GUID 5101

Leitfaden zur Prüfung der Informationssicherheit

INTOSAI Prinzipien sind durch die Internationale Organisation der Obersten Rechnungskontrollbehörden, INTOSAI, als Teil der Rahmenbedingungen für professionelle Verkündungen. Weitere Informationen unter www.intosai.org.

INTOSAI

INTOSAI

1) Im Jahr 2025 gebilligt

GUID 5101 ist in allen offiziellen INTOSAI-Sprachen verfügbar: Arabisch, Deutsch, Englisch, Französisch und Spanisch

INHALTSVERZEICHNIS

1

EINFÜHRUNG

1) Der GUID 5101 ergänzt den GUID 5100 durch Leitlinien zur Prüfung der Informationssicherheit. Die in diesem Leitfaden enthaltenen Leitlinien stehen im Einklang mit den allgemeinen Grundsätzen der staatlichen Finanzkontrolle (ISSAI 100) sowie mit den Grundsätzen der Recht- und Ordnungsmäßigkeitsprüfung (ISSAI 400).

2) Da die geprüften Stellen im öffentlichen Sektor zunehmend computergestützte Informationssysteme einsetzen und Informationen elektronisch verarbeiten, ist es von zwingender Notwendigkeit, dass die ORKB geeignete Fähigkeiten entwickeln, um die auf Informationssysteme bezogenen Kontrollen zu prüfen. Im Rahmen der Prüfung von Informationssystemen muss sichergestellt werden, dass die geprüften Stellen Kontrollen zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen und Daten (d. h. zur Gewährleistung der Informationssicherheit) konzipiert und angewandt haben.

3) Verstöße gegen die Informationssicherheit können in rechtlicher und finanzieller Hinsicht sowie in Bezug auf den Ruf und die Glaubwürdigkeit sowie die Produktivität schwerwiegende Schäden verursachen und weitere unbefugte Zugriffe ermöglichen. Sicherheitsverletzungen können auf Mängel und Schwachstellen zurückzuführen sein, die zu einer versehentlichen Offenlegung oder Weitergabe von Informationen an unbefugte Parteien, zum Verlust der Verfügbarkeit oder zu unbefugten Änderungen an Systemen und Daten führen.

2 ZIELE DES VORLIEGENDEN LEITFADENS

4) Die für die Prüfung von Informationssystemen geltenden Leitlinien sind dem GUID 5100 zu entnehmen. Ziel des vorliegenden Leitfadens ist es, spezifische und zusätzliche Leitlinien für eine Recht- und Ordnungsmäßigkeitsprüfung (Compliance-Prüfung) im Bereich der Informationssicherheit bereitzustellen.

5) Die Prüfung der Informationssicherheit kann als Compliance-Prüfung oder unter bestimmten Umständen als Gesamtprüfung, bei der Aspekte der Rechnungsführung, der Einhaltung rechtlicher Normen und/oder der Wirtschaftlichkeit geprüft werden, durchgeführt werden. Der vorliegende Leitfaden bezieht sich auf Prüfungen der Informationssicherheit, die entweder als eigenständige Compliance-Prüfung oder im Rahmen eines Gesamtprüfungsauftrags durchgeführt werden und mit denen festgestellt werden soll, ob das IT-Management die erforderlichen Standards und Anforderungen im Bereich der Informationssicherheit erfüllt.

6) Der Inhalt dieses Leitfadens kann von den Prüfern im Verlauf des Prüfungsprozesses in den Phasen der Planung, Durchführung, Berichterstattung und Weiterverfolgung angewandt werden. Im Leitfaden sind mögliche Prüfungsthemen, Risikofaktoren für die Informationssicherheit, Quellen für die Prüfungskriterien sowie übergeordnete Prüfungsfragen aufgeführt. Diese Auflistung dient der Veranschaulichung und ist nicht erschöpfend.

