

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE



Audit du projet Virtual Center

Skyguide

Bestelladresse	Contrôle fédéral des finances (CDF)
Adresse de commande	Monbijoustrasse 45
Indirizzo di ordinazione	3003 Berne
Ordering address	Suisse
Bestellnummer	1.19120.961.00483
Numéro de commande	
Numero di ordinazione	
Ordering number	
Zusätzliche Informationen	www.efk.admin.ch
Complément d'informations	info@efk.admin.ch
Informazioni complementari	twitter: @EFK_CDF_SFAO
Additional information	+ 41 58 463 11 11
Abdruck	Gestattet (mit Quellenvermerk)
Reproduction	Autorisée (merci de mentionner la source)
Riproduzione	Autorizzata (indicare la fonte)
Reprint	Authorized (please mention source)

Table des matières

L'essentiel en bref	4
Das Wesentliche in Kürze.....	6
L'essenziale in breve	9
Key facts.....	11
1 Mission et déroulement	14
1.1 Contexte	14
1.2 Objectif et questions d'audit	14
1.3 Etendue de l'audit et principe	15
1.4 Documentation et entretiens	15
1.5 Discussion finale	15
2 Pilotage, conduite et situation du programme	17
2.1 Un démarrage adéquatement mené.....	17
2.2 Le pilotage complexe reflète l'ampleur de la tâche	17
2.3 Des incertitudes pèsent sur le financement.....	18
2.4 La conduite de programme est globalement adaptée à la situation.....	19
2.5 ... mais la gestion des risques doit gagner en indépendance... ..	21
2.6 ... et la communication doit être mieux ciblée	22
2.7 Le programme VCT2 livre, mais avec du retard	23
3 Développement, déploiement et exploitation.....	25
3.1 Les défis des nouvelles démarches de développement	25
3.2 La mise en œuvre de l'architecture doit être mieux suivie	26
3.3 La sécurité de l'information mérite plus d'attention	27
3.4 Les tests sont menés de manière convaincante.....	29
3.5 L'organisation du déploiement et la préparation du domaine métier sont adéquates.	30
3.6 La difficile mutation de l'exploitation informatique.....	31
Annexe 1 : Bases légales	33
Annexe 2 : Abréviations	34
Annexe 3 : Glossaire	35

Audit du projet Virtual Center

Skyguide

L'essentiel en bref

Elément central dans la stratégie de Skyguide, le programme Virtual Center s'inscrit dans le contexte de l'évolution de l'espace aérien européen. Il vise à réaliser un système suisse de gestion du trafic aérien harmonisé entre les deux principaux sites de Wangen et de Genève ainsi qu'une plateforme technique commune. Le programme, initialement devisé à 262 millions de francs, comporte trois tranches, échelonnées entre 2011 et 2024.

Dans son audit, le Contrôle des finances (CDF) se focalise sur la deuxième tranche du programme (VCT2). Ce paquet pose les fondations d'une gestion des secteurs aériens indépendante des sites et établit de nouvelles méthodes de travail. Devisée à 122,5 millions de francs, cette tranche a démarré en 2016. Le CDF en a examiné le pilotage et la conduite, de même que la pertinence de son reporting et la fiabilité de la planification financière à moyen terme. Enfin, il s'est assuré de la prise en compte des exigences de la sécurité de l'information.

Lors de la révision, de nombreux résultats ont déjà été mis en œuvre. Cependant, le programme subit des retards et des dépassements de coûts sont à prévoir. Raison pour laquelle la direction du programme VCT2 recommande, entre autres, une hausse du budget à 133 millions de francs (+ 8 %), une fin des travaux en 2020 et une réduction du périmètre du programme.

Le pilotage et la conduite du programme sont globalement adaptés à l'ampleur de la tâche...

Le démarrage de VCT2 a été correctement mené, la priorisation du programme dans le portefeuille d'activités de Skyguide a été validée par la direction. L'organisation du programme et l'implication des instances dirigeantes et des offices fédéraux concernés sont adéquates. Basé sur des tranches de travail annuelles, le pilotage offre une mise en service par étape des résultats.

Les bases de la conduite du programme sont complexes mais appropriées. Le CDF relève notamment une démarche de planification et de suivi à plusieurs niveaux et l'emploi de méthodes de travail agiles. Le CDF n'a pas trouvé d'élément mettant en doute la pertinence et la validité des états permettant le suivi de l'avancement des travaux. Il estime globalement adéquats l'organisation et le processus de gestion de la qualité au sein du programme.

... mais des aménagements sont à prévoir et des incertitudes pèsent sur le financement

Le CDF estime aussi le processus de gestion des risques de VCT2 approprié. Il relève toutefois que sa responsabilité est confiée au directeur du programme et que l'indépendance de la fonction n'est pas assurée. Il a fait une recommandation pour corriger cet état de fait.

Lors de la révision, les plus grands risques identifiés concernent la gestion du changement organisationnel. Malgré les efforts consentis en termes de communication, la résistance au changement est difficile à surmonter. Pour faciliter la gestion du changement, le CDF a recommandé d'appliquer des mesures pour renforcer l'efficacité de la communication.

Dans son analyse de la capacité de financement, le CDF relève que le 80% du montant des redevances encaissées par Skyguide est régulé par la Commission européenne. Il est basé sur un plan de performance quinquennal soumis à l'approbation de Bruxelles. Durant la révision, Skyguide élaborait son plan pour la période dès 2020. Selon la décision de la Commission, l'entreprise pourrait se trouver face à des difficultés de financement à moyen terme. Le CDF encourage Skyguide dans sa volonté de prévoir dès l'automne 2019 des stratégies de financement alternatives pour assurer la continuité de l'exploitation.

La transition vers les nouvelles démarches de développement est en cours

Le CDF constate que la transition vers les nouvelles méthodes de travail – comme l'agilité ou les cycles de livraison courts – est en cours. Les utilisatrices et les utilisateurs peuvent formuler leurs exigences, et des prototypes sont réalisés. Les outils et plateformes mis en œuvre sont bien établis. Néanmoins, plusieurs aspects délicats doivent continuer d'être affinés (par exemple, les modalités des approbations dans des cycles courts de livraison). Les bases de la démarche architecturale sont définies, notamment les architectures de départ, la cible et les transitions annuelles nécessaires. Néanmoins, l'évaluation de l'atteinte des étapes de transition annuelles et leur actualisation ne s'est pas faite systématiquement. Le CDF insiste pour que celles-ci aient lieu dès l'automne 2019 comme prévu.

Les tests sont menés de manière professionnelle avec l'implication active des utilisatrices et des utilisateurs. Le CDF attend toutefois que les exigences en matière de sécurité de l'information soient mieux intégrées dans les tests. Leurs résultats sont intégrés dans les processus de validation avant les mises en service. Pour le déploiement des paquets de fonctionnalité, des étapes claires sont définies et suivies. Le domaine métier est activement impliqué dans la préparation des mises en service (formation, support). Malgré cela, des problèmes peuvent survenir après un déploiement. Des moyens appropriés sont mis en œuvre pour les prendre en charge.

Les défis de la sécurité et de l'exploitation informatique

Pour le CDF, les exigences accrues en matière de sécurité de l'information ne sont pas suffisamment prises en compte au sein du programme. Les instruments utilisés actuellement ne permettent pas une définition concrète et un suivi rigoureux des objectifs à atteindre en la matière. La situation en termes de protection et les risques résiduels ne sont pas clairement représentés. Les instances de pilotage ne peuvent ainsi pas les traiter en conséquence. Le CDF a recommandé à Skyguide de remédier à la situation.

Avec l'évolution technique de VCT2 et la délocalisation d'une partie des activités en Bulgarie, le rôle de l'exploitation informatique change. Le CDF a relevé des frictions dans les flux de travail, comme dans les interfaces avec les prestataires externes. Il recommande d'analyser et d'optimiser ces processus, de même qu'une surveillance accrue et systématique des activités des utilisatrices et des utilisateurs privilégiés dans les systèmes productifs.

Prüfung des Projekts Virtual Center

Skyguide

Das Wesentliche in Kürze

Das Programm Virtual Center ist ein zentrales Element der Strategie von Skyguide und ist im Kontext der Entwicklung des europäischen Luftraums zu sehen. Es zielt darauf ab, zwischen den beiden wichtigsten Standorten Wangen und Genf ein harmonisiertes Schweizer Flugverkehrsmanagementsystem sowie eine gemeinsame technische Plattform zu schaffen. Das Programm mit einem Budget von ursprünglich 262 Millionen Franken ist zwischen 2011 und 2024 in drei Etappen aufgeteilt.

Die Eidgenössische Finanzkontrolle (EFK) konzentriert sich in ihrer Prüfung auf die zweite Etappe des Programms (VCT2). In diesem Massnahmenpaket werden die Grundlagen eines standortunabhängigen Luftraummanagements gelegt und neue Arbeitsmethoden eingeführt. Die zweite Etappe ist mit einem Budget von 122,5 Millionen Franken versehen und wurde 2016 in Angriff genommen. Die EFK hat die Steuerung und die Führung sowie die Stichhaltigkeit des Reportings und die Zuverlässigkeit der mittelfristigen Finanzplanung geprüft. Schliesslich hat die EFK untersucht, ob den Anforderungen an die Informationssicherheit Rechnung getragen wird.

Viele Ergebnisse wurden schon während der laufenden Prüfung umgesetzt. Es zeichnen sich jedoch Verzögerungen im Programm ab, zudem sind Kostenüberschreitungen zu erwarten. Aus diesem Grund empfiehlt die Leitung des Programms VCT2 unter anderem eine Aufstockung des Budgets auf 133 Millionen Franken (+8 %), den Abschluss der Arbeiten im Jahr 2020 und eine Reduktion des Programmperimeters.

Die Steuerung und Führung des Programms werden im Grossen und Ganzen der Bedeutung der Aufgabe gerecht...

Der Programmstart von VCT2 erfolgte ordnungsgemäss, die Priorisierung des Programms im Tätigkeitsportefeuille von Skyguide wurde von der Direktion validiert. Die Programmorganisation und der Einbezug der leitenden Gremien und der betroffenen Bundesämter sind angemessen. Die auf jährlichen Arbeitsetappen basierende Steuerung sieht eine schrittweise, auf die Ergebnisse abgestimmte Inbetriebnahme vor.

Die Grundlagen der Programmführung sind komplex, aber angemessen. Die EFK hebt unter anderem die mehrstufige Planung und Überwachung und den Einsatz agiler Arbeitsmethoden hervor. Die EFK hat keine Anhaltspunkte gefunden, welche die Relevanz und die Stichhaltigkeit des Berichtswesens, die die Kontrolle des Projektfortschritts ermöglichen, infrage stellen würden. Die EFK ist der Meinung, dass die Organisation und der Qualitätssicherungsprozess im Programm im Allgemeinen angemessen sind.

