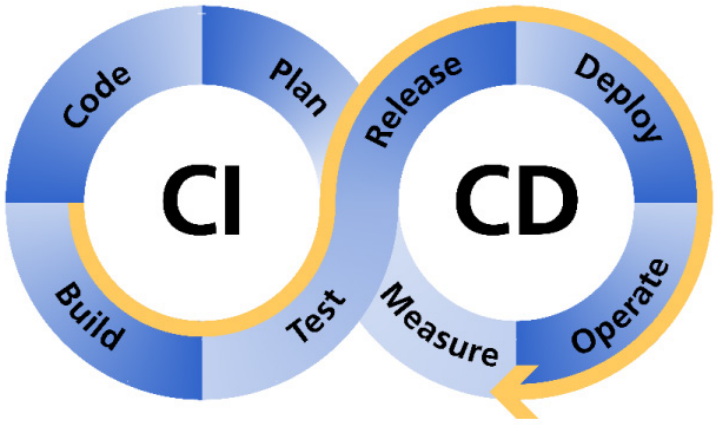


Figure 1 : Longées par la flèche jaune, les phases du cycle CI/CD prises en charge par la prestation de marché CI/CD, source OFIT.

Dans la phase « Release » du cycle CD, la version du programme est validée, les artefacts sont préparés pour la distribution et le déploiement vers les plateformes-cibles (phase « Deploy »). Une mise en production sur l'environnement RHOS n'est par ailleurs possible qu'au travers d'une exécution de cycle de pipeline. L'exploitation productive des solutions applicatives (phase « Operate ») s'ensuit.

Sur le plan de l'observabilité, les événements survenant dans les différentes étapes du cycle, échec, réussite, avertissements, alertes, messages d'erreur, etc. sont journalisés. Ces journaux sont conservés quelques jours dans les outils de la chaîne CI/CD, puis sont archivés dans des solution de récolte, de suivi et d'analyse de données machines, en aval des pipelines. Des statistiques de fonctionnement peuvent être éditées sur cette base (phase « Measure »).

Les pipelines CNCICD ont été réalisés sur ces bases. Concrètement, une collection d'outils a été mise en œuvre de manière intégrée, principalement pour piloter les étapes des cycles, gérer les versions des objets logiciels en cours de développement et les stocker dans des dépôts, analyser et tester ces versions et soutenir leur déploiement vers les infrastructures-cibles. En plus de ces fonctionnalités centrales, des composantes annexes ont été mises en œuvre, notamment pour permettre la journalisation et l'analyse des exécutions des cycles CI/CD. Sur le plan de la sécurité, des outils de stockage crypté (« vaults ») pour des données confidentielles telles que les identifiants sont intégrés. Une lacune de la plateforme précédente a ainsi été comblée. Les utilitaires permettant la signature cryptographique des artefacts et des définitions de pipelines ne sont par contre pas encore définis (voir ci-dessous).

L'équipe de projet a dû choisir au sein d'une vaste palette de produits disponibles sur le marché en matière de développement cloud natif. Elle a documenté ses décisions. Le programme a ainsi livré une collection de pipelines standard couvrant huit technologies de réalisation de solutions applicatives, telles que Java, .Net, Go et Angular. Des modèles, dans le sens d'environnements entièrement configurés, exempts de toute vulnérabilité et prêts pour servir de base au développement applicatif (« base images »), ont aussi été réalisés.

La plateforme CNCICD et ses pipelines ont déjà été utilisés dans plusieurs cas réels. Dans le cadre du programme Amboss, une application existante du Groupement Défense, la gestion des dossiers vétérinaires (en allemand « Verwaltung der Tierkrankengeschichten », VTKG), a été prise comme pilote et a été migrée vers l'infrastructure RHOS au moyen de pipelines. Au moment de l'audit, on comptait déjà 4 migrations achevées vers l'infrastructure RHOS, tandis qu'une quinzaine d'applications étaient en cours de travail. Par ailleurs, on dénombrait plus d'une centaine d'applications dans les différentes étapes préparatoires de la migration ou de l'implémentation sur la nouvelle plateforme. Sur la base de ces expériences, l'OFIT compte réévaluer les paramètres du fonctionnement des pipelines CNCICD, les adapter et étendre les cas d'usage si nécessaire.

