Rechnungshöfe des Bundes und der Länder

Grundsatzpapier zum Informationssicherheits-management

Stand Mai 2020

Inhaltsverzeichnis

0 Präambel 3

1 Informationssicherheitsmanagement 6

2 Organisation der Informationssicherheit 8

2.1 Aufbauorganisation 8

2.2 Ressourcenausstattung 10

3 Das CERT als wichtiges Element des operativen Informationssicherheitsmanagements 12

4 Erwartungen und Prüfungsmaßstäbe der Rechnungshöfe 13

0 Präambel

Der digitale Wandel stellt den Staat[1] vor neue Herausforderungen:

Die Ausübung der verfassungsrechtlich garantierten Aufgaben der judikativen, legislativen und exekutiven Staatsgewalten setzt einen sicheren und zuverlässigen Betrieb der Informationssysteme des Staates voraus.

Die Gewährleistung eines effektiven Rechtsschutzes gegen Akte der öffentlichen Gewalt nach Artikel 19 Abs. 4 GG und des Rechtsstaatsprinzips nach Artikel 20 Abs. 3 GG erfordern in der öffentlichen Verwaltung eine lückenlose und gegen Manipulationen geschützte Kommunikation und eine Dokumentation des Verwaltungshandelns.

Das Vertrauen der Bürger und Unternehmen in die Integrität des digitalen Staates wird erschüttert, wenn dieser seinen Aufgaben wegen funktionsunfähiger Informationssysteme nicht mehr nachkommen kann. Die Informationssysteme in den Staatsgewalten sind dadurch zu kritischen Infrastrukturen für das Gemeinwesen geworden.

Aktuelle Berichterstattungen in den Medien über nationale und internationale Cyber-Kriminalität zeigen, dass die Sicherheit von Daten gefährdet und das staatliche Gemeinwesen neuartigen Gefährdungslagen ausgesetzt ist.

Die elektronische Verwaltungsarbeit geht mit der Speicherung von elektronischen Daten in Netzwerken, E-Mail-Systemen und Dokumentenmanagementsystemen einher. Aktuelle Sicherheitsgefährdungen wie Schadsoftware können die unberechtigte Kenntnisnahme, Veränderung und Löschung von Daten und Einschränkungen der Verfügbarkeit elektronischer Systeme zur Folge haben. Aktuelle Studien schätzen den weltweiten Schaden durch Cyber-Kriminalität in der Größenordnung von 600 Milliarden US-Dollar. Die wirtschaftlichen Schäden durch Cyberkriminalität betragen mittlerweile fast das Dreifache der Schäden durch Naturkatastrophen. Die Europäische Kommission geht davon aus, dass

[1] Die unmittelbare und mittelbare Staatsverwaltung und alle seine Untergliederungen.

sich die wirtschaftlichen Auswirkungen von Cyber-Kriminalität zwischen 2013 und 2017 verfünffacht haben[2]. Mit dem fortschreitenden digitalen Wandel in den Staatsgewalten entwickeln sich parallel dazu die Hackerangriffe weiter. Ohne ein darauf ausgerichtetes Informationssicherheitsmanagement[3] (ISM) bzw. eingerichtete Informationssicherheitsmanagementsysteme (ISMS) könnte dies die Staatsgewalten in ihren Handlungen einschränken bzw. handlungsunfähig machen. Dies gilt umso mehr, je weiter in der Verwaltung die Einführung von elektronischen Akten voranschreitet. Wird das Dokumentenmanagementsystem in einem zentralen Rechenzentrum betrieben, so befindet sich auf diesem das gesammelte Verwaltungswissen der angeschlossenen Organisationseinheiten. Der digitale Verwaltungsvollzug und die damit verbundenen erheblichen Investitionen der öffentlichen Verwaltungen in ihre IT-Ausstattungen sind ohne ausreichende Informationssicherheit gefährdet. Angemessene Informationssicherheit ist daher auch ein Gebot der Wirtschaftlichkeit.

Die Schaffung eines angemessenen Maßes an Informationssicherheit ist mit personellen und finanziellen Aufwänden verbunden. Daher ist bei der Auswahl und Umsetzung geeigneter Maßnahmen darauf zu achten, dass das notwendige Sicherheitsniveau auch wirtschaftlich erreicht wird. Einerseits muss den bestehenden Gefährdungen wirkungsvoll begegnet werden, andererseits müssen die Maßnahmen auch am tatsächlichen Schutzbedarf und der Gefährdung ausgerichtet sein.

Die Rechnungshöfe haben daher das Thema Informationssicherheit in den vergangenen Jahren immer wieder aufgegriffen und eine Weiterentwicklung des Informationssicherheitsmanagements aktiv begleitet und befördert. Mit dem vorliegenden Grundsatzpapier und dessen Anlagen werden die Prüfungserkenntnisse der Rechnungshöfe zusammengefasst und zu

[2] KOM Cyber Security Factsheet: Resilience, Deterrence and Defence: Building strong cybersecurity in Europe, September 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=46998

[3] Unter Informationssicherheitsmanagement bzw. dem Informationssicherheitsmanagementsystem wird der Teil des gesamten Managementsystems verstanden, welcher auf Basis eines Risikoansatzes die Festlegung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.

ausgewählten Aspekten Empfehlungen für eine zukünftige Ausgestaltung der ISMS in Bund, Ländern und Kommunen abgegeben. Dieses Papier ergänzt damit die Mindestanforderungen der Rechnungshöfe zum Einsatz von Informations- und Kommunikationstechnik. Darüber hinaus stellen die Rechnungshöfe Empfehlungen für die Prüfung der Informationssicherheit bereit.

1 Informationssicherheitsmanagement

Die Informationssysteme und Netzwerke der öffentlichen Verwaltung in Deutschland sind Sicherheitsbedrohungen unterschiedlichster Art von Innen und Außen ausgesetzt. Die Regierungs- und Verwaltungsnetze werden täglich angegriffen. Mit Schadsoftware behaftete E-Mails zählen mit zu den häufigsten Angriffsmethoden. Zudem beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine konstant steigende Professionalisierung von Angreifern.[4]

Die öffentliche Verwaltung hat in den letzten Jahren auf diese Bedrohung mit dem Aufbau und Ausbau von ISMS reagiert.

Die derzeit im Bund und in den Ländern implementierten ISMS orientieren sich im Grundsatz an den Empfehlungen der DIN ISO/IEC 2700x-Reihe sowie den IT-Grundschutz-Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Der IT-Planungsrat[5] hat zur weiteren Standardisierung des Informationssicherheitsmanagements in Deutschland eine Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung[6] einschließlich eines Umsetzungsplans[7] beschlossen[8,9]. Diese Leitlinie definiert für den Bund und die Länder einen Rahmen, welche Anforderungen bestehen und welche organisatorischen Aspekte und Maßnahmen mindestens realisiert werden müssen.