... es sind aber Anpassungen zu erwarten und die Finanzierung ist nicht gesichert

Die EFK erachtet auch den Risikomanagementprozess von VCT2 als geeignet. Sie weist jedoch darauf hin, dass dessen Verantwortung beim Programmdirektor liegt und die Unabhängigkeit der Funktion nicht gewährleistet ist. Sie hat eine Empfehlung abgegeben, um dies zu korrigieren.

Die grössten bei der Prüfung festgestellten Risiken betreffen das organisatorische Change-Management. Trotz der Bemühungen im Bereich der Kommunikation hält sich ein hartnäckiger Widerstand gegen die anstehende Veränderung. Um das Change-Management zu vereinfachen, hat die EFK Massnahmen für eine wirksamere Kommunikation empfohlen.

Die EFK hält in ihrer Analyse der Finanzkapazität fest, dass 80 % der von Skyguide eingenommenen Gebühren durch die Europäische Kommission reguliert sind. Der Betrag beruht auf einem Fünf-Jahres-Leistungsplan, der von Brüssel genehmigt werden muss. Während der Prüfung arbeitete Skyguide seinen Plan für den Zeitraum ab 2020 aus. Je nach Entscheidung der Kommission könnte das Unternehmen mittelfristig mit Finanzierungsschwierigkeiten konfrontiert werden. Die EFK unterstützt die Absicht von Skyguide, ab Herbst 2019 für alternative Finanzierungsstrategien zu sorgen, um die Kontinuität des Betriebs sicherzustellen.

Der Übergang zu den neuen Entwicklungsansätzen ist im Gange

Die EFK stellt fest, dass der Übergang zu den neuen Arbeitsmethoden (u. a. Agilität, kurze Lieferrhythmen) eingesetzt hat. Die Userinnen und User können ihre Erwartungen formulieren und es werden Prototypen realisiert. Die umgesetzten Tools und Plattformen sind solide etabliert. Es gibt allerdings mehrere heikle Aspekte, an denen noch weitergearbeitet werden muss (bspw. die Modalitäten der Validierungen in kurzen Lieferzyklen). Die Grundlagen des architektonischen Vorgehensmodells sind definiert, insbesondere die Ist-Architektur, die Ziel-Architektur und die notwendigen jährlichen Übergänge. Dennoch wurden weder die Erreichung der jährlichen Übergänge noch deren Aktualisierung systematisch evaluiert. Die EFK beharrt darauf, dass dies ab Herbst 2019 wie geplant stattfindet.

Die Tests werden unter aktivem Einbezug der Userinnen und User professionell durchgeführt. Die EFK erwartet jedoch, dass die Anforderungen im Bereich der Informationssicherheit besser in die Tests integriert werden. Ihre Ergebnisse werden vor den Inbetriebnahmen in die Validierungsprozesse integriert. Für die Verteilung der Funktionspakete werden klare Etappen definiert und befolgt. Der Fachbereich ist aktiv an der Vorbereitung der Inbetriebnahmen beteiligt (Ausbildung, Support). Trotzdem können nach einer Installation Probleme auftreten. Es werden geeignete Massnahmen zur Lösung allfälliger Probleme getroffen.

Die Herausforderungen der Sicherheit und des Informatikbetriebssystems

Der EFK zufolge werden die höheren Anforderungen an die Informationssicherheit im Programm nicht ausreichend berücksichtigt. Die derzeit zum Einsatz kommenden Instrumente erlauben keine konkrete Definition und keine strenge Überwachung der angestrebten Ziele. Hinsichtlich des Schutzbedarfs und der Restrisiken wird die Situation nicht eindeutig abgebildet. Die Steuerungsorgane können deshalb keine entsprechende Risikobehandlung vornehmen. Die EFK hat Skyguide empfohlen, Abhilfe zu schaffen.

Die Rolle des Informatikbetriebs verändert sich im Zuge der technischen Entwicklung von VCT2 und der Auslagerung mancher Aktivitäten nach Bulgarien. Die EFK hat festgestellt,

dass es in den Arbeitsabläufen sowie an den Schnittstellen mit den externen Leistungserbringern Reibungen gibt. Sie empfiehlt eine Analyse und Optimierung dieser Prozesse sowie eine verstärkte und systematische Überwachung der Tätigkeiten der privilegierten Userinnen und User in den Produktionssystemen.

Originaltext auf Französisch

Verifica del progetto Virtual Center

Skyguide

L'essenziale in breve

Elemento fondamentale della strategia di Skyguide, il programma Virtual Center rientra nel contesto dell'evoluzione dello spazio aereo europeo e mira a creare un sistema svizzero di gestione del traffico aereo armonizzato tra i due principali siti di Wangen e Ginevra e una piattaforma tecnica comune. Il programma, la cui stima dei costi ammontava inizialmente a 262 milioni di franchi, è suddiviso in tre tranches, scaglionate tra il 2011 e il 2024.

Nella sua verifica, il Controllo federale delle finanze (CDF) si è concentrato sulla seconda parte del programma (VCT2), che getta le fondamenta per una gestione dei settori aerei indipendente dai siti e definisce nuovi metodi di lavoro. Essa è iniziata nel 2016, per un costo stimato di 122,5 milioni di franchi. Il CDF ne ha esaminato la direzione e la gestione, così come la pertinenza del suo reporting e l'affidabilità della pianificazione finanziaria a medio termine. Infine, si è accertato che i requisiti in materia di sicurezza dell'informazione fossero presi in considerazione.

Durante la revisione sono già stati attuati numerosi risultati. Tuttavia il programma registra ritardi e si prevedono sforamenti nei costi. Di conseguenza, la direzione del programma VCT2 raccomanda, tra l'altro, di aumentare il preventivo a 133 milioni di franchi (+ 8 %), di completare i lavori entro il 2020 e di ridurre il raggio d'azione del programma.

La direzione e la gestione del programma sono complessivamente in linea con l'importanza del compito...

L'avvio del programma VCT2 è stato effettuato correttamente, l'attribuzione di un ordine di priorità al programma all'interno del portafoglio di attività di Skyguide è stata convalidata dalla direzione. L'organizzazione del programma e il coinvolgimento degli organi dirigenziali e degli Uffici federali interessati risultano opportuni. Basandosi su tranches di lavoro annue, la direzione garantisce un'applicazione graduale dei risultati.

Le basi relative alla gestione del programma sono complesse ma opportune. Il CDF sottolinea in particolare un approccio di pianificazione e di verifica su più livelli e l'impiego di metodi di lavoro agili. Il CDF non ha riscontrato elementi che mettano in dubbio la pertinenza e la validità delle condizioni che permettono di verificare l'avanzamento dei lavori. Complessivamente ritiene che l'organizzazione e il processo di gestione della qualità all'interno del programma siano adeguati.

... tuttavia sono da prevedere adeguamenti e permangono incertezze sul finanziamento

Il CDF ritiene anche che il processo di gestione dei rischi concernenti la tranche VCT2 sia opportuno. Sottolinea tuttavia che la sua responsabilità è affidata al direttore del programma, pertanto non viene garantita l'indipendenza della funzione. Ha dunque formulato una raccomandazione per rimediare a tale situazione.

Durante la revisione, i maggiori rischi individuati hanno riguardato la gestione del cambiamento organizzativo. Malgrado gli sforzi consentiti a livello di comunicazione, le resistenze

nei confronti del cambiamento sono difficili da superare. Per facilitare la gestione del cambiamento, il CDF raccomanda di applicare misure per rafforzare l'efficacia della comunicazione.

Nella sua analisi sulla capacità di finanziamento, il CDF sottolinea che l'80 per cento dell'importo dei canoni riscossi da Skyguide è regolamentato dalla Commissione europea. Nello specifico, si basa su un piano di prestazioni quinquennale che soggiace all'approvazione di Bruxelles. Durante la revisione, Skyguide ha elaborato la propria pianificazione a partire dal 2020. Secondo la decisione della Commissione, l'impresa potrebbe ritrovarsi ad affrontare difficoltà di finanziamento a medio termine. Il CDF incoraggia Skyguide nella sua volontà di prevedere, a partire dall'autunno del 2019, strategie di finanziamento alternative per garantire la continuità dell'esercizio.

Transizione in corso verso nuovi approcci di sviluppo

Il CDF osserva che è in atto la transizione verso i nuovi metodi di lavoro come l'agilità o i cicli di consegna brevi. Gli utenti possono formulare le proprie esigenze, in base alle quali vengono poi realizzati prototipi. Gli strumenti e le piattaforme introdotti sono ben consolidati. Tuttavia, occorre definire nel dettaglio vari aspetti peculiari (ad es. le modalità di approvazione all'interno di cicli brevi di consegna). Le basi del processo architettonico sono definite, in particolare le architetture di partenza, l'obiettivo e le transizioni annue necessarie. Ciononostante la stima concernente il raggiungimento delle fasi di transizione annue e il relativo aggiornamento non sono stati effettuati sistematicamente. Il CDF insiste affinché questi punti si svolgano a partire dall'autunno del 2019 come concordato.

I test sono realizzati in modo professionale con il coinvolgimento attivo degli utenti. Tuttavia il CDF si aspetta che le esigenze in materia di sicurezza dell'informazione vengano meglio integrate nei test. I risultati sono inseriti nel processo di convalida prima dell'effettiva messa in esercizio. Per quanto concerne l'introduzione dei pacchetti di funzionalità, sono definite e seguite tappe precise. Il settore specialistico è attivamente coinvolto nella preparazione della messa in esercizio (formazione, supporto). Tuttavia possono verificarsi problemi dopo l'introduzione. Per risolvere tali difficoltà vengono adottate misure opportune.

Sfide in materia di sicurezza e di esercizio dei sistemi informatici

Per il CDF, gli elevati requisiti in materia di sicurezza dell'informazione non sono sufficientemente presi in considerazione all'interno del programma. Gli strumenti utilizzati attualmente non consentono una definizione concreta e una verifica approfondita degli obiettivi da raggiungere al riguardo. La situazione in termini di protezione e rischi residui non sono presentati in modo chiaro. Date le circostanze, le istanze di direzione non possono trattarli in modo efficace. Il CDF ha consigliato a Skyguide di porre rimedio alla situazione.

Dopo l'evoluzione tecnica della tranche VCT2 e il trasferimento di una parte delle attività in Bulgaria, il ruolo dell'esercizio dei sistemi informatici cambia. Il CDF ha constatato attriti nei flussi di lavoro e nelle interfacce con i fornitori esterni. Esso raccomanda di analizzare e di ottimizzare questi processi e di esercitare una vigilanza approfondita e sistematica sulle attività degli utenti privilegiati nei sistemi produttivi.

