



HESSISCHER LANDTAG

11. 09. 2026

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 12.01.2026

Cybersicherheit und IT-Resilienz der öffentlichen Verwaltung und Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Die Bedrohung aus dem Cyberraum nimmt stetig zu. Cyber-Angriffe auf öffentliche Verwaltungen, kritische Infrastrukturen und kommunale Einrichtungen haben in den vergangenen Jahren erheblich zugenommen. Die Hessische Landesregierung hat im November 2025 die Hessische Cybersicherheitsplattform (HCSP) ins Leben gerufen, um die Zusammenarbeit zwischen Staat, Wissenschaft und Wirtschaft zu stärken. Hessen führt seit der Gründung den Vorsitz in der Länderarbeitsgruppe Cybersicherheit und hat eine Cybersicherheitsstrategie entwickelt. Dennoch stellt sich die Frage, ob die vorhandenen Ressourcen, Kompetenzen und Maßnahmen ausreichen, um die öffentliche Verwaltung und kritische Infrastrukturen wirksam zu schützen. Insbesondere kleinere Kommunen verfügen oft nicht über ausreichende IT-Sicherheitskapazitäten und sind auf Unterstützung des Landes angewiesen. Für die Freien Demokraten ist klar: Cybersicherheit ist eine Daueraufgabe, die kontinuierliche Investitionen, Weiterbildung und die Vernetzung aller Akteure erfordert. Nur eine resiliente digitale Infrastruktur ermöglicht eine handlungsfähige und vertrauenswürdige Verwaltung.

Die Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, dem Minister für Bundes- und Europaangelegenheiten, Internationales und Entbürokratisierung und Bevollmächtigten des Landes Hessen beim Bund, dem Minister der Finanzen, dem Minister der Justiz und für den Rechtsstaat, dem Minister für Kultus, Bildung und Chancen, dem Minister für Wissenschaft und Forschung, Kunst und Kultur, dem Minister für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum, der Ministerin für Digitalisierung und Innovation, dem Minister für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat, der Ministerin für Familie, Senioren, Sport, Gesundheit und Pflege und der Ministerin für Arbeit, Integration, Jugend und Soziales wie folgt:

Frage 1 Wie viele Cyber-Angriffe auf Einrichtungen der hessischen Landesverwaltung, nachgeordnete Behörden und kommunale Einrichtungen wurden in den Jahren 2023, 2024 und 2025 jeweils registriert? Bitte nach Angriffstypen, zum Beispiel Ransomware, DDoS, Phishing aufschlüsseln.

In der hessischen Landesverwaltung, einschließlich der nachgeordneten Behörden, wurden im Jahr 2023 199 Sicherheitsvorfälle, im Jahr 2024 206 Sicherheitsvorfälle und im Jahr 2025 278 Sicherheitsvorfälle registriert, die als Cyberangriffe zu werten sind. Vorfälle weisen mehrere Angriffsvektoren auf, sodass eine trennscharfe statistische Zuordnung nach Angriffstypen nicht erfolgt.

Für hessische Kommunen besteht keine Meldepflicht. Die registrierten Vorfälle basieren auf freiwilligen Meldungen der Kommunen. Im Jahr 2023 wurden 31 Sicherheitsvorfälle, im Jahr 2024 13 Sicherheitsvorfälle und im Jahr 2025 15 Sicherheitsvorfälle gemeldet, die als Cyberangriffe zu werten sind.

Frage 2 Wie viele dieser Angriffe führten zu erfolgreichen Kompromittierungen von Systemen, Datenverlust oder Ausfällen kritischer IT-Dienste?

Frage 3 Welche Schäden entstanden dadurch (finanziell, operativ)?

Die Fragen 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.
Statistische Erfassungen im Sinne der Fragestellung liegen nicht vor.

Frage 4 Welche konkreten Aufgaben hat die im November 2025 gegründete Hessische Cybersicherheitsplattform (HCSP)?

Die HCSP hat die Aufgabe, Strategien zum Schutz der digitalen Infrastruktur in Hessen zu entwickeln, indem namhafte Vertreterinnen und Vertreter aus Staat, Wissenschaft, Wirtschaft und Zivilgesellschaft zusammengeführt werden und sich austauschen. Sie erarbeitet Handlungsempfehlungen und konkrete Maßnahmen zur Prävention, Erkennung und Bewältigung von Cyberangriffen.