3

BEGRIFFSBESTIMMUNGEN

a) **Informationssicherheit:** Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff sowie unbefugter Nutzung, Weitergabe, Störung, Änderung oder Vernichtung, um Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

b) **Cybersicherheit** Verhütung von Schäden an sowie Schutz und Wiederherstellung von Computern, elektronischen Kommunikationssystemen, elektronischen Kommunikationsdiensten, kabelgebundener und elektronischer Kommunikation, einschließlich der darin enthaltenen Informationen, um deren Verfügbarkeit, Integrität und Vertraulichkeit zu gewährleisten.

c) **Vertraulichkeit:** Aufrechterhaltung zugelassener Beschränkungen in Bezug auf den Zugang zu und die Weitergabe von Informationen, einschließlich der Ergreifung von Mitteln zum Schutz der Privatsphäre und interner Informationen; weitere Bedeutung: Schutz sensibler Informationen vor unbefugter Weitergabe. Die unbefugte Weitergabe von Informationen stellt einen Verlust der Vertraulichkeit dar.

d) **Integrität:** Schutz vor unsachgemäßer Änderung oder Vernichtung von Informationen, einschließlich der Gewährleistung der

Nichtabstreitbarkeit [1] und Authentizität [2] von Informationen; weitere Bedeutung: Genauigkeit und Vollständigkeit von Informationen sowie deren Gültigkeit im Einklang mit den Werten und Erwartungen der Einrichtung. Die unsachgemäße Veränderung oder Vernichtung von Informationen stellt einen Integritätsverlust dar.

e) **Verfügbarkeit:** Zeitnaher, zuverlässiger Zugang zu und Nutzung von Informationen oder Informationssystemen durch befugte Nutzer; weitere Bedeutung: aktuelle und künftige Verfügbarkeit von Informationen, wenn der betreffende Prozess dies erfordert, sowie Sicherung der erforderlichen Ressourcen und damit verbundenen Kapazitäten. Die Störung des Zugangs zu oder der Nutzung von Informationen oder Informationssystemen stellt einen Verlust an Verfügbarkeit dar.

f) **Schwachstellenanalyse/Penetrationstests:** Die Schwachstellenanalyse dient der systematischen und organisierten Ermittlung von Sicherheitsproblemen bei IT-Anwendungen, Arbeitsplatzrechnern oder dem gesamten Netzwerk einer Organisation und ermöglicht es den Prüfern, Sicherheitslücken entsprechend ihrem Risikoniveau zu klassifizieren, zu priorisieren und zu ordnen, um diese zeitnah zu beheben. Bei Penetrationstests, die ethischem Hacking ähneln, handelt es sich um zugelassene simulierte (Hacking-)Angriffe auf ein Computersystem, die zur Bewertung der Sicherheit des Systems durchgeführt werden.

[1] Nichtabstreitbarkeit bietet Schutz vor einer Person, die fälschlicherweise bestreitet, eine bestimmte Handlung vorgenommen zu haben, und ermöglicht darüber hinaus festzustellen, ob eine Person eine bestimmte Handlung vorgenommen hat, z. B. ob sie Informationen erstellt, eine Nachricht versendet, Informationen genehmigt oder eine Nachricht erhalten hat.

[2] Authentizität beschreibt die Eigenschaft, dass etwas echt ist, überprüft werden kann und vertrauenswürdig ist; Vertrauen in die Gültigkeit der Übermittlung, des Inhalts oder des Urhebers einer Nachricht.

4

PRÜFUNGSGEGENSTAND

7) Bei der Prüfung der Informationssicherheit bewertet der Prüfer, ob der Prüfungsgegenstand (die Informationssicherheit oder bestimmte Aspekte/Komponenten der Informationssicherheit) den geltenden Vorgaben (Gesetzen, Verordnungen, Strategien, Verfahren, Normen, Praktiken usw.) entspricht.

