Rechnungshöfe des
Bundes und der Länder

Grundsatzpapier zum Informationssicherheits-management

Inhaltsverzeichnis

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 sie ihren Aufgaben wegen funktionsunfähiger Informationssysteme nicht mehr nachkommen können. Die Informationssysteme in den Staatsgewalten sind dadurch zu kritischen Infrastrukturen für das Gemeinwesen geworden.

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

Die elektronische Verwaltungsarbeit geht mit der Speicherung von elektronischen Daten auf Netzlaufwerken, E-Mail-Systemen und Dokumentenmanagementsystemen einher. Aktuelle Sicherheitsgefährdungen wie Schadsoftware können die unberechtigte Kenntnisnahme, Veränderung und Löschung von Kerndaten zur Folge haben. Die europaweiten Schäden durch Schadsoftware schätzte Interpol für das Jahr 2012 auf ca. 750 Milliarden Euro.[2]

---

1 die unmittelbare und mittelbare Staatsverwaltung und alle seine Untergliederungen

2 Eröffnungsrede des Interpol Präsidenten Khoo Boon Hui auf der 41. Europäischen Regional Konferenz in Tel Aviv am 8. Mai 2012

Mit dem fortschreitenden digitalen Wandel in den Staatsgewalten entwickeln sich parallel dazu die Hacking-Angriffe weiter. Ohne ein darauf ausgerichtetes Informationssicherheitsmanagement (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. Die erheblichen Investitionen der öffentlichen Verwaltungen in ihre IT-Ausstattungen sind ohne ausreichende IT-Sicherheit gefährdet.

Die Rechnungshöfe haben das Thema Informationssicherheit in den vergangenen Jahren immer wieder aufgegriffen und eine Weiterentwicklung des Informationssicherheitsmanagement[3] aktiv begleitet und befördert. Mit dem vorliegenden Grundsatzpapier und dessen Anlagen werden die Prüfungserkenntnisse der Rechnungshöfe zusammengefasst und zu 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 vom November 2011. Darüber hinaus stellen die Rechnungshöfe Empfehlungen für die Prüfung der Informationssicherheit bereit.[4]

[3] Unter Informationssicherheitsmanagement bzw. dem Informationssicherheitsmanagementsystem wird der Teil des gesamten Managementsystems verstanden, welcher auf Basis eines Risikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt (DIN ISO/IEC 27001:2008-09, S. 9).

[4] vgl. Fragenkatalog der Rechnungshöfe des Bundes und der Länder zum Informationssicherheitsmanagement in der öffentlichen Verwaltung vom März 2015 (Anlage)

1 Informationssicherheitsmanagement

Die Informationssysteme und Netzwerke der öffentlichen Verwaltung in Deutschland sind Sicherheitsbedrohungen unterschiedlichster Art von Innen und Außen ausgesetzt. Im deutschen Regierungsnetz geht täglich eine Vielzahl mit Schadsoftware behaftete E-Mails[5] ein. Zudem beobachtet das BSI täglich gezielte Spionageangriffe[6] von hochprofessionellen Angreifern auf die Bundesverwaltung.

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[7] sowie den IT-Grundschutz-Standards des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Der IT-Planungsrat[8] hat zur weiteren Standardisierung des Informationssicherheitsmanagements in Deutschland im März 2013 eine Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung[9] einschließlich eines Umsetzungsplans[10] beschlossen. Diese Leitlinie definiert für den Bund und die Länder einen Rahmen, welche Anforderungen bestehen und welche organisatorischen Aspekte und Maßnahmen mindestens realisiert werden müssen.

---

5 BSI, Fokus IT-Sicherheit 2013 vom Juli 2013, S. 2

6 sog. „fortgeschrittene, andauernde Bedrohung“ (Englisch: Advanced Persistent Threats – APT)

7 vgl. DIN ISO/IEC 27001:2008-09, Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005) vom September 2008

8 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.

9 vgl. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html

10 vgl. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Umsetzungsplan.html

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.

Absichtserklärungen, wie die digitale Agenda für Europa, die digitale Agenda 2014-2017 oder das IT-Sicherheitsgesetz[11], messen der IT-Sicherheit einen hohen Stellenwert zu.

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

[11] Gesetzentwurf der Bundesregierung zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Dezember 2014

2 Organisation der Informationssicherheit

Folgend aus der allgemeinen Leitungsverantwortung[12] ist die Behördenleitung auch für die Informationssicherheit ihrer Behörde verantwortlich. Sie hat die notwendigen technischen und organisatorischen Maßnahmen zu veranlassen, die notwendig sind, 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 Bundesländer gelten (z. B. Berufung eines IT-Sicherheitsbeauftragten).