Testo originale in francese

Audit of the Virtual Centre project

Skyguide

Key facts

The Virtual Centre Programme is a key component of skyguide's strategy and is part of the ongoing developments in European airspace. Its aim is to create a harmonised Swiss air traffic management system between the two main sites in Wangen and Geneva, as well as a common technical platform. Initially budgeted at CHF 262 million, the programme is to be implemented in three stages between 2011 and 2024.

In its audit, the Swiss Federal Audit Office (SFAO) focused on stage 2 of the programme (VCT2). This lays the foundations for location-independent air traffic management and establishes new working methods. The second tranche, budgeted at CHF 122.5 million, began in 2016. The SFAO examined the steering and management of VCT2, as well as the relevance of its reporting and the reliability of its medium-term financial planning. Finally, it ensured that information security requirements were considered.

Many outcomes had already been implemented at the time of the audit. However, the programme is experiencing delays and cost overruns are to be expected. For this reason, the VCT2 programme management recommends, among other things, increasing the budget to CHF 133 million (+8%), completing the work in 2020 and reducing the scope of the programme.

Programme steering and management are generally adapted to the scale of the task...

VCT2 was correctly initiated and the prioritisation of the programme in skyguide's portfolio of activities was validated by management. The programme's organisation and the involvement of the governing bodies and federal offices concerned are adequate. The steering system, based on annual work stages, provides for a step-by-step commissioning process based on the results.

The basis for programme management is complex but appropriate. The SFAO noted in particular a multi-level planning and monitoring process and the use of agile working methods. The SFAO did not find any reason to doubt the relevance and validity of the conditions for monitoring work progress. Overall, the SFAO considers the organisation and the quality management process within the programme to be adequate.

... but changes are to be expected and financing uncertainties exist

The SFAO also considers the risk management process for VCT2 to be appropriate. However, the SFAO highlighted that the Programme Director is responsible for this process and that the independence of his role is not assured. The SFAO recommended correcting this.

During the audit, the greatest risks identified concerned the management of organisational change. Despite the efforts made in terms of communication, resistance to change is difficult to overcome. In order to facilitate change management, the SFAO recommended implementing measures to enhance the effectiveness of communication.

In its analysis of skyguide's financing capacity, the SFAO observed that 80% of the fees collected are regulated by the European Commission. This is based on a five-year performance plan which is submitted to Brussels for approval. During the audit, skyguide was preparing its plan for the period from 2020 onwards. Depending on the Commission's decision, the company could face financing difficulties in the medium term. The SFAO supports skyguide in its intention to plan alternative financing strategies from autumn 2019 in order to ensure the company's continued operation.

Transition to new development approaches under way

The SFAO noted that the transition towards new working methods, such as agility or short delivery cycles, is under way. Users can specify their requirements and prototypes are being produced. The tools and platforms implemented are well established. Nevertheless, several sensitive aspects need further refinement (e.g. the arrangements for approvals in short delivery cycles). The foundations for the architectural approach are defined, including the starting architectures, the target and the necessary annual transitions. However, the evaluation of the achievement of the annual transition milestones and their updating have not been systematic. The SFAO insists that this should be done from autumn 2019 as planned.

The tests are conducted professionally and users are actively involved. However, the SFAO expects information security requirements to be better integrated into the tests. Their results are incorporated into the validation processes prior to commissioning. Clear stages are defined and followed for the implementation of the functionality blocks. Skyguide specialists are actively involved in preparing for commissioning (training, support). Despite this, problems can occur after deployment. Appropriate measures are taken to deal with them.

Challenges in IT security and operation

In the SFAO's view, the programme does not take sufficient account of increased information security requirements. The instruments currently used do not allow for a concrete definition and rigorous monitoring of the objectives to be achieved in this area. In terms of protection and residual risks, the situation is not clearly represented. The steering bodies are therefore unable to deal with them accordingly. The SFAO recommended that skyguide remedy the situation.

The technical development of VCT2 and the relocation of some activities to Bulgaria are changing the role of IT operation. The SFAO observed friction in workflows and interfaces with external service providers. It recommends analysing and optimising these processes, as well as ensuring increased and systematic monitoring of privileged users' activities in the production systems.

Original text in French

Prise de position générale de Skyguide

La direction de skyguide remercie le Contrôle fédéral des finances (CDF) et son équipe d'audit pour le travail accompli. L'atmosphère a été constructive et les participants se sont sentis non seulement écoutés mais bien compris. Avec près de 40 personnes interviewées et plus de 200 éléments de preuve recueillis, l'audit a assuré une couverture des activités essentielles du programme et est dans ce sens conforme à son ampleur et à son importance pour skyguide.

Le rapport relate les faits de manière synthétique et précise en étant complètement transparent sur les défis et difficultés d'une telle entreprise. Skyguide partage les appréciations ainsi que les recommandations du rapport. Elle s'engage à poursuivre les efforts relevés dans les appréciations et décrit dans ses prises de position comment elle entend implémenter les recommandations.

Les recommandations et les engagements de skyguide seront insérés dans notre processus et outil de gestion des résultats d'audits. Ils seront suivis conformément au processus d'entreprise existant chez skyguide.

Concernant le volet financier du dossier, depuis le début de la préparation du plan de performance pour la période de référence 2020–2024, skyguide a régulièrement informé les différents organes de la Confédération (OFAC, DETEC, AFF) sur les risques de financement liés aux objectifs de performance économique formulés par la Commission européenne. La sensibilité du compte de résultat aux différents paramètres du plan de performance (notamment le référentiel de départ, les hypothèses de trafic et les objectifs de productivité) a été estimée et régulièrement communiquée. Dans le contexte complexe des discussions avec la Commission et dans lesquelles cette dernière a l'initiative, skyguide estime que la meilleure base de départ pour l'établissement du plan de performance correspond au scénario « best case » présenté au CDF lors de l'audit. Compte tenu de ce choix, il n'est pas utile à ce stade d'estimer la probabilité d'occurrence des deux autres scénarios. Les nouvelles projections de liquidités établies sur la base du scénario retenu et soumis selon le calendrier à la Commission européenne démontrent la viabilité de ce dernier. Conformément au rapport, skyguide va préparer des stratégies alternatives afin d'assurer la continuité de l'exploitation. Toutefois, comme indiqué dans le rapport, la marge de manœuvre est limitée, les activités soumises au plan de performance représentant 80 % du chiffre d'affaires de la société. Les alternatives mentionnées dans le rapport seront bien sûr étudiées, il faut ajouter à cela la possibilité pour la Suisse de contester, en tout ou en partie, les exigences de la Commission européenne. Il convient aussi de mentionner que parmi « la recherche de financement additionnel », le recours à l'actionnariat est une option qui doit être envisagée, en cas de mise en danger de la pérennité de l'entreprise.

Les développements du programme depuis le début de l'audit confirment les conclusions de ce dernier. Skyguide a décidé de procéder séquentiellement dans l'innovation en posant en priorité de solides fondations techniques et opérationnelles sur lesquelles elle pourra bâtir des bénéfices durables à moyen et long terme dans la dernière tranche du « Virtual Center ».

1 Mission et déroulement

1.1 Contexte

L'initiative de ciel unique européen (en anglais « Single European Sky » ou SES) adoptée en 2004 et 2009 par le Parlement européen, a pour but de faire évoluer l'organisation de l'espace aérien. Il s'agit d'en augmenter les capacités et de renforcer l'efficacité et la sécurité du trafic. L'initiative vise à atteindre ces objectifs notamment par la défragmentation des centres et systèmes de services de navigation aérienne. La Suisse est impliquée et a signé en 2010 un traité qui prévoit la mise en place avec cinq autres pays européens d'un bloc d'espace aérien fonctionnel commun.

Le modèle des centres virtuels est une des réponses apportées à la question de la fragmentation des fournisseurs de services de navigation aérienne (en anglais « Air Navigation Service Provider », ANSP). Il consiste à réaliser des arrangements permettant l'interopérabilité technique et opérationnelle entre les ANSP, tout en évitant les fermetures de centres de contrôle aérien.

Après une analyse des options en présence, Skyguide a promu en 2011 la mise en œuvre du concept de Centre Virtuel au rang d'objectif stratégique et a défini le programme « Virtual Center ». Le but est de réaliser un système suisse de gestion du trafic aérien harmonisé entre les deux principaux sites, basé sur une plateforme technique commune.

Le programme, initialement devisé à 262 millions de francs, comporte trois tranches :

- La première tranche (VCT1) vise à mettre en place les mesures minimales d'harmonisation entre les centres de contrôle Est et Ouest, et prépare le terrain pour les tranches suivantes. VCT1 a démarré en janvier 2011 et s'est achevé en septembre 2017, pour des coûts effectifs totaux d'environ 63,5 millions de francs ;
- La deuxième tranche (VCT2) a pour but de créer les fondations techniques d'une gestion des secteurs aériens flexible et indépendante des sites. Cette tranche, lancée officiellement en août 2016 et prévue initialement jusqu'à fin 2020, est devisée à 122,5 millions de francs. Des réflexions sur le périmètre, la date de fin et le budget final de la deuxième tranche sont en cours au moment de la révision ;
- La troisième tranche vise à la pleine mise en œuvre des opérations flexibles entre les deux sites. Elle est prévue de se dérouler entre 2021 et 2024.

1.2 Objectif et questions d'audit

Dans cette révision, le Contrôle fédéral des finances (CDF) évalue la deuxième tranche du programme Virtual Center (ci-après « programme VCT2 ») et les risques pouvant compromettre l'atteinte des objectifs définis. Pour ceci, il utilise la démarche d'audit des projets informatiques clés de la Confédération et vise à répondre aux questions suivantes :

- Le programme se déroule-t-il comme prévu en termes de résultats, de calendrier et de coûts, et est-il piloté de manière adéquate ?
- Est-ce qu'une gestion appropriée des risques et de la qualité est en place ?

- Le reporting adressé aux différents décideurs est-il fiable et plausible, depuis le responsable de l'informatique jusqu'au Parlement, en passant par la direction, le comité des projets du conseil d'administration, le conseil d'administration, la Confédération dans son rôle de propriétaire (Département fédéral de l'environnement, des transports, de l'énergie et de la communication – DETEC – et l'Administration fédérale des finances – AFF) et le Conseil fédéral?
- Des risques accrus existent-ils dans le choix de la solution organisationnelle et technique choisie, y compris dans les domaines de la gestion des fournisseurs, des nouvelles technologies, de l'interaction avec les autres projets de Skyguide et de l'intégration dans la sécurité aérienne européenne ?
- Les exigences accrues relatives à la sécurité de l'information, y compris les cybermenaces, sont-elles prises en compte dans le programme ?
- La planification financière à moyen terme de Skyguide prend-elle en compte de manière adéquate les nombreux gros projets informatiques de l'entreprise ? La planification financière à moyen terme est-elle robuste ?