Frage 5 Wie viele Mitarbeiterinnen und Mitarbeiter sind in der Landesverwaltung mit IT-Sicherheitsaufgaben betraut?

Frage 6 Wie hat sich diese Zahl in den vergangenen fünf Jahren entwickelt?

Die Fragen 5 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Eine „personenscharfe“ Darstellung war nicht in jedem Fall darstellbar, weil nicht alle Personen ausschließlich IT-Sicherheitsaufgaben wahrnehmen. Die nachfolgenden Angaben beruhen auf den jeweiligen Erfassungen der Ressorts und können hinsichtlich ihres organisatorischen Bezugs unterschiedlich weit reichen.

Die Landesregierung versteht unter IT-Sicherheitsaufgaben im Sinne der Fragestellung technische und organisatorische Tätigkeiten zur Gewährleistung der Sicherheit informationstechnischer Systeme, die den überwiegenden Teil der Beschäftigung darstellen.

In der Hessischen Staatskanzlei (HStK) sind derzeit vier Personen mit IT-Sicherheitsaufgaben betraut. Im Jahr 2021 waren es zwei Personen.

Im Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz (HMdI) sind derzeit 27 Personen mit IT-Sicherheitsaufgaben betraut. Im Jahr 2021 waren es 20 Personen.

Im Geschäftsbereich des Hessischen Ministers der Finanzen sind aktuell 85 Personen mit IT-Sicherheitsaufgaben betraut. Die Verteilung gestaltet sich wie folgt: Im Hessischen Ministerium der Finanzen übernehmen zwei Personen die Rolle der IT-Sicherheitsbeauftragten für das HMdF sowie für das Ressort. In den nachgeordneten Dienststellen des Ministeriums sind sieben Personen als IT-Sicherheitsbeauftragte tätig. Darüber hinaus sind 76 Personen in der konzeptionellen und operativen Informationssicherheit des Geschäftsbereichs eingesetzt. Die Anzahl der Mitarbeitenden ist in den letzten fünf Jahren kontinuierlich gestiegen.

Im Hessischen Ministerium der Justiz und für den Rechtsstaat (HMdJ) sowie in der IT-Stelle der hessischen Justiz (IT-Stelle) nehmen derzeit elf Personen IT-Sicherheitsaufgaben wahr. Konkret schlüsselt sich diese Zahl wie folgt auf: Im Ministerium nimmt eine Person die Aufgaben des IT-Sicherheitsbeauftragten des HMdJ wahr. Eine weitere Person in der IT-Stelle hat die Rolle des IT-Sicherheitsbeauftragten des Geschäftsbereichs der Justiz (ITSiBJ) inne. Der ITSiBJ ist zusätzlich Leiter der Abteilung 2 IT-Sicherheit in der IT-Stelle. Der Vizepräsident der IT-Stelle verantwortet den Bereich der IT-Sicherheit. In der konzeptionellen beziehungsweise operativen Sicherheit sind aktuell acht Personen beschäftigt. Eine weitere Stelle, die der stellvertretenden Referatsleitung der konzeptionellen IT-Sicherheit, befindet sich in der Besetzung. In den letzten Jahren ist die Stellenanzahl konstant geblieben.

Im Hessischen Ministerium für Kultus, Bildung und Chancen (HMKb) sind derzeit zwei Personen mit IT-Sicherheitsaufgaben betraut, eine Stelle befindet sich zudem aktuell im Besetzungsverfahren. Im Jahr 2021 waren es zwei Personen.

Im Hessischen Ministerium für Wissenschaft und Forschung, Kunst und Kultur (HMWK) sind vier Personen mit IT-Sicherheitsaufgaben betraut. Die Aufgabe des/der Ressort-Informationssicherheitsbeauftragten wurde entwickelt und zusätzlich etabliert. Die Anzahl der Beschäftigten mit IT-Sicherheitsaufgaben im Ressort hat sich in den letzten fünf Jahren in kleinen Schritten fortentwickelt.

