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

Prüfung der IT-Sicherheit des Zugangs zu GEVER

Bundesamt für Meteorologie und Klimatologie

EFK-21286 | inkl. Stellungnahmen | 22. Oktober 2021 | FinDel D6/2021

Bestelladresse	Eidgenössische Finanzkontrolle (EFK)
Adresse de commande	Monbijoustrasse 45
Indirizzo di ordinazione	3003 Bern
Ordering address	Schweiz
Bestellnummer	311.21286
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)

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Das Wesentliche in Kürze **4**

L'essentiel en bref **6**

L'essenziale in breve **8**

Key facts **10**

1 Auftrag und Vorgehen **12**

1.1 Ausgangslage 12

1.2 Prüfungsziel und -fragen 13

1.3 Prüfungsumfang und -grundsätze 13

1.4 Unterlagen und Auskunftserteilung 13

1.5 Schlussbesprechung 13

2 IKT-Sicherheit bei MeteoSchweiz **14**

2.1 Die IKT-Sicherheit weist eine hohe Maturität aus 14

2.2 Die Arbeitsplatzsicherheit entspricht den Anforderungen des Bundes 14

2.3 Die Netzwerksicherheit genügt den Vorgaben des Bundes 17

3 Keine Gefährdung von GEVER Bund durch Bearbeitung von Daten mit erhöhtem Schutzbedarf **19**

Anhang 1: Rechtsgrundlagen **20**

Anhang 2: Abkürzungen **21**

Anhang 3: Glossar **22**

Prüfung der IT-Sicherheit des Zugangs zu GEVER
Bundesamt für Meteorologie und Klimatologie

Das Wesentliche in Kürze

Das Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz) ist der nationale Wetterdienst. Im Auftrag des Bundes erbringt MeteoSchweiz Wetter- und Klimadienstleistungen zugunsten der Bevölkerung, der Behörden und des zivilen sowie militärischen Flugbetriebs. Vor diesem Hintergrund sind die Anforderungen an die Verfügbarkeit und Funktionstüchtigkeit der Informations- und Kommunikationstechnologien (IKT) sehr hoch, weshalb MeteoSchweiz auch vom Bundesamt für Zivilluftfahrt beaufsichtigt wird. Aufgrund der besonderen fachlichen und betrieblichen Anforderungen betreibt MeteoSchweiz mit wenigen Ausnahmen die IKT-Infrastruktur selber und ist daher nicht direkt in das Bundesnetz integriert, sondern nur kontrolliert angebunden.

Mit Einführung der GEVER-Verordnung müssen sämtliche Bundesstellen ihre geschäftsrelevanten Daten in einem elektronischen Geschäftsverwaltungssystem bearbeiten. Da MeteoSchweiz nicht direkt im Bundesnetz integriert ist, darf das Amt seit der Migration im Dezember 2020 im GEVER-System vorerst nur Daten ohne erhöhte Sicherheitsanforderungen bearbeiten. Um die Bearbeitung von Daten mit erhöhten Schutzanforderungen zu ermöglichen, benötigt MeteoSchweiz einen vollständigen Zugang. Dieser wurde im vergangenen Jahr beim Informatiksteuerungsorgan Bund (ISB)[1] beantragt. Für eine definitive Genehmigung machte das ISB gewisse Auflagen. Um die Erfüllung der Auflagen zu prüfen, wurde die Eidgenössische Finanzkontrolle (EFK) angefragt, eine unabhängige Beurteilung der Informationssicherheit bei MeteoSchweiz abzugeben. Die Prüfergebnisse sind insgesamt gut.

Die Informationssicherheit ist auf einem hohen Niveau

Sowohl der organisatorische als auch der technische Reifegrad der Informationssicherheit bei MeteoSchweiz weist eine hohe Maturität aus. Die Umsetzung der Bundesvorgaben, aber auch internationaler Standards, haben im Rahmen der Prüfung keine wesentlichen Abweichungen gezeigt. Die Netzwerk- und Arbeitsplatzsicherheit entspricht mindestens dem Niveau der Bundesverwaltung.

Um dem Risiko einer unbewussten oder fehlerhaften Manipulation entgegenzuwirken, sollte MeteoSchweiz beim Einsatz von Benutzerkonten mit privilegierten Rechten auf den Arbeitsplätzen eine gezieltere Sensibilisierung der betroffenen Mitarbeitenden schaffen.

Die Verschlüsselungssoftware «SecureCenter» ist bei MeteoSchweiz zwar vorhanden, aber noch nicht etabliert. Es kommen verschiedene andere Werkzeuge zum Schutz von vertraulichen Daten zur Anwendung. Dies birgt längerfristig ein Risiko, diese Informationen nicht mehr lesen zu können. Hier muss MeteoSchweiz mit einer flächendeckenden Information und Schulung aktiv werden.

[1] Seit 1. Januar 2021 Digitale Transformation und IKT-Lenkung bei der Bundeskanzlei

Im Rahmen der Prüfung konnte die EFK keine zusätzlichen Risiken feststellen, welche den vollumfänglichen Zugriff auf das GEVER-System durch MeteoSchweiz infrage stellen würden. Die Schutzvorkehrungen in den Systemen und auf den Netzen entsprechen den Vorgaben des Bundes und sind wirksam. Die oben erwähnten Empfehlungen haben aus Sicht der EFK keinen negativen Einfluss auf das GEVER-System des Bundes.

Audit de la sécurité informatique de l'accès à GEVER
Office fédéral de météorologie et de climatologie

L'essentiel en bref

L'Office fédéral de météorologie et de climatologie (MétéoSuisse) est le service météorologique national. Sur mandat de la Confédération, MétéoSuisse fournit des services météorologiques et climatologiques à la population et aux autorités, ainsi que pour les opérations de vol civiles et militaires. Dans ce contexte, les exigences en matière de disponibilité et de bon fonctionnement des technologies de l'information et de la communication (TIC) sont très hautes. C'est pourquoi MétéoSuisse est aussi soumis à la surveillance de l'Office fédéral de l'aviation civile. En raison des exigences techniques et opérationnelles particulières, MétéoSuisse exploite sa propre infrastructure informatique, à quelques exceptions près. L'office n'est donc pas directement intégré au réseau de la Confédération, mais seulement relié de manière contrôlée.