La représentation de la Confédération au sein du conseil d'administration de Skyguide ne fait pas l'objet de cet audit.

1.3 Etendue de l'audit et principe

L'audit a été mené du 10 juin au 18 juillet 2019. Il a été conduit par André Stauffer (responsable de révision), Virginie Bugnon, Hans Ulrich Wiedmer et Stefan Russian (Deloitte SA), sous la responsabilité de Bernhard Hamberger.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par Skyguide. Les documents (ainsi que 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 28 octobre 2019 en présence des représentants suivants de Skyguide:

- Le président du Comité de direction (CEO)
- La responsable de la Finance et des Services (CFO)
- Le responsable de l'Engineering et Technology
- Le responsable des Operations
- Le responsable du Portfolio et Change Management
- Le responsable du VCT2 Software Factory
- Le responsable de l'audit interne
- Le responsable du programme VCT2.

Le CDF était représenté par :

- Un responsable de centre de compétence
- Le responsable de révision.

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient aux directions d'offices et aux directions d'entreprises, respectivement aux secrétariats généraux et aux conseils d'administration, de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

2 Pilotage, conduite et situation du programme

2.1 Un démarrage adéquatement mené

En 2014, le plan de gestion de programme (« Program charter ») VC définit les motivations du programme, son périmètre, ses objectifs et son intégration dans le contexte du secteur du contrôle aérien européen. Il pose également les premières bases de la démarche de réalisation du programme. Plus tard, les tranches et leur contenu global sont définis.

En 2015, et parallèlement aux travaux de VCT1, des activités relatives à la mise en œuvre des éléments techniques du programme VC sont démarrées. Regroupées au sein de projets, ces activités sont intégrées au portefeuille des projets en cours et potentiels. Divers ateliers de priorisation des projets sont périodiquement conduits au niveau du comité de direction. Au cours de ces réunions, les impacts financiers et organisationnels de chaque projet sont notamment mis en perspective. En 2015, ces ateliers confirment le caractère prioritaire des projets précurseurs de VCT2.

Dès avril 2016, le conseil d'administration et le comité de direction décident de regrouper ces activités et assignent le mandat de définir et de réaliser le programme VCT2. Divers documents détaillent les éléments préparatoires de cette décision : des analyses du contexte de l'évolution du secteur et de coûts-bénéfices sont produites (ces dernières seront révisées en 2018). Le plan de gestion du programme VCT2 décrit le cadre réglementaire, ainsi que les moyens prévus pour en assurer la mise en œuvre. Il contient aussi une description des intervenants externes et de leurs prérogatives. Les principes des relations avec l'organe de surveillance (l'Office fédéral de l'aviation civile, OFAC) sont notamment détaillés. Une analyse des besoins de protection en termes de sécurité de l'information n'est par contre pas disponible à ce stade.

Sur ces bases, le programme VCT2 dans sa forme actuelle démarre officiellement en août 2016.

2.2 Le pilotage complexe reflète l'ampleur de la tâche

Le plan de gestion du programme VCT2 décrit les éléments du pilotage, notamment les instances responsables et leurs attributions :

- Le propriétaire du programme (rôle assumé par le chef de l'informatique) est responsable des résultats de VCT2,
- Le comité de direction pilote le programme, aidé par le comité des projets du conseil d'administration et le comité stratégique VC ; le comité de pilotage VCT2 est un autre organe consultatif au niveau du pilotage du programme,
- Le conseil d'administration, le comité de direction en charge de la gouvernance du changement et le comité de gestion du Virtual Center (UMB+ VC) approuvent les demandes (jalons et changements), selon des compétences formellement définies.

Des instances et représentants de l'Administration fédérale sont impliqués à divers niveaux du pilotage du programme. Le rôle de représentant de la Confédération est joué par le commandant des forces aériennes. Il siège au conseil d'administration et dans le comité des projets du conseil d'administration. Sur un plan plus général, le DETEC et l'AFF suivent l'évolution des affaires de Skyguide. Ils évaluent périodiquement l'atteinte des objectifs

stratégiques qui lui sont assignés, dont VC est une composante. L'entreprise livre les informations nécessaires à ces unités par le biais des rapports de gestion et financiers annuels et par les rapports du conseil d'administration sur la marche des affaires. Ces informations sont complétées par des discussions régulières. Le DETEC et l'AFF ont également la possibilité en tout temps de poser des questions. Ils préparent les informations pour le suivi par le Conseil fédéral et les commissions du Parlement. L'OFAC effectue de son côté un suivi rapproché spécifique de l'évolution du programme et des résultats. Il s'assure notamment du respect des règles sur la sécurité aérienne européenne. Ces unités n'interviennent néanmoins pas directement dans la gestion du programme, dont la responsabilité reste du ressort ultime du conseil d'administration.

Le pilotage fin du programme se base sur un concept de tranches annuelles. Ainsi, le conseil d'administration définit et valide formellement chaque automne un périmètre à réaliser et un budget pour l'année à venir. Dans le même temps, le progrès de l'année écoulée est évalué. Ces éléments sont documentés. Lors de la révision, le périmètre de l'année 2020 se trouvait en préparation, trois scénarios étaient étudiés pour la clôture du programme VCT2.

Appréciation

Pour le CDF, la décision de démarrage du programme VCT2 paraît fondée et correctement documentée. Il estime appropriées les méthodes de priorisation des programmes, le comité de direction peut ainsi régulièrement en réévaluer l'opportunité. Le CDF relève le caractère ambitieux du programme VCT2: il s'agit de livrer les fondations d'une plateforme technique indépendante des sites, de nouvelles fonctionnalités et d'introduire des méthodes de travail agiles.

Le rôle du mandant est défini en la personne du propriétaire de programme (rôle assumé par le chef de l'informatique). La gouvernance du programme est complexe, notamment les diverses instances définies, l'intervention des instances fédérales et la multiplicité des comités consultatifs. Ces rôles vont au-delà des recommandations du standard HERMES, la méthode de gestion de projet de l'administration fédérale. Cette organisation est adaptée à l'ampleur de la tâche.

Le CDF estime approprié le concept de pilotage par tranches annuelles, qui permet de livrer par étape les résultats et la fonctionnalité pour la mise en service. De ce fait, le programme évite le risque de travailler de longues années sur un projet avec au final un résultat peu ou pas utilisable.

2.3 Des incertitudes pèsent sur le financement

Le chiffre d'affaires de Skyguide est composé à 80% de produits de redevances régulées par l'Union Européenne. Les prestataires des services de navigation aérienne préparent un plan de performance quinquennal et le soumettent à la Commission européenne (CE). Celle-ci décide alors sur cette base du montant des redevances. La période de référence actuelle s'étend de 2015 à 2019, la prochaine de 2020 à 2024. Le délai d'approbation du nouveau plan de performance est fixé au 1^{er} mars 2020.

En 2018 déjà, Skyguide a établi des projections financières pour 2019 à 2024. Elles indiquent des difficultés financières à moyen terme (liquidités négatives de 6 millions de francs en 2024), même en intégrant le renouvellement hypothétique d'un prêt de près de 200 millions de francs en 2021. Courant 2019, la CE a communiqué de nouvelles hypothèses de calcul pour la préparation du plan de performance 2020–2024.

Au moment de la révision, Skyguide prépare ce plan de performance. L'entreprise a choisi de développer un scénario se basant sur l'évolution la plus favorable des événements, nommé « Best case ». Deux autres scénarios le « base case » et le « worst case » ne sont pas approfondis. L'entreprise n'a pas estimé les probabilités d'occurrence de chacune de ces options, mais juge le scénario « best case » le plus probable.

En parallèle, Skyguide établit de nouvelles projections financières pour cette période. Lors de l'audit, seules des estimations initiales du résultat net sont disponibles, mais elles montrent un résultat net positif. Elles indiquent aussi que Skyguide dispose d'un peu de marge dans son financement. Aucune projection sur les liquidités à moyen terme n'a toutefois encore été préparée. Le CDF n'a donc pas pu vérifier en détail ces éléments.

Appréciation

Les hypothèses du scénario « best case » du plan de performance 2020–2024 sont plausibles. Des incertitudes subsistent toutefois sur certaines variables de calcul, qui dépendent au final des décisions de la CE. Ces variables de calcul peuvent avoir des impacts significatifs sur les liquidités de l'entreprise. Si la CE refuse le plan de performance 2020–2024, les projections financières en cours de préparation seront caduques. Skyguide devra alors revoir sa stratégie afin d'éviter un problème de financement ou l'abandon des projets en cours.

Dans cette situation, Skyguide doit préparer des stratégies alternatives (recherche de financement additionnel, réduction de coûts, coupe dans le portefeuille de projets) afin d'assurer la continuité de l'exploitation. L'entreprise a prévu d'examiner les options possibles après la préparation du plan de performance à l'automne 2019. Le CDF renonce donc à émettre une recommandation à ce sujet.

2.4 La conduite de programme est globalement adaptée à la situation...

Les principes régissant la conduite du programme (objectifs, gouvernance, planification, etc.) sont élaborés dans le plan de gestion du programme VCT2 (« VCT2 Program Charter »). Créé au début des travaux en août 2016 et actualisé régulièrement, ce plan est formellement validé par le comité de pilotage et le comité de gestion de VC. Le cadre de la conduite du programme est en outre fixé par :

- La méthode ICM, un modèle interne à l'entreprise de gestion de projet en cascade,
- Le modèle de livraison hybride, qui détaille comment les démarches agiles et en cascade s'intègrent au sein du programme.

Le programme VCT2 est structuré de façon matricielle : des groupes de ressources travaillent à produire des fonctionnalités et des résultats regroupés au sein de paquets de livraison (« Delivery Items »). Ces paquets sont définis lors de la fixation du périmètre annuel et traités dans le cadre de sous-projets. La livraison effective est organisée périodiquement au sein d'étapes de déploiement opérationnel (« Operational Deployment Steps », ODS).

La planification des activités est effectuée et documentée à plusieurs niveaux :

- Un plan de livraison global, représentant les activités sur un cycle de quatre ans
- Le périmètre annuel déterminé dans le cadre du pilotage
- Un plan trimestriel détaillé de réalisation, rythmé par des « cérémonies » agiles de planification (Program Increment Planning Event, « PIPE-Meeting »).

