

Rechnungshöfe des Bundes und der Länder

Grundsatzpapier zum Informationssicherheits- management

Stand Juni 2026

Inhaltsverzeichnis

0	Präambel	3
1	Regelungen zur Informationssicherheit	3
2	Organisation der Informationssicherheit	5
2.1	Aufbauorganisation	5
2.2	Aufgaben und Ressourcenausstattung	7
3	IT-Notfallmanagement	8
4	Prüfungsmaßstäbe der Rechnungshöfe	9

0 Präambel

Die Ausübung der verfassungsrechtlich garantierten Aufgaben der Staatsgewalten erfordert einen sicheren und resilienten¹ Betrieb der Informationssysteme der öffentlichen Verwaltung. Gleichzeitig vergrößert sich die Angriffsfläche durch die fortschreitende Digitalisierung der Verwaltung und den umfassenden elektronischen Datenaustausch der Verwaltungen untereinander sowie mit Unternehmen, Bürgerinnen und Bürgern.

Die Informationssysteme der öffentlichen Verwaltung sind laut Bundesamt für Sicherheit in der Informationstechnik (BSI) innerhalb der EU im Branchenvergleich am stärksten von IT-Sicherheitsvorfällen betroffen.²

Ein Informationssicherheitsmanagement (ISM) und ein ergänzendes IT-Notfallmanagement sind essenziell für die Funktionsfähigkeit des Staates. Angemessene Informationssicherheit ist auch ein Gebot der Wirtschaftlichkeit und bewahrt die Handlungsfähigkeit der öffentlichen Verwaltung und schützt öffentliche Investitionen.

Die Rechnungshöfe haben daher eine Weiterentwicklung des ISM in den vergangenen Jahren aktiv begleitet und befördert. Das vorliegende Grundsatzpapier fasst wesentliche Regelungen sowie Prüfungserkenntnisse der Rechnungshöfe zusammen und gibt zu ausgewählten Aspekten Empfehlungen für eine künftige Ausgestaltung des ISM in der öffentlichen Verwaltung ab. Dieses Papier ergänzt damit die IT-Mindestanforderungen³ der Rechnungshöfe.

1 Regelungen zur Informationssicherheit

Öffentliche Verwaltungen haben in den letzten Jahren Informationssicherheitsmanagementsysteme (ISMS) auf- und ausgebaut.

¹ Beschreibt die Widerstands- und Anpassungsfähigkeit der gesamten IT-Infrastruktur bei Cyberangriffen.

² BSI, Die Lage der IT-Sicherheit in Deutschland 2024.

³ Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik Stand: 2025.

Die im Bund und in den Ländern implementierten ISMS orientieren sich an den Empfehlungen der DIN ISO/IEC 2700x-Normenreihe sowie den IT-Grundschutz-Standards des BSI.

Der IT-Planungsrat⁴ hat zur weiteren Standardisierung des Informations-sicherheitsmanagements in Deutschland Ende 2018 seine bisherige Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung⁵ sowie den Umsetzungsplan⁶ 2020 aktualisiert. Diese Leitlinie schreibt für den Bund und die Länder konkrete Anforderungen und Maßnahmen vor, die ein Mindestsicherheitsniveau realisieren sollen.

Weitere relevante gesetzliche Regelungen wie das IT-Sicherheitsgesetz⁷ oder die IT-Sicherheitsverordnung Portalverbund⁸ messen der Informationssicherheit bereits seit Jahren einen hohen Stellenwert zu. Die europäische NIS-2-Richtlinie⁹ steigert und standardisiert zudem die Anforderungen zur Cybersicherheit (als Teil der Informationssicherheit) für die öffentliche Verwaltung. Informationssicherheit nach dem Stand der Technik ist auch eine wesentliche Anforderung des Datenschutzrechts, insbesondere der technischen und organisatorischen Sicherheitsmaßnahmen nach der DSGVO.¹⁰ Ein ISMS unterstützt damit auch die Umsetzung der NIS-2-Richtlinie und des Datenschutzrechts.

⁴ Der IT-Planungsrat ist in Deutschland das zentrale Gremium für die föderale Zusammenarbeit des Bundes, der Länder und der Kommunen in der Informationstechnik (Artikel 91c GG). Er verwaltet u. a. das Verbindungsnetz der öffentlichen Verwaltungen und kann verbindliche IT-Interoperabilitäts- und IT-Sicherheitsstandards beschließen.