8) Die Prüfungsarbeit im Bereich der Informationssicherheit richtet sich nach den Zielen und dem Umfang der Prüfung. Die Prüfung kann sich auf verschiedene Themenbereiche erstrecken, z. B. auf Folgendes:

a) Kultur der Informationssicherheit, einschließlich Führung und Engagement; Ausrichtung und Strategien des Managements; Ziele der Informationssicherheit; Funktionen, Zuständigkeiten und Befugnisse in der Organisation (einschließlich mobiler Arbeit, Telearbeit usw.);

b) Risikomanagementprozesse im Bereich der Informationssicherheit, darunter:

i. die Bewertung des Risikos für die Informationssicherheit (einschließlich Schwellenwerten und Kriterien für die Akzeptanz von Risiken im Bereich der Informationssicherheit sowie der Ermittlung, Analyse und Priorisierung dieser Risiken) und Behandlung von Informationssicherheitsrisiken;

ii. die (interne und externe) Kommunikation und Dokumentation, die für das Informationssicherheitsmanagementsystem relevant sind;

iii. die Überprüfung und kontinuierliche Verbesserung der Informationssicherheit und des Risikomanagements;.

c) Informationssicherheit im Bereich der Lieferantenbeziehungen;

d) Sicherheit des Personals in verschiedenen Phasen vor der Beschäftigung, während der Beschäftigung und nach Beendigung des Beschäftigungsverhältnisses;

e) Verwaltung und Kontrolle von Informationswerten, einschließlich Bestandsaufnahme und Klassifizierung, Bestimmungen über die zulässige Nutzung, Beförderung, Rückgabe und Entsorgung;

f) Authentifizierung, Autorisierung und Zugangskontrolle – einschließlich Identitätsmanagement und Authentifizierung, kryptografischen Kontrollen sowie Autorisierung und Zugangskontrollen;

g) physische und umgebungsbezogene Sicherheit;

h) Netz- und Kommunikationssicherheit und Cybersicherheitsmanagement;

i) Management von Informationssicherheitsvorfällen sowie Sicherheitsprüfungen und -überwachung;

j) Sicherheit als Bestandteil der Anschaffung und Entwicklung von Systemen;

k) Betriebssicherheit, einschließlich betrieblicher Verfahren und Zuständigkeiten; Schutz vor Schadsoftware; Datensicherung/-wiederherstellung, Protokollierung und Überwachung von Daten;

l) Einhaltung externer und interner Anforderungen;

m) neue oder geänderte Gesetze.

5

PLANUNG EINER PRÜFUNG DER INFORMATIONSSICHERHEIT

9) Eine Prüfung der Informationssicherheit kann infolge einer Risikobewertung eingeleitet werden. Im Folgenden sind einige Risikofaktoren aufgeführt, die relevant sein können:

a) Die geprüfte Stelle hat ein neues Informationssystem entwickelt oder ein bestehendes Informationssystem (Anwendung und/oder Infrastruktur) ersetzt oder aufgerüstet, insbesondere in einem kritischen Bereich ihres Betriebs;

b) Seit Langem vorhandene alte Informationssysteme wurden nicht aktualisiert oder ersetzt, wobei die zugrunde liegende technologische Infrastruktur veraltet ist und derzeit nicht durch Sicherheitspatches/-aktualisierungen unterstützt wird;

c) Regelmäßige interne/externe Sicherheitsprüfungen – darunter Sicherheitsprüfungen von operativen Informationssystemen, insbesondere von Systemen, die im Hinblick auf Anwendungen oder Infrastruktur in erheblichem Umfang aufgerüstet wurden – wurden nicht durchgeführt;

d) Eine Post-mortem-Analyse wurde zu einem schwerwiegenden Sicherheitsvorfall bzw. einer schwerwiegenden Sicherheitsverletzung durchgeführt, der bzw. die sich nachteilig auf das betreffende Informationssystem ausgewirkt hat, oder ein Sicherheitsvorfall bzw. eine Sicherheitsverletzung hatte negative Folgen für vergleichbare Informationssysteme anderer geprüfter Stellen;