Im Hessischen Ministerium für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum (HMWW) sind drei Personen mit IT-Sicherheitsaufgaben betraut, eine weitere Stelle befindet sich in der Wiederbesetzung. Im Jahr 2021 waren es zwei Personen.

Im Hessischen Ministerium für Digitalisierung und Innovation (HMD) sind zwei Personen mit der Wahrnehmung von IT-Sicherheitsaufgaben betraut. Der IT-Service unterstützt die ISB bei technischen Fragestellungen. Die ISB-Stelle wurde mit Gründung des HMD im Jahr 2024 geschaffen. Im Jahr 2025 wurde die zusätzliche Sachbearbeitung zur Unterstützung der ISB eingestellt.

Im Geschäftsbereich des Hessischen Ministers für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat (HMLU) sind 30 Personen mit IT-Sicherheitsaufgaben betraut. Die Anzahl der zu besetzenden Stellen mit IT-Sicherheitsaufgaben hat sich in den letzten fünf Jahren erhöht.

Im Hessischen Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege (HMFG) ist eine Person mit IT-Sicherheitsaufgaben betraut. Eine Stellenentwicklung in diesem Bereich hat in den vergangenen fünf Jahren nicht stattgefunden, da das HMFG erst seit dem Jahr 2024 besteht.

Im Hessischen Ministerium für Arbeit, Integration, Jugend und Soziales (HMSI) sind zwei Personen mit der Wahrnehmung von IT-Sicherheitsaufgaben betraut. Die ISB-Stelle wurde im Jahr 2020 erstmals als Vollzeitstelle (vorher Nebenfunktion) besetzt, in den darauffolgenden Jahren kam eine weitere Referentenstelle hinzu.

Frage 7 Wie viele Personen der Landesverwaltung nahmen 2024 und 2025 an Aus- und Weiterbildungsmaßnahmen zur Stärkung der Cybersicherheitskompetenz teil?

Eine ressortübergreifend einheitliche statistische Erfassung der Teilnahme an Aus- und Weiterbildungsmaßnahmen zur Stärkung der Cybersicherheitskompetenz liegt nicht vor. Nachfolgend werden daher die jeweils verfügbaren Angaben der Ressorts dargestellt.

Eine vollumfängliche statistische Erfassung aller in der Landesverwaltung durchgeführten Aus- und Weiterbildungsmaßnahmen zur Stärkung der Cybersicherheitskompetenz findet nicht statt. Es können jedoch die nachfolgenden Angaben aus den jeweiligen Geschäftsbereichen gemacht werden.

Im Jahr 2024 wurden 75 Beschäftigte und im Jahr 2025 wurden 281 Beschäftigte der Hessischen Staatskanzlei im Bereich Informationssicherheit geschult. Des Weiteren hatte das Personal im ISMS-Bereich weiterführende Fachschulungen.

Das für Cybersicherheit zuständige und im Bereich des Informationssicherheitsmanagements tätige Fachpersonal nimmt regelmäßig an Fachschulungen teil. Zudem wird die durch das HMDI bereitgestellte zentrale Online-Schulung für alle Beschäftigten der hessischen Landesverwaltung „Grundlagen der Informationssicherheit“ sehr gut angenommen. Im Jahr 2024 wurden 57.903 Zugriffe auf die Schulung registriert. Im Jahr 2025 waren es bis zum 30. September 2025 21.987 Zugriffe. Eine Auswertung des 4. Quartals 2025 liegt noch nicht vor. An der Ringvorlesung Cybersicherheit, zu der alle Beschäftigten der Landesverwaltung eingeladen waren, nahmen 2024 3.900 Personen teil. Im Jahr 2025 waren es 4.100.

Im Geschäftsbereich des Hessischen Ministers der Finanzen haben nahezu 90 Prozent der Beschäftigten an allgemeinen oder spezialisierten Aus- und Weiterbildungsmaßnahmen teilgenommen. Sowohl in den Onboarding-Prozessen als auch in der regulären Personalausbildung sind Grundlagenschulungen zur Informationssicherheit fest verankert. Im Jahr 2025 wurde zusätzlich ein ressortweites E-Learning-Angebot zum Thema Informationssicherheit eingeführt, um die Sensibilisierung und das Fachwissen aller Beschäftigten verbindlich zu fördern.