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.

[12] vgl. Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrats, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html

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.[13] 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[14] entsprochen.

Eine reine dienstellenbezogene Ausrichtung des ISM, wie in den IT-Grundschutz-Standards des BSI empfohlen, 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 muss außerhalb des IT-Managements angesiedelt sein, um Interessen- und Rollenkonflikte zu vermeiden.[15] Zusätzlich ist eine intensivere Kontrolle des ISMS durch die Prüfungsinstanzen erforderlich.

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

[14] Der IT-Planungsrat bezeichnet die Rolle als Landes-IT-Sicherheitsbeauftragten.

[15] 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[16] haben zur Sicherstellung einer ausreichenden Informationssicherheit umfangreiche Aufgaben zu erfüllen. Sie müssen z. B.

- den Informationssicherheitsprozess steuern und bei allen damit zusammenhängenden Aufgaben mitwirken,
- 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,
- die Realisierung von Sicherheitsmaßnahmen initiieren und überprüfen,
- der Leitungsebene über den Status quo der Informationssicherheit berichten,
- sicherheitsrelevante Projekte koordinieren,
- Sicherheitsvorfälle untersuchen,
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit initiieren und koordinieren,
- bei der Einführung neuer Anwendungen und IT-Systeme mitwirken und
- die Beachtung von Sicherheitsaspekten bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, in den verschiedenen Projektphasen gewährleisten.

Die Rechnungshöfe haben in verschiedenen Prüfungen festgestellt, dass in vielen Bereichen der Verwaltung ein Mangel an ausreichend qualifiziertem

[16] z. B. IT-Sicherheitsbeauftragte, IT-Sicherheitsteam, Administratoren

und geschultem Personal besteht, um die gestiegenen und gesetzlich verankerten[17] Anforderungen an die Informationssicherheit zu erfüllen.

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

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

[17] vgl. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Referentenentwurf Stand 18.8.2014

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 2013 verabschiedete Leitlinie über die Informationssicherheit in der öffentlichen Verwaltung verpflichtet die Länder, bis 2016 ein CERT aufzubauen.

In Abgrenzung zum Informationssicherheitsmanagement wird das interne oder auch behördenübergreifende 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 IT-Sicherheitsbeauftragten des Bundes und der Länder sowie den CERT der Länder erforderlich.

4 Erwartungen und Prüfungsmaßstäbe der Rechnungshöfe

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

- die Informationssysteme zuverlässig und kontinuierlich zur Verfügung stehen,
- die Anforderungen an die Sicherheit der Informationsverarbeitung regelmäßig ermittelt und unverzüglich 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 Rechnungshöfe werden die Ordnungsmäßigkeit und Wirtschaftlichkeit der ISMS in Bund, Ländern und ggf. Kommunen 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 (Stand März 2015) erarbeitet. Dieser bildet zukünftig eine Grundlage für Prüfungen zur Informationssicherheit durch die Rechnungshöfe.

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

Fragenkatalog der Rechnungshöfe zum Informationssicherheitsmanagement

– Stand März 2015 –

Inhalt

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 der Landes-/ Bundesverwaltung?
IL 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? 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-IT-Sicherheitsbeauftragter ernannt und eingesetzt?
IL 3.2	Gibt es eine Vertretungsregelung für den IT-Sicherheitsbeauftragten?
IL 3.3	Ist der IT-Sicherheitsbeauftragte außerhalb einer operativ tätigen IT-Einheit angesiedelt?
IL 3.4	Verfügt der IT-Sicherheitsbeauftragte über eine ausreichende Qualifizierung (Zertifizierung sollte angestrebt werden)?

IL 3.5	Sind die Aufgaben, Verantwortungen und Kompetenzen des IT-Sicherheitsbeauftragten 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 IT-Sicherheitsbeauftragte?
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 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 apl-/üpl-Ausgaben infolge von Sicherheitsvorfällen?