e) Es gibt Bedenken im Hinblick auf den Datenschutz und den Schutz der Privatsphäre bei bestehenden IT-Systemen sowie die Notwendigkeit eines Upgrades bzw. einer Aktualisierung zur Einhaltung der neuesten geltenden gesetzlichen Vorschriften;

f) Im Rahmen anderer Prüfungen (interner Prüfungen oder Prüfungen durch ORKB bzw. externer Prüfungen), Evaluierungen oder Bewertungen wurden erhebliche Bedrohungen der Informationssicherheit in der Umgebung oder Informationssicherheitsrisiken in Bezug auf das Informationssystem der geprüften Stelle ermittelt, oder Kontrollmängel, die bei früheren Prüfungen der Informationssicherheit festgestellt wurden, wurden nicht oder nur teilweise behoben.

g) Die in der Organisation vorhandenen Strategien und Strukturen für das Management und die Implementierung von Informationssystemen, einschließlich der Informationssicherheit, wurden grundlegend geändert

10) Bei Anwendung eines risikobasierten Prüfungsansatzes kann der Prüfer den Risikomanagementprozess (einschließlich Risikoermittlung, -bewertung und -behandlung) der geprüften Stelle beurteilen und im Rahmen der Risikoermittlung und -bewertung frühere interne oder externe Prüfungen oder Bewertungen berücksichtigen.

11) Der Prüfer kann untersuchen, ob einschlägige Strategien und Verfahren vorhanden sind und ob diese in angemessenen Zeitabständen überprüft und erforderlichenfalls aktualisiert werden, und dabei die Funktionen innerhalb der Organisation beurteilen. Darüber hinaus kann der Prüfer bewerten, ob die Nutzer über ein angemessenes Bewusstsein und Verständnis, u. a. in Bezug auf die Kultur der Informationssicherheit, verfügen.

12) Eine Entscheidung über die Wesentlichkeit eines bei einer Prüfung der Informationssicherheit ermittelten Problems kann innerhalb des Gesamtrahmens einer ORKB für die Entscheidung über die Wesentlichkeit sowie auf der Grundlage spezifischer Leitlinien für die Wesentlichkeit bei Prüfungen von Informationssystemen getroffen werden.

5.1 Quellen für Prüfungskriterien

13) Der Prüfer kann national oder international anerkannte Rahmen für die Informationssicherheit als Quellen für Prüfungskriterien heranziehen.

14) Die als Quellen für Prüfungskriterien dienenden Rahmen könnten u. a. folgende Standards umfassen: die Reihe ISO/IEC 27000, den von der ISACA ausgearbeiteten/aktualisierten COBIT-Rahmen, die vom *National Institute of Standards and Technology* (NIST) ausgearbeiteten Standards und Rahmen für Informations- und Cybersicherheit sowie Kontrollen des *Center for Information Security* (CIS); zu den enger ausgerichteten bzw. sektorspezifischen Rahmen und Standards zählen die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, der Datensicherheitsstandard der Zahlungskartenbranche (*Payment Card Industry Data Security Standard*, PCI DSS), das US-amerikanische Gesetz über die Übertragbarkeit und Rechenschaftspflicht von Krankenversicherungen (*Health Insurance Portability and Accountability Act*, HIPAA) im Gesundheitssektor usw.

15) Die Wahl der Prüfungskriterien durch den Prüfer kann von Folgendem abhängen:
- spezifischer Kontext der ORKB und des Landes (einschließlich etwaiger rechtlicher und regulatorischer Anforderungen);
- betroffene geprüfte Stelle(n);
- Umfang der Prüfung.

5.2 Ressourcen

16) Überlegungen zur Zuweisung von Personal für Prüfungsaufträge im Bereich der Informationssysteme (einschließlich Prüfungen der Informationssicherheit) werden im GUID 5100 erörtert und gelten im Großen und Ganzen auch für Prüfungen der Informationssicherheit. Zusätzlich sollte berücksichtigt werden, dass Prüfer, die Umgang mit sensiblen und vertraulichen Informationen haben, möglicherweise einer speziellen Kontrolle durch die zuständigen Behörden unterzogen werden müssen.