Avec l'introduction de l'ordonnance GEVER, tous les services de l'administration fédérale doivent traiter leurs données importantes pour les affaires dans un système de gestion électronique des affaires. Comme MétéoSuisse n'est pas intégré au réseau de la Confédération, l'office ne peut, depuis la migration vers le système GEVER en décembre 2020, traiter que des données sans exigences de sécurité accrues. Afin de pouvoir traiter les données avec des exigences plus élevées en matière de protection, MétéoSuisse a besoin d'un accès complet. Cet accès a été demandé à l'Unité de pilotage informatique de la Confédération (UPIC)[1] l'année passée. L'autorisation définitive de l'UPIC a été assortie de certaines conditions. Pour vérifier si les conditions sont remplies, une évaluation indépendante de la sécurité de l'information chez MétéoSuisse a été confiée au Contrôle fédéral des finances (CDF). Dans l'ensemble, les résultats de l'audit sont bons.

Le niveau de sécurité informatique est élevé

La sécurité informatique chez MétéoSuisse présente un degré de maturité élevé, tant sur les plans organisationnel que technique. La mise en œuvre des directives fédérales et des normes internationales n'ont révélé aucune différence importante lors de l'audit. Le niveau de sécurité sur les réseaux et sur les postes de travail correspond au moins à celui de l'administration fédérale.

Afin d'éviter tout risque de manipulation involontaire ou erronée, MétéoSuisse devrait sensibiliser davantage les collaborateurs concernés lors de l'utilisation de comptes d'utilisateurs avec des droits privilégiés sur les postes de travail.

Le logiciel de cryptage « SecureCenter » est disponible au sein de MétéoSuisse, mais il n'est pas encore établi. Différents autres outils de protection des données confidentielles sont utilisés. Or cela comporte un risque à long terme de ne plus pouvoir lire ces informations. MétéoSuisse doit agir et mettre en place une information et une formation complètes dans ce domaine.

[1] Depuis le 1er janvier 2021, secteur Transformation numérique et gouvernance de l'informatique (TNI) à la Chancellerie fédérale.

Dans le cadre de l'audit, le CDF n'a pas identifié d'autres risques qui remettraient en question l'accès total de MétéoSuisse au système GEVER. Les mesures de protection dans les systèmes et les réseaux correspondent aux directives de la Confédération et sont efficaces. Les recommandations mentionnées plus haut n'ont pas d'influence négative sur le système GEVER de la Confédération du point de vue du CDF.

Texte original en allemand

Verifica della sicurezza informatica dell'accesso a GEVER
Ufficio federale di meteorologia e climatologia

L'essenziale in breve

L'Ufficio federale di meteorologia e climatologia (MeteoSvizzera) funge da servizio meteorologico nazionale. Su incarico della Confederazione, MeteoSvizzera fornisce servizi meteorologici e climatologici per la popolazione, le autorità nonché per il servizio e la sicurezza aerei civile e militare. In questo contesto, i requisiti in materia di disponibilità e funzionalità delle tecnologie dell'informazione e della comunicazione (TIC) sono molto elevati. Pertanto MeteoSvizzera è sottoposto anche alla vigilanza dell'Ufficio federale dell'aviazione civile. A causa dei particolari requisiti tecnici e operativi, MeteoSvizzera gestisce autonomamente l'infrastruttura TIC, a parte qualche eccezione. L'Ufficio non è quindi direttamente integrato nella rete della Confederazione, ma sotto il suo controllo.

Con l'introduzione dell'ordinanza GEVER, tutti gli uffici federali devono elaborare i propri dati pertinenti agli affari in un sistema di gestione elettronica degli affari. Poiché non è direttamente integrato nella rete della Confederazione, a partire dalla migrazione avvenuta nel mese di dicembre del 2020 MeteoSvizzera può elaborare nel sistema GEVER soltanto dati senza requisiti di sicurezza elevati. Per elaborare dati con esigenze elevate in materia di protezione dei dati, MeteoSvizzera deve poter disporre di un accesso completo. A tal fine, nel 2020 è stata inoltrata una domanda all'Organo direzione informatica della Confederazione (ODIC)[1] . Prima dell'approvazione definitiva, l'ODIC ha posto determinate condizioni. Per verificare il rispetto di queste condizioni, il Controllo federale delle finanze (CDF) è stato incaricato di fornire una valutazione indipendente sulla sicurezza delle informazioni di MeteoSvizzera. I risultati della verifica sono complessivamente buoni.

Il livello di sicurezza delle informazioni è elevato

La sicurezza delle informazioni di MeteoSvizzera presenta un grado di maturità elevato sia sul piano organizzativo sia su quello tecnico. Dalla verifica non sono emerse differenze significative nell'attuazione delle direttive della Confederazione come pure degli standard internazionali. Il livello di sicurezza nella rete e nelle postazioni di lavoro corrisponde almeno a quello dell'Amministrazione federale.

Per evitare eventuali rischi di manipolazione involontaria o errata, MeteoSvizzera dovrebbe sensibilizzare i collaboratori aventi diritti privilegiati nelle proprie postazioni di lavoro sui rischi connessi all'uso dei conti utente.

Il software di crittografia «SecureCenter» è disponibile presso MeteoSvizzera, ma non sempre viene utilizzato. L'Ufficio ricorre ad altri strumenti che consentono di proteggere i dati confidenziali. Tuttavia vi è il rischio che queste informazioni non siano più leggibili a lungo termine. MeteoSvizzera deve garantire quanto prima un'informazione capillare e una formazione esaustiva in tale ambito.

