~~INTERNE~~
DECLASSIFIE (selon la décision de la direction du 27 juin 2018)

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

Audit transversal de la sécurité informatique de la Confédération

Unité de pilotage informatique de la Confédération

CDF-16255 / prises de position incluses / 11 mai 2017

Audit transversal de la sécurité informatique de la Confédération
Unité de pilotage informatique de la Confédération

L'essentiel en bref

Dans ce quatrième audit transversal de la sécurité informatique de la Confédération depuis 2011, le Contrôle des finances (CDF) a examiné la mise en œuvre des mesures de protection de base des technologies de l'information. Ces mesures sont regroupées au sein d'un catalogue de 17 chapitres, édité par l'Unité de pilotage informatique de la Confédération (UPIC). Leur mise en œuvre est du ressort tant des fournisseurs (FP) que des bénéficiaires de prestations (BP), et doit être documentée. Les pratiques des sept départements, de la Chancellerie fédérale, de cinq fournisseurs de prestations et de l'UPIC ont été passées en revue. Douze applications critiques ont également été examinées. Enfin, le CDF a évalué la mise en œuvre du processus de gestion des risques liés à l'espionnage ainsi que celle des recommandations issues des audits transversaux antérieurs.

L'examen des pratiques des bénéficiaires de prestations révèle un paysage contrasté

La grande majorité des unités administratives (UA) examinées tiennent un inventaire actuel des applications en service. Sous l'angle de la sécurité, le CDF recommande toutefois de renoncer dans toute la mesure du possible au regroupement d'applications de moindre importance. Les documents de sécurité ne sont pas édités et actualisés pour toutes les applications. Des actions correctives sont en cours dans le sillage de l'affaire RUAG. Le CDF salue les améliorations en cours des outils permettant le contrôle des documents de sécurité. Il juge toutefois les contrôles de la mise en œuvre des mesures encore insuffisants.

Le contrôle périodique des droits d'utilisateurs est souvent négligé. Le CDF a émis des recommandations à l'attention des départements concernés. Il a en outre relevé que l'aspect de la sécurité pouvait être négligé dans le processus d'homologation des achats informatiques. Il a recommandé à l'UPIC de revoir son implication dans ces processus.

Pour une majorité des applications critiques examinées, des documents de sécurité actuels sont disponibles. Sur un plan matériel, le CDF considère que la majorité des concepts de sécurité répondent de manière appropriée aux besoins en protection. Il estime toutefois que dans un cas, les exigences en termes de confidentialité sont sous-estimées. Une solution est actuellement en cours de mise en place. Pour les trois applications recourant à la télémaintenance, les prescriptions sont respectées : Des comptes utilisateurs spéciaux sont définis, leur accès et leurs activités sont enregistrés et contrôlés. Aucune mesure d'amélioration immédiate n'est requise.

Les pratiques des fournisseurs de prestations sont globalement satisfaisantes

Les FP passés en revue s'impliquent activement dans l'édition et le contrôle des documents de sécurité des projets. Ils contrôlent également dans la majorité des cas la mise en œuvre des mesures de sécurité leur incombant. Ils mènent par ailleurs diverses activités d'amélioration continue en matière de sécurité. Le CDF juge la situation globalement satisfaisante.

Sur le plan de l'intégrité des systèmes, les FP ont mis en place les mesures de contrôle définies par l'UPIC. Le CDF constate toutefois que les techniques mises en œuvre diffèrent sensiblement entre fournisseurs. Il encourage l'UPIC à définir plus précisément les notions d'intégrité et d'en regrouper les prescriptions. En outre, les solutions à mettre en œuvre pour surveiller l'intégrité des systèmes en service doivent être coordonnées avec les FP.

La complexité croissante de la sécurité informatique

Les exigences de la protection de base évoluent vers une complexité croissante, reflétée dans les mises à jour périodiques par l'UPIC du catalogue des mesures. Leur mise en œuvre peut poser problème. Les plateformes techniques et les applications se multiplient. Les délégués à la sécurité ne disposent cependant pas toujours du temps suffisant pour gérer les tâches requises. Le CDF voit un risque dans cette situation et recommande à l'UPIC de simplifier et d'optimiser les mesures de la protection de base là où c'est possible.

Le contrôle de la mise en œuvre et de l'efficacité des mesures comporte des failles

En matière de contrôle et de documentation de la mise en œuvre et de l'efficacité des mesures, la qualité des pratiques varie sensiblement. Les BP ne les documentent pas systématiquement et n'exigent pas dans tous les cas les rapports de contrôle de la part des FP.

Le CDF voit ici un manque. Il estime en outre peu efficient le système actuel de documentation du contrôle des mesures. Selon la démarche en place, les FP répondent souvent de manière redondante aux mêmes questions. Le CDF a recommandé à l'UPIC de trouver les moyens de faciliter la documentation et la confirmation périodique par les FP du contrôle de la mise en œuvre des mesures de protection.

En outre, les BP définissent rarement explicitement les responsabilités et les processus de contrôle de la mise en œuvre et de l'efficacité des mesures de protection. Le CDF juge qu'un risque réel existe que ces mesures ne soient simplement pas appliquées, faute de contrôle. Il a recommandé à l'UPIC de compléter les instructions de la protection de base. Celles-ci devraient prescrire aux départements de définir les responsabilités et les processus de contrôle.