Au niveau de la conduite du projet, le suivi est effectué dans le cadre de réunions des divers comités et responsables du programme, selon des fréquences et des degrés de détails différenciés. Des réunions mensuelles et trimestrielles de suivi sont notamment conduites. Pour ce niveau de suivi, deux états mensuels documentent l'avancement des travaux :

- Un état financier basé sur des extractions des coûts depuis SAP,
- Un rapport d'avancement, dans lequel la direction du programme consolide les données de suivi détaillé (coûts, délais, résultats et risques).

Le domaine « Change and Portfolio Management » édite un rapport sur base trimestrielle pour le comité de direction et le conseil d'administration. Il présente de manière consolidée les informations sur les grands projets et programmes en cours, dont VCT2 fait partie. Les commentaires du propriétaire et du directeur du programme complètent la présentation des chiffres. Ces informations sont synthétisées dans les publications annuelles (rapports de gestion et financiers, rapport du conseil d'administration sur la marche des affaires).

Pour la définition et le suivi fin des tâches à exécuter, l'outil Jira est utilisé (carnet de produit, « Product backlog »). La coordination et le suivi des tâches sont effectués par les responsables des sous-projets au sein de diverses « cérémonies » agiles hebdomadaires.

Un plan décrit la démarche du management de la qualité au sein du programme. L'objectif est de définir le processus de validation des résultats livrés dans un contexte de développement agile et intégré à l'administration de l'infrastructure informatique (« DevOps »), mais hautement régulé. Editée en 2016, une première version du document n'a pas pu s'imposer dans la pratique. Ses destinataires (développeurs et spécialiste de l'intégration) ont trouvé les mécanismes proposés trop compliqués. Durant la révision, une nouvelle version cette fois-ci simplifiée se trouvait en cours de préparation.

L'assurance qualité dans le programme est confiée à la responsable de la « Safety and Compliance », un domaine directement rattaché au chef de l'informatique (CIO – « Chief Information Officer »). Les travaux d'assurance qualité sont conduits par deux spécialistes du domaine. Ils examinent au moyens de listes de contrôle la conformité des documents livrés pour les applications, le support et la formation d'une part, et l'infrastructure d'autre part. Les documents nécessaires à la clôture avant la mise en service font particulièrement l'objet de leur attention. L'OFAC participe aussi aux activités d'assurance qualité. Chaque proposition de mise en service est passée en revue par les spécialistes de l'office, notamment sous l'angle de la sécurité (« safety ») et de l'architecture. Ceux-ci se prononcent formellement dans une lettre d'acceptation de la demande de mise en service, et peuvent émettre des conditions supplémentaires préalables.

Appréciation

Les bases de la conduite du programme sont définies de manière appropriée. Les processus et l'organisation complexe reflètent ici aussi l'ampleur de la tâche à accomplir et les multiples dépendances. Le CDF relève notamment la démarche de planification et de suivi à plusieurs niveaux et l'emploi de démarches de type agile. Quant aux états permettant le suivi d'avancement, le CDF n'a pas pu constater d'éléments mettant en doute leur pertinence et leur validité.

Le CDF estime adéquate l'organisation de l'assurance qualité au sein du programme, le processus se déroule de manière satisfaisante. Les efforts pour élaborer des référentiels intégrant les aspects agiles et du « DevOps » dans un environnement hautement régulé doivent toutefois se poursuivre.

2.5 ... mais la gestion des risques doit gagner en indépendance...

Le processus de gestion des risques est soutenu depuis février 2019 par l'outil Jira : une probabilité et un impact sont assignés à chaque risque. Les mesures compensatoires ainsi que le statut du risque sont également rapportés. Une cartographie des risques est tirée mensuellement de l'outil et intégrée au rapport d'avancement.

Au moment de la révision, la situation est décrite comme délicate. Les deux risques suivants sont identifiés comme très importants:

- Les efforts d'apprentissage et de changement des pratiques ralentissent la livraison des résultats,
- L'incapacité à appliquer une exploitation informatique ordonnée et résiliente.

Selon l'appréciation de la direction du programme, les efforts de mitigation en cours pour ces deux risques peinent à développer leurs effets. En lien avec le premier risque, la résistance passive au changement et l'inertie de l'organisation sont également mentionnés.

La responsabilité de la gestion des risques de VCT2 repose sur le directeur du programme.

Appréciation

Le processus de gestion des risques est approprié. Le CDF estime plausible l'évaluation de la situation des risques et partage l'inquiétude de la direction du programme sur les effets limités de certains efforts de mitigation. Ceux-ci doivent être poursuivis (voir les remarques ci-dessous sur la communication). Il s'étonne néanmoins de l'absence de risque identifié au titre de la sécurité de l'information (voir ci-dessous pour une recommandation).

Le CDF relève aussi que l'assignation de la responsabilité de la gestion des risques de VCT2 au directeur du programme ne garantit pas la nécessaire indépendance de la fonction. Cet état de fait doit être corrigé.

Recommandation 1 (Priorité 1)

Le CDF recommande à Skyguide d'assigner la fonction de gestionnaire des risques au sein du programme à une autre personne que le directeur de VCT2. Dans l'organisation du programme, cette personne devra rapporter directement au mandant (« Program owner »). La fonction peut éventuellement être assurée par un spécialiste externe à l'entreprise.

Prise de position de Skyguide

La direction de skyguide accepte sans réserve l'appréciation de la situation et la recommandation. Elle va confier dès le 01.01.2020 la gestion des risques du programme VCT2 à l'unité Safety, Quality, Security & Risk Management. Cela assurera une gestion des risques indépendante du programme. L'unité participera au rapport d'avancement mensuel pour comprendre l'évolution de la situation et procédera à l'identification, la formulation et à la gestion des risques et des mitigations. Elle participera aux séances du comité de soutien où elle rapportera elle-même sur l'état de la situation. Du fait de sa fonction première, elle intégrera automatiquement ses conclusions au niveau des risques d'entreprise.

2.6 ... et la communication doit être mieux ciblée

Un plan définit les modalités de la communication du programme VCT2 pour le personnel de Skyguide. Divers canaux et média sont engagés, une planification détaillée des actions de communication est élaborée. Une spécialiste dédiée s'occupe de ces activités.

Une analyse des parties prenantes au programme VC dans son ensemble est visible dans le plan de gestion du programme, mais se concentre surtout sur les interlocuteurs externes à l'entreprise. Pour le personnel de l'entreprise, des groupes de parties prenantes à VCT2 sont identifiés, mais une analyse détaillée et documentée n'est pas disponible.

Les possibilités de retour d'information lors des actions de communication existent. Par exemple, le personnel peut poser des questions aux responsables de l'entreprise lors d'événements organisés à cet effet (« Town hall Meetings »). Les questions et les réponses sont consignées dans un feuillet d'information à l'attention de toutes et tous. D'autres moyens, non spécifiques à VCT2 (rapports techniques internes ; enquêtes de satisfaction tous les deux ans), permettent de signifier des retours d'information, de manière anonyme. Le CDF n'a pas pu vérifier si ces retours sont systématiquement traités.

Appréciation

Les efforts en matière de communication doivent être poursuivis et renforcés. L'évolution du facteur humain dans le programme doit être mesurée régulièrement (prise de pouls) et publiée à tous les niveaux (ligne, conduite et pilotage). La transparence renforce la crédibilité des efforts de gestion du changement. L'analyse des parties prenantes internes de Skyguide gagnerait également à être approfondie. Ainsi, les bases d'une communication plus ciblée seraient posées.

En outre, le CDF constate que les canaux de retour d'information dédié au programme existent, mais sous forme ouverte (« Town hall meetings »). Il n'existe pas de canaux dédiés permettant des retours anonymes. Les enquêtes de satisfaction du personnel sont trop peu spécifiques et fréquentes pour récolter des retours d'information directement utilisables.

Recommandation 2 (Priorité 1)

Le CDF recommande à Skyguide de mettre en œuvre un plan de mesures pour renforcer l'efficacité de la communication du programme et faciliter la gestion du changement. Ce plan comprendra par exemple la mesure régulière de l'évolution du facteur humain et de l'efficacité de la communication dans le programme. L'analyse des parties prenantes internes du programme devra aussi être approfondie et documentée. Enfin, les canaux pour les retours d'information seront adaptés pour faciliter une communication bidirectionnelle dédiée au programme.

Prise de position de Skyguide

La direction de skyguide accepte sans réserve l'appréciation de la situation et partage les préoccupations et les recommandations qui précèdent. Pour approfondir sa compréhension du facteur humain à tous les niveaux du « Virtual Center » et pour intégrer un retour d'information plus « anonymisé », elle compte mettre sur pied, dès 2019 déjà, des « Focus/Pulse Check groups ».

Cet instrument fournira les informations nécessaires pour mieux cibler son action et sa communication. Il soutiendra le nécessaire changement de culture et l'évolution des mentalités et compétences qui permettront au personnel de mieux intégrer les transformations

à venir. La démarche sera accompagnée par un professionnel du domaine. Cette démarche ne concernera pas seulement le « Virtual Center » mais sera également ouverte à l'ensemble des transformations que skyguide doit entreprendre. Cet effort impliquera le département de la Communication, la ligne hiérarchique et l'unité de gestion de la transformation qui ensemble établiront un plan de communication global pour les années 2020 et 2021. Ce plan contiendra les éléments spécifiques pour le Virtual Center.

2.7 Le programme VCT2 livre, mais avec du retard

Depuis son commencement en août 2016, le programme a livré bon nombre de résultats, notamment : des nouvelles fonctionnalités pour la gestion du trafic aérien, des bases importantes pour une architecture système unifiée et la mise en œuvre de nouvelles méthodes de travail. Ces résultats sont déployés dans les systèmes productifs et utilisés au quotidien par les collaborateurs des opérations et les techniciens.

A fin 2018, des livraisons de résultats étaient toutefois en retard ou incomplètes. La nouvelle gestion des routes (« New Route Handling »), la gestion des opérations indépendante du site et la réalisation du centre de calcul unique étaient notamment touchées. Pour 2019, des retards sont également attendus, et concernent principalement la nouvelle gestion des routes et les travaux de l'usine logicielle (« Software factory »). Lors de la révision, des mesures correctives sont en cours de définition, par exemple des re-priorisations de tâches et la recherche de moyens pour augmenter la productivité du développement.

Le programme VCT1 a encouru des coûts de 59,8 millions de francs, soit un dépassement de 12 % par rapport au montant initialement prévu. Pour VCT2, la somme des coûts réels et estimés jusqu'à fin 2019 (prévision à fin d'affaire, « EAC ») s'élève à 114,5 millions de francs (calcul de fin mai 2019). Le budget total jusqu'à fin 2020 est fixé à 122,5 millions de francs.