[1] Dal 1° gennaio 2021 settore Trasformazione digitale e governance delle TIC della Cancelleria federale.

Nel quadro della verifica, il CDF non ha individuato altri rischi che potrebbero compromettere l'accesso completo di MeteoSvizzera al sistema GEVER. Le misure di protezione applicate nei sistemi e nelle reti sono conformi alle direttive della Confederazione e sono efficaci. Secondo il CDF, le raccomandazioni summenzionate non hanno alcun effetto negativo sul sistema GEVER della Confederazione.

Testo originale in tedesco

Audit of the IT security for access to GEVER
Federal Office of Meteorology and Climatology

Key facts

The Federal Office of Meteorology and Climatology (MeteoSwiss) is the national weather service. On behalf of the Confederation, MeteoSwiss provides weather and climate services for the benefit of the public, the authorities and civil and military aviation. As a result, the requirements for the availability and functionality of information and communication technologies (ICT) are very high, which is why MeteoSwiss is also supervised by the Federal Office of Civil Aviation. Due to the special technical and operational requirements, MeteoSwiss operates the ICT infrastructure itself with only a few exceptions and is therefore not directly integrated into the federal network. Instead, it is only connected in a controlled manner.

Following the introduction of the GEVER Ordinance, all federal units must process their business-relevant data in an electronic business management system. Since the migration in December 2020, MeteoSwiss may only process data with no enhanced security requirements in the GEVER system, because it is not directly integrated into the federal network. MeteoSwiss needs full access in order to be able to process data with increased protection requirements. A request for this was submitted to the Federal IT Steering Unit (FITSU)[1] last year. The FITSU imposed certain conditions in order to grant final approval. In order to check compliance with the conditions, the Swiss Federal Audit Office (SFAO) was asked to provide an independent assessment of IT security at MeteoSwiss. Overall, the audit findings were good.

IT security is of a high standard

Both the organisational and the technical maturity of IT security at MeteoSwiss are advanced. No significant deviations were found in the implementation of the federal requirements and international standards during the audit. The network and workplace security is at least equivalent to the level of the Federal Administration.

In order to counteract the risk of unconscious or erroneous tampering, MeteoSwiss should take a more targeted approach to raising the awareness of the employees concerned when using user accounts with privileged rights on workstations.

The SecureCenter encryption software is available at MeteoSwiss, but is not yet well established. Various other tools are used to protect confidential data. In the longer term, this creates a risk of no longer being able to read this information. MeteoSwiss must play an active role here by providing comprehensive information and training.

During the audit, the SFAO was unable to identify any additional risks that would jeopardise MeteoSwiss' full access to the GEVER system. The safeguards in the systems and the networks comply with the federal requirements and are effective. In the SFAO's view, the above recommendations have no negative impact on the federal GEVER system.

Original text in German

[1] Since 1 January 2021: Digital Transformation and ICT Steering unit of the Federal Chancellery

Generelle Stellungnahme von MeteoSchweiz

Das Bundesamt für Meteorologie und Klimatologie MeteoSchweiz bedankt sich für den vorliegenden Bericht und ist mit den darin enthaltenen Aussagen einverstanden. Es freut uns, dass die EFK der MeteoSchweiz eine hohe Maturität der IT-Sicherheit attestiert und die Umsetzung des vollumfänglichen Zugriffs auf das GEVER-System für MeteoSchweiz bestätigt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz) erbringt im Auftrag des Bundes Wetter- und Klimadienstleistungen zum Schutz und zum Nutzen der Schweiz. Die geschäftskritischen Tätigkeiten von MeteoSchweiz setzen einen 7x24-Stunden-Einsatz und höchste Verfügbarkeit der Informations- und Kommunikationstechnologie (IKT) voraus. Serviceausfälle können sich insbesondere auf den zivilen Flugbetrieb, die Bevölkerung und die Krisenstäbe von Bund und Kantonen in Unwettersituationen auswirken. Im Bereich des Flugwetters untersteht MeteoSchweiz internationalen, europäischen und nationalen Regulationen und wird daher regelmässig vom Bundesamt für Zivilluftfahrt (BAZL) sowie von der europäischen Flugsicherheitsbehörde (EASA) geprüft. Die Erfüllung regulatorischer Vorgaben ist eine zwingende Voraussetzung für die Erbringung der Flugwetterdienstleistungen.

Gemäss der GEVER-Verordnung[2] muss die Bundesverwaltung (BV) ihre geschäftsrelevanten Informationen in elektronischen Geschäftsverwaltungssystemen bearbeiten. Um die elektronische Geschäftsverwaltung (GEVER) gemäss den entsprechenden Gesetzesgrundlagen konform nutzen zu können, benötigt MeteoSchweiz den vollen Zugang zu GEVER. Da MeteoSchweiz eine eigene Netzwerkzone betreibt, erfolgt der Zugriff via ein kontrolliertes Transitnetz zwischen MeteoSchweiz und dem Bundesamt für Informatik und Telekommunikation (BIT). Aus diesem Grund muss der Zugriff für die Bearbeitung von Dokumenten mit erhöhtem Schutzbedarf[3] für die Anbindung von MeteoSchweiz explizit freigeschaltet werden.