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 ergänzende Sicherheitsanalyse und (falls notwendig) eine ergänzende 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 IT-Sicherheitsbeauftragten benannt und eingesetzt?
IB 3.2	Ist der IT-Sicherheitsbeauftragte 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 IT-SiBe im Nebenamt auch Aufgaben im IT-Betrieb?
IB 3.5	Sind der IT-Sicherheitsbeauftragte 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 IT-Sicherheitsbeauftragten und des ISM-Teams innerhalb des Sicherheitsprozesses klar definiert, zugewiesen und dokumentiert?
IB 3.8	Falls ein externer IT-Sicherheitsbeauftragter bestellt wurde: Umfasst der hierzu geschlossene Dienstleistungsvertrag alle Aufgaben des IT-Sicherheitsbeauftragten 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, Verfügbarkeit0) 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? Bestehen 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 den 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 IT-Sicherheitsbeauftragten (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 apl-/üpl-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 IT-Sicherheitsbeauftragten 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 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 diesen 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	Wurden geeignete Filterregeln definiert und sind diese nachvollziehbar dokumentiert?
NL 13	Sind Ansprechpartner sowohl für organisatorische als auch technische Fragestellungen der Netzanbindung und Datenaustausch benannt?
NL 14	Gibt es zentrale VPN-Lösungen?

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	Wurden für das Netz ein Sicherheitskonzept und ein Netzkonzept erstellt?
NB 4	Gibt es innerhalb des Netzes Teilnetze mit unterschiedlichem Schutzbedarf? Wenn ja, werden diese durch Zugriffsberechtigungen, Paketfilter oder Sicherheitsgateways (Firewall) getrennt?
NB 5	Wurde berücksichtigt, dass VLANs mit unterschiedlichem Schutzbedarf bezüglich der Vertraulichkeit oder der Integrität der übertragenen Daten nicht ohne weiteres als VLANs auf demselben Switch realisiert werden?
NB 6	Wird die Betriebssoftware der Netzkomponenten regelmäßig aktualisiert (Updates)?
NB 7	Werden Updates vor dem Einspielen in einer Testumgebung getestet bevor sie in die Produktivumgebung übernommen werden?
NB 8	Welche Notfallvorsorgemaßnahmen in Abhängigkeit der Verfügbarkeitsanforderungen gibt es für die Netzinfrastruktur?
NB 9	Werden voreingestellte Standardpasswörter durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert, bevor IT -Systeme in Betrieb genommen werden?

NB 10	Ist bei allen Zugriffsarten der Fernadministration dafür gesorgt, dass Unberechtigte keinen Zugriff haben können?
NB 11	Wird die sichere Konfiguration der aktiven Netzkomponenten im Rahmen des Netzkonzeptes festgelegt?
NB 12	Wie wird verhindert, dass Unberechtigte IT-Systeme am internen Netz anschließen?
NB 13	Wird das Netz von einer zentralen Instanz (Organisationseinheit) verwaltet, koordiniert und administriert?
NB 14	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 15	Werden die Konfigurationsdaten der aktiven Netzkomponenten regelmäßig gesichert?
NB 16	Gibt es einen definierten Prozess für Konfigurationsänderungen?
NB 17	Gibt es ein Netz- und/oder Systemmanagement?
NB 18	Welche Tools zum Netz-/Systemmanagement befinden sich im Einsatz?
NB 19	Werden regelmäßige Sicherheitschecks (mindestens monatlich) des Netzes durchgeführt?
NB 20	Erfolgt der Zugriff auf das Netz von außerhalb (z.B. Fernwartung oder Telearbeit) unter Einsatz eines VPN (Remote-Access-VPN)?
NB 21	Welche VPN-Lösungen sind im Einsatz?
NB 22	Sofern VPN zum Einsatz kommt: Gibt es dafür eine Sicherheitsrichtlinie?
NB 23	Welche sonstigen Maßnahmen wurden ergriffen, um eine sichere Kommunikation beim Zugriff auf das Netz von außerhalb (z.B. Telearbeit, Fernwartung) zu gewährleisten?
NB 24	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	Gibt es eine Geschäftsordnung für die Zusammenarbeit im VerwaltungsCERT-Verbund?
AL 3	Sind die Aufgaben, Kompetenzen und Erreichbarkeiten des LandesCERT klar geregelt?
AL 4	Verfügt das LandesCERT über ausreichende personelle und finanzielle Ressourcen?
AL 5	Sind die Mitarbeiter des LandesCERT ausreichend qualifiziert?
AL 6	Welche Maßnahmen gibt es zur Erkennung von IT-Sicherheitsvorfällen?
AL 7	Wurden Prozesse, Informationswege, Meldeverfahren und Meldewege zu IT-Sicherheitsvorfällen sowohl innerhalb des VerwaltungsCERT-Verbundes als auch innerhalb des LandesCERT geschaffen?
AL 8	Wird im Rahmen des VerwaltungsCERT-Verbundes ein übergreifender IT-Sicherheitslagebericht erstellt?
AL 9	Welche präventiven IT-Sicherheitsmaßnahmen werden durch das LandesCERT ergriffen?
AL 10	Gibt es innerhalb des VerwaltungsCERT-Verbundes und auch innerhalb des LandesCERTs Prozesse zur Bewältigung von IT-Krisen?
AL 11	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 12	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 13	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 (mindestens 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 zur Standardisierung und Produktsicherheit