L'étude de coûts-bénéfices a été révisée en 2018. L'atteinte du seuil de rentabilité, initialement prévue pour 2028, a dû être repoussée à 2030, en raison de l'évolution défavorable des coûts du programme.

Pour la suite des événements et les activités jusqu'au bouclage du programme, la direction de VCT2 propose 3 scénarios:

- « Coming short », avec un budget total de 122 millions de francs (tenue de l'objectif budgétaire), une fin du programme à mi-2020 et un périmètre fonctionnel viable, mais notablement diminué par rapport à l'objectif initial,
- « Tech foundation », avec un budget total de 133 millions de francs (+8% par rapport à l'objectif budgétaire), une fin du programme à fin 2020 (comme prévu) et un périmètre plus étendu, mais en deçà de l'objectif initial, notamment en termes d'indépendance du site pour certains systèmes,
- « One Sky-by-One System », avec un périmètre équivalent à l'objectif initial, mais une fin de programme en 2021 et un budget de 149 millions de francs (+21% par rapport à l'objectif budgétaire).

La direction de VCT2 préconise le deuxième scénario, les instances de pilotage du programme doivent prendre une décision dans l'automne 2019.

Appréciation

Le CDF prend note du retard encouru par le programme. Pour atteindre le périmètre fonctionnel défini initialement, des moyens additionnels seront nécessaires et les dates de fin prévues ne pourront pas être tenues. Les prévisions de rentabilité initiales ne pourront pas non plus être atteintes. L'ampleur du dépassement est visible dans les scénarios préparés par la direction du programme, ce qui contribue à la transparence du processus décisionnel. Le CDF estime que les instances de pilotage ont des éléments suffisants pour décider de la suite des événements. La Confédération dispose également de moyens d'information nécessaires pour apprécier la situation.

3 Développement, déploiement et exploitation

3.1 Les défis des nouvelles démarches de développement

Le développement des applications suit la démarche agile SAFe (Scaled Agile Framework), qui vise à assurer l'alignement et la collaboration lorsqu'un grand nombre d'équipes agiles sont à l'œuvre. Les analystes récoltent les exigences des utilisateurs finaux et les priorisent avec eux. Elles sont ensuite transcrites en récits utilisateurs (« user stories »), complétés par des critères d'acceptation et regroupés au sein d'épopées (« epics »). Tous ces récits constituent le carnet du produit (« Product backlog »), base exhaustive des tâches de développement à réaliser. Les dépendances et les points à corriger y sont également définis.

Pour chaque application, un premier prototype est rapidement généré, permettant la validation par les utilisateurs finaux. Une fois validés, les prototypes servent de base au développement complet des composants et objets logiciels, assuré par la société SkySoft-ATM S.A. de Meyrin. Cette coentreprise créée en 2001 par Skyguide est hébergée sur son site. Des membres de la direction et du conseil d'administration de Skyguide siègent à celui de skysoft-ATM. A terme, une fusion des usines logicielles des deux entreprises est prévue. D'autres ressources externes soutiennent l'effort de développement, selon un modèle d'externalisation. Les fonctionnalités d'intégration sont quant à elles développées par des équipes internes de Skyguide. Divers standards et normes (conventions de nommage, modèles – « templates ») encadrent les activités de développement.

Des « cérémonies » agiles rythment le travail de développement et permettent la coordination entre les différents intervenants. Le CDF note en particulier les réunions hebdomadaires de synchronisation et les événements trimestriels « PIPE » (voir 2.4.). Développeurs, intégrateurs et représentants des utilisateurs finaux sont conviés à ces derniers. La chaîne d'outils se base sur des produits comme Jira, Confluence, TIBCO, Sonarqube et des environnements de développement de type Java. Le matériel choisi est constitué de plateformes communes dans le domaine de la virtualisation.

Parallèlement à la démarche agile, des pratiques d'intégration continue et de type DevOps sont mises en œuvre. Celles-ci visent à des cycles courts de livraison du logiciel et à une meilleure collaboration entre développement et administration de l'infrastructure informatique. VCT2 doit servir de premier cas concret d'utilisation de ces méthodes à grande échelle, un important travail de définition et de mise en place est nécessaire.

Les défis sont multiples. Le paysage informatique de Skyguide comprend de nombreux équipements et applications plus anciens (« legacy systems »), que les développements actuels doivent intégrer. Cette coexistence de générations de composants logiciels et matériels est une source de complexité, notamment sous l'angle des interfaces à adapter. Par ailleurs, la mise en service des nouveaux composants continue d'être soumise à des procédures d'approbation formelle, pour des motifs de régulation et de sécurité. L'approbation est liée à une série de contrôles et de validations qui est nécessaire, mais lourde et en contradiction avec une approche de cycles courts de livraison. Sur le plan technique, il faut définir, enchaîner et optimiser des activités de développement, d'intégration, de test et de déploiement dans ce contexte hybride. Sur le plan organisationnel, ces nouvelles approches exigent de redéfinir les rôles des intervenants dans la chaîne de livraison du logiciel et du matériel. Cela peut provoquer des incompréhensions et des frictions. Des concepts et approches continuent d'être élaborés pour traiter ces points, leur mise en œuvre est en cours.

Appréciation

Sur le plan du développement, la démarche agile mise en place dans le cadre de VCT2 semble porter ses fruits. Les utilisateurs finaux sont intégrés au processus et peuvent transmettre leurs exigences. Le CDF note que la complexité des fonctionnalités à mettre en place peut rendre ardu le travail de spécification. L'utilisation de prototypes permet pour le moins de favoriser la communication entre développeurs et utilisateurs. Les cérémonies agiles facilitent et structurent le travail itératif. Les outils et le matériel mis en œuvre sont bien établis sur le marché, les ingénieurs de SkySoft-ATM sont proches et bien intégrés au processus de développement. Le CDF n'a pas trouvé d'élément lui permettant d'identifier un risque important à ce niveau.

Sur le plan de la mise en œuvre des cycles courts, le CDF prend note que les bases sont établies. Les travaux visant à affiner ces démarches doivent se poursuivre.

3.2 La mise en œuvre de l'architecture doit être mieux suivie

En 2015, la démarche architecturale du programme VC est élaborée. Elle définit l'architecture existante, la cible et les pas intermédiaires nécessaires (architectures de transition). A fin 2016, un plan architectural technique pour VCT2 est conçu. Dès 2017, des réflexions portant sur l'architecture métier sont initiées. Un comité d'architecture existe au sein de l'entreprise, il a pour objectif de piloter la mise en œuvre de l'architecture stratégique définie et d'arbitrer les éventuels conflits en la matière.

Au début de VCT2, des évaluations des options en présence sur le plan de l'infrastructure techniques sont menées, notamment par des preuves de concept (« Proof of concept »). Durant la révision, un risque de goulot d'étranglement pour la mise à disposition de machines virtuelles est identifié. Des activités complémentaires d'analyse des besoins de capacité au niveau du matériel sont en cours.

Des plans annuels définissent les architectures de transition pour le programme VCT2, y compris pour l'infrastructure et la constitution du centre de calcul principal à Wangen. L'atteinte de ces plans n'a jusqu'à maintenant pas été évaluée dans le cadre de la clôture des tranches annuelles. Skyguide prévoit de procéder une première fois à cette évaluation lors du bouclage de la tranche 2019 du programme et du lancement de la tranche 2020.

Appréciation

Les bases de la démarche architecturale sont correctement posées. Il note toutefois qu'un suivi systématique de la mise en œuvre des plans définis a fait défaut jusqu'à maintenant. L'évaluation périodique de l'atteinte des étapes de transition doit avoir lieu comme prévu à l'automne 2019. Le plan de transition de la tranche 2020 sera adapté en conséquence. Il incorporera notamment les résultats des analyses des risques de capacités matérielles insuffisantes. Enfin, et en prévision de VCT3, les travaux de mise en place de la démarche de l'architecture métier doivent être poursuivis.

3.3 La sécurité de l'information mérite plus d'attention

La sécurité de l'information est en mutation chez Skyguide. Une nouvelle organisation a été définie, basée sur quatre domaines traitant de la gouvernance, de l'architecture de la sécurité, des services de sécurité et de la cybersécurité. Ce dernier domaine est en cours de constitution. Une stratégie de sécurité de l'information a défini les priorités, une feuille de route montre les activités prévues pour les prochaines années. Un cadre de référence et de bonnes pratiques existe sous la forme d'une dizaine de principes. L'intégrité des systèmes et leur disponibilité demeurent prioritaires. Les processus relatifs à la sécurité de l'information sont en grande partie définis, leur opérationnalisation est en cours. L'entreprise met aussi en œuvre les mesures correctives issues d'un audit de la sécurité de l'information mené en novembre 2018 sur mandat de l'OFAC.

Skyguide gère une infrastructure critique sur les plans nationaux et internationaux. Le programme VCT2 a un impact important sur le profil de risques de l'entreprise en termes de sécurité de l'information. Les nouvelles démarches et technologies, notamment la mise en réseau, l'utilisation de matériel standard et la mise en œuvre d'une plateforme unique augmentent les risques. Le programme les traite en impliquant les spécialistes de la sécurité. Il définit aussi des mesures de protection de base (« Get the basics right ») au niveau de l'infrastructure et des applications.

Les spécialistes de la sécurité de l'information sont impliqués dans le programme VCT2. Le responsable de la sécurité de l'information (CISO – « Chief Information Security Officer »,) est membre du comité de pilotage. A ce titre, il participe aux séances de validation de passage de portes (« Gates ») et peut s'exprimer sur le respect des exigences de la sécurité de l'information. Les ingénieurs de sécurité participent aux travaux opérationnels du programme en définissant des architectures et des modèles d'implémentation. Ils communiquent régulièrement avec les développeurs et coordonnent les activités, notamment au travers des mécanismes du PIPE.

Au niveau de la sécurité de l'infrastructure, les systèmes composant le paysage du programme sont évalués et mis en œuvre sur la plateforme orientée services (« Service Oriented Infrastructure »). Un catalogue d'exigences documentées doit être satisfait pour qu'un système puisse prétendre à son admission sur la plateforme. Diverses activités de surveillance de l'infrastructure (contrôles des vulnérabilités, tests de pénétration) sont régulièrement menées. Les faiblesses découvertes sont répertoriées, les mises à jour planifiées pour y remédier. Dans l'état actuel des travaux, celles-ci peuvent devoir attendre quelques mois. L'exploitation de la plateforme matérielle est confiée à un prestataire de services externe opérant en mode délocalisé depuis la Bulgarie.