Mit Antrag vom 8. Mai 2020[4] hat MeteoSchweiz den «SN2-Zugriff für GEVER via Transitnetz-Verbindungen» beim Informatiksteuerungsorgan des Bundes (ISB)[5] beantragt. Nach der Beurteilung des Informatiksicherheitsbeauftragten für die Standarddienste kam die Geschäftsleitung des ISB zum Schluss, der Anforderung unter Auflagen zu entsprechen:

- Die Netze von MeteoSchweiz bieten einen adäquaten Schutz (Analog APS Zone[6]) und setzen die Massnahmen des Informationssicherheits- und Datenschutzkonzepts (ISDS) GEVER um;
- Die Arbeitsplätze von MeteoSchweiz erfüllen die Massnahmen des ISDS-Konzepts «Arbeitsplatz Büroautomation» und des ISDS-Konzepts «Secure Center»;
- Es gibt keine zusätzlichen Risiken für die SN2-Daten in GEVER und das GEVER Bund System, die aus der Integration von MeteoSchweiz entstehen könnten;
- Die obigen Auflagen werden durch ein IKT-Sicherheitsaudit (extern oder Finanzkontrolle) im Auftrag des ISB überprüft und müssen als erfüllt beurteilt werden. Das Audit vergleicht die Anforderungen und Massnahmen der ISDS-Konzepte der betroffenen Standarddienste mit den ISDS-Konzepten von MeteoSchweiz und beurteilt die konkreten Implementierungen in deren Umfeld.

---

[2] Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (SR 172.010.441) vom 3. April 2019 (Stand am 1. Januar 2021)

[3] Schutzstufe 2 (SN2), siehe Zugriffsmatrix Anhang B der Si003 – Netzwerksicherheit in der Bundesverwaltung vom 19. Dezember 2013 (Stand 1. April 2021)

[4] P035-Antrag; Anf2020-049

[5] Seit 1. Januar 2021 Digitale Transformation und IKT-Lenkung (DTI) bei der Bundeskanzlei (BK)

[6] APS Zone – Unterzone der Client Zone (CZ) für Client-Systeme, die als Arbeitsplatzsysteme (APS) ausgelegt sind und ausschliesslich für den IKT-Standarddienst BA/UCC eingesetzt werden. Siehe Si003 – Netzwerksicherheit in der Bundesverwaltung vom 19. Dezember 2013 (Stand 1. April 2021)

1.2 Prüfungsziel und -fragen

Die Prüfung soll aufzeigen, ob die Sicherheit der Netzzonen und der Clients von MeteoSchweiz die Anforderungen an die Bearbeitung von Daten mit erhöhtem Schutzbedarf erfüllen.

Die Prüffragen lauteten:

1. Bieten die Netze einen adäquaten Schutz (analog APS Zone) und setzt MeteoSchweiz die Massnahmen des ISDS-Konzepts GEVER um?
2. Erfüllen die Arbeitsplätze die Massnahmen der beiden ISDS-Konzepte «Arbeitsplatz Büroautomation» und «Secure Center»?
3. Bestehen keine zusätzlichen Risiken für die SN2-Daten in GEVER und das GEVER Bund System, die aus der Implementation der MeteoSchweiz entstehen könnten?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roland Gafner (Revisionsleiter), Warren Paulus und Christian Brunner vom 12. April bis 14. Mai 2021 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger.

Die Beurteilungen orientieren sich an der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV), dem «IKT-Grundschutz der Bundesverwaltung» und der «Netzwerksicherheit in der Bundesverwaltung». Weiter kamen die Empfehlungen der International Organization for Standardization (ISO/IEC) Standards 2700x zur Anwendung.

Die Ergebnisbesprechung hat am 30. April 2021 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von MeteoSchweiz umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 13. September 2021 statt. Teilgenommen haben seitens MeteoSchweiz der Direktor, der Abteilungsleiter ICT - Informations- und Kommtechnik, der Abteilungsleiter PKS – Sicherheit und Qualität und der Chief Information Security Officer. Das Nationale Zentrum für Cybersicherheit (NCSC) wurde durch den Leiter Informatiksicherheit Bund vertreten. Die Digitale Transformation und IKT-Lenkung (DTI) wurden auf dem Zirkularweg begrüsst. Seitens EFK haben der Federführende und der Revisionsleiter teilgenommen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 IKT-Sicherheit bei MeteoSchweiz

2.1 Die IKT-Sicherheit weist eine hohe Maturität aus

Die Ziele, Aufgaben und Aktivitäten im Bereich der Informationssicherheit sind innerhalb der Strategie festgehalten und werden im ordentlichen Prozess jährlich oder bei Bedarf überprüft. Detaillierte unternehmensweite Vorgaben stehen allen Mitarbeitenden zur Verfügung. Die Rollen und Verantwortlichkeiten für die IKT-Sicherheit, den Datenschutz und das Risikomanagement sind unternehmensweit definiert und werden gelebt. Die Prozess- und Qualitätssysteme sind sehr umfangreich und die daraus hervorgehenden Massnahmen werden umgehend bewertet und zur Umsetzung weitergeleitet. Ein Information Security Management System (ISMS) ist im Aufbau und soll helfen, die Informationssicherheit künftig dauerhaft zu steuern und fortlaufend zu verbessern.

Die Informatikumgebungen und insbesondere die flugwetterrelevanten Infrastrukturen weisen eine überdurchschnittlich hohe Maturität aus. Die Infrastrukturen für den Flugbetrieb sind auf hohe Verfügbarkeit ausgerichtet und daher oft redundant aufgebaut.

Aufgrund der für den Flugbetrieb relevanten Tätigkeiten wird MeteoSchweiz regelmässig durch das Bundesamt für Zivilluftfahrt (BAZL) auditiert. Diese Prüfungen betreffen auch die IKT-Sicherheit. Der entsprechende Bericht des BAZL lag der EFK vor.

Beurteilung

MeteoSchweiz hat erkannt, dass dem Sicherheitsbewusstsein jedes einzelnen Mitarbeitenden ein sehr hoher Stellenwert beikommt. Daher gilt es, dieses zu schärfen. Das Sicherheitsbewusstsein ist bei den Mitarbeitenden nicht zuletzt aufgrund des Arbeitsumfeldes am Flughafen Zürich deutlich wahrnehmbar und auf einem hohen Niveau.