---

4 BSI, Die Lage der IT-Sicherheit in Deutschland 2019.

5 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.

6 Vgl. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html, aufgerufen am 18.11.2019.

7 Vgl. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Umsetzungsplan.html, aufgerufen am 18.11.2019.

8 Zuletzt im März 2019 aktualisiert.

9 Vgl. https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/ 28_Sitzung/TOP12_Anlage_Leitlinie.html, aufgerufen am 18.11.2019

Im Hinblick auf die Grundsätze der Wirtschaftlichkeit und Sparsamkeit hat die Verwaltung bei der Realisierung der Informationssicherheit widerstreitende Aspekte zu beachten. Ein ISMS bindet personelle und finanzielle Ressourcen. Es ist trotzdem notwendig, um hohe materielle und immaterielle Schäden abzuwenden, die der öffentlichen Verwaltung durch Datenverlust, Datenmanipulation oder das Ausspähen von Daten entstehen würden.

Gesetzliche Regelungen, wie das IT-Sicherheitsgesetz, messen der IT-Sicherheit einen hohen Stellenwert zu.

Der Arbeitskreis Organisation und Informationstechnik der Rechnungshöfe des Bundes und der Länder hat erstmals im Juni 2014 beschlossen, basierend auf Prüfungsfeststellungen durch ein Grundsatzpapier Anregungen für eine Weiterentwicklung des ISM bzw. der ISMS zu geben.

2 Organisation der Informationssicherheit

Folgend aus der allgemeinen Leitungsverantwortung ist die Behördenleitung auch für die Informationssicherheit ihrer Behörde verantwortlich. Sie hat die notwendigen technischen und organisatorischen Maßnahmen unter wirtschaftlichen Gesichtspunkten zu veranlassen, um dem ermittelten Schutzbedarf Rechnung zu tragen und ein ISMS einzurichten.

Eine hundertprozentige Informationssicherheit ist nicht erreichbar. Die vorhandenen Restrisiken müssen deshalb ermittelt sowie deren Auswirkungen beschrieben und bewertet werden.

Eine angemessene Aufbauorganisation und Ressourcenausstattung stellen wichtige Voraussetzungen für ein wirkungsvolles ISMS dar.

2.1 Aufbauorganisation

Empfehlungen zur konkreten Umsetzung eines ISM in der öffentlichen Verwaltung sind in der Regel nicht Gegenstand der internationalen und nationalen Normen und Standards. Ausnahme bilden die IT-Grundschutz-Standards des BSI, die als Vorgaben für die Bundesverwaltung bzw. als Empfehlungen für die Länder[10] gelten (z. B. Berufung eines Informationssicherheitsbeauftragten).

In den öffentlichen Verwaltungen haben sich intern und übergreifend unterschiedliche Ausgestaltungen des ISM entwickelt. Befördert wurde diese Entwicklung durch den heterogenen Aufbau des IT-Managements sowie der IT-Infrastrukturen in Bund, Ländern und Kommunen.

In den Prüfungen stellen die Rechnungshöfe seit Jahren einen Trend hin zu einer stärkeren Zentralisierung der Serviceerbringung in der IT fest. Diese Entwicklung wurde durch die Virtualisierung der IT in den letzten Jahren verstärkt.

[10] In den Ländern bestehen teilweise Regelungen, die eine verbindliche Anwendung aller oder ausgewählter IT-Grundschutz-Standards vorgeben.

Nach den Erhebungen der Rechnungshöfe hat die Vernetzung und Digitalisierung in der öffentlichen Verwaltung einen solchen Verdichtungsgrad erreicht, dass in der Bundesverwaltung und in den einzelnen Ländern perspektivisch jeweils ein zentrales ISM mit Befugnissen zum Durchgriff in die Ressortverantwortlichkeiten erforderlich wird.[11] Ein zentrales ISM schafft gemeinsame Strukturen zur verwaltungsübergreifenden Aufgabenerledigung. Es ermöglicht der Verwaltung, zu kooperieren und die Aufgabenwahrnehmung zu koordinieren. Ein zentrales ISM schränkt die Ressorthoheit nicht ein. Der Notwendigkeit zur Zentralisierung wurde zum Teil mit der Vorgabe des IT-Planungsrates nach Bundes- bzw. Landes-Informationssicherheitsbeauftragten entsprochen.

Eine reine dienststellenbezogene Ausrichtung des ISM ist aufgrund der fehlenden Sicht auf die Gesamtarchitektur nicht mehr zeitgemäß. Diese hat in der Vergangenheit oft genug zu kleinen, nicht vernetzten Insellösungen geführt.

Im Hinblick auf die weiter voranschreitende Zentralisierung von Dienstleistungen in der IT, ist die Entwicklung eines serviceorientierten ISM notwendig. Verantwortlichkeiten in der IT sollten daher nicht mehr primär nach Organisationsgrenzen, sondern auf Dienste bezogen festgelegt werden.

Für angemessene Informationssicherheit zu sorgen, gehört zu den Aufgaben des zentralen IT-Managements. Der IT-Sicherheitsbeauftragte soll außerhalb des IT-Managements angesiedelt sein, um Interessen- und Rollenkonflikte zu vermeiden.[12] Zusätzlich ist eine intensivere Kontrolle des ISMS durch die Prüfungsinstanzen erforderlich.

[11] In der Übergangsphase kann ein zusätzliches dienststellenbezogenes ISM erforderlich sein. Hierbei ist eine enge Kommunikation und Kooperation mit der zentralen Instanz notwendig.

[12] Die Aufgabenwahrnehmung könnte z. B. in der Zentralabteilung, außerhalb des IT-Referats, oder vergleichbaren Organisationseinheiten erfolgen.

2.2 Ressourcenausstattung

Die mit der Informationssicherheit in den Behörden befassten Personen[13] haben – jeweils im Rahmen der ihnen zugewiesenen Rollen – zur Sicherstellung einer ausreichenden Informationssicherheit umfangreiche Aufgaben zu erfüllen. Sie müssen z. B.

- den Informationssicherheitsprozess steuern und koordinieren,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit erlassen,
- den Realisierungsplan für die Sicherheitsmaßnahmen erstellen und deren Realisierung initiieren und überprüfen,
- der Leitungsebene über den Status Quo der Informationssicherheit berichten,
- sicherheitsrelevante Projekte koordinieren,
- sicherheitsrelevante Zwischenfälle untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit initiieren und steuern.