Dans le domaine de la sécurité des applications, les priorités sont définies pour chaque tranche annuelle et discutées avec les architectes. En 2019, la mise à disposition de modèles d'implémentation sécurisant les échanges de messages au sein du paysage du programme (par ex. par le cryptage des messages) est priorisée.

Le CDF n'a pas en sa possession de liste des objets de protection critiques (applications et infrastructures) du paysage informatique du programme. La situation des risques du programme ne fait pas mention d'un risque relatif à la sécurité de l'information. Le CDF n'a pas connaissance d'un document spécifique à VCT2 détaillant les besoins relatifs à la sécurité de l'information (analyse des besoins de protection) et les mesures à prendre pour les couvrir (concept de protection de l'information). Une vue d'ensemble de l'état de la mise en

œuvre des mesures de protection et de leur efficacité fait également défaut. Enfin, un répertoire actuel des risques résiduels en matière de sécurité de l'information pour la plateforme du programme manque. Le CDF note enfin que la mise en œuvre de la continuité d'entreprise (Business Continuity Management, BCM) et des plans de reprise d'activité (Disaster Recovery Planning, DRP) ne sont pas dans le périmètre du programme VCT2.

Appréciation

Le domaine de la sécurité de l'information est en pleine évolution chez Skyguide. Les stratégies, les priorités et les bases de l'organisation et des processus sont posées, mais leur opérationnalisation n'est pas achevée. Au regard de son caractère d'infrastructure critique, Skyguide doit poursuivre ses efforts en la matière.

Les exigences accrues en matière de sécurité de l'information ne sont pas suffisamment prises en compte au sein du programme VCT2. Des résultats importants manquent ou sont trop peu détaillés (analyse des risques, notamment ceux liés à l'exploitation délocalisée en Bulgarie, listes des objets de protection, analyses des besoins de protection, concept de protection de l'information). Les instruments actuellement utilisés ne permettent pas une définition très concrète, une priorisation et un suivi rigoureux des objectifs à atteindre en la matière. Ils ne représentent pas non plus clairement les risques résiduels en matière de sécurité de l'information. Les instances de pilotage ne peuvent ainsi pas les apprécier et les traiter en conséquence. Enfin, le CDF s'interroge sur la décision de ne pas définir les plans de reprise d'activité à ce stade du programme. De manière générale, il craint que faute d'une visibilité et d'un poids suffisants, les impératifs de la sécurité de l'information au sein du programme passent au second plan.

Le CDF s'exprime dans un chapitre ci-dessous sur les aspects sécuritaires de l'externalisation de l'exploitation de la plateforme.

Recommandation 3 (Priorité 1)

Le CDF recommande à Skyguide de mettre en œuvre des instruments plus efficaces pour l'incorporation des aspects de la sécurité de l'information de VCT2. Les risques du programme en termes de sécurité de l'information doivent être réévalués. Un concept de protection de l'information et un plan de mise en œuvre doivent être définis.

Prise de position de Skyguide

La direction de skyguide accepte sans réserve l'appréciation de la situation et la recommandation. Cette dernière vient confirmer les décisions récentes de « Virtual Center Tranche 2 » (VCT2) sur les questions de sécurité de l'information.

Il a en effet été décidé que 5 bonnes pratiques sécuritaires de base devraient être satisfaites lors de la migration des plateformes historiques (« legacy ») vers les nouvelles infrastructures orientées service. Cette initiative se nomme « Legacy on-boarding on SOI ». Il est cependant à noter que le périmètre des applications de VCT2 est limité et que ces efforts devront se poursuivre au-delà du rôle de vecteur du changement que joue la tranche 2. Il faut aussi impérativement industrialiser les fondations existantes de certains services fondamentaux sur lesquels s'appuient nos efforts.

VCT2 a également publié récemment des modèles de bonnes pratiques sécuritaires obligatoires pour toute implémentation de service sur son nouveau « Enterprise Service Bus » pour l'échange d'information. Elles concernent l'authentification et l'encryptage et utilisent pour leur implémentation des solutions reconnues sur le marché ayant fait leur preuve à

maintes reprises. Compte tenu du caractère partiel du périmètre de VCT2, l'analyse des risques de sécurité de l'information doit s'effectuer à un niveau plus global dans les processus du service de sécurité de notre entreprise. L'ensemble des composants VCT2 seront donc intégrés dans une initiative qui est en cours de lancement sur la question des risques. Les résultats de cette initiative seront intégrés au fur et à mesure dans les efforts du « Virtual Center ».

3.4 Les tests sont menés de manière convaincante

Historiquement, les activités de test chez Skyguide ont été appliquées aux équipements à mettre en service. Avec VCT2, dans son contexte de développement agile et de cycles courts, l'attention se porte désormais sur les services mis à disposition. Ceux-ci représentent une vue logique et transversale d'un ensemble de composants logiciels et matériels. Le paysage système comporte les plateformes locales de développement, et des environnements d'intégration, de validation, de pré-production et de production. Au moment de la révision, le document décrivant les nouvelles stratégies de test était en cours d'approbation. L'approche de test au sein de VCT2 est définie et se base sur le modèle en V, mettant en regard les activités de production et de validation et proche des démarches en cascade du développement traditionnel. La méthode prescrit les artéfacts à produire pour les tests (par ex. les plans de test). Une matrice de traçabilité permet de s'assurer que chaque exigence du carnet du produit soit couverte par au moins un cas de test.

Le test des services est effectué à divers niveaux : unitaire (principalement chez le développeur), composant, application (groupe de services), fonctionnel (de bout en bout), validation et vérification, validation utilisateur (« User Acceptance Testing », UAT). Différentes méthodes de test sont utilisées, telles que la simulation, les tests de retour en arrière (« rollback »), de robustesse, de performance, de régression et d'interfaces. Divers outils soutiennent ces activités et permettent une automatisation partielle.

Les activités de test peuvent donner lieu à des exercices de grande ampleur. Les tests de validation et de vérification impliquent par exemple des utilisatrices et des utilisateurs finaux et l'usage de simulateurs, sur la base de données réelles de vols. Les tests sont donc planifiés en conséquence, pour s'assurer de la disponibilité des ressources (en particulier les contrôleurs aériens). Dans d'autres cas, des tests finaux sont effectués lors d'un déploiement nocturne sur l'environnement de production, avec restauration de l'état initial après exécution des tests. Ils nécessitent également une préparation importante. Les problèmes identifiés sont documentés dans Jira et donc intégrés au carnet de produit pour traitement. Un rapport de test est édité.

L'approbation formelle de la mise en service (« Gate 3 ») est subordonnée à la validation des résultats des tests.

Appréciation

Le CDF constate que les tests sont une discipline établie au sein du programme. Ils sont menés de manière professionnelle, sont documentés et soutenus par des outils. Enfin ils impliquent à bon escient les utilisateurs finaux pour les étapes clés de l'approbation des solutions. Le CDF attend que les exigences de la sécurité de l'information soient pleinement intégrées dans le processus de test.

3.5 L'organisation du déploiement et la préparation du domaine métier sont adéquates

La préparation du déploiement des solutions se fait sous la responsabilité du groupe « Business Change Delivery » du programme VCT2. Ce groupe s'occupe d'aspects relevant du domaine métier (par ex. la sécurité des opérations – « safety » –, les facteurs humains, la formation, la définition du périmètre opérationnel et les tests d'acceptation) et technique (le déploiement opérationnel).

L'organisation du domaine métier (les opérations) a été adaptée avec la mise en œuvre du programme VC : une unité dédiée « Virtual Center » a été créée. Son responsable, qui est directement subordonné au chef des opérations, siège au comité de pilotage de VCT2 et officie comme propriétaire métier (« Business owner »). Au niveau de la conduite du programme, les opérations sont également fortement impliquées. Leurs représentants définissent les besoins, posent les bases de l'harmonisation des pratiques entre les sites et participent aux tests.

Le domaine métier porte aussi la responsabilité de l'opérationnalisation des nouveaux systèmes et processus. Celle-ci implique selon les cas d'importants efforts d'adaptation pour les utilisateurs finaux. Diverses mesures accompagnent le changement : communication, formation, actualisation des manuels de travail, etc.

Le déploiement opérationnel technique fait l'objet d'une organisation et d'un processus particuliers. Le plan de transition est le document central régissant la mise en service, conçu en collaboration avec les utilisateurs finaux (les opérations). Différenciant les phases avant et après le déploiement opérationnel, il décrit les mesures qui en assurent le bon déroulement. En cas de dysfonctionnement grave, et si le point de non-retour n'est pas atteint, le retrait de la solution déployée peut également être envisagé.

Appréciation

Pour le CDF, le domaine métier est impliqué de manière adéquate dans le programme VCT2. Le CDF constate toutefois que les enquêtes de satisfaction des collaborateurs de 2018 trahissent un certain scepticisme face à la mise en œuvre de la stratégie VC. Les négociations difficiles ayant entouré le renouvellement des conventions collectives peuvent expliquer partiellement ces résultats. Tout effort de changement provoque des incertitudes et des mécontentements, le CDF renvoie à sa recommandation ci-dessus d'améliorer l'efficacité de la communication.

L'organisation des déploiements est adaptée au modèle DevOps et de cycles courts de livraison. La démarche offre l'avantage de déploiements échelonnés de blocs plus petits de solution par rapport à un modèle « big bang ». L'organisation est mise plus souvent à contribution, mais pour une charge plus modérée. Le CDF note qu'une procédure systématique de déploiement est définie et suivie, et que les besoins des opérations sont pris en compte. Malgré toutes ces précautions, et vu la complexité des plateformes, des problèmes surviennent après le déploiement des solutions. Le CDF relève que les moyens existent pour les prendre en charge.

3.6 La difficile mutation de l'exploitation informatique

Avec le programme VCT2, une migration est en cours vers de nouvelles plateformes techniques indépendantes du site et une orientation vers les services. De nombreux changements en découlent. Des nouvelles méthodes de travail, nécessitant de nouvelles compétences, sont introduites et certaines activités sont externalisées. La coexistence entre les nouvelles infrastructures et applications d'une part, et les plateformes historiques (« legacy ») d'autre part doit être gérée. Enfin, l'approche de monitoring et de contrôle des applications et plateformes doit s'adapter à cette nouvelle configuration.

L'exploitation informatique se voit donc confrontée à une évolution profonde de sa mission. Divers documents mettent en évidence les tenants et aboutissants de cette transformation. Sur le plan du monitoring, l'unité en charge n'a été impliquée que récemment dans le programme VCT2. Au moins peut-elle maintenant définir ses exigences pour qu'elles soient prises en compte dans le carnet de produit. De manière générale, une certaine inquiétude s'exprime sur le calendrier et les modalités de l'évolution, ainsi que sur les compétences à développer pour s'adapter aux changements.

