GUID 5100

Leitfadens zur Prüfung von Informationssystemen

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, 2019

INHALTSVERZEICHNIS

1. Einführung	**4**
2. Zielsetzung dieser GUID	**6**
3. Definitionen	**7**
4. Umfang	**8**
5. Planung der IS-Prüfung	**9**
6. Durchführung von IS-Prüfungen	**15**
7. Berichterstattung über die IS-Prüfung	**21**
8. Follow up	**23**

1 EINFÜHRUNG

1.1 Die GUID 5100 bildet den übergreifenden Rahmen für die Durchführung von Prüfungen von Informationssystemen innerhalb des IFPP. Die GUID soll die Grundlage für die Entwicklung zukünftiger GUIDs in der Serie 5100-5109 zum Themenbereich der Prüfung von Informationssystemen im IFPP bilden.

1.2 Der in dieser GUID festgelegte Rahmen steht im Einklang mit den Grundprinzipien der öffentlichen Finanzkontrolle (ISSAI 100), den Grundprinzipien der Finanzprüfung (ISSAI 200), den Grundsätzen der Wirtschaftlichkeitsprüfung (ISSAI 300) und den Grundsätzen der Konformitätsprüfung (ISSAI 400).

1.3 Die Obersten Rechnungskontrollbehörden (ORKBn) sind beauftragt, Regierungen und ihre Unternehmen gemäß ihren jeweiligen Prüfungsmandaten zu prüfen.[1] Mit ihren Aktivitäten wollen die ORKBn die Effizienz, Rechenschaftspflicht, Effektivität und Transparenz der öffentlichen Verwaltung fördern[2].

1.4 Regierungen und andere Unternehmen des öffentlichen Sektors haben kontinuierlich Innovationen in der Informationstechnologie (IT) in ihre Informationssysteme übernommen, um die Effizienz und Effektivität ihrer Funktionsweise und Erbringung verschiedener öffentlicher Dienstleistungen zu verbessern. Denn die IT hat es ermöglicht, Informationen elektronisch zu erfassen, zu speichern, zu verarbeiten, abzurufen und auf elektronischem Wege zu übermitteln, was wiederum einen erheblichen Spielraum für die Verbesserung der Genauigkeit, Vertraulichkeit und Aktualität der Messdaten von Informationssystemen schafft. Darüber hinaus wandelt sich der Erbringungsmodus öffentlicher Dienstleistungen rasch von physisch zu elektronisch, so dass die Regierungen als digitale Plattformen

1 INTOSAI-P 1 Die Lima-Erklärung
2 Resolution A/66/209 der Generalversammlung der Vereinten Nationen

fungieren müssen, welche Dienste und Infrastruktur für andere IT-gesteuerte Informationssysteme bereitstellen.

1.5 Dieser Übergang zu computergestützten Informationssystemen und zur elektronischen Verarbeitung durch geprüfte Unternhemen des öffentlichen Sektors hat zu einem erheblichen Wandel im Umfeld der ORKBn geführt. Die Ausgaben des öffentlichen Sektors für IT wachsen. Es muss auch sichergestellt werden, dass interne IT-Kontrollen zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten von öffentlichen Unternehmen übernommen wurden. Daher ist es für die ORKBn unerlässlich, angemessene Kapazitäten zu entwickeln, um eine gründliche Prüfung der Kontrollen im Zusammenhang mit Informationssystemen durchzuführen.

2 ZIELSETZUNG DIESER GUID

2.1 Die ISSAI 100, 200, 300 und 400 legen die Grundprinzipien der Prüfung in Bezug auf Finanzprüfung, Wirtschaftlichkeitsprüfung und Konformitätsprüfung fest. Diese ISSAI beziehen sich auf allgemeine Grundsätze, Verfahren, Normen und Erwartungen an einen Wirtschaftsprüfer. Sie gelten gleichermaßen auch für die Prüfung von Informationssystemen.

2.2 Ziel dieser GUID ist es, Wirtschaftsprüfern Hinweise zu geben, wie sie Leistungs- und / oder Konformitätsprüfungen im Zusammenhang mit dem spezifischen Gegenstand von Informationssystemen durchführen können oder wo die Prüfung von Informationssystemen Teil eines größeren Prüfungsauftrags sein kann, der Finanz-, Konformitäts- oder Leistungsprüfung sein kann

2.3 Der Inhalt dieser GUID kann von Wirtschaftsprüfern auf die Phasen Planung, Durchführung, Berichterstattung und Follow-up[3] des Prüfungsprozesses angewendet werden.