Die Prüfung der Umsetzung der IKT-Sicherheitsvorgaben des Bundes und der relevanten internationalen Normen hat keine bedeutenden Schwachstellen ergeben. Die gesamte Infrastruktur ist sehr gut gegen physische Zugriffe geschützt. Eine permanente Überwachung der Systeme und Netze und zweckmässige Redundanzen fördern einen reibungslosen Betrieb. Sämtliche IKT-Prozesse werden durch geeignete Werkzeuge unterstützt und Konfigurationsänderungen können jederzeit nachverfolgt werden.

Aus Sicht der EFK ist die IKT-Sicherheit bei MeteoSchweiz auf einem hohen Stand. Die geplante Einführung eines ISMS ist eine wichtige Massnahme, um das erreichte gute Niveau langfristig und konsequent halten zu können.

2.2 Die Arbeitsplatzsicherheit entspricht den Anforderungen des Bundes

Die erforderliche Dokumentation zur Sicherheit der Arbeitsplatzsysteme liegt detailliert vor. Die Grundschutzanforderungen werden über alle Bereiche eingehalten und es bestehen keine Ausnahmeregelungen. Die Anforderungen und abzudeckenden Risiken im ISDS-Konzept für den Arbeitsplatz gehen basierend auf Anforderungen teilweise über die Vorgaben der BV hinaus.

Die Arbeitsplätze sind nach gängigen Praktiken geschützt

Für die Härtung der Arbeitsplatzsysteme werden die gängigen Microsoft-Base-Lines[7] verwendet. Darüber hinaus werden die BIT-Spezifikationen berücksichtigt. Sicherheitsrichtlinien werden in einer Datenbank aufgezeichnet und alle Änderungen sind nachvollziehbar dokumentiert. Die zur Anwendung kommenden Gruppenrichtlinienobjekte (GPO) ermöglichen es, die Richtlinien auf Server und Clients anzuwenden (z. B. Regeln für Passwörter, Endpoint Protection, Windows Defender, BitLocker usw.). Der Start von ausführbaren Dateien wird mit AppLocker kontrolliert, einer Software, welche die Ausführung von unerwünschten und unbekannten Anwendungen unterbindet. Dabei werden Signaturen, Zertifikate oder kryptografische Funktionen eingesetzt. Der Datenverkehr zwischen dem Client und dem Internet wird konsequent und auch ausserhalb der Büroräumlichkeiten über eine sichere und kontrollierte Verbindung geleitet.

Die Verwaltung und Überwachung der sicherheitsrelevanten Systeminformationen erfolgen zentral. Dabei werden Versionen und Patch-Level geprüft und allfällige Anomalien können erkannt werden.

Beurteilung

MeteoSchweiz hat eine Reihe von in der Windows-Umgebung verfügbaren Sicherheitsmassnahmen implementiert. Das Management und die Überwachung der Systeme erfolgen zentral, wodurch sicherheitsrelevante Ereignisse früh erkannt werden können. Der Client weist mindestens die Härtungsmassnahmen des Bundesarbeitsplatzes auf. In Bezug auf die Internetverbindung ist durch die erzwungene Verwendung sicherer Verbindungen sogar noch eine zusätzliche Sicherheitsmassnahme implementiert.

Das Bewusstsein der Risiken bei der Arbeit mit lokalen Administratorenrechten muss gefördert werden

Für einige Arbeiten im Bereich der Entwicklung und den Messnetzen sind administrative Rechte erforderlich. Hierfür kommen bei MeteoSchweiz Administratorenkonten mit eingeschränkten Rechten zum Einsatz. Diese Konten sind zwar an definierte Geräte gebunden, doch gibt es im Bereich der Entwicklung auch Konten, welche mit dem persönlichen Büroautomationsgerät verbunden sind. Dadurch können Veränderungen an Konfigurationen vorgenommen oder sogar nicht freigegebene Software installiert werden. Der direkte Zugriff auf die Linux-Systeme, welche die Daten halten, ist jedoch nicht möglich, da mit dem privilegierten Account nur Windows-Systeme angesprochen werden können. Somit wird ein mögliches Ausbreiten von Malware auf die Windows-Systeme beschränkt. Die Anmeldungen an den Systemen werden geloggt, jedoch nicht die Aktionen, die in diesem Benutzerkontext vorgenommen werden.

Beurteilung

Der Einsatz von Konten mit erhöhten Privilegien ist im Bereich der Entwicklung und den Messnetzen kaum zu vermeiden und nachvollziehbar. Kommen einzelne dieser Konten jedoch auf der persönlichen Büroinfrastruktur zum Einsatz, besteht das Risiko, dass durch Fehlmanipulationen Sicherheitsmechanismen ausgehebelt werden. Durch das Aufzeichnen der Anmeldevorgänge kann zwar rückblickend ermittelt werden, wer sich wann und auf welchem Gerät eingeloggt hat, aber dies hilft in einem Schadensfall nur bedingt um zu verstehen, wie ein Schaden entstanden ist. Es ist wichtig, dass sich die Inhaber dieser privilegierten Konten bewusst sind, dass die Risiken für die IKT-Sicherheit mit diesen Berechtigungen erhöht sind.

[7] https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines

Empfehlung 1 (Priorität 2)

Die EFK empfiehlt MeteoSchweiz, sämtliche Mitarbeitenden mit Administratorenkonten speziell zu sensibilisieren und bei der Vergabe von Administratorenkonten mittels einer Kurzbeschreibung auf die Risiken und den Umgang damit hinzuweisen.

Stellungnahme des Bundesamts für Meteorologie und Klimatologie

MeteoSchweiz wird die Massnahme gemäss Empfehlung umsetzen und die Mitarbeitenden mit Administratorenkonten sensibilisieren. Es wird eine entsprechende Kurzbeschreibung erstellt und in den Prozess für die Vergabe von Administratorenkonten integriert.