APPRÉCIATION

Les travaux de mise en œuvre de la plateforme et des pipelines CNCICD ont débouché sur une combinaison complexe d'outils et de processus. Certains points ouverts subsistent (voir ci-dessous), mais cette première version a le mérite de fonctionner, exemples à la clé, et de répondre déjà en partie aux exigences posées en termes de SCI à une chaîne d'outils CI/CD. Le processus d'adoption est en cours, l'OFIT et les bénéficiaires de prestations accumulent de l'expérience. Des ajustements du fonctionnement des pipelines restent possibles. A ce stade, ces points sont positifs et représentent un progrès par rapport à la situation précédente.

2.2 Le respect des exigences n'est que partiellement testé dans les pipelines CNCICD standard

Pour les exigences fonctionnelles posées aux solutions applicatives, la définition, la mise en œuvre et les tests restent de la responsabilité des analystes d'affaires et des développeurs. Dans le modèle CI/CD adopté par l'OFIT, ceux-ci doivent par exemple continuer de définir et d'exécuter les tests unitaires de leurs solutions, dans la phase « Code », donc en amont des pipelines CNCICD. Aucun contrôle automatique n'est prévu pour l'instant. Une majorité d'exigences non-fonctionnelles, telles que la satisfaction des besoins relatifs à la conformité architecturale, au SCI, à la performance et aux droits d'accès, ne sont pas non plus analysées automatiquement dans les pipelines standard.

Pour ces catégories d'exigences, des contrôles peuvent toutefois être intégrés dans les cycles CI/CD sous la forme d'étapes à valider manuellement par un utilisateur humain (« quality gates »). Par exemple, ces validations peuvent prendre la forme d'un changement de la valeur d'un statut ou de la saisie d'une adresse indiquant les plateformes-cibles pour le déploiement. Des points d'ancrage peuvent aussi être définis dans les cycles pour lancer des exécutions de séries de tests dans des outils ad hoc. L'utilisation de cette fonctionnalité est toutefois optionnelle et les configurations sont du ressort du client.

En revanche, des tests automatiques en matière de sécurité sont intégrés dans les pipelines standard. Ils répondent à des exigences de la protection informatique de base dans l'administration fédérale et sont mis en œuvre principalement au travers d'outils de recherche de vulnérabilités ou d'identifiants apparents. Ces tests, selon leur résultat et la configuration, peuvent interrompre le cycle d'exécution du pipeline (pour trois des outils), ou produire des avertissements. Cinq de ces outils ne peuvent pas être désactivés. Dans le domaine de la sécurité, les éventuels besoins de protection accrus ne sont par contre pas testés de manière automatique.

APPRÉCIATION

Les tests automatiques des pipelines CNCICD ne couvrent que certaines exigences relatives à la protection informatique de base. Pour les autres types d'exigences, fonctionnelles ou portant sur la performance, des besoins accrus de protection, du SCI ou de conformité architecturale, des outils de test automatiques n'ont pas été mis en œuvre. Dans ces cas, ils nécessitent en effet un important travail de définition spécifique à chaque application. De nombreux allers-retours avec les bénéficiaires de prestations en auraient résulté. Comme solution de rechange, les pipelines permettent l'introduction d'étapes de test manuelles, à effectuer hors chaîne.

Pour cette première version des pipelines, l'OFIT a préféré en faciliter l'adoption par les développeurs et les bénéficiaires de prestations. Une voie médiane permettant une automatisation modérée, l'intégration d'étapes manuelles, et une relative acceptation par les bénéficiaires de prestations a été privilégiée. Le CDF estime que cette première mouture offre un point de départ raisonnable en termes d'incorporation du contrôle des exigences, notamment non-fonctionnelles. Il part du principe que l'OFIT continuera de surveiller l'évolution technologique en matière d'outils de test et de pousser l'automatisation dans la mesure du possible.

2.3 Des conditions suffisantes sont réunies pour que les développeurs internes et externes mettent les exigences en œuvre

Les solutions applicatives peuvent être développées à l'OFIT par des développeurs internes ou externes, ou être mises à disposition clé en main par des fournisseurs tiers. L'utilisation des pipelines CNCICD est obligatoire pour toutes les applications mises en œuvre sur la plateforme-cible RHOS, un déploiement manuel n'est pas possible. Diverses mesures ont été élaborées pour faciliter l'utilisation des pipelines.