3 ISSAI 100

3 DEFINITIONEN

3.1 Informationssysteme: Informationssysteme können definiert werden als eine Kombination von strategischen, betriebswirtschaftlichen und operativen Aktivitäten, die mit der Sammlung, Verarbeitung, Speicherung, Verteilung und Nutzung von Informationen und damit verbundenen Technologien verbunden sind. Die Komplexität eines solchen Informationssystems kann von einem einfachen Buch, in dem die Einträge für den Geldeingang und die Zahlung manuell gepflegt werden, bis hin zu einem komplexeren IT-gesteuerten System, wie beispielsweise einem System zur Steuerveranlagung, bei dem alle Prozesse - Datenerfassung (z.B. Steuererklärungen über das Online-Webportal), Speicherung auf Servern, Verarbeitung der Veranlagung (auf der Grundlage der Programmierung nach den Steuervorschriften) und Kommunikation der Steuernachfrage, Rückerstattung und Bestätigung (in Echtzeit oder in vorgeschriebenen Abständen) - automatisiert werden. Die Informationstechnologie umfasst die Hardware, Software, Kommunikation und andere Einrichtungen, die zur Eingabe, Speicherung, Verarbeitung, Übertragung und Datenausgabe in jeglicher Form dienen.

3.2 Die Prüfung von Informationssystemen kann definiert werden als die Prüfung von Kontrollen im Zusammenhang mit IT-gesteuerten Informationssystemen, um Fälle von Abweichungen von den Kriterien zu ermitteln, die wiederum anhand der Art des Prüfungsauftrags - d.h. Finanzprüfung, Konformitätsprüfung oder Wirtschaftlichkeitsprüfung - ermittelt wurden.

4 UMFANG

4.1 Diese GUID kann von Wirtschaftsprüfern verwendet werden, um Leistungs- und/oder Konformitätsprüfungen zu dem spezifischen Thema der Informationssysteme durchzuführen, sowie wenn die Prüfung von Informationssystemen Teil eines größeren Prüfungsauftrags ist, der eine Finanz-, Konformitäts- und/oder Leistungsprüfung sein kann.

4.2 Diese Richtlinie enthält weitere Hinweise, wie eine Prüfung von Informationssystemen durch eine Finanz-, Leistungs- und Konformitätsprüfung durchgeführt werden könnte, und enthält keine weiteren Anforderungen an die Durchführung der Prüfung.

5 PLANUNG DER IS-PRÜFUNG

5.1 ORKBn können eine risikobasierte Prüfungsplanung für IS-Prüfungen in Übereinstimmung mit dem in ISSAI 100, ISSAI 200 (Finanzaudit), ISSAI 300 (Wirtschaftlichkeitsprüfung) und ISSAI 400 (Konformitätsprüfung) beschriebenen Prozess durchführen, je nach den Zielen des Prüfungsauftrags.

5.2 Die IS-Prüfarbeit wird durch das Ziel und den Umfang der Prüfung bestimmt. Beispiele können sein:

1) Bewertung der relevanten allgemeinen Kontrollen[4] und Anwendungskontrollen[5], die sich auf die Zuverlässigkeit von Daten aus Informationssystemen auswirken, die sich wiederum auf den Jahresabschlüsse des geprüften Unternehmens auswirken.

2) Sicherstellung der Konformität der Prozesse der Informationssysteme mit den für das geprüfte Unternehmen geltenden Gesetzen, Richtlinien und Normen.

3) Sicherstellung, dass die IT-Ressourcen es ermöglichen, die Unternehmensziele effizient und effektiv zu erreichen, und dass die relevanten allgemeinen Kontrollen und Anwendungskontrollen wirksam sind, um Überschreitungen, Extravaganzen und Ineffizienzen bei der Nutzung und Verwaltung von Informationssystemen zu verhindern, zu erkennen und zu korrigieren.

4 Allgemeine Kontrollen sind manuelle oder automatisierte Verfahren, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in der physischen Umgebung zu gewährleisten, in der Informationssysteme entwickelt, gewartet und betrieben werden.

5 Anwendungskontrollen sind IT-abhängige manuelle oder automatisierte Verfahren innerhalb eines Informationssystems, die sich auf die Verarbeitung von Transaktionen auswirken und sich auf die Validierung von Eingangsdaten, die genaue Verarbeitung von Daten, die Bereitstellung von Ausgangsdaten und die Kontrolle der Integrität von Stammdaten beziehen können.