⁵ https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf aufgerufen am 30.05.2026.

⁶ https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-05_TOP_09_Umsetzungsplan.pdf aufgerufen am 30.05.2026.

⁷ Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, 18.05.2021.

⁸ §5 Onlinezugangsgesetz in Verbindung mit der IT-Sicherheitsverordnung Portalverbund.

⁹ Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148.

¹⁰ Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der

2 Organisation der Informationssicherheit

Für die Informationssicherheit einer Behörde ist die Behördenleitung verantwortlich.¹¹ Sie hat ein ISMS einzurichten und den Schutzbedarf zu ermitteln. Auf dieser Grundlage sind die notwendigen personellen, technischen und organisatorischen Maßnahmen unter wirtschaftlichen Gesichtspunkten zu veranlassen. Eine angemessene Organisation und Ressourcenausstattung stellen wichtige Voraussetzungen für ein wirkungsvolles ISMS dar.

Die IT-Grundschutz-Standards des BSI geben konkrete Vorgaben und Empfehlungen für die Aufbau- und Ablauforganisation (z. B. Benennung einer oder eines Informationssicherheitsbeauftragten, Initiierung eines Sicherheitsprozesses).

2.1 Aufbauorganisation

In den Prüfungen beobachten die Rechnungshöfe seit Jahren einen Trend hin zu einer stärkeren Zentralisierung der Serviceerbringung in der IT.

Infolgedessen haben einzelne Verwaltungen begonnen, ein übergreifendes ISMS zu entwickeln und die dezentralen Zuständigkeiten zusammenzuführen. Damit soll den Risiken aus der gemeinsamen Nutzung von Fachverfahren und Infrastrukturen adäquat begegnet werden.

Die Vernetzung und Digitalisierung in der öffentlichen Verwaltung haben eine sehr hohe Komplexität erreicht. Daher sollte in der Bundesverwaltung und in den Ländern zusätzlich zu behördenbezogenen ISM jeweils ein zentrales ISM eingerichtet werden. Dieses sollte mit Befugnissen zum Durchgriff in die Ressortverantwortlichkeiten ausgestattet sein. Informationssicherheit sollte organisations- und ebenenübergreifend gedacht werden. Ein zentrales ISM definiert die Strukturen zur

Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG).

¹¹ Dies ergibt sich aus der allgemeinen Pflicht, die Organisation so auszugestalten, dass wesentliche Risiken erkannt und gesteuert werden, vgl. Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung der Arbeitsgruppe Informationssicherheit des IT-PLR, Version 2.0 vom 06.12.2018.

verwaltungsübergreifenden Informationssicherheit. Dies ermöglicht den Verwaltungen eine gemeinsame Planung und Umsetzung von Maßnahmen. Ein zentrales ISM schränkt die Ressorthoheit nicht ein, vielmehr fördert dieses die Wirtschaftlichkeit und Wirksamkeit der Maßnahmen innerhalb der ISMS. Der Notwendigkeit zur Zentralisierung wurde zum Teil mit der Vorgabe des IT-Planungsrates zur Bestellung von Bundes- bzw. Landes-Informationssicherheitsbeauftragten entsprochen.¹² Zur Erstellung von Lagebildern und der Einführung von zentralen Sicherheitsmaßnahmen sollte die oder der Bundes- bzw. Landes-Informationssicherheitsbeauftragte über den aktuellen Reifegrad der ISMS in den Ressorts und Behörden informiert sein.

Im Hinblick auf die weiter voranschreitende Zentralisierung von Dienstleistungen in der IT und der zunehmenden Kooperation bei der Digitalisierung von Verwaltungsleistungen (EfA-Prinzip¹³) ist die Integration eines ISM in die behördenübergreifenden betrieblichen Prozesse notwendig. Informationssicherheit muss im gesamten Lebenszyklus von IT berücksichtigt werden. Verantwortlichkeiten im ISM sollten daher nicht mehr primär nach Organisationsgrenzen, sondern auf Dienste und die zugrundeliegenden Geschäftsprozesse bezogen festgelegt werden.