Le matériel mis en œuvre dans le cadre du programme VCT2 est physiquement hébergé dans les centres de calcul de Skyguide. L'exploitation informatique des nouvelles plateformes virtuelles est cependant confiée à un prestataire externe, opérant en mode délocalisé. Le CDF a pu consulter le contrat et les accords de niveau de services formant la base de la collaboration. Il a également pu prendre connaissance de divers rapports d'incident décrivant des situations problématiques dans les flux de travail entre Skyguide et le prestataire. Ces flux de travail ne sont que partiellement intégrés, si bien qu'un transfert manuel de certaines informations est nécessaire (par exemple tickets d'incidents, parce que les deux entreprises ont des systèmes différents de gestion). Les rapports d'incidents pointent également des incertitudes dans la répartition des tâches et responsabilités entre Skyguide et le prestataire.

Dans le cadre de leur travail, les spécialistes du prestataire ont un accès privilégié aux plateformes déployées dans le cadre du programme VCT2. Divers contrôles techniques sont en place pour assurer une connexion sécurisée aux serveurs. Toutefois, le CDF n'a pas pu obtenir de rapport de monitoring des activités effectuées par les utilisateurs privilégiés sur les plateformes productives. Le contrôle de ces activités ne peut ainsi pas être effectué.

Appréciation

Une incorporation précoce et poussée de l'exploitation informatique dans les travaux de projets constitue un point central d'une démarche de type DevOps. Dans le cas du programme VCT2, le CDF constate une évolution vers une implication plus large de l'exploitation. Diverses frictions subsistent toutefois dans les processus d'exploitation des objets livrés (matériel et logiciel), notamment des inefficiences dans l'interface entre Skyguide et le prestataire externe. Ces points doivent être traités au sein du programme.

Le CDF prend note de l'ampleur de la tâche et des inquiétudes provoquées par la mutation en cours dans l'organisation de l'exploitation informatique. Les efforts d'accompagnement du changement (communication – voir recommandation ci-dessus –, formation, définition des processus) doivent être poursuivis dans ce domaine.

Recommandation 4 (Priorité 1)

Le CDF recommande à Skyguide d'analyser les processus entre son exploitation interne et le prestataire externe en charge de l'exploitation de la plateforme virtuelle. Cette analyse devra être menée au sein du programme VCT2. L'objectif est de découvrir les points de friction et les inefficiences et de mettre en œuvre des mesures d'amélioration.

Prise de position de Skyguide

La direction de skyguide accepte sans réserve l'appréciation de la situation et la recommandation. L'organisation concernée a déjà commencé à analyser cette question et l'unité responsable de l'exploitation technique en lien avec notre prestataire externe DXC va produire un rapport d'analyse d'ici mars 2020. Ce rapport mettra en évidence les frictions et inefficacités dans la collaboration. Il documentera également les mesures actuellement mises en œuvre et si nécessaire les mesures complémentaires à développer.

Le CDF relève que les modifications dans les systèmes productifs par des utilisateurs possédant des droits privilégiés ne sont pas journalisées et validées périodiquement. Un important contrôle pour assurer l'intégrité des plateformes manque et doit être introduit.

Recommandation 5 (Priorité 1)

Le CDF recommande à Skyguide d'introduire un instrument permettant de journaliser automatiquement les modifications apportées directement dans les systèmes productifs par des utilisateurs possédant des droits privilégiés (administrateurs). Ces journaux doivent être visés périodiquement par des responsables de l'exploitation informatique de Skyguide.

Prise de position de Skyguide

La direction de skyguide accepte sans réserve l'appréciation de la situation et la recommandation. Elle reconnaît que la gestion des accès privilégiés constitue une contribution importante à la sécurité de ses opérations. Dans ce contexte, la journalisation actuelle sous forme d'enregistrement des sessions de travail extérieures doit être complétée par d'autres mesures. Ces dernières sont prises en considération dans la feuille de route de skyguide sur la sécurité (« Security Roadmap »). Elles couvriront complètement la gestion des accès privilégiés, qu'il s'agisse aussi bien de personnes internes ou externes que de prévention ou de détection. Par conséquent, les questions de journalisation et de validation seront traitées dans ces initiatives. Ces mesures vont être mises en place conformément à l'agenda de la feuille de route.

Annexe 1 : Bases légales

Texte législatif

Loi fédérale sur l'aviation (LA) du 21 décembre 1948 – RS 748.0

Ordonnance sur le service de la navigation aérienne (OSNA) du 18 décembre 1995
– RS 748.132.1

Messages et directives

Objectifs stratégiques assignés à Skyguide par le Conseil fédéral de 2016 à 2019
(Feuille fédérale 2015 8007)

Annexe 2 : Abréviations

AFF	Administration fédérale des finances
CDF	Contrôle fédéral des finances
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
OFAC	Office fédéral de l'aviation civile

Annexe 3 : Glossaire

Agile (méthode)	Groupe de pratiques de pilotage et de réalisation de projets, reposant sur un cycle de développement itératif, incrémental et adaptatif
ANSP	Fournisseur de services de navigation aérien (en anglais Air Navigation Service Provider)
Base case (scenario)	Scénario se basant sur une évolution neutre des événements
Best Case (scenario)	Scénario se basant sur l'évolution la plus favorable des événements
Big Bang (approach)	Modèle de déploiement d'un système consistant à mettre en service en une fois l'ensemble de la fonctionnalité (par opposition à une mise en service échelonnée)
Business Continuity Management	Plan de continuité d'activité (BCM) : concept, procédure et document permettant à une entreprise de fonctionner même en situation de crise majeure.
Cérémonie (agile)	Dans une démarche agile, réunion de travail
CIO	Responsable de l'informatique (en anglais Chief Information Officer)
CISO	Responsable de la sécurité de l'information (en anglais Chief Information Security Officer)
Cybermenaces	Toute circonstance ou tout événement potentiels susceptibles de porter atteinte aux réseaux et systèmes d'information ou à leurs utilisateurs
Delivery Item	Paquet de fonctionnalités et de résultats à livrer
DevOps	Mouvement et pratique de l'ingénierie informatique visant à l'unification du développement logiciel et de l'administration des infrastructures informatiques et des systèmes
Disaster Recovery Planning	Plan de reprise d'activité (DRP) : ensemble de procédures permettant à une entreprise de reconstruire et remettre en route un système d'information en cas de sinistre
EAC	Prévision à fin d'affaire (en anglais Estimate at completion), méthode d'extrapolation des coûts à la fin d'un projet en partant des coûts réels actuels et du reste des résultats à mettre en œuvre.

Epic	(litt. épopée) dans une démarche agile, regroupement de récits utilisateurs retranscrivant leurs exigences à l'adresse du produit à développer
Gate	Littéralement « portail », dans la démarche de projet de Skyguide, jalon défini dans le cadre d'un projet ou programme et nécessitant une validation formelle.
Gate 3	Dans la démarche de projet de Skyguide, jalon constituant l'approbation formelle de la mise en service
HERMES	eCH-0054 : HERMES Méthode de management de projets 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. Cette méthode est à disposition du public, selon les standards de l'Association eCH.
ICM (méthode)	Démarche de gestion du portefeuille de projets et des projets, propre à Skyguide (en anglais Innovation and Change Management)
Jira	Logiciel de gestion de projets et de suivi d'incidents
Legacy (system)	Système de génération plus ancienne en service dans un paysage informatique
Modèle en V	Approche d'organisation des activités d'un projet mettant en regard les phases de production successives avec les phases de validation correspondantes.
New Route Handling	Groupe de fonctionnalités permettant la gestion des routes aériennes, dont la mise en place est prévue dans le cadre de VCT2.
ODS	Etape de déploiement opérationnel (en anglais Operational Deployment Step) et de mise en service d'un groupe de paquets de livraison
PIPE (meeting)	Cérémonie agile trimestrielle de planification du programme (en anglais Program Increment Planning Event)
Product backlog	Carnet du produit, liste ordonnée des éléments requis (besoin, amélioration, correctif) et unique source des besoins pour tous les changements à effectuer sur le produit
Product owner	Propriétaire du produit, rôle agile, représentant du client et de l'utilisateur dans le processus de développement

Program Charter	Plan de gestion de programme, document définissant les bases d'un programme, ses objectifs, ressources, processus, organisation, etc.
Rollback (test)	(litt. Retour en arrière), test constituant à rétablir un système dans l'état qu'il avait avant une modification
Service Oriented Infrastructure	Dans la terminologie de Skyguide, Infrastructure permettant l'hébergement de service dans un environnement virtualisé
SAFe	Démarche agile permettant un travail coordonné lorsqu'un grand nombre d'équipes de développeurs sont à l'œuvre (en anglais Scaled Agile Framework)
SAP	Progiciel de gestion des ressources utilisé chez Skyguide soutenant les processus financiers, de la gestion du personnel et de la logistique.
Scrum	Cadre de développement agile, basé sur une méthode de travail itérative
SES	Initiative de ciel unique européen (en anglais Single European Sky) adoptée en 2004 et 2009 par le Parlement européen, ayant pour but de faire évoluer l'organisation de l'espace aérien.
Sprint	Itération de développement dans la méthodologie Scrum
Template	Dans le développement logiciel, modèle d'objet à utiliser, contribue à accélérer et à améliorer la qualité d'un objet logiciel.
Ticketing (system)	Système de saisie et de suivi des incidents
TOGAF	The Open Group Architecture Framework: Cadre et méthodologie d'architecture d'entreprise
User Acceptance Test	Test de validation utilisateur (UAT)
User story	(litt. Récit utilisateur), dans une démarche agile, retranscription des exigences des utilisateurs à l'adresse du produit à développer
UMB+ VC	Comité de gestion du programme Virtual Center (en anglais Unit Management Board Virtual Center)
VC	Virtual Center, programme défini par Skyguide et visant à réaliser un système suisse de gestion du trafic aérien harmonisé entre les deux principaux sites Est (Wangen bei Dübendorf) et Ouest (Genève)

VCT1	Première tranche du programme Virtual Center visant à mettre en places les mesures minimales d'harmonisation entre les centres de contrôle Est et Ouest
VCT2	Deuxième tranche du programme Virtual Center, elle-même définie comme un programme, visant à créer les fondations techniques pour une gestion flexible et indépendante du site des secteurs aériens
VCT3	Troisième tranche du programme Virtual Center, visant à opérationnaliser les changements.
Worst case (scenario)	Scénario se basant sur l'évolution la plus défavorable des événements

Priorités des recommandations

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).