Le processus de gestion des risques liés à l'espionnage doit être simplifiée et clarifié

Les UA passées en revue appliquent les nouvelles directives relatives à la méthode de gestion des risques visant à réduire les activités d'espionnage de service de renseignement (GRAES). Elles estiment que la démarche répond à un risque réel, mais qu'elle occasionne un travail trop important. Elles s'interrogent en outre sur la pertinence de certains critères d'analyse, leur pondération et sur les mesures à adopter pour les objets présentant un risque GRAES. Les UA ont pu exprimer ces objections lors des discussions en vue d'une deuxième version du processus.

Le CDF partage les réserves des départements sur l'efficacité du processus GRAES dans sa forme actuelle. [redacted] Le CDF a recommandé à l'UPIC de simplifier le processus et de clarifier les mesures à adopter pour les objets présentant un risque GRAES. La nouvelle version de la démarche pourrait s'inspirer des processus simplifiés définis dans certains départements.

La plupart des recommandations d’audits transversaux antérieurs ont été mises en œuvre

Le CDF constate que douze des quinze recommandations d’audits transversaux de sécurité informatique antérieurs encore ouvertes dans son système de suivi ont été mises en œuvre. Pour les trois recommandations restantes, les travaux sont en bonne voie.

Querschnittsprüfung IT-Sicherheit des Bundes
Informatiksteuerungsorgan des Bundes

Das Wichtigste in Kürze

In der vierten Querschnittsprüfung der IT-Sicherheit des Bundes seit 2011 hat die Eidgenössische Finanzkontrolle (EFK) die Massnahmenumsetzung des IKT-Grundschutzes geprüft. Die Massnahmen sind in einem 17 Kapitel umfassenden Katalog enthalten, das vom Informatiksteuerungsorgan des Bundes (ISB) herausgegeben wird. Ihre Umsetzung obliegt sowohl den Leistungserbringern (LE) als den Leistungsbezügern (LB) und muss dokumentiert werden. Unter die Lupe genommen wurden die Praktiken der sieben Departemente, der Bundeskanzlei, von fünf LE und des ISB. Ausserdem wurden zwölf als kritisch beurteilte Anwendungen untersucht. Schliesslich hat die EFK die Umsetzung des Risikomanagementprozesses im Zusammenhang mit der nachrichtendienstlichen Ausspähung sowie die Umsetzung der Empfehlungen aus früheren Querschnittsprüfungen evaluiert.

Die Prüfung der Praktiken der Leistungsbezüger zeigt ein kontrastreiches Bild

Die überwiegende Mehrheit der untersuchten Verwaltungseinheiten (VE) führt ein aktuelles Inventar der bestehenden Anwendungen. Vom Standpunkt der Sicherheit aus betrachtet empfiehlt die EFK jedoch, möglichst auf die Zusammenlegung von kleineren Anwendungen zu verzichten. Die Sicherheitsdokumente werden nicht für alle Anwendungen herausgegeben und aktualisiert. Im Zuge der RUAG-Affäre sind Korrektivmassnahmen im Gang. Die EFK begrüsst die laufenden Verbesserungen der Tools, mit denen die Sicherheitsdokumente kontrolliert werden können. Ihres Erachtens sind die Kontrollen der Massnahmenumsetzung allerdings noch ungenügend.

Die periodische Kontrolle der Nutzerrechte wird oft vernachlässigt. Die EFK hat zuhanden der betroffenen Departemente Empfehlungen abgegeben. Sie hat zudem festgestellt, dass im Zulassungsprozess der Informatikbeschaffungen der Sicherheitsaspekt bisweilen vernachlässigt werden kann. Sie hat dem ISB empfohlen, seine Rolle in diesen Prozessen zu überprüfen.

Für die meisten der untersuchten kritischen Anwendungen sind aktuelle Sicherheitsdokumente verfügbar. Auf materieller Ebene ist die EFK der Auffassung, dass die Mehrheit der Sicherheitskonzepte dem Schutzbedürfnis inhaltlich angemessen Rechnung trägt. In einem Fall werden die Vertraulichkeitsanforderungen aber unterschätzt. Die Umsetzung einer Lösung ist bereits in Gang. Bei den drei Anwendungen mit Fernwartung werden die Vorschriften eingehalten: Es werden spezielle Anwenderkonten definiert, deren Zugang und Aktivitäten gespeichert und kontrolliert werden. Es ist keinerlei sofortige Verbesserungsmassnahme notwendig.

Die Praktiken der Leistungserbringer sind insgesamt zufriedenstellend

Die untersuchten LE arbeiten aktiv bei der Erarbeitung und der Kontrolle der projektbezogenen Sicherheitsdokumente mit. In den meisten Fällen kontrollieren sie auch die Umsetzung der Sicherheitsmassnahmen, die ihnen obliegen. Ausserdem führen sie regelmässig verschiedene Tätigkeiten durch, die der ständigen Verbesserung der Sicherheit dienen. Die EFK erachtet die Situation als insgesamt zufriedenstellend.

Die LE haben die vom ISB definierten Kontrollmassnahmen in Bezug auf die Systemintegrität umgesetzt. Die EFK stellt jedoch bei den umgesetzten Techniken der einzelnen LE beträchtliche Unterschiede fest. Sie ermutigt das ISB, die Integritätsbegriffe genauer zu definieren und die einschlägigen

Vorschriften zusammenzufassen. Zudem sind die Lösungen, mit denen die Integrität der laufenden Systeme überwacht wird, mit den LE zu koordinieren.