5.1 Fragen auf Bundes-/Landesebene zur Standardisierung und Produktsicherheit

SL	
SL 1	Welche Basiskomponenten gibt es auf Ebene Bund-Länder?
SL 2	Welche Basiskomponenten davon sind bei Ihnen im Einsatz?
SL 3	Gibt es Überschneidungen von Basiskomponenten zu anderen, von Ihnen eingesetzten Ebenen-übergreifenden Verfahren?
SL 4	Welche weiteren Basiskomponenten auf Ebene Bund-Länder wären Ihrer Ansicht nach notwendig?
SL 5	Welche Basiskomponenten gibt es auf Landesebene?
SL 6	Welche weiteren Basiskomponenten auf Landesebene wären Ihrer Ansicht nach notwendig?
SL 7	Gibt es eine (bundes- oder landesspezifische) Festlegung von Mindestsicherheitsanforderungen für sichere Produkte, Systeme und Verfahren?
SL 8	Wurden standardisierte Datenformate zum Datenaustausch insb. für die Ebenen-übergreifenden Verfahren definiert?
SL 9	Existieren dokumentierte Bundes-/Landesstandards für Hard- und Software?

5.2 Fragen auf Behördenebene zur Standardisierung und Produktsicherheit

SB	
SB 1	Welche der angebotenen Basiskomponenten nutzen Sie?
SB 2	Gibt es eine Basiskomponente, für die Sie federführend sind?
SB 3	Welche weiteren Basiskomponenten auf Landesebene wären Ihrer Ansicht nach notwendig?
SB 4	Gibt es Überschneidungen von Basiskomponenten zu anderen, von Ihnen eingesetzten Verfahren?
SB 5	Wird innerhalb ihrer Organisation (soweit möglich) Standardsoftware eingesetzt?
SB 6	Wurde diese vor dem Einsatz ausreichend getestet und deren Einsatz freigegeben?
SB 7	Gibt es für Zugangs- und Zugriffsberechtigungen Standardprofile, die den Funktionen und Aufgaben der Nutzer entsprechen?

SB 8	Existieren dokumentierte Hausstandards für Hard- und Software?
SB 9	Gibt es ein Konzept zur Konvention von Namens-, Adress- und Nummernräumen?
SB 10	Werden für Schnittstellen (zwischen Hard- und Softwarekomponenten) soweit möglich Standardformate bzw. -protokolle genutzt?
SB 11	Sind für die Behörde Standardarbeitsplätze definiert?
SB 12	Gibt es für die Server eine sichere vordefinierte Grundinstallation?

6 Detailfragen zur Informationssicherheit für eine vertiefte Prüfung in Ergänzung zu den anderen Fragestellungen

W 1 Personal	
W 1.1	Werden neue Mitarbeiter auf die bestehenden Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen und verpflichtet diese einzuhalten?
W 1.2	Werden Administratoren bei der Einstellung (soweit möglich und notwendig) auf ihre Vertrauenswürdigkeit verifiziert?
W 1.3	Wurde dafür gesorgt, dass für Schlüsselpositionen Vertretungsregelungen vorhanden sind?
W 1.4	Gibt es Regelungen für den Fall, dass Mitarbeiter versetzt oder entlassen werden (Entzug von Berechtigungen wie Zutritt oder Zugriff, Rückgabe von Unterlagen, Einarbeitung von Nachfolgern, Verschwiegenheitsverpflichtung)?
W 2 Versions- und Änderungsmanagement	
W 2.1	Gibt es ein Patch- und Änderungsmanagement?
W 2.2	Gibt es Richtlinien oder Vorgaben für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten?
W 2.3	Werden alle Änderungen geplant, getestet, genehmigt und dokumentiert?
W 2.4	Werden Rückfall-Lösungen erarbeitet, bevor Änderungen durchgeführt werden?
W 2.5	Wird bei größeren Änderungen das Informationssicherheitsmanagement beteiligt?
W 3 Notfallkonzept	
W 3.1	Wurden Rollen und Verantwortlichkeiten festgelegt?
W 3.2	Gibt es ein behördenweites Notfallvorsorgekonzept?

