



A-Priority CH-3003 Bern

DU Chefin VBS

Referenz/Aktenzeichen: GS-VBS-D-FEFD3401/12
Bern, Datum digitale Unterschrift

**Umsetzung der Empfehlungen aus der IT-Prüfung «Schutz der sensitiven Daten bei externen IT-Partnern des VBS in deren Entwicklungs- und Testumgebungen»
(I 2024-03)**

Sehr geehrter Herr Generalsekretär
Sehr geehrter Herr Staatssekretär
Sehr geehrter Herr Chef der Armee
Sehr geehrter Herr Rüstungschef
Sehr geehrte Frauen Direktorinnen
Sehr geehrte Herren Direktoren

Die Interne Revision VBS stellte Ihnen am 4. Februar 2025 den Bericht zur oben erwähnten Prüfung zu. Wie Sie daraus entnehmen können, besteht bei den nachfolgenden Themen Handlungsbedarf:

Empfehlung 1: Weisungen überarbeiten (Kap. 4)

Die Interne Revision VBS empfiehlt dem Generalsekretariat (GS-VBS), aufgrund der neuen rechtlichen Grundlagen, die aktuellen Weisungen über die Herausgabe und das Zugänglichmachen von Informationen in elektronischer Form durch IKT-Leistungserbringer zu analysieren sowie zeitnah zu überarbeiten und von der Geschäftsleitung zu verabschieden.

Empfehlung 2: Prozessdokumentation und Schlüsselkontrollen (Kap. 5.2)

Die Interne Revision VBS empfiehlt Verwaltungseinheiten des VBS, einen einheitlichen Prozess zu definieren. Im Prozess sind auch relevante Schlüsselkontrollen einzubauen. Der formal dokumentierte Prozess soll anschliessend durch die Sicherheitsverantwortlichen der entsprechenden Verwaltungseinheit freigegeben und geschult werden.

Empfehlung 3: Vertragsnachträge (Kap. 5.3)

Die Interne Revision VBS empfiehlt den Verwaltungseinheiten des VBS, in Zusammenarbeit mit dem Bundesamt für Rüstung (armasuisse) sowie dem Bundesamt für Bauten und Logistik (BBL), sicherzustellen, dass die Verträge mit externen IT-Lieferanten einer kritischen Prüfung unterzogen und bei Bedarf durch Nachträge ergänzt werden. Dabei sollten insbesondere Aspekte wie Datenschutz und Datensicherheit, Klauseln zum Schutz der Informatikmittel vor Cyberangriffen, Meldepflichten sowie das Auditrecht zur Überprüfung der Einhaltung von Informationssicherheits- und Datenschutzanforderungen bei externen IT-Lieferanten berücksichtigt werden.

Empfehlung 4: Schulung und Sensibilisierung (Kap. 5.4)

Die Interne Revision VBS empfiehlt den Verwaltungseinheiten des VBS, sicherzustellen, dass primär die Projektleitenden, die Anwendungsverantwortlichen und die Beschaffungsverantwortlichen im Bereich der Informationssicherheit regelmässig geschult und sensibilisiert werden.

Empfehlung 5: Betriebssicherheitsverfahren (Kap. 5.4)

Die Interne Revision VBS empfiehlt den Verwaltungseinheiten des VBS, in Zusammenarbeit mit der Fachstelle für Betriebssicherheit, bei Bedarf ein Betriebssicherheitsverfahren unverzüglich einzuleiten.

Empfehlung 6: Risikoorientierte Durchführung von Audits bei Dritten (Kap. 5.4)

Die Interne Revision VBS empfiehlt den Verwaltungseinheiten des VBS, in Koordination mit der Fachstelle des Bundes für Betriebssicherheit, sicherzustellen, dass die Informationssicherheit bei Dritten im Rahmen von regelmässigen Audits risikobasiert überprüft wird.

Darf ich Sie bitten, die aufgeführten Empfehlungen bis Ende Juni 2026 in geeigneter Form umzusetzen. Gerne erwarte ich nach Ablauf dieser Frist Ihre schriftliche Rückmeldung.

Die Interne Revision VBS übernimmt das Monitoring zu dieser Prüfung.

Für Ihre Bemühungen bedanke ich mich.

Freundliche Grüsse

Viola Amherd
Bundesrätin

z. K. an
– Leiter Interne Revision VBS