5.3 Basierend auf einer Risikobewertung kann der Umfang einer IS-Prüfung aus einem oder allen der folgenden Bereiche[6] des geprüften Unternehmens gezogen werden:

1) Unternehmensrichtlinien für die IT-Branche[7]
2) Unternehmensführungsstruktur zum Thema IT
3) Allgemeine Kontrollen im zu automatisierenden Geschäftsbereich
4) Asset-Management
5) Entwicklung, Beschaffung und Wartung von Informationssystemen, einschließlich der Abbildung von Geschäftsprozessen und der zugehörigen Programmierlogik
6) IT Betriebsführung
7) Management der physischen Umgebung
8) Personalmanagement
9) Kommunikationsmanagement
10) Informationssicherheitsmanagement[8]
11) Gesetzliches Compliance Management
12) Business Continuity und Notfallwiederherstellungsmanagement
13) Management von Anwendungssteuerungen

5.4 ORKBn können den Zeitraum für die Prüfungsanalyse (z.B. ein Jahr, drei Jahre usw.) bei der Festlegung des Umfangs des Prüfungsauftrags von IS wählen. Es kann ein angemessener Zeitraum gewählt werden, welcher für die für den Prüfungsauftrag festgelegten Ziele relevant ist.

5.5 Ist eine IS-Prüfung Teil eines Prüfungsauftrags, kann die ORKB sicherstellen, dass das Prüfungsteam als Ganzes integriert arbeitet, um das allgemeine Prüfungsziel zu erreichen. Um eine wirksame Integration zu erreichen, können ORKBn in Betracht ziehen:

1) Umfassende Dokumentation der von den IS-Wirtschaftsprüfern zu erbringenden Leistungen
2) Formulierung eines Protokolls für den Informationsaustausch zwischen den IS-Wirtschaftsprüfern und anderen Wirtschaftsprüfern;

6 Die meisten der beschriebenen Bereiche wurden von der ISO/IEC 27001 übernommen
7 Einschließlich Aspekte des strategischen Managements
8 Einschließlich Cybersicherheit

3) Festlegung, welche Informationssysteme und Kontrollziele in den Geltungsbereich der Prüfung fallen;

5.6 ORKBn können sicherstellen, dass das Prüfungsteam aus Mitgliedern besteht, die gemeinsam befugt sind, IS-Prüfungsaufträge zur Erreichung der beabsichtigten Prüfungsziele durchzuführen.

5.7 Die erforderlichen Kenntnisse, Fähigkeiten und Kompetenzen können durch eine Kombination aus Schulung, Einstellung und Einsatz externer Ressourcen gemäß dem strategischen Plan der ORKB erworben werden.

5.8 Die ORKBn können sicherstellen, dass die IS-Prüfungsteams gemeinsam die Fähigkeit haben, Folgendes zu tun

1) Verstehen der technischen Elemente eines IT-gesteuerten Informationssystems, einschließlich aller relevanten Instanzen der verwendeten Anwendung, um auf die IT-Infrastruktur zugreifen und diese für den Prüfungsprozess nutzen zu können
2) Verstehen der bestehenden Regeln, Vorschriften und das Umfeld, in dem die IT-gesteuerten Informationssysteme des geprüften Unternehmens betrieben werden
3) Verstehen der Abbildung von Geschäftsprozessen in die Programmierlogik für das Informationssystem des geprüften Unternehmens
4) Anwendung von Geschäfts- und IT-Kenntnissen zur Bewertung des Risikos einer manuellen Überschreibung eines Systemprogramms oder einer Systemkonfiguration, die eine außergewöhnliche Verarbeitung von Transaktionen ermöglichen würde
5) Bewertung des Designs und Prüfung der operativen Wirksamkeit von Anwendungskontrollen in relevanten Informationssystemen
6) Verstehen der Prüfungsmethodik, einschließlich der relevanten Prüfungsstandards und Richtlinien, die für die ORKB gelten
7) Verstehen der IT-Leistungs-/Konformitätskriterien, mit denen die Prüfungsergebnisse verglichen werden sollen, einschließlich der Rahmenbedingungen für das IS-Management, wie z.B. COBIT, ITIL, TOGAF

8) Verstehen von IS-Techniken zur Erfassung der Prüfungsnachweise aus automatisierten Systemen