6 DURCHFÜHRUNG EINER PRÜFUNG DER INFORMATIONSSICHERHEIT

6.1 Zweck der Prüfungshandlungen [3]

17) Die Prüfungshandlungen für eine Prüfung der Informationssicherheit werden so konzipiert, dass sie insbesondere dem Zweck dienen, Folgendes zu bewerten: a) die Vertraulichkeit, b) die Integrität – einschließlich der Nichtabstreitbarkeit – und c) die Verfügbarkeit von Daten und IT-Systemen, die Gegenstand des Prüfungsauftrags sind.

6.2 Prüfungshandlungen zum Erlangen von Prüfungsnachweisen

18) Die Prüfungshandlungen können eine Kombination aus Folgendem umfassen: a) Überprüfung der Dokumentation, b) Beobachtung, Durchlauftests, Befragungen, Fragebögen, c) Analyse elektronischer Daten, z. B. in Bezug auf Audit-Protokolle verschiedener Art, d) Schwachstellenanalyse/Penetrationstests. Ist eine Schwachstellenanalyse bzw. sind Penetrationstests durch den Prüfer vorgesehen, so müssen möglicherweise Vorkehrungen und Vereinbarungen mit der geprüften Stelle getroffen werden, um einen derartigen Eingriff zu ermöglichen, gegebenenfalls einschließlich rechtlicher Garantien und Entschädigungen. Hat ein Dritter eine Schwachstellenanalyse bzw. Penetrationstests durchgeführt, so können die Ergebnisse der Schwachstellenanalyse bzw. der Penetrationstests in die Prüfungsnachweise aufgenommen werden. In diesem Fall erlangt der Prüfer ein ausreichendes Verständnis des Umfangs der Schwachstellenanalyse bzw. der Penetrationstests sowie der betreffenden Feststellungen und ihrer Bedeutung.

19) Zur Bewertung der physischen und umgebungsbezogenen Sicherheit kann der Prüfer neben der Dokumentenprüfung, Befragungen usw. als zusätzliche

[3] Zur Veranschaulichung sind im Anhang übergeordnete Prüfungsfragen aufgeführt.

Prüfungshandlung einen physischen Besuch (oder eine gemeinsame Kontrolle) des Rechenzentrums in Erwägung ziehen.

20) Der Prüfer kann die Angemessenheit der Standards, Leitlinien und Verfahren prüfen, die zur Umsetzung der Politik im Bereich der Informationssicherheit und der Strategien für die Meldung und Bewältigung von Vorfällen/Problemen ausgearbeitet wurden.

21) Im Zuge der Prüfung des Risikomanagementprozesses kann auch die Häufigkeit der regelmäßigen Risikoüberprüfungen und die Angemessenheit der Folgemaßnahmen zur Minderung der ermittelten und bewerteten Risiken untersucht werden. Die Entscheidung über die Schwellenwerte für die Risikoakzeptanz (und die sich daraus ergebende Akzeptanz von Restrisiken) obliegt dem Management.

22) Der Risikomanagementprozess (insbesondere die Risikoermittlung und -bewertung) steht im Zusammenhang mit den Strategien zur Ermittlung, Klassifizierung und Kontrolle von Informationswerten. Im Rahmen der Prüfungshandlungen kann u. a. untersucht werden, ob die Strategien von den Nutzern verstanden werden und ob diese Strategien wirksam umgesetzt werden.

23) Bei den Prüfungshandlungen in Bezug auf Authentifizierung, Autorisierung und Zugangskontrollen kann u. a. untersucht werden, ob eine Multi-Faktor-Authentifizierung (in der Regel zusätzlich zur passwortbasierten Authentifizierung) durchgeführt wird und ob diese Authentifizierung im Rahmen einer Strategie oder eines Vertrags festgelegt oder vorgeschrieben ist.