Die Verschlüsselungs-Software ist verteilt, kommt jedoch kaum zum Einsatz

Die Verschlüsselungs-Software «SecureCenter» wird benötigt, um Dokumente mit erhöhtem Schutzbedarf zu bearbeiten. Mit der Migration auf die GEVER-Lösung «Acta Nova» wurde auch «SecureCenter» auf allen Arbeitsplätzen von MeteoSchweiz installiert. Der Zugang zu den Zertifikaten, welche «SecureCenter» benötigt, ist für MeteoSchweiz noch nicht vollumfänglich gewährleistet. Dies ist zum Prüfzeitpunkt nur im Mail-System sichergestellt. In Zukunft soll der vollständige Zugang über den sogenannten Datenbezugspunkt der BV sichergestellt werden. Die heutige Version von «SecureCenter» unterstützt dies jedoch noch nicht. Dies ist ein Grund, weshalb das Arbeiten mit «SecureCenter» bei MeteoSchweiz noch nicht flächendeckend gefördert wurde. Ein weiterer Grund ist, dass bei MeteoSchweiz sehr wenige Daten mit einer höheren Vertraulichkeit (< 1 %) bearbeitet werden.

Um sensible Daten dennoch vor unberechtigtem Zugriff zu schützen, kommen alternative Werkzeuge zum Einsatz. So werden Dokumente beispielsweise mittels Passwörtern geschützt. Eine einheitliche Anwendung dieser Werkzeuge und ein erforderliches Passwort- bzw. Schlüsselmanagement ist nicht etabliert. Dies kann dazu führen, dass bei Verlust der Passwörter, z. B. infolge eines Austritts, Daten nicht mehr gelesen werden können.

Beurteilung

Mit der Installation der Standardsoftware «SecureCenter» hat MeteoSchweiz die erforderliche Basis für die Verschlüsselung sensibler Informationen geschaffen. Eine flächendeckende Nutzung der Software ist zum Prüfzeitpunkt jedoch nicht etabliert. Durch den Einsatz alternativer Werkzeuge besteht ein erhebliches Risiko, dass Daten längerfristig nicht mehr gelesen werden können. Mit dem Zugang zu GEVER-Ablagen mit integrierter Verschlüsselung (SN2) kann diesem Umstand sicher entgegengewirkt werden. Dennoch muss MeteoSchweiz den Einsatz von «SecureCenter» gezielt fördern.

Empfehlung 2 (Priorität 2)

Die EFK empfiehlt MeteoSchweiz, den Einsatz der Verschlüsselungssoftware «SecureCenter» bei allen Mitarbeitenden zu schulen und nicht konform verschlüsselte oder passwortgeschützte Daten zu ermitteln und mit «SecureCenter» zu verschlüsseln. Sofern der Zugang (SN2) für das GEVER-System freigegeben wird, können diese auch in den entsprechenden Bereichen abgelegt und durch GEVER verschlüsselt werden.

Stellungnahme des Bundesamts für Meteorologie und Klimatologie

Die Massnahme wird im GEVER-System umgesetzt. Bereits existierende verschlüsselte Dateien werden identifiziert und direkt in das GEVER-System migriert. Betroffene Mitarbeiter werden zum Umgang mit vertraulichen Informationen sensibilisiert und es wird eine Anlaufstelle geschaffen. Dadurch wird die Verschlüsselung vereinheitlicht und das Schlüsselmanagement wie auch eine Kontinuität sichergestellt.

2.3 Die Netzwerksicherheit genügt den Vorgaben des Bundes

MeteoSchweiz verfügt über eine detailliert dokumentierte Netzwerkinfrastruktur. Diese weist sowohl auf logischer wie auch auf physischer Ebene einen hohen Segmentierungsgrad auf. Kritische Systeme wie Messanlagen oder Partnernetze sind bewusst in getrennten Zonen und haben keine direkte Verbindung in das Netz der Büroautomation. Das Management der Netzkomponenten erfolgt in einer dedizierten Management-Zone. Die Netzübergänge sind konsequent durch redundant aufgebaute Firewalls gesichert.

Das interne Netzwerk ist zudem mittels Network Access Control gesichert. Dadurch wird verhindert, dass Fremdgeräte unerlaubt in die Umgebung von MeteoSchweiz eingebunden werden können. Oft wird der Datenverkehr innerhalb des Netzwerks auf applikatorischer Ebene verschlüsselt.

Die Zugriffe auf das GEVER-System erfolgen über ein kontrolliertes Transitnetz

Der Zugriff auf das GEVER-System erfolgt über eine Punkt-zu-Punkt-Verbindung mittels einer Standleitung des Providers. Auch hier kommen sowohl auf Seite MeteoSchweiz als auch auf Seite des BIT eine Firewall zum Einsatz. Auf der zentralen Login-Infrastruktur des Bundes (eIAM) werden die Zugriffe auf das GEVER-System verwaltet. Die Authentisierung der Mitarbeitenden erfolgt mittels der elektronischen Identitäten der Smartcard (siehe Abbildung 1).