Die Rechnungshöfe haben in verschiedenen Prüfungen festgestellt, dass in vielen Bereichen der Verwaltung ein Mangel an ausreichend qualifiziertem und geschultem Personal besteht, um die gestiegenen und gesetzlich verankerten[14] Anforderungen an die Informationssicherheit zu erfüllen.

[13] Informationssicherheitsbeauftragte sowie ISM-Team. Dieses unterstützt den Informationssicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

[14] Vgl. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015.

Der personelle Bedarf muss nach wirtschaftlichen Aspekten erhoben und fortgeschrieben werden.

Neben dem Personal sind entsprechend der Informationssicherheitsleitlinie des Bundes und der Länder die zur Erreichung der Sicherheitsziele erforderlichen Sachmittel zur Verfügung zu stellen.

3 Das CERT als wichtiges Element des operativen Informationssicherheitsmanagements

Ein Computer Emergency Response Team (CERT) ist eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen als Koordinatoren mitwirken, Warnungen zu Sicherheitslücken herausgeben und Lösungsansätze anbieten.

Die vom IT-Planungsrat verabschiedete Leitlinie über die Informationssicherheit in der öffentlichen Verwaltung verpflichtete die Länder, ein CERT aufzubauen.

In Abgrenzung zum Informationssicherheitsmanagement wird das CERT u. a. vom Sicherheitsmanagement genutzt, um

- Informationen über mögliche Sicherheitsvorfälle bereitzustellen,
- ggf. bereits im Vorfeld hierzu Beratungsleistungen vorzuhalten,
- Alarm- und Warnmeldungen zu generieren,
- Sicherheitswerkzeuge zu entwickeln und einzusetzen,
- ggf. befallene technische Infrastruktur zu analysieren,
- Sicherheitsvorfälle zu bearbeiten und
- ggf. bei Wiederherstellung nach Sicherheitsvorfällen mitzuwirken.

Die Rechnungshöfe sehen in der Einrichtung eines CERT einen wichtigen Baustein für das operative ISM. Aufgrund des erheblichen Aufwands für die Einrichtung und den Betrieb eines CERT ist eine länderübergreifende Kooperation naheliegend. Darüber hinaus ist eine enge Zusammenarbeit zwischen dem BSI, den Informationssicherheitsbeauftragten des Bundes und der Länder sowie den CERT der Länder erforderlich.

4 Erwartungen und Prüfungsmaßstäbe der Rechnungshöfe

Da die Verwaltung nahezu flächendeckend und durchgehend IT-gestützt arbeitet, hängt ihre Funktionsfähigkeit maßgeblich von Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und Informationsbestände ab. Diese zu gewährleisten, ist damit auch ein Gebot der Wirtschaftlichkeit.

Die Herstellung einer angemessenen Informationssicherheit ist in der aktuellen Verwaltungsarbeit eine wesentliche Herausforderung. Die Verwaltung hat angesichts der bestehenden Gefährdungen vorrangig sicherzustellen, dass

- die Informationssysteme zuverlässig und kontinuierlich zur Verfügung stehen,
- die Anforderungen an die Sicherheit der Informationsverarbeitung regelmäßig ermittelt und umgesetzt werden,
- die in Informationssysteme getätigten Investitionen gesichert werden,
- die ISMS organisatorisch, personell und finanziell die Anforderungen erfüllen können,
- die ISMS die Auswirkungen und Kosten eines IT-Sicherheitsvorfalls reduzieren und damit zu einem wirtschaftlichen Verwaltungshandeln beitragen.

Die Verwaltung hat die hierfür erforderlichen Maßnahmen unter wirtschaftlichen Gesichtspunkten auszuwählen.

Die Rechnungshöfe werden die Ordnungsmäßigkeit und Wirtschaftlichkeit der ISMS in Bund, Ländern und ggf. Kommunen u.a. anhand von gemeinsamen Mindeststandards untersuchen. Der Arbeitskreis „Organisation und Informationstechnik“ der Rechnungshöfe des Bundes und der Länder hat hierzu in Erweiterung des vorliegenden Grundsatzpapiers einen

Fragenkatalog[15] erarbeitet, den die Rechnungshöfe bei ihren Prüfungen verwenden können.

[15] Sh. Fragenkatalog der Rechnungshöfe des Bundes und der Länder zur Prüfung der Informationssicherheit in der öffentlichen Verwaltung vom Mai 2020 (Anlage).

Arbeitsgruppe Informationssicherheitsmanagement
des Arbeitskreises Organisation und IT
der Rechnungshöfe des Bundes und der Länder