24) Wenn Protokolle zu überprüfen sind, um zu beurteilen, ob die Zugangskontrolle wie geplant durchgeführt wurde, umfasst die Analyse der Protokolle unter Umständen den Erhalt von Datenausgaben oder -auszügen. Übermittelt die geprüfte Stelle Datenausgaben zum Zwecke der elektronischen Analyse, kann der Prüfer in Erwägung ziehen, ein Schreiben gemäß Punkt 6.4 GUID 5100 zur Sicherstellung der Authentizität, einschließlich der Integrität und Nichtabstreitbarkeit der Daten, anzufordern.

25) Zur Prüfung des Umgangs mit Informationssicherheitsvorfällen kann der Prüfer zusätzlich zur Überprüfung der Prozesse und der Dokumentation im Zusammenhang mit der Feststellung und Protokollierung von Vorfällen sowie deren Bewertung und Behebung in Erwägung ziehen, anhand einer

Stichprobe von Nutzern (die Vorfälle festgestellt und gemeldet haben) zu untersuchen, ob der Vorfall angemessen behoben wurde.

26) Im Rahmen einer Prüfung der Informationssicherheit kann die Planung und Umsetzung der Aufrechterhaltung des Betriebs und der Wiederherstellung nach Notfällen bewertet werden, um den Aspekt der "Verfügbarkeit" von Informationsdiensten sowie die Informationssicherheit bei der Wiederherstellung des Betriebs nach einem Notfall zu beurteilen. Alternativ können solche Aspekte im Rahmen einer Prüfung des Betriebsmanagements von Informationssystemen abgedeckt werden.

6.3 Überlegungen im Zusammenhang mit Auslagerungs - vereinbarungen

27) Was die Informationssicherheit in Bezug auf Beziehungen zu Anbietern bzw. Auslagerungsbeziehungen betrifft, so bleibt die geprüfte Stelle für die Informationssicherheit verantwortlich, auch wenn die Verantwortung für bestimmte Tätigkeiten im Bereich von Informationssystemen an einen externen Anbieter ausgelagert wurde. Darüber hinaus sind Aspekte wie die Trennung miteinander in Konflikt stehender Aufgaben (und deren Aufteilung z. B. auf Entwicklungs-, Test- und Produktionsteams) von Bedeutung, unabhängig davon, ob die Entwicklung, die Umsetzung, der Betrieb oder die Wartung des Informationssystems intern oder durch einen externen Anbieter erfolgen.

7

BERICHTERSTATTUNG ÜBER EINE PRÜFUNG DER INFORMATIONSSICHERHEIT

28) Im Falle von Prüfungen der Informationssicherheit kann auf die in der ISSAI 400 enthaltenen Leitlinien für die Bewertung von Prüfungsnachweisen und die Berichterstattung sowie auf die im GUID 5100 enthaltenen zusätzlichen Leitlinien zur Berichterstattung (Abschnitt 7; darin wird auch darauf hingewiesen, dass es sensibel ist, Sicherheitsrisiken zu melden, bevor die zur Minderung der Risiken erforderlichen Kontrollen eingeführt wurden) zurückgegriffen werden.

29) Bei der Berichterstattung über die Informationssicherheit können die Prüfer die potenziellen betrieblichen Auswirkungen der Offenlegung von technischen Mängeln und Sicherheitsrisiken gegenüber der Öffentlichkeit berücksichtigen. In solchen Fällen kann der Prüfer auf geeignete Mechanismen zurückgreifen, u. a. auf die Schwärzung sensibler Informationen oder auf Prüfungsmitteilungen, in denen die geprüften Stellen über Einzelheiten und mögliche Auswirkungen des Risikos informiert werden.