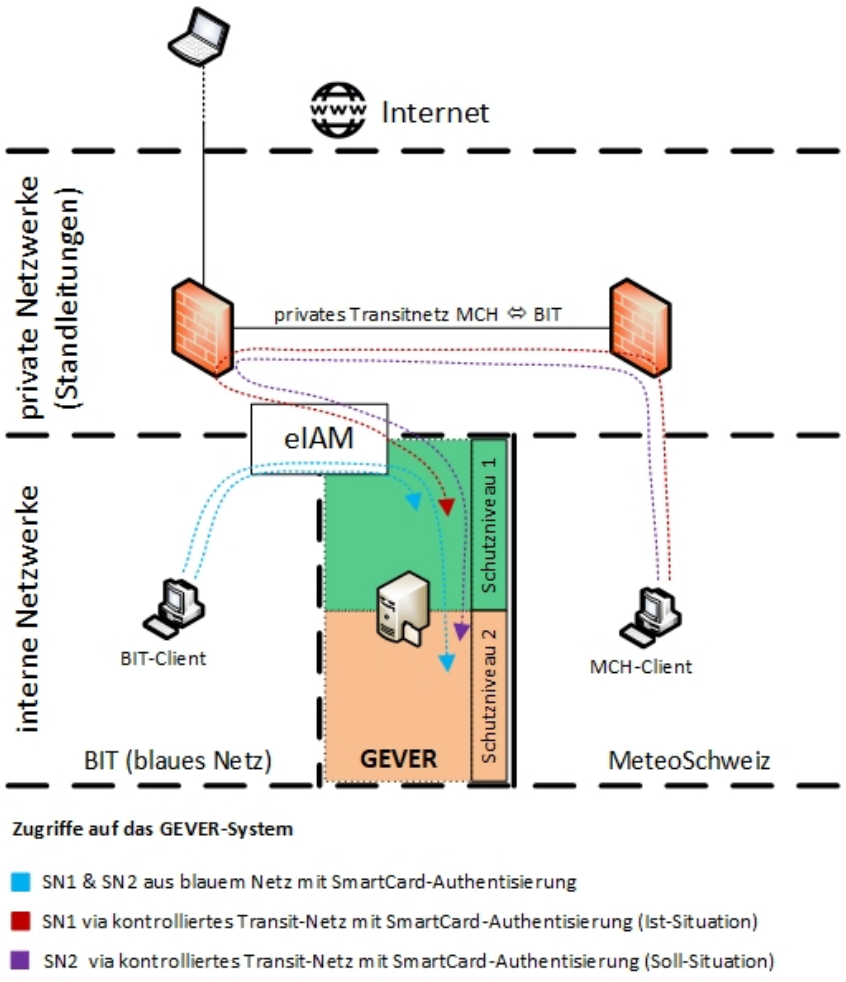

Abbildung 1: Schematische Darstellung der Verbindung auf das GEVER-System (Quelle: MeteoSchweiz, EFK-Darstellung)

Die Überwachung der Netze erfolgt weitgehend durch das CSIRT BIT

Da MeteoSchweiz aufgrund einer Ausnahmebewilligung selber Internet-Übergänge betreibt, ist sie grundsätzlich für den entsprechenden Schutz und die Überwachungsmechanismen verantwortlich. Das Gleiche gilt für die Überwachung und den Schutz der Büroautomationssysteme vor Angriffen. Hierfür sammelt MeteoSchweiz Log-Daten verschiedener Quellen und wertet diese bei Bedarf mit einer Analyse-Infrastruktur aus.

Das Computer Security Incident Response Team (CSIRT) erbringt im Rahmen einer Dienstleistungsvereinbarung (DLV) Monitoring-Leistungen auf Basis bestimmter Logdaten für MeteoSchweiz. MeteoSchweiz liefert die Logdaten (z. B. von Proxies, Firewalls, …) kontinuierlich an die Logdaten-Infrastruktur des BIT. Die Analyse erfolgt automatisiert und ad hoc mittels der vom BIT betriebenen Loganalyse-Software.

Im Rahmen der DLV wird dem IT-Sicherheitsbeauftragten auch der Quartalsbericht des CSIRT zur Verfügung gestellt. Daraus gewinnt MeteoSchweiz Informationen zum Lagebild sowie Hinweise für mögliche Verbesserungen. Werden Angriffe erkannt oder Anomalien beobachtet, wird der IT-Sicherheitsbeauftragte von MeteoSchweiz informiert.

Beurteilung

Der Aufbau und der Betrieb des Netzwerkes von MeteoSchweiz entsprechen den heutigen Anforderungen an ein Netzwerk-Management. Das Netz weist einen hohen Segmentierungsgrad auf. Mit der Netzwerkzonierung hat MeteoSchweiz gemäss den Vorgaben und dem Schutzbedarf Schutzzonen im Netzwerk eingerichtet. Sensitive Systeme wurden dabei in speziell gesicherte Netzwerkzonen ausgelagert. Der Zugriff wird eingeschränkt, womit das Eindringen in Systeme erschwert wird.

Der Datentransfer auf die GEVER-Systeme erfolgt über eine Standleitung mit Firewalls auf beiden Seiten. Dadurch wird eine deutlich höhere Sicherheit als bei einem Zugang über das Internet erreicht.

Die Überwachung der Netzwerkkomponenten und Sicherheitsinfrastruktur erfolgt durch das BIT und damit in der Qualität der bundesinternen Überwachung.

3 Keine Gefährdung von GEVER Bund durch Bearbeitung von Daten mit erhöhtem Schutzbedarf

MeteoSchweiz wechselte die bestehende Geschäftsverwaltung im Jahr 2020 auf die GEVER-Lösung «ActaNova» der BV. Die Migration war aus Risikoüberlegungen in drei Etappen aufgeteilt. Seit Dezember 2020 können alle Mitarbeitenden auf dem neuen System Daten ohne erhöhte Schutzanforderungen (SN1) bearbeiten. Die bestehenden Daten sind zum Prüfzeitpunkt noch nicht vollständig überführt worden. Dies soll bis Ende 2022 erfolgen.

Die zuständigen Stellen bei MeteoSchweiz sind in den operativen Gremien im Kontext von GEVER vertreten und arbeiten aktiv an der Weiterentwicklung der Plattform mit. Damit ist auch der Austausch mit den Vorgabestellen und dem Departement sichergestellt.

MeteoSchweiz arbeitet seit rund einem halben Jahr auf dem GEVER-System des Bundes. Während dieser Zeit kam es zu keinen sicherheitsrelevanten Ereignissen im Zusammenhang mit Zugriffen durch MeteoSchweiz.

Das System ist so aufgebaut, dass jedes Departement eine Instanz hat und die Ämter jeweils einen eigenen Mandanten. Durch diese Trennung ist ein direkter Zugriff auf Dokumente anderer Ämter bzw. Departemente technisch unterbunden. Eine Ausbreitung von Malware ist daher nicht direkt möglich. Zudem werden die Daten auf den Arbeitsplatzsystemen und in der GEVER-Ablage auf allfällige Malware geprüft.