Fragenkatalog der Rechnungshöfe zum Informationssicherheitsmanagement

– Stand Mai 2020 –

Inhalt

Inhalt 1

1 Fragen zum Informationssicherheitsmanagement 2

1.1 Fragen auf Bundes-/Landesebene zum Informationssicherheitsmanagement 2

1.2 Fragen auf Behördenebene zum Informationssicherheitsmanagement 4

2 Fragen zur Absicherung der Netzinfrastruktur 7

2.1 Fragen auf Bundes-/Landesebene zur Absicherung der Netzinfrastruktur 7

2.2 Fragen auf Behördenebene zur Absicherung der Netzinfrastruktur 8

3 Fragen zu einheitlichen Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren ... 10

3.1 Fragen auf Bundes-/Landesebene zu einheitlichen Sicherheitsstandards 10

3.2 Fragen auf Behördenebene zu einheitlichen Sicherheitsstandards 11

4 Fragen zur gemeinsamen Abwehr von IT-Angriffen 11

4.1 Fragen auf Bundes-/Landesebene zur gemeinsamen Abwehr von IT-Angriffen 11

4.2 Fragen auf Behördenebene zur gemeinsamen Abwehr von IT-Angriffen 12

5 Fragen zum IT-Notfallmanagement 13

5.1 Fragen auf Bundes-/Landesebene zum IT-Notfallmanagement 13

5.2 Fragen auf Behördenebene zum IT-Notfallmanagement 14

1 Fragen zum Informationssicherheitsmanagement

1.1 Fragen auf Bundes-/Landesebene zum Informationssicherheitsmanagement

IL 1	**Strategie und Leitlinie**
IL 1.1	Gibt es eine verbindliche Leitlinie für die Informationssicherheit (IS) der Landes-/ Bundesverwaltung?
IL 1.2	Werden in dieser Leitlinie der Stellenwert der Informationssicherheit, der Geltungsbereich, die Verantwortung der Leitung, die Leitaussagen der Sicherheitsstrategie sowie die Organisationsstruktur für die Informationssicherheit geregelt und die Sicherheitsziele festgelegt? Fordert die IS-Leitlinie die Ermittlung der behördlichen Anforderungen an IS (Vertraulichkeit, Integrität, Verfügbarkeit)?
IL 1.3	Wurde und wird die Leitlinie allen Beschäftigten bekanntgegeben?
IL 1.4	Sind die Sicherheitsziele und Strategien angemessen (Kompromiss zwischen Kosten, Aufwand und Nutzen → Wirtschaftlichkeit) und werden diese regelmäßig überprüft und aktualisiert?
IL 1.5	Welche weiteren übergreifenden IT-Sicherheitsrichtlinien für die Landes- oder Bundesverwaltung gibt es?
IL 2	**Grundsätzliche Fragen des ISM**
IL 2.1	Werden der Sicherheitsprozess, die Sicherheitskonzepte, die Leitlinie zur Informationssicherheit, Richtlinien und die Organisationsstruktur für Informationssicherheit regelmäßig auf Wirksamkeit und Angemessenheit überprüft, aktualisiert und nachvollziehbar dokumentiert?
IL 2.2	Orientiert sich die Etablierung des Informationssicherheitsmanagements am IT-Grundschutz des BSI bzw. der ISO 27001?
IL 2.3	Werden die nachgeordneten (Landes-, Bundes-) Behörden zur Erstellung und Umsetzung von Sicherheitskonzepten verpflichtet?
IL 3	**IS-Organisation**
IL 3.1	Wurde ein Landes-/Bundes-Informationssicherheitsbeauftragter ernannt und eingesetzt?
IL 3.2	Gibt es eine Vertretungsregelung für den Informationssicherheitsbeauftragten?
IL 3.3	Ist der Informationssicherheitsbeauftragte außerhalb einer operativ tätigen IT-Einheit angesiedelt?
IL 3.4	Verfügt der Informationssicherheitsbeauftragte über eine ausreichende Qualifizierung (Zertifizierung sollte angestrebt werden)?

IL 3.5	Sind die Aufgaben, Verantwortungen und Kompetenzen des Informationssicherheits-beauftragten und der weiteren IS-Organisation innerhalb des Sicherheitsprozesses klar definiert, zugewiesen und dokumentiert?
IL 3.6	Gibt es für die wesentlichen Behörden ihres Bundeslands (oder Bundesbehörden) weitere Informationssicherheitsbeauftragte?
IL 3.7	Gibt es Festlegungen und Dokumentationen für die Abläufe, den Umgang und die Behandlung von IT-Sicherheitsvorfällen?
IL 4	**Operative Aufgaben des ISM**
IL 4.1	Hat das Management einen Überblick über die landesweite[1] Sicherheitslage (Überblick über alle Ressorts)?
IL 4.2	Hat das Management einen Überblick über die geschäftskritischen Informationen, die Fachaufgaben und Geschäftsprozesse?
IL 4.3	Gibt es regelmäßige Management-Berichte des Landes IT-Sicherheitsbeauftragen oder des IS-Management-Teams an die Leitungsebene?
IL 4.4	Durch welche Maßnahmen wird die Information, die Weiterbildung und Sensibilisierung der öffentlichen Verwaltung zu Themen der Informationssicherheit unterstützt?
IL 4.5	Wird das Management bei der Sensibilisierung zur Informationssicherheit einbezogen?
IL 4.6	Wird der Wert/Nutzen der IS dokumentiert und kommuniziert?
IL 5	**Umfeld IS**
IL 5.1	Sind die finanziellen und personellen Ressourcen für die Informationssicherheit angemessen?
IL 5.2	Ist die IS im Projektmanagement verankert? Sind die Anforderungen der IS bei allen laufenden (IT-) Projekten eingeplant?
IL 5.3	Ist IS in die Regelungen zum behördlichen Schriftgut (vollständiger Informations-Lebenszyklus!, inkl. E-Mail) eingebettet?
IL 5.4	Ist das IS-Risikomanagement in ein ggf. existierendes übergreifendes Risikomanagement eingebettet?
IL 5.5	Sind die Mittel für ISM im Haushalt klar ausgewiesen?
IL 5.6	Gab es außerplanmäßige/überplanmäßige Ausgaben infolge von Sicherheitsvorfällen?

[1] Die Begriffe landesweit und Land stehen im Folgenden stellvertretend für bundes-, landes-, gemeinde- und anstalts-/unternehmensweit bzw. für Bund, Land, Gemeinde, Anstalt/Unternehmen.

1.2 Fragen auf Behördenebene zum Informationssicherheitsmanagement

IB 1	Strategie und Leitlinie
IB 1.1	Gibt es eine behördenspezifische Leitlinie zur IS? Wurde diese von der Behördenleitung verabschiedet? Steht sie im Einklang mit der Leitlinie für die Informationssicherheit der Landesverwaltung?
IB 1.2	Werden in dieser Leitlinie der Stellenwert der Informationssicherheit, der Geltungsbereich, die Verantwortung der Leitung, die Sicherheitsstrategie sowie die Organisationsstruktur für die Informationssicherheit geregelt und die Sicherheitsziele festgelegt?
IB 1.3	Wurde und wird die Leitlinie allen Mitarbeitern bekanntgegeben? Wie?
IB 1.4	Sind angemessene Sicherheitsziele und Strategien festgelegt worden (Kompromiss zwischen Kosten, Aufwand und Nutzen → Wirtschaftlichkeit) und werden diese regelmäßig überprüft und aktualisiert?

IB 2	Grundsätzliche Fragen des ISM
IB 2.1	Hat die Behörden- bzw. Unternehmensleitung deutlich sichtbar die Verantwortung für Informationssicherheit übernommen?
IB 2.2	Wird der Informationssicherheitsprozess von der Leitungsebene initiiert, gesteuert, kontrolliert?
IB 2.3	Orientiert sich die Etablierung des Informationssicherheitsmanagements am IT-Grundschutz des BSI bzw. der ISO 27001?
IB 2.4	Wird die Informationssicherheit ständig überprüft und in alle Prozesse integriert? Wurden erkannte Schwachstellen beseitigt?
IB 2.5	Werden der Sicherheitsprozess, die Sicherheitskonzepte, die Leitlinie zur Informationssicherheit, Richtlinien und die Organisationsstruktur für Informationssicherheit regelmäßig auf Wirksamkeit und Angemessenheit überprüft, aktualisiert und nachvollziehbar dokumentiert?
IB 2.6	Wurde für die Komponenten mit hohem oder sehr hohem Schutzbedarf eine explizite Risikoanalyse durchgeführt?
IB 2.7	Sind zum Schutz der Werte der Zutritt zu Räumen, der Zugang zu IT-Systemen und Anwendungen und der Zugriff auf Informationen geregelt?
IB 2.8	Welche weiteren Sicherheitsrichtlinien gibt es? Wurden diese den Betroffenen bekannt gemacht? Wie?
IB 2.9	Sind die Ergebnisse aller Phasen des Sicherheitsprozesses ausreichend und aktuell dokumentiert?
IB 2.10	Welche Regelungen gibt es, um die Vertraulichkeit der Dokumente zum ISM zu wahren?