9) IS-Prüfungsinstrumente verstehen, um die Ergebnisse einer solchen Analyse zu sammeln, zu analysieren und zu reproduzieren oder die geprüften Funktionen erneut auszuführen

10) Zugriff und Nutzung der IS-Infrastruktur zur Erfassung und Aufbewahrung von Prüfungsnachweisen

11) Zugriff und Verwendung von IS-Prüfungswerkzeugen zur Analyse der gesammelten Beweise

5.9 ORKBn können verschiedene Optionen für die Zuweisung von Personal für IS-Prüfungsaufträge in Betracht ziehen. Dies könnte die Einrichtung einer zentralen Gruppe mit IT-Spezialisten sein, die andere Prüfungsteams in der ORKB bei der Durchführung dieser Prüfungen unterstützen oder IT-Spezialisten nach Bedarf einsetzen. Mit steigender Anzahl der durchgeführten IS-Prüfungsaufträge können ORKBn die Einrichtung einer speziellen IS-Prüfungsgruppe oder -funktion in Betracht ziehen. Diese Gruppe kann mit der Verantwortung betraut werden, alle IS-Prüfungsaufträge für die ORKB durchzuführen und mit anderen Teams der ORKB zu interagieren, die über Altkenntnisse des geprüften Unternehmens verfügen, um schnell ein Verständnis für die Funktionen des Unternehmens und die damit verbundenen Geschäftsprozesse zu erlangen. Da die Technologie immer mehr in Informationssysteme eingebettet wird, können ORKBn sicherstellen, dass alle Wirtschaftsprüfer geeignete IS-Prüfungskenntnisse erwerben.

5.10 ORKBn können in Fällen von Ressourcenbeschränkungen externe Ressourcen wie IT-Berater, Auftragnehmer, Spezialisten und Experten mit der Durchführung von IS-Prüfungen beauftragen. ORKBn können sicherstellen, dass diese externen Ressourcen angemessen geschult und für die auf die ORKB anwendbaren Richtlinien für das professionelle Verhalten und für Prozesse und Produkte der IS-Prüfung sensibilisiert sind und dass ihre Arbeit durch einen dokumentierten Vertrag oder eine Dienstleistungsvereinbarung und eine angemessene Beteiligung der Mitarbeiter der ORKB an den Phasen Planung, Durchführung, Berichterstattung und Follow-Up der Prüfung angemessen überwacht wird. ORKBn können daher qualifizierte und sachkundige Teammitglieder innerbetrieblich benötigen, um die Arbeit externer Ressourcen zu überwachen und die Einhaltung von Richtlinien und

Dienstleistungsvereinbarungen durchzusetzen.

5.11 Bei der Durchführung der Risikobewertung für IS-Prüfaufträge können die in den ISSAI 100, 200, 300 und 400 festgelegten Grundsätze von den Wirtschaftsprüfern zusätzlich zu denjenigen angewandt werden, die bei der Durchführung bestimmter Themen der IS-Prüfung verwendet werden, wie nachstehend beschrieben:

1) Das inhärente Risiko besteht in der Wahrscheinlichkeit, dass bestimmte Merkmale der IT-gesteuerten Informationssysteme eines geprüften Unternehmens naturgemäß negative Auswirkungen auf die Erbringung der von dem Unternehmen zu erbringenden Funktion haben können. So birgt beispielsweise ein Informationssystem eines geprüften Unternehmens, das verpflichtet ist, Informationen für alle Mitglieder der Öffentlichkeit zugänglich zu machen, das inhärente Leistungsrisiko, dass das Informationssystem über eine erwartete maximale Benutzeranzahl hinaus nicht reagieren kann und die Informationen keinem Benutzer zur Verfügung stehen würden. Während das geprüfte Unternehmen Kontrollen zur Minderung der inhärenten Risiken einführen kann, muss das Unternehmen in vielen Fällen das Bestehen solcher Risiken innerhalb eines akzeptablen Risikoniveaus einfach tolerieren. Das inhärente Risiko kann bewertet werden, bevor der Einfluss von Kontroll- oder Entdeckungsrisiken von den Wirtschaftsprüfern berücksichtigt wird.