30) Bei der Berichterstattung kann der Prüfer über die üblichen Interessenträger von Prüfungen des öffentlichen Sektors hinaus auch die spezifische Sichtweise von Interessenträgern wie etwa Anbietern ausgelagerter technischer Unterstützung für die geprüften Stellen berücksichtigen.

31) Der Prüfer kann Empfehlungen zur Verbesserung der Informationssicherheit aussprechen. Bei der Ausarbeitung der Empfehlungen kann der Prüfer etwaige praktische Auswirkungen auf die geprüfte Stelle, einschließlich der Durchführungskosten, berücksichtigen.

8

KONTROLLPRÜFUNG

32) Der Prüfer zieht gemäß den in der ISSAI 400 festgelegten Grundsätzen der Recht- und Ordnungsmäßigkeitsprüfung die Durchführung von Kontrollprüfungen in Betracht.

33) IT-Systeme werden ständig weiterentwickelt. Beispielsweise sind IT-Systeme zunehmend webgestützt/cloudbasiert. Bei der Festlegung des Zeitpunkts von Kontrollprüfungen kann der Prüfer solchen erheblichen Änderungen Rechnung tragen.

34) Bei der Planung einer Kontrollprüfung kann der Prüfer Faktoren wie die verfügbare Technologie, die geschätzten Kosten und die Systemkompatibilität berücksichtigen, die sich auf die Fähigkeit der geprüften Stelle auswirken können, den Prüfungsfeststellungen Rechnung zu tragen und die Empfehlungen umzusetzen.

Vorgeschlagene übergeordnete Prüfungsfragen

Dieser Anhang enthält übergeordnete Prüfungsfragen zum Prüfungsgegenstand der Informationssicherheit, die als Orientierungshilfe dienen, lediglich Hinweischarakter haben und nicht erschöpfend sind. Die Bedeutung der Ziele hängt davon ab, ob die geprüfte Stelle gesetzlich oder anderweitig verpflichtet ist, die in den Zielen festgelegten Kriterien zu erfüllen. Detaillierte Prüfungsfragebögen würden sich nach der Art des Informationssystems, der Organisation, den Rahmenbedingungen und dem Umfang des Prüfungsauftrags usw. richten.

Nr.	Bereich der Informationssicherheit	Ziel	Anmerkungen
1	Strategie für Informationssicherheit	Wurde eine solche Strategie festgelegt, angenommen und kommuniziert?	Die Strategie muss auch in regelmäßigen Abständen überprüft werden.
2	Organisationsstruktur in Bezug auf die Informationssicherheit	Wurde einer solchen Governance-Struktur klar die Verantwortung für die Informationssicherheit übertragen?	Die Prüfer können diesbezüglich die Klarheit der Beschreibungen, des Aufbaus, der Zusammensetzung und des Mandats überprüfen.
		Wurden die für das Personal im Rahmen dieser Governance-Struktur geltenden Bedingungen, die jeweiligen Funktionen und der Berichterstattungs-mechanismus festgelegt?	Innerhalb der Organisation sollte es eine Aufgabentrennung geben, wobei jede Position mit unterschiedlichen Funktionen und Zuständigkeiten einhergeht und eine Berichtshierarchie für die Meldung von Problemen vorgegeben ist.
		Wurde den Sicherheitsaspekten im Zusammenhang mit Personal, das im Bereich der Informationssysteme tätig ist, Rechnung getragen?	Personalkontrollen sind in allen Phasen der Personalverwaltung durchzuführen.
		Fördert die Organisation unter den Mitarbeitern auf allen Ebenen eine Kultur der Informationssicherheit?	Die Organisationskultur spielt eine wichtige Rolle bei der Bestimmung des Maßes an Informationssicherheit in einer Organisation.
3	Verwaltung der Informationswerte	Wurde regelmäßig eine Bestandsaufnahme der mit Informationssystemen zusammenhängenden Werte durchgeführt und wurden Sicherheitsanforderungen für die einzelnen Arten von Werten festgelegt?	Informationswerte sollten angemessen klassifiziert, gekennzeichnet und verwaltet werden.
4	Entwicklung, Anschaffung und Wartung von Informationssystemen	Wurden für die einzelnen Prozesse Sicherheitsaspekte definiert, angenommen und kommuniziert?	Der Informationssicherheit muss während des gesamten Lebenszyklus entscheidende Bedeutung beigemessen werden.
		Wird die Informationssicherheit von den Anbietern bei allen Interaktionen gewährleistet?	Abhängig von den Risiken ist zu überprüfen, ob die geprüfte Stelle den Code und die Module des entwickelten/angeschafften Informationssystems durch qualifizierte interne oder