IB 2.11	Werden bei Lieferanten/ Diensterbringer-Beziehungen auch die Sicherheitsanforderungen berücksichtigt?
IB 2.12	Erfolgt eine durchgängige Trennung von Entwicklung, Test und Betrieb?
IB 3	**IS-Organisation**
IB 3.1	Hat die Behördenleitung einen Informationssicherheitsbeauftragten benannt und eingesetzt?
IB 3.2	Ist der Informationssicherheitsbeauftragte organisatorisch außerhalb der IT-Einheit angesiedelt? Hat er ein direktes Vortragsrecht bei der Behördenleitung?
IB 3.3	Gibt es einen Stellvertreter?
IB 3.4	Hat der Informationssicherheitsbeauftragte im Nebenamt auch Aufgaben im IT-Betrieb?
IB 3.5	Sind der Informationssicherheitsbeauftragte und der Vertreter ausreichend qualifiziert? Wie erfolgt die Fortbildung der für ISM verantwortlichen Personen?
IB 3.6	Gibt es in der Behörde eine weitere Organisationsstruktur für Informationssicherheit (z.B. bei größeren Behörden ein Sicherheitsmanagementteam)?
IB 3.7	Sind die Aufgaben, Verantwortungen und Kompetenzen des Informationssicherheitsbeauftragten, des ISM-Teams und weiterer Verantwortlicher innerhalb des Sicherheitsprozesses klar definiert, zugewiesen und dokumentiert?
IB 3.8	Falls ein externer Informationssicherheitsbeauftragter bestellt wurde: Umfasst der hierzu geschlossene Dienstleistungsvertrag alle Aufgaben des Informationssicherheitsbeauftragten sowie die damit verbundenen Rechte und Pflichten und wurde eine Vertraulichkeitsvereinbarung abgeschlossen?
IB 4	**Operative Aufgaben des ISM**
IB 4.1	Wird der Wert/Nutzen der IS dokumentiert und kommuniziert?
IB 4.2	Wurde/n für die Behörde ein Sicherheitskonzept/e erstellt und dabei alle relevanten Komponenten / Werte (assets) (z.B. Anwendungen, IT-Systeme, Räume usw.) strukturiert erfasst und deren Schutzbedarf festgestellt? Sind die Anforderungen an IS (Vertraulichkeit, Integrität, Verfügbarkeit) ressortweit oder für die Behörde klar dokumentiert?
IB 4.3	Existieren durchgängig Sicherheitsdokumentationen für die einzelnen IT-Verfahren? Ist IS in den Betriebsdokumentationen der IT-Verfahren hinreichend berücksichtigt? Verweise zur Sicherheitsdokumentation?
IB 4.4	Wie werden die Mitarbeiter (auch das Management, extern Beschäftigte oder Projektmitarbeiter) systematisch und zielgruppengerecht zu Sicherheitsrisiken sensibilisiert und zu Fragen der Informationssicherheit geschult?
IB 4.5	Werden Verstöße (ggf. disziplinarisch) sanktioniert?

IB 4.6	Hat das Management einen Überblick über die geschäftskritischen Informationen, die Fachaufgaben und Geschäftsprozesse?
IB 4.7	Sind Kommunikationswege geplant, beschrieben, bekannt gemacht und eingerichtet worden? Ist festgelegt, wer wen wann und in welchem Umfang informiert?
IB 4.8	Wird die Leitungsebene regelmäßig zum Umsetzungsstand, den Zielterminen und zum Ressourceneinsatz informiert?
IB 4.9	Werden regelmäßig Sicherheitsrevisionen von qualifizierten und unabhängigen Personen durchgeführt?
IB 4.10	Sind die ermittelten Ergebnisse der Revisionen nachvollziehbar dokumentiert (Revisionsbericht)?
IB 4.11	Gibt es regelmäßige Management-Berichte des Informationssicherheitsbeauftragen oder des IS-Management-Teams an die Leitungsebene?
IB 4.12	Enthalten die Management-Berichte die wesentlichen relevanten Informationen über den Status des IS-Prozesses und die Ergebnisse von Überprüfungen (z. B. Audits, Datenschutzkontrollen, Sicherheitsvorfälle, Erfolge, Probleme) sowie klar priorisierte und mit realistischen Abschätzungen des Umsetzungsaufwands versehene Maßnahmenvorschläge?
IB 4.13	Werden die Management-Berichte aussagekräftig bewertet, unterschrieben und archiviert?
IB 4.14	Sind die Management-Entscheidungen über erforderliche Aktionen, Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen dokumentiert und archiviert?
IB 5	**IS-Maßnahmen**
IB 5.1	Wurden für die gesamte Informationsverarbeitung ausführliche und angemessene (wirtschaftliche) Sicherheitsmaßnahmen festgelegt und die für die Umsetzung erforderlichen Ressourcen beziffert?
IB 5.2	Wurden alle Maßnahmen umgesetzt? Wenn nein, gibt es eine klare Realisierungsplanung der noch umzusetzenden Maßnahmen?
IB 5.3	Werden oder wurden die Sicherheitsmaßnahmen gemäß dem Realisierungsplan umgesetzt? Wenn nein, was sind die Gründe dafür?
IB 5.4	Ist der Umsetzungsgrad der Sicherheitsmaßnahmen dokumentiert?
IB 6	**Umfeld IS**
IB 6.1	Stehen dem Informationssicherheitsbeauftragten (und der IS-Organisation) ausreichend Ressourcen zur Verfügung und wird er in die Prozesse zur Informationssicherheit eingebunden?