Zunehmende Komplexität der Informatiksicherheit

Die Anforderungen an den Grundschutz werden zunehmend komplexer, was sich in den periodischen Aktualisierungen des Massnahmenkatalogs durch das ISB niederschlägt. Die Umsetzung der Massnahmen kann zu Problemen führen. Es gibt immer mehr technische Plattformen und Anwendungen. Nicht alle Sicherheitsbeauftragten verfügen über genug Zeit, um ihre Aufgaben zu erfüllen. Die EFK erachtet dies als Risiko und empfiehlt dem ISB, die Grundschutzmassnahmen wo immer möglich zu vereinfachen und zu optimieren.

Lückenhafte Kontrolle der Umsetzung und der Wirksamkeit der Massnahmen

Die Kontrolle und die Dokumentation der Umsetzung und Wirksamkeit der Massnahmen sind qualitativ sehr unterschiedlich. Sie werden von den LB nicht systematisch dokumentiert, Letztere fordern die Kontrollberichte von den LE nicht immer an.

Die EFK erachtet dies als Mangel. Sie beurteilt ausserdem das aktuelle Dokumentationssystem als unwirksam. Gemäss aktuellem Verfahren liefern die LE oft redundante Antworten auf gleichbleibende Fragen. Die EFK hat dem ISB empfohlen, Wege zu finden, um die Dokumentation und die periodische Bestätigung der Kontrolle der Umsetzung der Schutzmassnahmen durch die LE zu vereinfachen.

Ausserdem definieren die LB selten ausdrücklich die Verantwortlichkeiten und die Kontrollprozesse für die Umsetzung und Wirksamkeit der Schutzmassnahmen. Nach Meinung der EFK besteht ein echtes Risiko, dass diese Massnahmen mangels Kontrolle schlicht und einfach nicht angewendet werden. Sie hat dem ISB empfohlen, die Weisungen zum Grundschutz dahingehend zu ergänzen, dass den Departementen die Definition von Zuständigkeiten und Kontrollprozessen vorgeschrieben wird.

Das Risikomanagement der nachrichtendienstlichen Ausspähung muss vereinfacht und geklärt werden

Die untersuchten VE wenden die neuen Weisungen über die Risikomanagementmethode zur Reduktion der nachrichtendienstlichen Ausspähung (RINA) an. Sie erachten die Vorgehensweise zwar für nötig, da sie als Reaktion auf ein echtes Risiko erfolgt, halten den dadurch verursachten Aufwand aber für zu gross. Die VE stellen zudem die Relevanz gewisser Analysekriterien und ihre Gewichtung sowie die zu ergreifenden Massnahmen für Objekte mit einem RINA-relevanten Risiko infrage. Die VE konnten diese Einwände in Gesprächen über eine Neuauflage des Prozesses äussern.

Die EFK teilt die Bedenken der Departemente hinsichtlich der Wirksamkeit des RINA-Prozesses in seiner aktuellen Form. [redacted] Die EFK hat dem ISB empfohlen, den Prozess zu vereinfachen und abzuklären, welche Massnahmen zu treffen sind, wenn ein Objekt ein RINA-relevantes Risiko aufweist. Die neue Version der Vorgehensweise könnte sich an den vereinfachten Prozessen orientieren, wie sie in einigen Departementen definiert wurden.

Die Mehrheit der Empfehlungen aus früheren Querschnittsprüfungen wurde umgesetzt

Die EFK stellt fest, dass 12 der 15 in ihrem Monitoringsystem erfassten, noch offenen Empfehlungen aus früheren Querschnittsprüfungen der IT-Sicherheit zwischenzeitlich umgesetzt worden sind. Die Arbeiten für die Umsetzung der drei noch verbleibenden Empfehlungen sind auf Kurs.

Prise de position générale de l’UPIC

L’UPIC salue l’audit transversal mené par le CDF ainsi que les différentes recommandations. Il en tiendra compte notamment lors des différentes mises à jour des directives de sécurité effectuées périodiquement qui tendent à une simplification et à une augmentation de clareté, tout en gardant un niveau de sécurité nécessaire.