			externe Ressourcen hat überprüfen lassen, um sicherzustellen, dass es keine versteckten Merkmale gibt, die die Vertraulichkeit, Integrität und Verfügbarkeit der Daten beeinträchtigen könnten.
5	IT-Operationen	Wurden Sicherheitsaspekte der IT-Operationen definiert, angenommen und kommuniziert?	Verträge/Dienstleistungs-vereinbarungen, die mit Dritten geschlossen wurden, an die IT-Operationen ausgelagert wurden, sind zu überprüfen, um sicherzustellen, dass sie Vertraulichkeitsklauseln, Wettbewerbsverbote, Bestimmungen über die Nichtänderung ohne Genehmigung und die Nichtweitergabe sowie sonstige Standardbestimmungen enthalten, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten.
6	Physische und umgebungsbezogene Sicherheit	Wird die Sicherheit der physischen Umgebung des Informationssystems gewährleistet?	Es ist zu überprüfen, ob physische Barrieren (externe Eingänge/Schranken, Innentüren, Sicherheitspersonal) vorhanden sind, die dafür sorgen, dass die Identität des Personals festgestellt und der Zugang zu Speicherhardware wie Servern auf befugtes Personal beschränkt wird. Das Gebäude- und Anlagenmanagement ist ein wichtiger Aspekt des gesamten Sicherheitsökosystems.
7	Netz- und Kommunikations-sicherheit	Ist die Informationssicherheit während der Kommunikation gewährleistet?	Es sollte überprüft werden, ob eine Verschlüsselung der Nachrichten durch die Kommunikationskanäle gewährleistet ist, sodass ein Abhören durch Dritte und ein Verlust der Vertraulichkeit verhindert wird; zudem ist zu überprüfen, ob bei digitaler Kommunikation mit formalem Charakter kryptografische Kontrollen eingesetzt werden.
		Eignet sich die Sicherheitsarchitektur des	Gegebenenfalls können die Prüfer untersuchen, ob

		Netzwerks zur Gewährleistung der Informationssicherheit?	kryptografische und sonstige Cybersicherheitskontrollen vorhanden sind.
8	Aufrechterhaltung des Betriebs und Wiederherstellung nach Notfällen	Wurde den Sicherheitsaspekten im Zusammenhang mit diesen Prozessen Rechnung getragen und ist die Informationssicherheit im Falle der Wiederherstellung nach Notfällen für den Übergang und den Betrieb angemessen?	Die Prüfer können kontrollieren, ob die Informationssicherheits-einrichtung während des Prozesses der Wiederherstellung des Betriebs nach einem Notfall angemessen ist.
9	Einhaltung der gesetzlichen Vorschriften	Werden die gesetzlichen Anforderungen im Zusammenhang mit Aspekten der Informationssicherheit erfüllt?	Die Prüfer müssen die Einhaltung der Rechts- und Verwaltungsvorschriften in allen anderen relevanten Bereichen überprüfen. Möglicherweise ist vorgeschrieben, dass Einrichtungen in Bezug auf die Informationen bestimmte Bescheinigungen bzw. eine bestimmte Gewähr erlangen müssen. Die Prüfer können auch den Umfang und die Gültigkeit einer solchen Bescheinigung untersuchen.