IB 6.2	Sind die finanziellen und personellen Ressourcen für die Informationssicherheit angemessen?
IB 6.3	Ist die IS im Projektmanagement verankert? Sind die Anforderungen der IS bei allen laufenden (IT-) Projekten eingeplant?
IB 6.4	Ist die IS im Change Management verankert?
IB 6.5	Werden die Anforderungen an IS auch bei Notfall-Changes (emergency changes) beachtet?
IB 6.6	Ist das IS-Risikomanagement in ein ggf. existierendes übergreifendes Risikomanagement eingebettet?
IB 6.7	Gab es außerplanmäßige/ überplanmäßige Ausgaben infolge von Sicherheitsvorfällen? Sind die Mittel für IS im Haushalt klar ausgewiesen? Gibt es separate Ansätze für IS?
IB 6.8	Sind die Dienste des Informationssicherheitsmanagements vollständig und wirksam in das IT-Servicemanagement integriert?
IB 6.9	Sind die Anforderungen an IS in allen abgeschlossenen SLAs aufgenommen worden?

2 Fragen zur Absicherung der Netzinfrastruktur

2.1 Fragen auf Bundes-/Landesebene zur Absicherung der Netzinfrastruktur

NL	
NL 1	Werden die auf Grundlage des §4 IT-Netz-G definierten Anschlussbedingungen zwischen Bund und Ländern eingehalten? Werden dabei auch sicherheitsrelevante Aspekte berücksichtigt?
NL 2	Erstrecken sich der Geltungsbereich der Informationssicherheitsleitlinie und die Zuständigkeit des Informationssicherheitsbeauftragten auch auf die Netzinfrastruktur und gibt es für diese ein Sicherheitskonzept? Wenn nein, gibt es dafür ein eigenes ISMS?
NL 3	Wurde der Schutzbedarf für das Landesnetz festgestellt und wurden die Standards des BSI entsprechend dem Schutzbedarf umgesetzt?
NL 4	Wurde der hohe Schutzbedarf für Netzwerkverbindungen, über die kritische IT-gestützte Ebenen-übergreifende Geschäftsprozesse laufen, festgelegt?
NL 5	Gibt es Abweichungen von den festgelegten Sicherheitsanforderungen in den Anschlussbedingungen? Wenn ja, welche?
NL 6	Wurden die Abweichungen dem IT-Planungsrat und dem Betreiber des Verbindungsnetzes mitgeteilt?

NL 7	Wann wurde die letzte Qualitätssicherung in Form einer Auditierung durchgeführt?
NL 8	Welche Mängel wurden bei der Auditierung festgestellt und wie werden/wurden diese beseitigt?
NL 9	Gibt es innerhalb des Landesnetzes Teilnetze mit unterschiedlichem Schutzbedarf und wie wird diesem Umstand Rechnung getragen?
NL 10	Wird die Kommunikation von und in Netze Dritter über ein Sicherheitsgateway (Firewall) geführt?
NL 11	Wurden die Anforderungen an das Sicherheitsgateway durch eine Sicherheitsrichtlinie und Policy definiert?
NL 12	Wurde das Gesamtnetz in mindestens drei Sicherheitszonen (internes Netz, DMZ und Außenanbindungen (z.B. Internet)) physisch separiert?
NL 13	Werden die Zonenübergänge durch eine Firewall abgesichert?
NL 14	Wurden geeignete Filterregeln definiert und sind diese nachvollziehbar dokumentiert?
NL 15	Wird für das Management der IR-Infrastruktur ein eigenes Out-of-Band-Management eingesetzt?
NL 16	Sind Ansprechpartner sowohl für organisatorische als auch technische Fragestellungen der Netzanbindung und Datenaustausch benannt?
NL 17	Werden IT-Systeme mit unterschiedlichem Schutzbedarf in verschiedenen Sicherheitssegmenten platziert?
NL 18	Gibt es zentrale VPN-Lösungen?
NL 19	Werden schützenswerte Informationen durch sichere Protokolle übertragen bzw. wird die Übertragung angemessen verschlüsselt und authentisiert?
NL 20	Gibt es regelmäßige Überprüfungen, ob das Netz dem Soll-Zustand entspricht?
NL 21	Gibt es ein Netzmanagement?
NL 22	Ist die Netzarchitektur in der Notfallplanung berücksichtigt?

2.2 Fragen auf Behördenebene zur Absicherung der Netzinfrastruktur

NB	
NB 1	Welche Vorgaben für Landes-/Bundesverwaltungen zum Anschluss an die Netzinfrastruktur des Landesnetzes gibt es?
NB 2	Existiert eine aktuelle und nachvollziehbare Dokumentation der Netzsituation?

NB 3	Gibt es eine Sicherheitsrichtlinie für das Netz, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Netze sicher konzipiert und aufgebaut werden?
NB 4	Wurden für das Netz ein Sicherheitskonzept und ein Netzkonzept erstellt?
NB 5	Werden schützenswerte Informationen durch sichere Protokolle übertragen bzw. wird die Übertragung angemessen verschlüsselt und authentisiert?
NB 6	Gibt es regelmäßige Überprüfungen, ob das Netz dem Soll-Zustand entspricht?
NB 7	Werden IT-Systeme mit unterschiedlichem Schutzbedarf in verschiedenen Sicherheitssegmenten platziert?
NB 8	Gibt es ein Netzmanagement?
NB 9	Werden die Sitzungsdaten aller administrativen Zugriffe protokolliert und gespeichert?
NB 10	Wird für den administrativen Zugriff auf die Netzkomponenten sowie für den Zugriff auf die Netzmanagement-Lösung eine dem Stand der Technik entsprechende Authentisierungsmethode verwendet?
NB 11	Werden Software, Firmware und Konfigurationsdaten für die Netzkomponenten automatisiert über das Netz verteilt?
NB 12	Wird die Betriebssoftware der Netzkomponenten regelmäßig aktualisiert (Updates)?
NB 13	Werden Updates vor dem Einspielen in einer Testumgebung getestet bevor sie in die Produktivumgebung übernommen werden?
NB 14	Ist die Netzarchitektur in der Notfallplanung berücksichtigt?
NB 15	Welche Notfallvorsorgemaßnahmen in Abhängigkeit der Verfügbarkeitsanforderungen gibt es für die Netzinfrastruktur?
NB 16	Werden voreingestellte Standardpasswörter durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert, bevor IT-Systeme in Betrieb genommen werden?
NB 17	Ist bei allen Zugriffsarten der Fernadministration dafür gesorgt, dass Unberechtigte keinen Zugriff haben können?
NB 18	Wird die sichere Konfiguration der aktiven Netzkomponenten im Rahmen des Netzkonzeptes festgelegt?
NB 19	Wie wird verhindert, dass Unberechtigte IT-Systeme am internen Netz anschließen?
NB 20	Wird das Netz von einer zentralen Instanz (Organisationseinheit) verwaltet, koordiniert und administriert?