In Verantwortung des HMDI werden Sensibilisierungskampagnen für Informationssicherheit innerhalb der Hessischen Justiz durchgeführt. Erstmals wurden hier im Zeitraum vom 16. Oktober 2023 – 31. Januar 2024 1.242 Beschäftigte des Justizressorts geschult. Im Rahmen einer zweiten Sensibilisierungskampagne wurden im Zeitraum vom 1. August 2024 bis 30. April 2025 insgesamt 8.678 Teilnehmerinnen und Teilnehmer geschult. Über die gesamte Laufzeit beider Kampagnen zur Informationssicherheit wurden insgesamt 9.920 Bedienstete der Hessischen Justiz sensibilisiert und geschult.

Im Jahr 2025 nahmen im HMD alle Beschäftigten (200 Beschäftigte) an einer verpflichtenden allgemeinen Schulung zu Themen der Cybersicherheit teil. Zusätzlich wurde im Jahr 2025 für alle Beschäftigten ein Phishing-Awareness-Training durchgeführt. Darüber hinaus nahmen zwei Personen erfolgreich am Zertifizierungslehrgang „Informationssicherheitsbeauftragte der öffentlichen Verwaltung“ an der Bundesakademie für öffentliche Verwaltung teil. In den Jahren 2024 und 2025 wurden darüber hinaus jeweils zehn Mitarbeiterinnen und Mitarbeiter in einem zweitägigen Seminar zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik geschult.

Im Geschäftsbereich des Ministers für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat nahmen insgesamt 1.040 Personen an Maßnahmen im Sinne der Fragestellung teil.

Im HMKB nahmen in den Jahren 2024 und 2025 alle Beschäftigten an einer verpflichtenden allgemeinen Schulung zu Themen Cybersicherheit teil. Zudem haben zwei Mitarbeiterinnen beziehungsweise Mitarbeiter am einwöchigen Zertifikatslehrgang BSI IT-Grundschutz-Praktiker teilgenommen.

An Awareness-Schulungen nehmen alle Beschäftigten im Ressort des Ministers für Wissenschaft und Forschung, Kunst und Kultur teil. Neben dem E-Learning-Angebot wurden im HMWK im Jahr 2025 für alle Mitarbeiterinnen und Mitarbeiter (280 Personen) Awareness-Schulungen in Präsenz und online durchgeführt.

Frage 8 Wie unterstützt das Land hessische Kommunen, insbesondere kleine und mittlere Städte und Gemeinden, bei der Verbesserung ihrer IT-Sicherheit?

Neben der Förderung der Interkommunalen Zusammenarbeit in diesem Bereich unterstützt die Landesregierung die Gemeinden, Städte und Landkreise mit gezielten und nachhaltigen Maßnahmen. Mit dem Aktionsprogramm Kommunale Cybersicherheit (AKC) bietet das Land in vier zentralen Handlungsfeldern (IT-Infrastruktur, Notfallplanung, Notfallhilfe, Awareness) kostenfreie technische und organisatorische Unterstützungsangebote zur Stärkung ihrer Resilienz und Informationssicherheit an. Diese beinhalten beispielsweise Audits, Pentesting, Erstellung eines Business-Continuity-Managements, Incident-Response-Service, mobiles Soforthilfe-Paket-Kommunikation, eLearning und Beratung. Das Angebot steht allen hessischen Kommunen offen und kann gerade für kleine und mittlere Kommunen eine wirksame Hilfe sein. Das AKC wurde gemeinsam mit den Kommunalen Spitzenverbänden entwickelt. Mit dem AKC verfügt Hessen über ein bundesweit besonders umfassendes Unterstützungsangebot. Die Nutzerzahlen zeigen, dass die Landesregierung mit diesen Angeboten auf dem richtigen Weg ist.