Table des matières

1 Mission et déroulement de l’audit 10

1.1 Contexte 10

1.2 Objectifs et questions d’audit 10

1.3 Etendue de l’audit, principes et documentation 10

2 Mise en œuvre des mesures de la protection de base des TIC 11

2.1 Des instructions actuelles et des campagnes de sensibilisation régulières 11

2.2 Le défi de la complexité croissante de la sécurité informatique 12

2.3 Inventaire des objets à protéger et actualité des documents de sécurité : des lacunes 12

2.4 Le contrôle périodique des droits d’utilisateur est souvent négligé 13

2.5 Une collaboration à renforcer dans l’homologation des achats informatiques 13

2.6 Protection de base des applications: une mise en œuvre globalement satisfaisante 14

2.7 Les fournisseurs de prestations satisfont dans l’ensemble aux exigences de la protection de base 14

2.8 Contrôles assurant l’intégrité des systèmes : des efforts à poursuivre 15

2.9 Le contrôle de l’efficacité des mesures doit être amélioré 16

2.10 Une simplification du processus GRAES s’impose 17

3 Suivi de la mise en œuvre de recommandations 18

4 Entretien final 18

Annexe 1 : Bases légales 19

Annexe 2 : Abréviations, glossaire, priorité des recommandations du CDF 20

Annexe 3 : Questions et unités administratives examinées 22

1 Mission et déroulement de l'audit

1.1 Contexte

Le Contrôle des finances (CDF) a procédé entre les mois d'août et décembre 2016 au quatrième audit transversal de la sécurité informatique de la Confédération depuis 2011. Les trois éditions précédentes se sont concentrées sur la mise en œuvre des mesures définies dans les décisions du Conseil fédéral des 16 décembre 2009 et 4 juin 2010. Le présent exercice traite des mesures de contrôle de l'intégrité des systèmes et de protection de base des technologies de l'information et de la communication (TIC). La mise en œuvre de la méthode de gestion des risques visant à réduire les activités d'espionnage de services de renseignement (processus GRAES) est également examinée. Enfin, la présente révision fait le point sur la mise en œuvre des recommandations des précédents audits transversaux de sécurité informatique.

1.2 Objectifs et questions d'audit

L'audit a pour objectif de répondre aux questions suivantes :

1. Des mesures adéquates sont-elles définies et mises en œuvre pour assurer la sécurité des systèmes informatiques, notamment :
   - 1.1. Les mesures de contrôle de l'intégrité des systèmes au sens du chiffre 2g de la décision de Conseil fédéral du 16 décembre 2009 sont-elles correctement mises en œuvre ?
   - 1.2. Des documents de sécurité (analyse des besoins de protection et concept de sûreté de l'information et de protection des données SIPD) valides existent-ils pour les applications critiques contenant des données sensibles?
   - 1.3. L'accès de personnes externes aux infrastructures informatiques de la Confédération est-il suffisamment protégé et surveillé ?
   - 1.4. Les mesures de protection de base des TIC édictées par l'Unité de pilotage informatique de la Confédération (UPIC) dans ses directives du 19 décembre 2013 (version 3.0 du 1er janvier 2016) sont-elles mises en œuvre ?
2. Le processus GRAES est-il mis en œuvre ?
3. Les recommandations émanant des trois précédents audits transversaux de sécurité informatique sont-elles mises en œuvre ?

1.3 Etendue de l'audit, principes et documentation

L'audit a été exécuté dans la période du 24 août au 19 décembre 2016 par Mme Cornelia Simmen et M. André Stauffer, responsable d'audit. Pour répondre aux questions d'audit, les auditeurs ont procédé à des analyses documentaires et à des entretiens approfondis avec les spécialistes de la sécurité informatique. Pour la protection de base, ils se sont concentrés sur les mesures n'ayant pas encore été examinées dans des audits transversaux précédents.

Pour évaluer la protection de base des applications critiques, les auditeurs ont sélectionné une douzaine d'applications, soutenant des processus critiques de chaque département[1]. Ils ont mené divers entretiens, examiné sous un angle formel et matériel les documents de sécurité et évalué les modalités de la télémaintenance. Cette sélection ne saurait toutefois constituer un échantillon représentatif.

Les unités administratives (UA) auditées incluaient des bénéficiaires de prestations (entre autres départements et Chancellerie fédérale), des fournisseurs de prestations et l'UPIC (voir annexe 3 pour la liste des questions et des unités examinées). Ce rapport ne contient que les recommandations interdépartementales.

Le CDF remercie l'ensemble des personnes impliquées dans cette révision pour leur disponibilité et leur collaboration.

2 Mise en œuvre des mesures de la protection de base des TIC

2.1 Des instructions actuelles et des campagnes de sensibilisation régulières

L'UPIC édite et actualise périodiquement un catalogue étendu des mesures de protection de base des TIC. Le Comité de la Sécurité Informatique (C-SI), représentant la voix des spécialistes de la sécurité des départements, est impliqué dans les travaux d'actualisation. Ces directives, adaptées des standards internationaux reconnus (ISO 27002 :2013), forment la base de la pratique dans le domaine civil de l'administration fédérale. Le domaine militaire édite en supplément ses propres directives sur la protection des TIC. Elles reprennent et adaptent les mêmes standards internationaux. Ces directives sont complétées par les instructions éditées par les départements à l'attention de leurs collaborateurs.

Toutes les UA passées en revue procèdent à des activités régulières de sensibilisation à la sécurité informatique. Les nouveaux collaborateurs reçoivent à leur entrée en fonction les instructions portant sur les comportements à adopter et sont formés dans ce sens. Divers moyens sont par ailleurs périodiquement mis en œuvre pour rappeler aux collaborateurs les moyens de se protéger contre les dernières menaces informatiques. Ainsi, les départements font usage du matériel des campagnes de sensibilisation de l'UPIC. Ils les complètent selon les besoins par des démonstrations et des événements spécifiques.

Le CDF estime globalement adéquats les processus de définition des instructions de protection de base des TIC. La mise en œuvre des activités de sensibilisation à la sécurité informatique est jugée satisfaisante.

[1] Selon le rapport final du 18 février 2015 adressé à l'UPIC „Überprüfung der Katastrophenvorsorge in der Bundesverwaltung".

2.2 Le défi de la complexité croissante de la sécurité informatique

Les instructions en matière de protection de base des TIC et les plateformes et applications en service évoluent vers une complexité croissante. Les fournisseurs de prestations (FP) estiment en outre que certaines instructions sont particulièrement difficiles ou coûteuses à mettre en œuvre. Par ailleurs, les DSIO et DSID cumulent souvent plusieurs fonctions en plus de leurs activités liées à la sécurité informatique. Ainsi, divers DSIO sont « Integration Managers » ou impliqués dans des activités de management de la qualité. Pour certains de ces spécialistes, la part du temps dédiée à la sécurité est inférieure à 50 %. Dans certaines unités, les DSIO et DSID doivent s'occuper de centaines d'applications.