Pour les développements à l'OFIT, des ressources décrivant les différents aspects de l'utilisation des pipelines CNCICD sont à la disposition des intervenants :

- Une abondante documentation (principes, standards de développement, détails du fonctionnement des pipelines, listes de contrôle) est accessible en ligne.
- Des capsules vidéo expliquent les premiers pas avec la plateforme et montrent des exemples.
- Des spécialistes (« champions ») et les intervenants au projet de mise en place des pipelines peuvent répondre aux questions les plus pointues.
- La méthode HERMES et ses modèles de résultats continuent de s'appliquer dans un contexte agile.

Un « contrôle des connaissances » n'est pas explicitement mis en place et l'efficacité des mesures de facilitation de l'utilisation des pipelines n'est pas formellement mesurée. L'OFIT attend que les intervenants soient d'un niveau suffisant pour emmagasiner les informations nécessaires et utiliser la plateforme de manière judicieuse.

Pour les applications livrées clé en main par les fournisseurs externes, un type spécial de pipeline CNCICD a été défini (« applications génériques »). Dans ce cas de figure, le fournisseur livre des artefacts dans un conteneur, et l'ensemble fait l'objet des tests et des étapes définis dans le pipeline, notamment pour la recherche de vulnérabilités. Des pages Confluence documentent l'architecture et la marche à suivre pour intégrer ces applications.

APPRÉCIATION

Les mesures mises en œuvre pour assurer la compréhension et une utilisation judicieuse de la plateforme par les utilisateurs internes et externes (documentation, guides, etc.) sont suffisantes en l'état. Les contrôles automatiques définis dans les pipelines CNCICD standard posent des bases adéquates pour que les tests liés à la protection de base soient exécutés. La mise en œuvre des autres exigences (besoin accru de protection, autres exigences non-fonctionnelles et fonctionnelles) n'est pas assurée par des étapes des pipelines standard, mais peut être contrôlée au moyen d'étapes manuelles. Les bénéficiaires de prestations restent ainsi responsables que ces points soient traités, il leur incombe de s'assurer de la mise en œuvre correcte des exigences. Avec les processus de validation mis en œuvre, l'OFIT ne peut pas garantir, ni techniquement ni procéduralement, que les développeurs tant internes qu'externes mettent en œuvre les exigences. Il a toutefois créé de bonnes bases qui devraient être utilisées par les équipes de développement.

2.4 Des possibilités licites existent pour contourner les tests prévus dans les pipelines

Les pipelines CNCICD standard lancent des tests automatiques qui vont rechercher des vulnérabilités dans le code d'une application et les composantes qui lui sont liées. Divers niveaux de gravité sont définis en fonction de l'importance du défaut constaté. Le résultat des tests est consigné automatiquement dans les journaux d'exécution des chaînes CNCICD. Les développeurs peuvent ainsi éditer la liste des vulnérabilités détectées auxquelles ils devront remédier. Pour cinq des outils de contrôle, les résultats ne peuvent pas être ignorés. Pour trois d'entre eux, un échec lié à des défauts d'un niveau de gravité élevé provoque l'interruption de la chaîne CI/CD et l'artefact ne peut pas être déployé.

Toutefois, dans certains cas des faux positifs peuvent se produire : le test signale par exemple la présence d'une vulnérabilité alors qu'en réalité elle n'est pas avérée ou ne s'applique pas. La chaîne est interrompue à tort et l'artefact concerné ne peut pas être déployé. Dans d'autres cas, les bénéficiaires de prestations peuvent être dans l'obligation de déployer rapidement une application et ils sont prêts à accepter le risque lié à la vulnérabilité détectée.

Pour traiter ces cas de figure, le processus CNCICD prévoit la possibilité de définir des exceptions (« whitelist »). Celles-ci signalent que pour un artefact particulier, le processus doit passer outre le signalement d'une vulnérabilité donnée. La définition d'exceptions doit respecter plusieurs conditions : le bénéficiaire de prestations doit éditer et signer un formulaire de demande. L'exception est temporaire et un calendrier de remise en conformité doit être défini. Enfin, la demande doit être validée par deux représentants de l'OFIT. Quand ces conditions sont réunies, l'échec d'un test peut être contourné, mais il est consigné dans le journal de l'exécution des étapes du pipeline.

2.5 L'intégrité des pipelines ne peut pas encore être complètement assurée

La configuration des pipelines CNCICD et des images de base est gérée par les spécialistes de l'OFIT, qui sont les seuls à posséder les droits d'accès nécessaires à ces activités. Quand les clients veulent utiliser ces éléments, ils les instancient et travaillent sur des copies des originaux. Dans certains cas de figure, il est possible de désactiver des contrôles obligatoires dans ces copies. Ces pipelines dépourvus de contrôles peuvent alors en principe être utilisés pour déployer des solutions applicatives vers la plateforme RHOS productive. Des artefacts compromis peuvent ainsi être mis en production de manière non conforme.