W 3.3	Gibt es weitere IT-spezifische Notfallvorsorgekonzepte?
W 3.4	Gibt es ein Notfallhandbuch?
W 3.5	Gibt es Alarmpläne und Wiederanlaufpläne?
W 3.6	Wurden die Meldewege definiert?
W 3.7	Wurden die Mitarbeiter auf eine Notfallsituation geschult bzw. wurden Notfallübungen durchgeführt?
W 4 Datensicherung	
W 4.1	Werden Datensicherungen (Backups) durchgeführt?
W 4.2	Gibt es ein Datensicherungskonzept, welches die Zuständigkeiten, das Datensicherungsverfahren und den Umfang der Datensicherung regelt?
W 4.3	Wird regelmäßig kontrolliert, dass die Speichermedien noch ausreichend Speicherkapazität aufweisen?
W 4.4	Werden die Datensicherungen räumlich getrennt (anderer Brandabschnitt) von den IT-Systemen aufbewahrt?
W 4.5	Haben nur berechtigte Personen Zugriff auf die Datensicherungen?
W 4.6	Wird das Einspielen von Datensicherungen regelmäßig getestet?
W 5 Outsourcing	
W 5.1	Welche Arbeits- oder Geschäftsprozesse wurden ganz oder teilweise zu einem externen Dienstleister ausgelagert?
W 5.2	Wurden mit dem Dienstleister vertraglich die IT-Sicherheitsanforderungen, die Kriterien zur Messung der Servicequalität und Sicherheit, die Auskunfts-, Mitwirkungs- und Revisionspflichten, die Eigentumsrechte an Hard- und Software und die Rückgabe der Datenbestände bei Vertragskündigung festgehalten?
W 5.3	Werden regelmäßige Kontrollen zur Überprüfung der Vereinbarungen durchgeführt und dokumentiert?
W 6 Kryptokonzept	
W 6.1	Gibt es Vorgaben, welche Daten oder Datenträger zu verschlüsseln sind?
W 6.2	Welche Möglichkeiten haben die Mitarbeiter, Daten selbst zu verschlüsseln oder zu signieren?
W 6.3	Wurden die Mitarbeiter im Umgang mit der Verschlüsselungssoftware geschult?

W 7 Löschen und Vernichten von Daten	
W 7.1	Gibt es innerhalb Ihrer Behörde Vorgaben und Verfahren zum sicheren Löschen von Daten bzw. Vernichten von Datenträgern (sowohl elektronische als auch papiergebundene)?
W 7.2	Existiert eine klar definierte Vorgehensweise zur Außerbetriebnahme von IT -Systemen und Datenträgern?
W 7.3	Werden bei allen Arten von IT -Systemen und Datenträgern vor einer Aussonderung alle gespeicherten Daten sorgfältig gelöscht?
W 8 Hard- und Softwaremanagement	
W 8.1	Existiert eine Regelung zur ausschließlichen Nutzung von lizenzierter Software und ist diese allen Mitarbeitern bekannt gemacht?
W 8.2	Gibt es ein Lizenzmanagement?
W 8.3	Existiert eine Übersicht aller eingesetzten Software-Versionen?
W 8.4	Ist die Nutzung nicht zugelassener Hard- und Software technisch und/oder organisatorisch unterbunden?
W 8.5	Wurden alle Mitarbeiter über das Verbot der Nutzung nicht freigegebener Hard- und Software informiert?
W 8.6	Existiert eine Regelung zur Abnahme, Test, Freigabe, Installation und Nutzung von Hard- und Software? Sind IS-Testfälle in Testplänen vorgesehen?
W 8.7	Kennen die Benutzer ihre Ansprechpartner für IT -Problemfälle?
W 8.8	Gibt es eine geregelte Vorgehensweise zur Einrichtung von Benutzern und Benutzergruppen?
W 8.9	Sind die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert?
W 8.10	Gibt es einen Prozess zur Koordination und Genehmigung bei Beschaffung, Installation und Betrieb von IT-Komponenten aller Art?
W 8.11	Gibt es Regelungen (z.B. Verschlüsselung) für die Mitnahme von Datenträgern und Komponenten außer Haus?
W 8.12	Werden je nach Schutzbedarf (der IT-Systeme und IT-Anwendungen) angemessene Identifikations- und Authentisierungsmechanismen eingesetzt?
W 8.13	Wird die Konfiguration der Anwendungen, Systeme und Netze nachvollziehbar dokumentiert und die Systemkonfiguration in die Datensicherung eingeschlossen?
W 8.14	Wurden für alle IT-Systeme und Netze entsprechende Administratoren sowie deren Stellvertreter bestimmt?