Face à cette évolution, le CDF craint que les spécialistes de la sécurité ne soient plus à même de traiter efficacement le domaine. Il estime qu'un pourcentage de travail minimum doit être alloué aux DSIO et DSIS pour remplir correctement leurs tâches. Pour sa part, l'UPIC devra tenter dans la mesure du possible de simplifier les instructions de la protection de base.

A la prochaine mise à jour des instructions, l'UPIC devra également veiller à en analyser la faisabilité et le rapport coûts/utilité, en collaboration avec les FP. Les processus et les instances à cet effet existent déjà et doivent incorporer ces aspects de manière renforcée.

2.3 Inventaire des objets à protéger et actualité des documents de sécurité : des lacunes

Une grande majorité des UA passées en revue tient un inventaire actuel des objets à protéger, à l'aide de l'outil Cockpit ICT. Les militaires possèdent leur propre application, pour des raisons de confidentialité. Les quelques exceptions qui accusent un retard en la matière s'emploient à le combler. Quelques départements font par ailleurs usage de la possibilité, prévue par les instructions du Cockpit ICT, de regrouper les applications de moindre importance sur le plan financier. Dans ces cas, l'inventaire détaillé est incomplet du fait du regroupement.

L'édition des documents de sécurité (analyse des besoins de protection, concept SIPD, mise en œuvre des besoins de protection de base des TIC) est une pratique bien établie dans les projets informatiques des UA passées en revue. Plus de la moitié des départements n'a par contre pas une vue claire de l'actualité des documents de sécurité pour toutes leurs applications en service. Il n'y a pas de point d'accès central à ces documents, et pour diverses applications, ils sont obsolètes ou manquent carrément. Ce même constat a été dressé dans le cadre des analyses lancées dans le sillage de l'affaire RUAG. Des analyses approfondies de la situation et des actions correctives sont en cours au sein des départements lors de l'audit du CDF. L'UPIC finalise en outre une nouvelle version du Cockpit ICT. Celle-ci permettra la tenue des dates de validité des documents de sécurité pour les objets informatiques gérés.

Pour le CDF, un inventaire à jour et complet des objets à protéger constitue un préalable indispensable à la détermination du périmètre de défense. Par ailleurs, les UA doivent disposer de moyens simples pour accéder aux documents de sécurité et en contrôler la validité. Le CDF salue donc les compléments prévus à cet effet dans le Cockpit ICT et les réflexions pour un accès central aux documents (solution en cours d'évaluation). Il estime toutefois que pour le suivi des objets sous l'angle de la sécurité informatique, le regroupement d'applications ne devrait plus être admis (celui-ci devrait rester possible sous l'angle du suivi financier). Il souligne en outre que l'outil ne va pas réduire les risques de données incomplètes, inadéquates ou de documents périmés. Pour ceci, la responsabilité du contrôle de ces éléments doit être réglée (voir ci-dessous).

Recommandation 20.1 (priorité 1) :

Le CDF recommande à l'UPIC de préconiser la tenue de la liste complète des applications et des informations de sécurité (liens vers les documents de sécurité et validité) dans les outils prévus, dans toute la mesure du possible sans regroupement pour le volet de la sécurité informatique.

Prise de position de l'UPIC :

Die Umsetzung der Empfehlung ist bereits in die Wege geleitet: Das ISB prüft zurzeit verschiedene Varianten für ein Werkzeug zur Unterstützung der Informatiksicherheitsbeauftragten im Bereich der Sicherheitsdokumentation. Bis Mitte 2017 soll die Variante bestimmt sein und damit auch ein Fahrplan zur Einführung festgelegt werden.

2.4 Le contrôle périodique des droits d'utilisateur est souvent négligé

Les exigences en matière de contrôle périodique des droits d'utilisateurs octroyés (contrôles annuels et confirmation au DSIO) ne sont que partiellement remplies. La pratique est conforme aux exigences pour certaines applications et certains départements, dans d'autres cas, des mesures d'amélioration sont prévues. Les évidences de la mise en œuvre des contrôles et les confirmations manquent toutefois dans la majorité des cas.

Le CDF a émis des recommandations à l'attention des départements concernés.

2.5 Une collaboration à renforcer dans l'homologation des achats informatiques

Les départements traitant de données confidentielles signalent la prise en compte insuffisante des risques de sécurité lors de l'achat par l'Office fédéral des constructions et de la logistique (OFCL) [redacted] Selon l'UPIC, l'estimation des risques de sécurité d'un nouvel appareil doit être prévue dans le processus d'homologation, qui est du ressort de l'OFCL.

[redacted]. Le CDF estime nécessaire de rappeler à l'OFCL la problématique de la sécurité informatique des appareils bureautiques sur la base de cet exemple.

Recommandation 20.2 (priorité 2) :

Le CDF recommande à l'UPIC de revérifier les risques liés à l'utilisation [redacted] *de définir les éventuelles mesures compensatoires et d'organiser une information à l'attention des unités administratives concernées.*

Prise de position de l'UPIC :

L'UPIC est d'avis que ces risques doivent être traités dans le cadre du processus d'achat et d'homologation de matériel informatique et vérifiera en collaboration avec l'OFCL [redacted].