Les étapes de ces mises en production illicites sont consignées dans les journaux d'exécution des pipelines, si bien qu'on peut les détecter après coup. Par contre, la protection en amont de l'intégrité des pipelines n'est pas encore complètement assurée. La mise en œuvre d'un système de signature cryptographique des définitions des pipelines était dans le périmètre du programme Amboss. Des versions abouties d'outils à cet effet et compatibles avec la plateforme CNCICD ne sont toutefois pas encore disponibles sur le marché. L'OFIT ne peut pas fournir de calendrier plus précis pour la solution du problème mais garde cette lacune dans sa liste de points à régler.

APPRÉCIATION

Parce qu'il doit être documenté en amont, qu'il a une durée de validité réduite et que ses effets sont consignés dans les journaux d'exécution des pipelines, le procédé des demandes d'exception constitue une entorse contrôlée à l'obligation de tester les applications avant leur mise en production.

La protection des pipelines est par contre encore insuffisante en l'état. Des risques existent que cette lacune soit utilisée pour contourner l'obligation de test et mettre en production des solutions applicatives non conformes, même si cela présuppose un effort conséquent. Puisqu'une détection a posteriori par l'analyse des journaux est possible et que cette lacune reste sur la liste des points ouverts de l'OFIT, le CDF renonce à une recommandation.

2.6 Des travaux sont en cours pour les activités d'ordre supérieur mais la perspective du SCI doit être renforcée

Un comité CI/CD, actif depuis janvier 2024, traite des questions de pilotage et de développement des pipelines CNCICD. Il sert d'interface entre le domaine Business Solutions (BS), qui s'occupe du portefeuille applicatif mis en œuvre sur les plateformes de l'OFIT pour ses clients, et celui des Platform Services (PS), qui se charge de l'infrastructure mise à disposition. Parmi ses attributions, le comité fournit des prestations de conseil et définit des standards pour les aspects de la sécurité, de l'architecture et du financement des pipelines. Par ailleurs, il inventorie ces derniers, réceptionne et traite les demandes d'extension, et valide leur mise en production. Il peut aussi mandater des audits de la plateforme. Le comité se réunit régulièrement et compte parmi ses membres des représentants des domaines BS et PS et des spécialistes de la sécurité. La perspective du SCI n'est pas contre pas spécifiquement représentée en son sein.

Le comité a élaboré un modèle de référence des pipelines CNCICD, qui en décrit les concepts et les fonctions. D'une part, les exigences de la qualité et la sécurité continues sont rappelées. Les fonctions centrales liées à l'intégration et au déploiement sont énumérées. D'autre part, des fonctions d'ordre supérieur applicables aux pipelines sont définies, liées à la surveillance de leur bonne marche (système de mesures), à la réponse en cas d'incident, à la gestion de leurs versions et à leur gouvernance.

Au moment de l'audit du CDF, le modèle de référence était encore en cours de validation. En conséquence, les processus de controlling et de surveillance des pipelines, de même que les détails des responsabilités de l'exploitation, n'étaient pas encore tous formellement définis et pleinement opérationnalisés. Diverses activités d'ordre supérieur ont néanmoins déjà été menées et des outils mis en œuvre pour suivre le fonctionnement des plateformes CNCICD et de détecter les éventuelles lacunes :

- Des contrôles de sécurité ont été menés fin 2023 sur sept types de pipelines. Des lacunes et des propositions de solution ont été documentées. Ces contrôles se font sur demande, il n'est pas prévu pour l'instant de les effectuer périodiquement.
- Les processus et les responsabilités définis à l'OFIT pour le traitement des lacunes et des incidents de sécurité s'appliquent aussi à la plateforme CNCICD et sont opérationnels. Un exemple de vulnérabilité critique découverte fin mars 2024 dans le monde Linux[3] a ainsi poussé les spécialistes de sécurité de l'OFIT à analyser rapidement les composantes de la plateforme et les solutions applicatives liées (elles n'étaient pas affectées).
- Plusieurs outils de surveillance et de mesure du bon fonctionnement des pipelines existent, un reporting périodique en bonne et due forme n'est par contre pas encore en place. Sur cette thématique, les travaux sont en cours.
- De tels outils existent aussi pour le contrôle périodique des objets constituant les solutions applicatives en cours de développement et en production.