W 8.15	Wurde die Aufgabenteilung zwischen den einzelnen Administratoren so vorgenommen, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen?
W 8.16	Hat jeder Administrator und jeder Vertreter eines Administrators eine eigene, eindeutige Administratorkennung?
W 8.17	Existiert ein Konzept, das den Umfang und die Auswertung der Protokollierung festlegt?
W 8.18	Werden Software-Updates und Patches regelmäßig eingespielt?
W 9 Elektrische Verkabelung, IT-Verkabelung, Versorgungsleitungen	
W 9.1	Wurde die Verkabelung für Berechtigte nachvollziehbar dokumentiert?
W 9.2	Wurden die Kabel strukturiert verlegt und nicht mehr verwendete Kabel entfernt?
W 10 Zutrittskontrolle	
W 10.1	Ist der Zutritt zu schützenswerten Gebäuden und Räumen wie z. B. Rechenzentrum, Serverraum durch ein Zutrittskontrollsystem gesichert?
W 10.2	Sind die Berechtigungen nachvollziehbar dokumentiert?
W 10.3	Gibt es Regelungen für den Umgang mit Externen oder Besuchern (z. B: Begleitung durch internes Personal)?
W 10.4	Kann der Zutritt zu schützenswerten Räumen nachvollzogen werden (wer war wann wo?)?
W 11 Brandschutz	
W 11.1	Gibt es einen Brandschutzbeauftragten?
W 11.2	Gibt es ein Brandschutzkonzept?
W 11.3	Werden Brandschutzübungen durchgeführt?
W 12 Klimatisierung	
W 12.1	Gibt es im Serverraum bzw. Rechenzentrum eine ausreichend dimensionierte Klimaanlage?
W 12.2	Wird die Funktionsfähigkeit der Klimaanlage überwacht?
W 12.3	Wird die Klimaanlage regelmäßig gewartet?
W 12.4	Kann die Klimaanlage im Störungsfall schnell wieder in Betrieb genommen werden (z.B. Vereinbarung entsprechender Reaktionszeiten mit Drittfirmen)?

W 13 Stromversorgung	
W 13.1	Sind die IT-Systeme an eine USV angeschlossen?
W 13.2	Wird die USV regelmäßig gewartet?
W 13.3	Hat die USV ausreichend Kapazität, um bei Stromausfall die IT-Systeme geregelt herunterzufahren bzw. bis die Netzersatzanlage in Betrieb genommen werden kann?
W 13.4	Gibt es eine Netzersatzanlage (Dieselaggregat)?
W 14 Sichere Grundkonfiguration der Server und Clients	
W 14.1	Wird eine sichere Grundkonfiguration aller eingesetzten IT-Systeme entsprechend den Vorgaben der Sicherheitsrichtlinie definiert und vorgenommen?
W 14.2	Wurden nicht benötigte Benutzerkonten, Dienste und Schnittstellen deaktiviert oder entfernt?
W 15 Berechtigungsvergabe	
W 15.1	Gibt es Rollen- und Benutzerkonzepte?
W 15.2	Werden die Zugriffsberechtigungen auf Grund der Aufgaben und Rollen vergeben?
W 15.3	Gibt es eine verbindliche Regelung für den Passwortgebrauch (Komplexität, Wechsel, Geheimhaltung)?
W 15.4	Wurden alle IT-Systeme mit einem Passwortschutz gesichert?
W 15.5	Werden administrative Passwörter an einem sicheren Ort hinterlegt?
W 16 Mobile Endgeräte und mobile Datenträger	
W 16.1	Gibt es eine Bestandsübersicht der mobilen Endgeräte und Datenträger?
W 16.2	Werden sensible Daten auf dem mobilen Endgerät bzw. Datenträger verschlüsselt?
W 16.3	Gibt es Regelungen, Sicherheitsrichtlinien oder Handlungsanweisungen zum Umgang mit mobilen Endgeräten und Datenträgern?
W 17 E-Mail / Webauftritt	
W 17.1	Gibt es Regelungen zur privaten Nutzung von E-Mail und Internet?
W 17.2	Wurde der Webauftritt gegen Angriffe gehärtet und auf Schwachstellen z. B. durch einen Penetrationstest überprüft?