Die Informationssicherheitsbeauftragten sollen außerhalb des IT-Managements angesiedelt werden und nicht aktiv am IT-Einsatz beteiligt sein, um Interessen- und Rollenkonflikte zu vermeiden.¹⁴

Die vom IT-Planungsrat verabschiedete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung verpflichtet Bund und Länder, ein Computer Emergency Response Team (CERT) zu betreiben und weiterzuentwickeln. Es soll bei der Lösung von konkreten

¹² Punkt 5 der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung der Arbeitsgruppe Informationssicherheit des IT-PLR, Version 2.0 vom 06.12.2018.

¹³ Das EfA-Prinzip (Einer für Alle) ist ein zentrales Konzept der Verwaltungsdigitalisierung. Es sieht vor, dass digitale Verwaltungsleistungen einmal entwickelt und anschließend bundesweit genutzt werden können.

¹⁴ Die Aufgaben könnten z. B. in der Zentralabteilung außerhalb des IT-Referats oder vergleichbaren Organisationseinheiten wahrgenommen werden.

IT-Sicherheitsvorfällen als Koordinator mitwirken, Warnungen zu Sicherheitslücken herausgeben und Lösungsansätze anbieten.

Bund und Länder sollen perspektivisch die CERTs zu CSIRTs¹⁵ im Sinne der NIS-2-Richtlinie fortentwickeln.

2.2 Aufgaben und Ressourcenausstattung

Die mit der Informationssicherheit in den Behörden befassten Personen¹⁶ haben – jeweils im Rahmen der ihnen zugewiesenen Rollen – zur Gewährleistung einer ausreichenden Informationssicherheit umfangreiche Aufgaben zu erfüllen. Sie müssen

- den Informationssicherheitsprozess mitsteuern und koordinieren,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit unterstützen
- ihr über den Stand der Informationssicherheit laufend berichten,
- jederzeit direkten Zugang zur Behördenleitung haben,
- die Erstellung der erforderlichen Konzepte und Regelungen koordinieren,
- den Realisierungsplan für die Sicherheitsmaßnahmen erstellen und deren Umsetzung initiieren und überprüfen,
- sicherheitsrelevante Projekte koordinieren,
- sicherheitsrelevante Zwischenfälle untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit initiieren und steuern.

¹⁵ Computer Security Incident Response Team.

¹⁶ Informationssicherheitsbeauftragte sowie ISM-Team. Das ISM-Team unterstützt den Informationssicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

Die mit der Informationssicherheit befassten Personen sollen an sicherheitsrelevanten Entscheidungen sowie bei allen Geschäftsprozessen und Fachaufgaben ausreichend beteiligt werden.

Die Rechnungshöfe haben festgestellt, dass in vielen Bereichen der Verwaltung ein Mangel an ausreichend qualifiziertem und geschultem Personal besteht, um die gestiegenen und gesetzlich verankerten¹⁷ Anforderungen an die Informationssicherheit zu erfüllen. Insbesondere sind die Informationssicherheitsbeauftragten ausreichend zu qualifizieren.

Zur Erreichung der festgelegten Sicherheitsziele müssen die notwendigen Sachmittel und das erforderliche Personal zur Verfügung stehen. Dies sollte nach anerkannten Methoden erhoben und fortgeschrieben werden.¹⁸

3 IT-Notfallmanagement

Das IT-Notfallmanagement ist Bestandteil eines umfassenden ISM. Es beinhaltet ein systematisches Vorgehen, um

- die Behörde vor ungeplanten IT-Betriebsunterbrechungen zu schützen,
- im Falle einer IT-Betriebsunterbrechung den Normalbetrieb schnellstmöglich wiederherzustellen sowie
- gesetzliche und regulatorische Anforderungen für den IT-Betrieb zu erfüllen.

Das IT-Notfallmanagement ist in ein übergeordnetes Business Continuity Management einzubinden.¹⁹ Maßnahmen des IT-Notfallmanagements müssen risikoorientiert geplant, regelmäßig überprüft und an aktuelle Gefährdungslagen angepasst werden. Dies setzt eine strategische Einbindung in die Gesamtorganisation sowie klare Zuständigkeiten und Abläufe im Notfall voraus.