Das Hessen CyberCompetenceCenter (Hessen3C) im HMdI hilft Kommunen darüber hinaus bei akuten Informationssicherheitsvorfällen über eine rund um die Uhr erreichbare Notfallnummer (0611/353-9900). Daneben unterstützt es die IT- und Informationssicherheitsbeauftragten in den Kommunen mit Services wie dem Warn- und Informationsdienst oder dem Tool Hessen Leak Checker.

Das KOMPASS-Cybersicherheitssiegel des Landes Hessen zeichnet Kommunen aus, die ihre IT-Systeme systematisch vor Cyberangriffen schützen und ihre digitale Widerstandsfähigkeit erhöhen

Frage 9 Welche finanziellen Mittel hat die Landesregierung in den Jahren 2023, 2024 und 2025 jeweils für Cybersicherheitsmaßnahmen (Personal, Technik, Schulungen, Forschung) aufgewendet?

Soweit eine gesonderte Erfassung der in der Fragestellung genannten Ausgaben erfolgt, werden die entsprechenden Angaben nachfolgend dargestellt. Im Übrigen werden die jeweils verfügbaren Angaben der Ressorts wiedergegeben.

In der HStK sind für Technik, Schulung und Weiterentwicklung des Informationssicherheitsmanagements im Jahr 2023 rund 90.000 Euro, im Jahr 2024 rund 105.000 Euro und im Jahr 2025 rund 170.000 Euro ausgegeben worden.

Im HMdI entfielen auf präventive und reaktive Leistungen sowie Personal im Bereich Cyber-, IT- und Informationssicherheit in der Landesverwaltung im Jahr 2023 insgesamt 11.840.299,83 Euro, im Jahr 2024 10.457.486,57 Euro, im Jahr 2025 12.290.017,13 Euro.

Im Geschäftsbereich des Hessischen Ministers der Finanzen wurden in den Haushaltsjahren 2023 bis 2025 die finanziellen Mittel für Cybersicherheitsmaßnahmen in den Bereichen Personal, Technik, Schulungen und Forschung wie folgt aufgewendet:

- Personal: Die finanziellen Mittel wurden für internes und externes Personal aufgewendet, das mit der Planung, Konzeption und Umsetzung von IT- und Cybersicherheitsmaßnahmen betraut ist. Dies umfasst auch die Erstellung von IT-Sicherheits- und IT-Notfallkonzepten, Beratung in Fragen der Informations- und Cybersicherheit sowie die Durchführung regelmäßiger Penetrationstests und Sicherheitsaudits.
- Technik: In diesem Bereich wurden die finanziellen Mittel für die Beschaffung, den Betrieb sowie die Lizenzierung notwendiger Hard- und Softwarekomponenten aufgewendet, um das Schutzniveau der IT-Infrastruktur kontinuierlich zu gewährleisten.
- Schulungen: Zur Sensibilisierung und Qualifizierung der Beschäftigten wurden die finanziellen Mittel für ein ressortweites, verpflichtendes E-Learning zum Thema Informationssicherheit sowie für zielgruppenspezifische Fortbildungen aufgewendet. Dazu gehören unter anderem Incident-Response-Trainings und die Ausbildung zum Informationssicherheitsbeauftragten.
- Forschung: Im Berichtszeitraum wurden im Geschäftsbereich des HMdF keine spezifischen Finanzmittel für Cybersicherheitsforschung verausgabt.

Im Verantwortungsbereich des HMdJ wurden in den Jahren 2023 bis 2025 insgesamt 7.190.652,83 Euro für Cybersicherheitsmaßnahmen aufgewendet.

Das HMKB hat im Jahr 2025 59.908,15 Euro für Schulungen im Bereich Informationssicherheit aufgewendet.