[3] Découverte d'une porte dérobée sur le logiciel XZ Utils, 29 mars 2024, vulnérabilité CVE-2024-3094 sur le site du National Institute of Standards and Technology www.nist.gov.

Au chapitre du système de contrôle interne, le CDF n'a pas pu évaluer l'efficacité des contrôles mis en place dans les pipelines CNCICD.

Le procédé aurait consisté à tirer un échantillon des mises en production sur la plateforme RHOS, et pour chaque cas, analyser les journaux des événements survenus dans l'exécution de la chaîne CI/CD, notamment le résultat des exécutions de tests. Les systèmes de mesure et de journalisation gardent ces données, mais leur regroupement en fonction d'une mise en production et leur représentation synthétique sont malaisés pour l'instant. L'OFIT a pu reconstituer ces informations pour un cas de solution applicative en production sur la plateforme RHOS, mais le procédé n'est pas encore industrialisé.

APPRÉCIATION

Les bases pour la définition et la mise en œuvre des activités d'ordre supérieur (pilotage, direction du développement futur de la plateforme, surveillance) sont globalement posées : Un comité CI/CD ad hoc se réunit régulièrement, un cadre de référence est en passe d'être adopté. De telles activités sont d'ailleurs déjà menées, soutenues par une palette d'outils déjà opérationnels (journalisation des événements, contrôle de la sécurité). Les processus et responsabilités liés à ce cadre de référence ne sont toutefois pas encore tous définis et institutionnalisés. Au vu de l'agenda du comité CI/CD, le CDF estime toutefois que l'OFIT est en voie de poursuivre les travaux vers une meilleure opérationnalisation des activités d'ordre supérieur et un renforcement de la gouvernance de la plateforme. Sur ce point, il renonce à une recommandation. Par contre, le CDF considère que la perspective et les exigences du SCI sont encore insuffisamment prises en compte au sein du comité CI/CD et dans sa feuille de route.

RECOMMANDATION 1 — PRIORITÉ 1

Le CDF recommande à l'OFIT d'assurer la représentation de la perspective du système de contrôle interne au sein du comité CI/CD et de mieux en intégrer les exigences dans son agenda.

PRISE DE POSITION DE OFFICE FÉDÉRAL DE L'INFORMATIQUE ET DE LA TÉLÉCOMMUNICATION

La recommandation est acceptée.

Das BIT akzeptiert die Empfehlung. Das Change Management der Pipelines wird durch das CI/CD Board weitgehend koordiniert. Der Prozess ist dokumentiert. Darin wird stets vor Produktivsetzung ein Code-Review durchgeführt (hinsichtlich Sicherheit und Qualität). Der Vorsitz vom CI/CD Board BS/PS inklusive einer Person mit Verantwortlichkeiten im Bereich des IKS (Kontrollen im Bereich des Change Managements bezüglich der Produktivsetzung). Gleichzeitig laufen durch das CTO Arbeiten, um die Entscheidungskompetenzen der verschiedenen Boards und Arbeitsgruppen zu schärfen. Gleichzeitig wird mit dem BIT Change Management die Freigabe von Pipelines (Änderungen, Neuerstellung) abgestimmt. Vor der Produktivsetzung einer neuen respektive geänderten Pipeline wird auch zukünftig eine Stichprobe durchgeführt hinsichtlich der inhaltlichen Passung des produktiv zu setzendenden Codes und den entsprechenden Jira Tickets stammend von genehmigten Aufträgen (Changes, Bug Fixes, etc.) und des korrekten Funktionierens des Code Reviews. Es wird geprüft, ob man unter Berücksichtigung des Kosten-Nutzenverhältnis die Logs der Pipelineruns noch schneller und effizienter darstellen kann.

ANNEXE 1 – DIRECTIVES ET STRATÉGIES

DIRECTIVES

Directive sur la Protection informatique de base dans l'administration fédérale du 1er mars 2022, Version 5.0, Centre national pour la cybersécurité NCSC

STRATÉGIES

Stratégie d'informatique en nuage de l'administration fédérale du 18 décembre 2020, Secteur Transformation numérique et gouvernance informatique de la Chancellerie fédérale.