NB 21	Welche Regelungen gibt es für die Protokollierung (z. B. von definierten Ereignissen und Zuständen innerhalb eines Netzmanagementsystems oder an bestimmten aktiven Netzkomponenten) der Aktivitäten im Netz?
NB 22	Werden die Konfigurationsdaten der aktiven Netzkomponenten regelmäßig gesichert?
NB 23	Gibt es einen definierten Prozess für Konfigurationsänderungen?
NB 24	Werden regelmäßige Sicherheitschecks (mindestens monatlich) des Netzes durchgeführt?
NB 25	Erfolgt der Zugriff auf das Netz von außerhalb (z.B. Fernwartung oder Telearbeit) unter Einsatz eines VPN (Remote-Access-VPN)?
NB 26	Welche VPN-Lösungen sind im Einsatz?
NB 27	Sofern VPN zum Einsatz kommt: Gibt es dafür eine Sicherheitsrichtlinie?
NB 28	Welche sonstigen Maßnahmen wurden ergriffen, um eine sichere Kommunikation beim Zugriff auf das Netz von außerhalb (z.B. Telearbeit, Fernwartung) zu gewährleisten?
NB 29	Sofern schutzbedürftige Daten über nicht vertrauenswürdige Netze (z.B. Internet) übertragen werden, wie werden diese geschützt?

3 Fragen zu einheitlichen Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren

3.1 Fragen auf Bundes-/Landesebene zu einheitlichen Sicherheitsstandards

VL	
VL 1	Welche Ebenen-übergreifende IT-Verfahren befinden sich im Einsatz?
VL 2	Welche davon werden als kritische Ebenen-übergreifende IT-Verfahren bezeichnet?
VL 3	Gibt es Verfahrensbeschreibungen zu den einzelnen Ebenen-übergreifenden IT-Verfahren?
VL 4	Wurden der Schutzbedarf für die Ebenen-übergreifenden IT-Verfahren und die Sicherheitsaspekte in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Daten und Kommunikationswege festgelegt?
VL 5	Wie sind die Verantwortlichkeiten für die einzelnen Ebenen-übergreifenden Verfahren geregelt? Hat man sich auf ein einheitliches Sicherheitsniveau geeinigt?
VL 6	Erfolgt der Datenaustausch über das Verbindungsnetz?

VL 7	Wurden für die Ebenen-übergreifenden IT-Verfahren und insbesondere für die kritischen Ebenen-übergreifenden IT-Verfahren Notfallvorsorgemaßnahmen (z.B. Rückfallebenen) ergriffen?
VL 8	Wird bei der Planung und Anpassung Ebenen-übergreifender IT-Verfahren der IT-Grundschutz des BSI angewandt?

3.2 Fragen auf Behördenebene zu einheitlichen Sicherheitsstandards

VB	
VB 1	Welche Ebenen-übergreifende IT-Verfahren nutzen Sie?
VB 2	Handelt es sich dabei um kritische Ebenen-übergreifende IT-Verfahren?
VB 3	Liegt die Verantwortung eines dieser Ebenen-übergreifenden IT-Verfahren in Ihrem Zuständigkeitsbereich?
	Sofern Frage 3 mit ja beantwortet wurde und die Fragen nicht bereits landesspezifisch gestellt wurden:
VB 4	Wurden der Schutzbedarf für die Ebenen-übergreifenden IT-Verfahren und die Sicherheitsaspekte in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Daten und Kommunikationswege festgelegt?
VB 5	Wie sind die Verantwortlichkeiten für die einzelnen Ebenen-übergreifenden Verfahren geregelt? Hat man sich auf ein einheitliches Sicherheitsniveau geeinigt?
VB 6	Erfolgt der Datenaustausch über das Verbindungsnetz?
VB 7	Wurden für die Ebenen-übergreifenden IT-Verfahren und insbesondere für die kritischen Ebenen-übergreifenden IT-Verfahren Notfallvorsorgemaßnahmen (z.B. Rückfallebenen) ergriffen?
VB 8	Wird bei der Planung und Anpassung Ebenen-übergreifender IT-Verfahren der IT-Grundschutz des BSI angewandt?

4 Fragen zur gemeinsamen Abwehr von IT-Angriffen

4.1 Fragen auf Bundes-/Landesebene zur gemeinsamen Abwehr von IT-Angriffen

AL	
AL 1	Wurde im Rahmen des VerwaltungsCERT-Verbunds von Bund und Ländern ein LandesCERT eingerichtet?
AL 2	Sind die Aufgaben, Kompetenzen und Erreichbarkeiten des LandesCERT klar geregelt?

AL 3	Verfügt das LandesCERT über ausreichende personelle und finanzielle Ressourcen?
AL 4	Sind die Mitarbeiter des LandesCERT ausreichend qualifiziert?
AL 5	Welche Maßnahmen gibt es zur Erkennung von IT-Sicherheitsvorfällen?
AL 6	Wurden Prozesse, Informationswege, Meldeverfahren und Meldewege zu IT-Sicherheitsvorfällen sowohl innerhalb des VerwaltungsCERT-Verbundes als auch innerhalb des LandesCERT geschaffen?
AL 7	Wird im Rahmen des VerwaltungsCERT-Verbundes ein übergreifender IT-Sicherheitslagebericht erstellt?
AL 8	Welche präventiven IT-Sicherheitsmaßnahmen werden durch das LandesCERT ergriffen?
AL 9	Gibt es innerhalb des VerwaltungsCERT-Verbundes und auch innerhalb des LandesCERTs Prozesse zur Bewältigung von IT-Krisen?
AL 10	Sind die folgenden für IT-Krisen relevanten Stellen identifiziert und deren Erreichbarkeit für die IT-Krisenreaktion gewährleistet? Organisationen - auf ministerieller Ebene - in der Kopfstelle und LandesCERT - Betreiber des Verwaltungsnetzes - Betreiber von IT-Dienstleistungen - weitere relevante Behörden und Einrichtungen
AL 11	Verfügt das LandesCERT über Ansprechstellen und Kommunikationsmöglichkeiten zu Behörden von Verfassungsschutz, Datenschutz und Strafverfolgung sowie zum Nationalen Cyber-Abwehrzentrum, IT-Krisenreaktionszentrum, BSI, CERT-Bund und zu sonstigen Interessengruppen?
AL 12	Wie werden im Verwaltungsnetz die für IT-Sicherheit zuständigen Stellen in die Prozesse des VerwaltungsCERT-Verbunds eingebunden?