2) Das Kontrollrisiko für ein IS würde aus der Wahrscheinlichkeit bestehen, dass IT-Kontrollen, die von dem geprüften Unternehmen übernommen wurden, die negativen Auswirkungen, die als Reaktion auf sie entworfen wurden, nicht abschwächen können. So kann beispielsweise ein Informationssystem eines geprüften Unternehmens, das verpflichtet ist, sicherzustellen, dass der Zugang zu vertraulichen Daten auf autorisiertes Personal beschränkt ist, die Kontrolle übernehmen, dass von dem Personal, das versucht, Zugang zu erhalten, die Vorlage eines Benutzernamens und eines Passworts verlangt wird. Das Kontrollrisiko in dieser Situation besteht darin, dass der Benutzername und das Passwort nicht ausreichend sicher sind und von Unbefugten durch wiederholte Versuche erraten werden können, was zum Verlust der Vertraulichkeit und möglichen negativen Auswirkungen auf das Unternehmen führt. Ein Unternehmen, das auf der Verwendung sicherer, nicht trivialer Passwörter besteht,

die eine Kombination aus Alphabeten, Zahlen und speziellen Symbolen aufweisen, und sicherstellt, dass das Informationssystem den Zugriff auf den Benutzernamen ab einer bestimmten Anzahl von fehlgeschlagenen Zugriffsversuchen verhindert, hätte ein geringeres Kontrollrisiko als eines, das diese Funktionen nicht aufweist.

3) Das Entdeckungsrisiko würde aus der Wahrscheinlichkeit bestehen, dass das Fehlen, Versagen oder die Unzulänglichkeit der von einem Unternehmen angenommenen IT-Kontrollen, die potenziell nachteilige Auswirkungen auf das Unternehmen haben können, vom Wirtschaftsprüfer nicht erkannt werden.

5.12 Für die Durchführung risikobasierter Bewertungen von IT-gestützten Systemen können ORKBn eine für ihren Zweck geeignete Methodik wählen. Diese Methoden können von einfachen Klassifizierungen des Risikoprofils der IT-Umgebung des geprüften Unternehmens als hoch, mittel und niedrig auf der Grundlage des Verständnisses der ORKB für das Unternehmen und sein Umfeld und der fachlichen Beurteilung des IS-Prüfungsteams einer ORKB bis hin zu komplexeren und numerischen Berechnungen reichen, welche die Risikoeinstufung auf der Grundlage objektiver Daten, die von dem geprüften Unternehmen gesammelt wurden, quantifizieren[9].

5.13 Die Wesentlichkeit einer IS-Prüfungsfrage kann nach dem allgemeinen Rahmen für die Entscheidung über die Wesentlichkeit in einer ORKB entschieden werden. Die Perspektive der Wesentlichkeit kann je nach Art des Prüfungsauftrags der IS-Prüfung variieren. Die Wesentlichkeit für die Finanz-, Leistungs- und Konformitätsprüfungen des öffentlichen Sektors, aus denen der IS-Auditauftrag gezogen werden soll, wurden in den ISSAI 100, 200, 300 und 400 beschrieben[10].

9 WGITA IDI Handbuch für IT-Prüfungen für Oberste Rechnungskontrollbehörden

10 ISSAI 200 Finanzprüfungsgrundsätze, ISSAI 300 Wirtschaftlichkeitsprüfungsgrundsätze, ISSAI 400 Konformitätsprüfungsgrundsätze

6 DURCHFÜHRUNG VON IS-PRÜFUNGEN

6.1 Die ORKBn können IS-Prüfungen in Übereinstimmung mit dem beschriebenen Prozess für Finanzprüfung (ISSAI 200), Wirtschaftlichkeitsprüfung (ISSAI 300) und Konformitätsprüfung (ISSAI 400) durchführen, je nach Art des Auftrags.

6.2 Insbesondere für eine IS-Prüfung können die Wirtschaftsprüfer eine ordnungsgemäße Zusammenarbeit und Unterstützung des geprüften Unternehmens bei der Durchführung der Prüfung, einschließlich des Zugangs zu Aufzeichnungen und Informationen, anfordern. Die Wirtschaftsprüfer können in Absprache mit dem geprüften Unternehmen die Art und Weise des Zugangs zu elektronischen Daten in dem Format festlegen, das für die Analyse erforderlich ist. Die Art und Weise des Zugriffs auf Daten wäre ORKB-spezifisch.

6.3 Vor Beginn der Bewertung von Kontrollen in einem Informationssystem können die Wirtschaftsprüfer ein Verständnis der Systemarchitektur sowie der zugrunde liegenden Daten und ihrer Quellen entwickeln, um die erforderlichen Prüfungsinstrumente und -techniken zu ermitteln.