ANNEXE 2 – ABRÉVIATIONS

BS	Business Solutions (domaine de l'OFIT)
CDF	Contrôle fédéral des finances
OFIT	Office fédéral de l'informatique et de la télécommunication
PS	Platform Services (domaine de l'OFIT)
SCI	Système de contrôle interne

ANNEXE 3 – GLOSSAIRE

Agilité	Ensemble de principes et de pratiques utilisés entre autres dans l'ingénierie logicielle. L'agilité se caractérise par la collaboration entre des équipes auto-organisées et leurs clients, la fixation autonome des objectifs et des cycles itératifs de développement.
Amboss	Programme de l'OFIT visant au renouvellement de l'environnement de gestion des conteneurs informatiques sur le cloud privé Atlantica. Le passage du produit Cloud Foundry à Red Hat OpenShift, ainsi que la mise en œuvre d'une plateforme automatisée pour l'intégration et le déploiement continus, sont notamment dans le périmètre du programme.
Base image	Environnement en conteneur entièrement configuré, auto-suffisant et exempt de vulnérabilités pouvant servir de base à un développement applicatif.
CAE	Prestation de marché de l'OFIT visant à offrir un cadre pour la mise en œuvre d'un environnement d'application en conteneurs (angl. *Container application environment*).
Cloud natif (CN)	Approche d'ingénierie logicielle visant à une exploitation d'un maximum des nouvelles possibilités offertes par les architectures de type cloud.
CNCICD	Abréviation utilisée par l'OFIT pour caractériser ses processus et chaînes d'outils automatisés permettant une mise en œuvre de solutions applicatives selon une approche cloud natif (CN), en passant par des étapes d'intégration (CI) et de déploiement continus (CD).
Conteneur	Paquet logiciel unique regroupant le code d'une application, les fichiers de configuration, les bibliothèques et les dépendances requises pour que l'application puisse s'exécuter. En grande partie auto-suffisant, il peut facilement être déplacé et exécuté sur une infrastructure quelconque.
Déploiement continu (CD)	Processus de livraison de logiciels qui utilise des tests automatisés pour valider si les changements apportés à une base de code sont corrects et stables en vue d'un déploiement autonome immédiat dans un environnement de production.
DevOps	Philosophie et ensemble de pratiques techniques de l'ingénierie informatique pour l'intégration des rôles du développement et de l'administration des infrastructures.
Exigences non-fonctionnelles	Exigences décrivant des propriétés que le système doit avoir, par exemple en matière de sécurité, de performance, de disponibilité, etc. Par contraste, les exigences fonctionnelles décrivent ce que le système doit être capable de faire, quelles fonctions il doit soutenir (« règles métier »).
GitOps	Approche systématique de contrôle des versions pour le développement d'éléments d'infrastructure et d'applications.
HERMES	HERMES est une méthode de management de projets pour l'informatique, les services et prestations de services ainsi que l'organisation des affaires. Elle a été développée au sein de l'administration fédérale.
Informatique en nuage	Modèle de fourniture de prestations consistant à utiliser des serveurs informatiques à distance, hébergés dans des centres de données connectés à Internet pour stocker, gérer et traiter des données, plutôt qu'un serveur local ou un ordinateur personnel (angl. *cloud computing*).

Intégration continue (CI)	Pratique de génie logiciel qui consiste à automatiser l'intégration des changements de code réalisés par plusieurs contributeurs dans un seul et même projet de développement.
Nuage privé	Dans la stratégie d'informatique en nuage de l'administration fédérale, modèle d'approvisionnement consistant à mettre à disposition des services informatiques opérés sur la propre infrastructure de la Confédération (par opposition au nuage public).
Pipeline	Dans le contexte du génie logiciel, chaîne d'outils et de processus soutenant diverses étapes de l'intégration et du déploiement de solutions applicatives.
Red Hat OpenShift (RHOS)	Plateforme de l'éditeur Red Hat, permettant de gérer l'infrastructure et les environnements soutenant les applications en conteneur.
SAFe	Scaled Agile Framework, modèle d'organisation et de processus destiné à déployer la méthode agile à grande échelle.
VTKG	Solution applicative du Groupement Défense soutenant la gestion des dossiers vétérinaires (en allemand *Verwaltung der Tierkrankengeschichten*).
Whitelist	Liste d'exceptions définies comme ne présentant pas de risque de malveillance.
Zero Trust	Stratégie de sécurité informatique selon laquelle aucun appareil connecté à un système ne doit recevoir des accès par défaut.