Die Bearbeitung von Daten mit erhöhtem Schutzbedarf und die Nutzung der Verschlüsselungsfunktion in GEVER durch MeteoSchweiz stellt für den Betreiber keine zusätzlichen Herausforderungen dar. Es entstehen dadurch auch keine zusätzlichen Risiken.

Beurteilung

Die heute implementierten Schutzmechanismen für den Zugang zum GEVER-System erweisen sich als wirksam. So kam es seit der Inbetriebnahme zu keinen sicherheitsrelevanten Vorfällen. Durch den Einsatz der Verschlüsselungsfunktionen wird die Sicherheit zudem erhöht und allfällige Umgehungslösungen (siehe Empfehlung 2) fallen weg.

Durch die architektonische Trennung der einzelnen Systeme ist eine laterale Ausbreitung einer unentdeckten Malware eingeschränkt, somit wäre bei einem Befall des Mandanten von MeteoSchweiz nicht mit einer unmittelbaren Gefährdung anderer Mandanten oder Instanzen zu rechnen.

Durch die Bearbeitung von Daten mit erhöhten Schutzanforderungen (SN2) durch MeteoSchweiz entsteht für das Gesamtsystem aus Sicht der EFK keine grössere Gefährdung als bisher.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisiken-verordnung, CyRV), vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73
V001 – Verordnung über die digitale Transformation und die Informatik (VDTI)
Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. Januar 2014), SR 235.1
Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 16. Oktober 2012), SR 235.11
Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung, SR 172.010.441

Anhang 2: Abkürzungen

BAZL	Bundesamt für Zivilluftfahrt
BIT	Bundesamt für Informatik und Telekommunikation
BV	Bundesverwaltung
CSIRT	Computer Security Incident Response Team
DLV	Dienstleistungsvereinbarung
DTI	Digitale Transformation und IKT-Lenkung
EASA	Agentur der Europäischen Union für Flugsicherheit (European Union Aviation Safety Agency)
EFK	Eidgenössische Finanzkontrolle
eIAM	eGovernment Identity & Access Management (siehe Glossar)
GPO	Group Policy Object (Gruppenrichtlinienobjekt)
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan des Bundes
ISDS	Informationssicherheits- und Datenschutzkonzept
ISMS	Information Security Management System (siehe Glossar)
NASP	National Aviation Safety Plan (siehe Glossar)
NCSC	Nationales Zentrum für Cybersicherheit

Anhang 3: Glossar

AppLocker	Application-Whitelisting-Technologie, die mit dem Betriebssystem Windows 7 von Microsoft eingeführt wurde. Sie ermöglicht die Einschränkung, welche Programme Benutzer basierend auf dem Pfad, dem Herausgeber oder dem Hash des Programms ausführen können.
BitLocker	Proprietäre Festplattenverschlüsselung von Microsoft.
eIAM	Zentrales Zugriffs- und Berechtigungssystem der Bundesverwaltung für Webapplikationen und mobile Apps.
Endpoint Protection	Endpunktsicherheit oder Endpunktschutz ist ein Ansatz zum Schutz von Computernetzwerken, die remote mit Clientgeräten verbunden sind.
Firewall	Sicherungssystem, welches ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
GEVER	Jedes Bundesorgan führt zur Registrierung, Verwaltung, Indexierung und Kontrolle von Schriftenverkehr und Geschäften ein Informations- und Dokumentationssystem (elektronische Geschäftsverwaltung).
Hash-(Funktion)	Eine Hashfunktion ist eine Abbildung, die eine grosse Eingabemenge (die Schlüssel) auf eine kleinere Zielmenge (die Hashwerte) abbildet.
ISMS	Verfahren und Vorgaben innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.
ISO/IEC 27001:2013	Die internationale Norm ISO/IEC 27001 definiert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS).
National Aviation Safety Plan	Der nationale Flugsicherheitsplan (NASP) ist das Masterplanungsdokument, das die strategische Ausrichtung eines Staates für das Management der Flugsicherheit festlegt. Dieser Plan listet Sicherheitsfragen auf, legt Ziele für die Flugsicherheit fest und stellt eine Reihe von Initiativen zur Verbesserung der Sicherheit vor, um festgestellte Sicherheitsmängel zu beheben und die nationalen Sicherheitsziele zu erreichen.

Network Access Control	Network Access Control ist eine Technik, die die Abwehr von Viren, Würmern und unautorisierten Zugriffen aus dem Netzwerk heraus unterstützt.
P035 – Prozess	Die IKT-Vorgabe regelt den Umgang mit Anforderungen und Vorgaben zur Bundesinformatik gemäss Ziffer 4 der Weisungen des EFD vom 19. Februar 2013 zur Umsetzung der Bundesinformatikverordnung (WUBinfV) sowie gemäss P000 – Informatikprozesse in der Bundesverwaltung.
Proxy	Kommunikationsschnittstelle in einem Netzwerk aus Rechnern in Form eines physischen Computers. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
SecureCenter	Die Sicherheitssoftware SecureCenter wird für die Bearbeitung von schutzwürdigen elektronischen Informationen eingesetzt. Der Standarddienst des Bundes kann auf jedem Arbeitsplatzsystem mit dem Betriebssystem Windows verwendet werden.
Smartcard	Eine Smartcard ist eine Chipkarte (Mikroprozessorkarte), die grundsätzlich verschiedenste Funktionalitäten (Dienste) zur Verfügung stellen kann. Aktuell wird in der BV die Karte primär als Träger von digitalen Zertifikaten verwendet. Der Zugriff auf die Smartcard kann nur durch Eingabe des bei der Ausstellung der Smartcard festgelegten persönlichen PIN-Codes (PIN) erfolgen.
Windows Defender	Microsoft Defender Antivirus ist eine von Microsoft für dessen Windows entwickelter Virenschutz zur Erkennung von potenziell unerwünschter Software.

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).