Im Rahmen der Haushaltsverhandlungen zum Doppelhaushalt 2023/24 sind im HMWK ab dem Jahr 2023 dauerhafte Sachmittel in Höhe von 250.000 Euro in den Haushalt eingestellt worden. Dem Bereich IT-Sicherheit im Geschäftsbereich des Ministers für Wissenschaft und Forschung, Kunst und Kultur stehen diese Sachmittel unter anderem auch für das Abrufen von Leistungen aus Rahmenverträgen mit externen Dienstleistern zur Erhöhung der Informationssicherheit zu. Die Personalkosten können nicht beziffert werden, da von den oben genannten Personen mit IT-Sicherheitsaufgaben nicht alle ausschließlich diese Aufgaben wahrnehmen. Im Rahmen des Hessischen Digitalpaktes Hochschulen wurden in den Jahren 2023 bis 2025 Fördermittel in Höhe von bis zu neun Millionen Euro für Maßnahmen zur Erhöhung der Informationssicherheit, insbesondere der IT-Sicherheit, bewilligt. Darüber hinaus wurde dem Universitätsklinikum Frankfurt am Main im Jahr 2024 zur Bewältigung der Folgen des am 6. Oktober 2023 festgestellten IT-Sicherheitsvorfalls ein Zuschuss in Höhe von bis zu 15 Millionen Euro gewährt. Die Mittel dienen der Wiederherstellung und Aufrechterhaltung des IT-Betriebs; hierbei wurden auch Maßnahmen mit Bezug zur IT-Sicherheit finanziert, ohne dass hierfür ein gesondert bezifferbarer Anteil ausgewiesen werden kann.

Im HMD wurde für die erwähnte Cybersicherheitsschulung (inklusive Phishing-Awareness-Training aller Beschäftigten) insgesamt ein Betrag von 9.808,58 Euro aufgewendet. Für den Zertifizierungslehrgang „Informationssicherheitsbeauftragte der öffentlichen Verwaltung“ wurden insgesamt 7.600 Euro aufgewendet. Für weitere Ausgaben erfolgte in den Jahren 2024 und 2025 keine gesonderte Erfassung der für Cybersicherheitsmaßnahmen aufgewendeten finanziellen Mitteln. Entsprechende Aufwendungen sind Bestandteil der jeweiligen Projekte, IT- und Organisationshaushaltsansätze und betreffen insbesondere Personalaufwände, Schulungs- und Sensibilisierungsmaßnahmen sowie sicherheitsrelevante Leistungen im Rahmen von durch externe IT-Dienstleister betriebenen Verfahren. Eine weitere trennscharfe Abgrenzung der ausschließlich der Cybersicherheit zuzuordnenden Ausgaben ist daher nicht möglich.

Im Geschäftsbereich des Ministers für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat wurden im Jahr 2023 circa 1,8 Millionen Euro, im Jahr 2024 circa 2,3 Millionen Euro und im Jahr 2025 circa 2,5 Millionen Euro an Mitteln genutzt.

Das HMFG nutzt derzeit die Infrastruktur des HMSI und hat kein eigenes Budget abgerufen.

Im HMSI werden Mittel für Cybersicherheitsmaßnahmen nicht explizit als solche ausgewiesen. Vielmehr sind diese in den Mitteln des IT-Betriebes enthalten. So ist es zum Beispiel essentiell, dass die Server aktuell sind, aktuelle Betriebsversionen und Tools eingesetzt werden oder sich das Personal fortbildet. All diese Investitionen zahlen auf das Themenfeld Cybersicherheit mit ein.

Frage 10 Werden regelmäßige Penetrationstests und Sicherheitsaudits für die IT-Systeme der Landesverwaltung durchgeführt?

Ja, in der Regel durch die Hessische Zentrale für Datenverarbeitung (HZD). Die Dienststellen der Landesverwaltung sind verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) gemäß BSI-Standards umzusetzen. Dies umfasst unter anderem die Anforderungen zur Durchführung von Audits, Revisionen und Penetrationstests. Im HMdI wurde zusätzlich eine Pentest-Richtlinie erlassen, welche Verfahren und Methoden für die Durchführung von Penetrationstests regelt. Eine Pentest-Richtlinie für die gesamte Landesverwaltung befindet sich in Abstimmung mit den Ressorts.

In Teilen der Ressorts finden zusätzlich neben den Penetrationstests regelmäßige Sicherheitsaudits statt, die sowohl interne Systemprüfungen als auch unabhängige Prüfungen durch externe Wirtschaftsprüfungsgesellschaften umfassen. Diese Prüfungen beziehen sich auf IT-Systeme, Prozesse und Richtlinien.

Wiesbaden, 1. September 2026

Prof. Dr. Roman Poseck