2.6 Protection de base des applications: une mise en œuvre globalement satisfaisante

Pour une majorité des douze applications passées en revue, les documents de sécurité – analyses des besoins de protection et concepts SIPD – sont disponibles et actuels. Les approbations formelles manquent toutefois à diverses reprises. Par ailleurs, la preuve de la mise en œuvre des mesures de la protection de base fait défaut pour une des applications. Une recommandation a été émise à l'unité concernée. Dans un des cas analysés, le concept SIPD n'a pas été actualisé en raison de l'imminence de la mise en production d'une nouvelle application. En cas de report de la mise en service, le DSIO devra produire le document pour l'application existante.

Sur un plan matériel, la révision fait ressortir que la majorité des concepts SIPD répondent de manière appropriée aux exigences de l'analyse des besoins en protection. Les éventuels risques résiduels sont également correctement mis en évidence. Le CDF remet toutefois en question l'analyse des besoins de protection d'une des applications passées en revue. Il estime que les exigences de confidentialité des données sont sous-estimées. La problématique est connue des responsables applicatifs et une solution est en cours de réalisation.

Des activités de télémaintenance sur les environnements productifs sont effectuées pour trois des applications de l'échantillon. Dans ces cas, les prescriptions réglant la télémaintenance sont respectées : d'une part, les comptes utilisés pour l'accès à distance sont définis séparément, et l'OFIT enregistre leurs connexions et déconnexions. D'autre part, les activités de télémaintenance dans les applications sont journalisées. Les bénéficiaires de prestations (BP) contrôlent la réalisation de leurs demandes.
Pour le reste de l'échantillon examiné, aucun recours à la télémaintenance n'est constaté. Soit les prestataires externes n'ont accès qu'aux environnements de développement. Ils doivent alors utiliser les moyens techniques d'accès prévus par l'OFIT et leur accès sont enregistrés. Soit les prestataires externes doivent effectuer leur travail sur place.

De l'avis du CDF, aucune autre mesure corrective n'est requise à cet égard.

2.7 Les fournisseurs de prestations satisfont dans l'ensemble aux exigences de la protection de base

Pour les projets informatiques, tous les FP passés en revue sont impliqués dans l'édition ou le contrôle des documents de sécurité. Ils tiennent également les preuves de la mise en œuvre des mesures de protection de base des TIC leur incombant à disposition des BP.

De manière générale, le CDF note que divers projets d'amélioration continue sont en cours chez les FP en matière de sécurité. Il relève notamment les efforts d'épuration des utilisateurs des services d'annuaire centralisés fournis par l'OFIT. Ce point avait fait l'objet de plusieurs recommandations dans des audits de sécurité antérieurs. Le CDF n'a pas constaté de manquement important dans les pratiques de la protection de base des TIC par les FP. Tout au plus a-t-il recommandé à un FP l'extension de l'enregistrement des activités d'administration système à toutes les applications productives en service dans son centre de calcul.

Le CDF ne propose en l'état aucune autre mesure d'amélioration immédiate.

2.8 Contrôles assurant l'intégrité des systèmes : des efforts à poursuivre

Dans sa décision du 16.12.2009, chiffre 2g, le Conseil fédéral a donné mandat à l'UPIC de définir les concepts et mesures de contrôle afin d'assurer l'intégrité des systèmes. L'UPIC considère avoir intégré ces mesures dans la partie des instructions relatives à la protection de base des TIC portant sur l'exploitation. Les FP passés en revue mettent en œuvre la majorité des mesures définies. Une certaine confusion règne toutefois autour du concept d'intégrité des systèmes et des moyens de l'assurer. Les techniques mises en œuvre par les FP en vue du contrôle des logiciels en service (vérification de l'authenticité et analyse des modifications) diffèrent sensiblement. Des procédés de vérification à l'aide de signature de code sont occasionnellement utilisés. Des outils d'analyses des modifications couvrent partiellement les plateformes en service. Dans tous les cas, les FP audités attendent unanimement des compléments d'information sur le sujet.

Le CDF considère qu'un premier pas a été fait dans la mise en œuvre des mesures de contrôle assurant l'intégrité des systèmes. Il encourage l'UPIC à poursuivre la démarche en précisant les notions d'intégrité et en regroupant les prescriptions. Pour le CDF, le contrôle des logiciels en service (selon la définition de la protection de base, chiffre 12.5) revêt en outre une importance particulière et doit être concrétisé. Les possibilités d'un recours accru aux technologies de signature de code, déjà partiellement mises en œuvre au sein de la Confédération, doivent notamment être considérées.

Recommandation 20.3 (priorité 1) :

Le CDF recommande à l'UPIC de clarifier la notion d'intégrité des systèmes et de concrétiser les prescriptions de sécurité qui s'y rapportent. Ces éléments doivent former la base des mesures à mettre en œuvre par la suite.

Prise de position de l'UPIC : L'UPIC propose d'étudier la création d'un outil d'aide ou d'une recommandation à la protection de base des TIC spécifique à la vérification de l'intégrité des systèmes.

Recommandation 20.4 (priorité 2) :

Le CDF recommande à l'UPIC de définir en collaboration avec les fournisseurs de prestations les solutions à mettre en œuvre pour surveiller l'intégrité des logiciels en service. L'opportunité de la coordination des outils et procédés, la possibilité d'achats groupés de ces outils ainsi que l'étendue de la couverture des plateformes devraient notamment être déterminées.