4.2 Fragen auf Behördenebene zur gemeinsamen Abwehr von IT-Angriffen

AB	
AB 1	Verfügen Sie neben dem LandesCERT über ein eigenes CERT? Wenn ja: - Wurden die Aufgaben dieses CERTs festgelegt und wie erfolgt die Zusammenarbeit mit dem LandesCERT? - Wurden die Erreichbarkeiten und Verantwortlichkeiten festgelegt und mit dem LandesCERT ausgetauscht?
AB 2	Besteht innerhalb Ihrer Organisation eine Ansprechstelle für das LandesCERT?

AB 3	Werden Sie durch das LandesCERT ausreichend zu IT-Sicherheitsrisiken informiert und bei IT-Sicherheitsvorfällen im Bedarfsfall unterstützt?
AB 4	Welche Maßnahmen gibt es zur Erkennung von IT-Sicherheitsvorfällen?
AB 5	Gibt es Verhaltensregeln für die Mitarbeiter beim Auftreten eines Sicherheitsvorfalls?
AB 6	Wurden Prozesse, Richtlinien, Informationswege, Meldeverfahren, Meldewege und Eskalationsstrategien zu IT-Sicherheitsvorfällen innerhalb Ihrer Behörde geschaffen?
AB 7	Wird das Managementsystem zur Behandlung von Sicherheitsvorfällen regelmäßig auf seine Aktualität und Wirksamkeit geprüft?
AB 8	Wurden Rollen und Verantwortlichkeiten (Kompetenzen, Aufgaben) für den Umgang mit IT-Sicherheitsvorfällen festgelegt und definiert?
AB 9	Werden definierte IT-Sicherheitsvorfälle an das LandesCERT und/oder weitere Stellen gemeldet?
AB 10	Wurden die Erfahrungen aus vergangenen Sicherheitsvorfällen genutzt, um daraus Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu erstellen?
AB 11	Werden alle Sicherheitsvorfälle nach einem standardisierten Verfahren dokumentiert?
AB 12	Werden auf den IT-Systemen Virenschutzprogramme eingesetzt und diese regelmäßig aktualisiert (mind. täglich)?
AB 13	Gibt es Regelungen, dass infizierte IT-Systeme unverzüglich von allen Datennetzen bis zur vollständigen Bereinigung getrennt werden müssen?
AB 14	Informieren Sie sich regelmäßig bei verschiedenen Quellen über neu bekannt gewordene Schwachstellen?

5 Fragen zum IT-Notfallmanagement

5.1 Fragen auf Bundes-/Landesebene zum IT-Notfallmanagement

EL	
EL 1	Gibt es eine verbindliche Leitlinie für das IT-Notfallmanagement der Landes-/ Bundesverwaltung?
EL 2	Wurde ein am IT-Grundschutzstandard des BSI orientierter IT-Notfallmanagement-Prozess etabliert?
EL 3	Gibt es eine geeignete Organisationsstruktur für das IT-Notfallmanagement und stehen ausreichend Ressourcen zur Verfügung?

EL 4	Wurden Rollen sowie deren Aufgaben, Pflichten und Kompetenzen festgelegt?
EL 5	Gibt es ein landesweites IT-Notfallkonzept?
EL 6	Gibt es weitere IT-spezifische Notfallkonzepte?
EL 7	Wurden Maßnahmen zur IT-Notfallvorsorge und IT-Notfallbewältigung getroffen bzw. geplant?
EL 8	Wurden die Meldewege im IT-Notfall definiert?
EL 9	Gibt es IT-Notfallübungen?
EL 10	Ist das IT-Notfallmanagement Teil des ganzheitlichen Notfall- oder Krisenmanagements?
EL 11	Werden die Prozesse des IT-Krisenmanagements in das allgemeine Krisenmanagement integriert?
EL 12	Werden die Prozesse, Vorgaben und Verantwortlichkeiten im IT-Notfallmanagement mit dem Sicherheitsmanagement, dem Risikomanagement und dem Krisenmanagement abgestimmt?
EL 13	Ist der Ablauf des IT-Notfallmanagement-Prozesses, die Arbeitsergebnisse der einzelnen Phasen und die Entscheidungen dokumentiert?
EL 14	Wird die Dokumentation im IT-Notfallmanagement regelmäßig aktualisiert?
EL 15	Werden das IT-Notfallmanagementsystem sowie alle IT-Notfallmaßnahmen regelmäßig und anlassbezogen (z.B. bei größere Änderungen) auf Wirksamkeit und Einhaltung überprüft?

5.2 Fragen auf Behördenebene zum IT-Notfallmanagement

EB	
EB 1	Gibt es eine Leitlinie zum IT-Notfallmanagement?
EB 2	Wurde ein IT-Notfallmanagement-Prozess gem. dem IT-Grundschutzstandard des BSI etabliert?
EB 3	Gibt es eine geeignete Organisationsstruktur für das IT-Notfallmanagement und stehen ausreichend Ressourcen zur Verfügung?
EB 4	Wurden Rollen sowie deren Aufgaben, Pflichten und Kompetenzen festgelegt?
EB 5	Gibt es ein behördenweites IT-Notfallkonzept?
EB 6	Gibt es weitere IT-spezifische Notfallkonzepte?

EB 7	Wurden Maßnahmen zur IT-Notfallvorsorge und IT-Notfallbewältigung getroffen bzw. geplant?
EB 8	Gibt es ein IT-Notfallhandbuch?
EB 9	Gibt es Alarmpläne und Wiederanlaufpläne?
EB 10	Wurden die Meldewege definiert?
EB 11	Gibt es IT-Notfallübungen?
EB 12	Wurden die Mitarbeiter auf eine IT-Notfallsituation geschult?
EB 13	Ist das IT-Notfallmanagement Teil des ganzheitlichen Notfall- oder Krisenmanagements?
EB 14	Werden die Prozesse, Vorgaben und Verantwortlichkeiten im IT-Notfallmanagement mit dem Sicherheitsmanagement, dem Risikomanagement und dem Krisenmanagement abgestimmt?
EB 15	Sind der Ablauf des IT-Notfallmanagement-Prozesses, die Arbeitsergebnisse der einzelnen Phasen und die Entscheidungen dokumentiert?
EB 16	Wird die Dokumentation im IT-Notfallmanagement regelmäßig aktualisiert?
EB 17	Werden das IT-Notfallmanagementsystem sowie alle IT-Notfallmaßnahmen regelmäßig und anlassbezogen (z.B. größere Änderungen) auf Wirksamkeit und Einhaltung überprüft?