Durch ein systematisches IT-Notfallmanagement werden Risiken reduziert und die Resilienz der Organisation erhöht. Es soll sowohl präventive als

¹⁷ Vgl. Art. 21 NIS-2-Richtlinie.

¹⁸ Leitsätze für die Personalbedarfsermittlung der Rechnungshöfe von Bund und Ländern vom 03.06.2024.

¹⁹ BSI-Standard 200-4 Business Continuity Management.

auch reaktive Maßnahmen umfassen. Ziel präventiver Maßnahmen ist es, das Risiko von Verfügbarkeitseinschränkungen zu reduzieren und mögliche Schadensauswirkungen zu begrenzen. Reaktive Maßnahmen werden im Schadensfall durchgeführt und legen den Schwerpunkt auf die schnellstmögliche Wiederherstellung des oder der IT-Verfahren.

Aus Sicht der Rechnungshöfe sind insbesondere die nachfolgend genannten Maßnahmen durchzuführen, um ein systematisches und wirksames IT-Notfallmanagement zu etablieren:

- Mittels Business-Impact-Analysen (BIA) ist die Kritikalität der wesentlichen Geschäftsprozesse der Behörde festzustellen.
- Eine Notfalldokumentation mit der Planung von proaktiven und reaktiven Maßnahmen ist zu erstellen sowie aktuell zu halten.
- Es ist ein IT-Notfallbeauftragter zu bestimmen. Dieser unterstützt die Behördenleitung in ihrer Gesamtverantwortung.
- Bei verfügbarkeitsrelevanten Gefährdungen sollten über eine Risikoanalyse proaktive und reaktive Sicherheitsmaßnahmen für die einzelnen IT-Verfahren definiert werden.
- Regelmäßig ist durch Notfallübungen der Reifegrad der Notfallorganisation zu überprüfen.
- Der für den IT-Betrieb verantwortliche Personenkreis ist zu den IT-Notfallkonzepten und -plänen zu schulen.

Die Verantwortlichen sollen nach Bewältigung eines Notfalls diesen analysieren und nachbereiten.

4 Prüfungsmaßstäbe der Rechnungshöfe

Die Herstellung und Aufrechterhaltung einer angemessenen Informationssicherheit ist für die Verwaltung verpflichtend. Die Verantwortung dafür trägt die Behördenleitung. Die Verwaltung hat sicherzustellen, dass insbesondere

- die Anforderungen an die Informationssicherheit regelmäßig ermittelt werden,
- Sicherheitskonzepte für Verwaltungsprozesse, IT-Services, Fachverfahren sowie Behörden und Einrichtungen vor

Inbetriebnahme erstellt, umgesetzt und sukzessive fortgeschrieben werden,

- die Informationssicherheit bei neuen Fachverfahren bzw. bei der Modernisierung von Fachverfahren von Anfang an integriert wird (Security by Design),
- die Sicherheitsmaßnahmen dem Stand der Technik entsprechen und zur Gewährleistung der jeweiligen Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität geeignet und angemessen sind,
- die ISMS organisatorisch, personell und finanziell die Anforderungen erfüllen können,
- die in IT getätigten Investitionen gesichert werden,
- die ISMS die Auswirkungen und Kosten eines IT-Sicherheitsvorfalls reduzieren und damit zu einem wirtschaftlichen Verwaltungshandeln beitragen,
- Risiken für die Informationssicherheit fortlaufend analysiert, bewertet und systematisch behandelt werden (Risikomanagement),
- die ISMS ein Sicherheitsniveau anstreben, welches keine hohen Risiken akzeptiert,
- die Verwaltung IT-Notfälle und IT-Krisen bewältigen kann,
- die Planung und Umsetzung der Informationssicherheit revisionssicher dokumentiert wird,
- die ISMS durch geeignete Audit-Strukturen regelmäßig auf ihre Wirksamkeit hin überprüft werden und
- bei externen Unterstützungsleistungen sichergestellt ist, dass Arbeitsergebnisse eine möglichst breite Verwendung finden und eine Fortschreibung der Arbeitsergebnisse auch ohne externe Unterstützung möglich ist.

Eine hundertprozentige Informationssicherheit ist nicht erreichbar. Die Verwaltung hat die erforderlichen Maßnahmen risikoorientiert und unter wirtschaftlichen Gesichtspunkten auszuwählen.