Prise de position de l'UPIC :

En fonction des résultats de l'analyse effectuée dans le cadre de la recommandation 20.3, de telles possibilités seront évaluées.

2.9 Le contrôle de l'efficacité des mesures doit être amélioré

Selon les directives relatives à la protection de base des TIC, la responsabilité de la mise en œuvre des prescriptions et mesures incombe selon leur nature aux BP, aux FP ou aux utilisateurs. Les directives du Conseil fédéral sur la sécurité informatique dans l'administration fédérale prescrivent aux BP de documenter et contrôler la mise en œuvre des mesures ainsi que leur efficacité.

Dans une majorité de cas, les BP documentent pour chaque projet ou application les mesures mises en œuvre au moyen de l'outil à cet effet utilisé dans l'organisation. Ils invitent les FP à documenter les mesures qui leur incombent. Ceux-ci s'exécutent en complétant pour chaque projet ou application les rubriques de l'outil qui leur sont dévolues, ou au moyen de rapports.

Les pratiques sont par contre très variées en matière de contrôle et de documentation de la mise en œuvre et de l'efficacité des mesures. Pour les mesures de leur ressort, les BP ne contrôlent et documentent la mise en œuvre et l'efficacité que dans les meilleurs cas. Ces pratiques ne sont cependant pas systématiques. Pour les mesures incombant aux FP, ceux-ci fournissent dans certains cas des rapports de contrôle ou d'audit externe aux BP, automatiquement ou sur demande. Toutefois, les BP ne disposent souvent pas des évidences de la mise en œuvre et de l'efficacité des mesures, et ne les demandent pas.

Le CDF estime que le système actuel de contrôle des mesures et de leur efficacité est peu efficient. Les outils utilisés et leurs 17 chapitres, occasionnent une charge de travail conséquente. Ils impliquent que les FP répondent aux mêmes questions pour chaque application ou projet, alors que les plateformes mises en œuvre répondent souvent aux mêmes exigences. La démarche pourrait être simplifiée, en s'inspirant de la pratique de certains FP. Pour leurs plateformes techniques, ces derniers garantissent le respect global des mesures leur incombant, en notant uniquement les éventuelles exceptions. Ils s'épargnent ainsi la répétition des réponses détaillées documentées dans les outils actuels.

Le CDF regrette également que les BP ne définissent pas systématiquement les processus et les responsabilités des contrôles de la mise en œuvre et de l'efficacité des mesures. Il existe un risque réel que certaines prescriptions de la protection de base ne soient simplement pas appliquées, faute de contrôle. La découverte de vulnérabilités suite à des incidents de sécurité peut ainsi occasionner de coûteux exercices d'analyse de la situation et de remise en conformité. Chaque département devrait rester libre d'assigner la responsabilité des contrôles aux instances qu'il juge les plus compétentes. Toutefois, cette responsabilité devrait être explicitement définie et les processus décrits.

Recommandation 20.5 (priorité 1) :

Le CDF recommande à l'UPIC de concevoir et mettre en place les moyens permettant un contrôle facilité de la mise en œuvre des mesures de la protection de base. L'objectif à poursuivre est d'éliminer les redondances dans la documentation et d'assurer que les processus du contrôle de mise en œuvre fonctionnent efficacement dans les départements.

Prise de position de l'UPIC:
L'UPIC considère qu'il est bon de rappeler aux unités adminstratives qu'elles sont responsables de la mise en œuvre des mesures de sécurité. Afin de les aider à en effectuer le contrôle, une adaptation de la documentation sera étudiée.

2.10 Une simplification du processus GRAES s'impose

L'UPIC a intégré le processus GRAES dans les outils de l'analyse des besoins de protection. Les nouvelles instructions sont applicables à tous les projets informatiques pour lesquels un mandat d'initialisation est émis dès le 1er janvier 2016. Les UA appliquent les nouvelles directives à leurs projets en phase de démarrage. La nouvelle version des documents d'analyse des besoins de protection, incluant le questionnaire GRAES, est en effet utilisée à large échelle.

Les UA passées en revue estiment que le principe de la GRAES répond à un risque réel. Elles considèrent cependant que la démarche occasionne un travail trop important et que certains critères d'analyse sont peu fondés. [redacted]. La pondération des critères est également remise en question. Certains départements ont d'ailleurs édité leur propre marche à suivre simplifiée pour l'identification des objets présentant un risque sur le plan de la GRAES. Les UA émettent en outre des réserves sur les mesures à adopter pour les projets identifiés. Elles s'interrogent enfin sur le traitement des applications déjà en service.

Les UA ont eu l'occasion d'exprimer ces objections à l'UPIC lors des discussions sur l'état de la première mouture de la GRAES à fin 2016. Pendant la révision du CDF, l'UPIC a entamé le travail en vue d'une deuxième version du processus.

Le CDF partage les réserves émises par les départements sur l'efficacité du processus GRAES dans sa forme actuelle. [redacted] De plus, le CDF estime que la marche à suivre en cas de risque GRAES avéré, pour les projets, mais aussi pour les applications et infrastructures en service, doit être mieux définie. Pour ces dernières, le coût d'éventuelles analyses et mesures devra être pris en considération. La nouvelle version du processus GRAES pourrait s'inspirer des processus simplifiés définis dans certains départements.

Recommandation 20.6 (priorité 1) :

Le CDF recommande à l'UPIC de simplifier fortement les critères d'analyse du processus GRAES et de définir plus clairement la marche à suivre en cas de risque avéré d'un projet ou d'applications ou infrastructures en service.

Prise de position de l'UPIC: Le processus GRAES a été, comme mentionné dans ce rapport, déjà adapté en une version 1.1 simplifiée. [redacted] Sur la bases des expériences des unités administratives, l'UPIC poursuivra la recherche de simplification dans la mesure où le niveau de sécurité à atteindre le permet.

3 Suivi de la mise en œuvre de recommandations

Le CDF avait encore quinze recommandations de précédents audits transversaux de la sécurité informatique encore ouvertes dans son système de suivi au démarrage de la révision. Le CDF constate que douze d'entre elles ont été mises en œuvre et les clôt.

Une des recommandations restantes concerne le stockage centralisé des documents de sécurité dans un département. La deuxième concerne la mise en œuvre d'exigences relatives à la protection de l'information et des données dans un département. La troisième est adressée à un FP et concerne la mise hors service d'un outil permettant la gestion de droits d'administrateur local. Les travaux de mise en œuvre des trois recommandations restantes sont en cours et feront l'objet de contrôles ultérieurs.

4 Entretien final

Les résultats de la révision ont été discutés le 7 avril avec le Délégué de l'UPIC, le Chef de la sécurité en matière de TIC (SEC) et la Déléguée à la sécurité informatique de la Confédération

Le CDF était représenté par la Directrice suppléante, le Responsable de centre de compétences et le Responsable de révision.

Les représentants de l'UPIC ont pris connaissance des constats de la révision et en ont accepté les conclusions.

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

CONTRÔLE FEDERAL DES FINANCES

Annexe 1 : Bases légales

Loi sur le Contrôle des finances (LCF, RS 614.0)

Ordonnance sur l'informatique dans l'administration fédérale (OIAF, RS 172.010.58)

Directives du Conseil fédéral concernant la sécurité informatique dans l'administration fédérale du 1er juillet 2015

Lignes directrices relatives à la sécurité informatique dans l'administration fédérale du 1er mars 2015

Directives sur la protection informatique de base dans l'administration fédérale du 19 décembre 2013, version 3.0 du 1er janvier 2016

Annexe 2 : Abréviations, glossaire, priorité des recommandations du CDF

Abréviations

BAC	Base d'aide au commandement
BP	Bénéficiaires de prestations informatiques
CDF	Contrôle des finances
C-SI	Comité de la sécurité informatique
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DSID	Délégué à la sécurité informatique du département
DSIO	Délégué à la sécurité informatique de l'unité
FP	Fournisseur de prestations informatiques
ISCeco	Centre de services informatiques du DEFR
ISC-EJPD	Centre de services informatiques du DFJP
OFCL	Office fédéral des constructions et de la logistique
OFIT	Office fédéral de l'informatique et de la télécommunication
TIC	Technologies de l'information et de la communication
UA	Unité administrative
UPIC	Unité de pilotage informatique de la Confédération

Glossaire

Cockpit ICT	Outil de gestion du portefeuille informatique de la Confédération
Concept SIPD	Concept de sureté de l'information et de protection des données, partie de la documentation de sécurité d'une application informatique
ISO 27002 :2013	Norme international concernant la sécurité de l'information
LDAP	Lightweight directory access protocol, protocole permettant l'interrogation et la modification de services d'annuaires
Processus GRAES	Processus relatif à la méthode de gestion des risques visant à réduire les activités d'espionnage de services de renseignement

Priorité des recommandations du CDF:

Le CDF priorise ses recommandations en se fondant sur des 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).

Annexe 3 : Questions et unités administratives examinées

Questions examinées et acteurs prioritairement concernées

Question d’audit	Bénéficiaires de prestations	Fournisseurs de prestations
1.1 Intégrité des systèmes		X
1.2 Existence et validité des documents de sécurité pour les applications critiques	X	
1.3 Accès de personnes externes aux infrastructures informatiques		X
1.4 Mise en œuvre des mesures de protection de base	X	X
2. Mise en œuvre du processus GRAES	X	
3. Suivi des recommandations	X	X

Unités administratives examinées

Départements, représentés par leur délégué à la sécurité informatique (DSID) :

- Département fédéral des affaires étrangères (DFAE)
- Département fédéral de l’intérieur (DFI)
- Département fédéral de justice et police (DFJP)
- Département fédéral de la défense, de la protection de la population et des sports (DDPS)
- Département fédéral des finances (DFF)
- Département fédéral de l’économie, de la formation et de la recherche (DEFR)
- Département fédéral de l’environnement, des transports, de l’énergie et de la communication (DETEC)

Autres unités administratives :

- Chancellerie fédérale, représentée par son délégué à la sécurité informatique (DSIO)
- Unité de pilotage informatique de la Confédération, représentée par le chef de la sécurité en matière de TIC

Fournisseurs de prestations, représentés par leur DSIO :

- Centre de services informatiques du DFJP (ISC-EJPD)
- Centre de services informatiques du DEFR (ISCeco)
- Informatique DFAE
- Office fédéral de l’informatique et de la télécommunication (OFIT)
- Base d’aide au commandement du DDPS (BAC)

Unités administratives propriétaires des applications, représentées par leurs responsables applicatifs et leurs DSIO