6.4 Im Falle des Erhalts von Datenausgaben[11] von dem geprüften Unternehmen können die Wirtschaftsprüfer sicherstellen, dass jede Datenasugabe von einem Schreiben des geprüften Unternehmens begleitet wird. In einem solchen Weiterleitungsschreiben kann Folgendes festgelegt werden

1) Die Quelle (durch Bezugnahme auf den Zeitstempel der Erzeugung der Datenausgabe/Hash-Nummer für die Datenausgabe) der Daten zum

11 Datenausgabe ist definiert als eine große Menge an Daten, die von einem System oder Standort auf einen anderen übertragen werden

Zwecke der Sicherstellung der Datenintegrität, Authentifizierung[12] und Unleugbarkeit[13]

2) Die Parameter der Extraktion, die zum Erstellen der Datenausgabe verwendet werden, d.h. verwendete Abfragen/Berichte.

Wenn ein solches Weiterleitungsschreiben des geprüften Unternehmens nicht eingeht, können interne Dokumente erstellt werden, in denen die Wirtschaftsprüfer wichtige Informationen angeben, wie z.B. das Datum, an dem die Daten übergeben wurden, aus welcher Datei die Datenausgabe erstellt wurde, und ob die Daten aus der Produktionsumgebung oder aus einer anderen Umgebung stammen usw.

6.5 Die Wirtschaftsprüfer können eine Bewertung der von dem geprüften Unternehmen angenommenen IT-Kontrollen (allgemeine und Anwendungskontrollen) durchführen, um deren Zuverlässigkeit und Angemessenheit zu überprüfen. Die Bewertung kann mit einer geeigneten Kombination der folgenden Techniken durchgeführt werden: Interview, Fragebogen, Beobachtung, Walk Through, Ablaufdiagramme, Datenerfassung und -analyse, Verifizierung, Neuberechnung, Wiederaufbereitung und Bestätigung durch Dritte. Der Umfang der Bewertung von IT-Kontrollen kann folgende Prüfungen umfassen:

1) Die IS-Richtlinie wurde definiert, verabschiedet und kommuniziert
2) Die IS Steuerungsstruktur ist vorhanden und funktionsfähig
3) Die Inventur der IS-Anlagen wurde regelmäßig durchgeführt und die Anforderungen an die Erweiterung, den Austausch und die Entfernung wurden ermittelt
4) Prozesse für die gemeinsame Nutzung der Infrastruktur und der gemeinsamen Dienste für Informationssysteme mit anderen öffentlichen Unternehmen sind vorhanden und funktionieren
5) Prozesse für die Entwicklung, Beschaffung und Wartung von Informationssystemen wurden definiert, übernommen und kommuniziert (einschließlich des Change-Managements)

12 Authentifizierung ist definiert als der Akt der Überprüfung der Identität eines Benutzers - ISACA Glossar der Begriffe

13 Unleugbarkeit ist definiert als die Zusicherung, dass eine Partei später die Herkunft der Daten nicht leugnen kann; Vorlage des Nachweises der Integrität und Herkunft der Daten und kann von einem Dritten überprüft werden - ISACA Glossar der Begriffe

6) Prozesse für den IT-Betrieb (In-sourcing, Outsourcing, Serviceverträge) wurden definiert, übernommen und kommuniziert

7) Maßnahmen zur Gewährleistung der physischen Sicherheit und der beabsichtigten physischen Arbeitsbedingungen wurden ergriffen.

8) Maßnahmen zur Schulung und Sensibilisierung der Personalressourcen, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie die Einhaltung der Anforderungen der IS-Richtlinie und der Governance-Struktur zu gewährleisten, wurden ergriffen

9) Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit verschiedener Kommunikationsmodi und -kanäle wurden ergriffen

10) Maßnahmen für das Informationssicherheitsmanagement wurden ergriffen

11) Maßnahmen für das gesetzmäßige Compliance-Management wurden ergriffen

12) Maßnahmen für Business Continuity und Disaster Recovery Management wurden ergriffen

13) Anwendungskontrollen, die in jedem Informationssystem eingeführt werden, sind angemessen und zuverlässig. Eine solche Bewertung kann die Identifizierung wesentlicher Anwendungskomponenten, die Identifizierung der Kritizität der Anwendung für das Unternehmen, die Überprüfung der verfügbaren Dokumentation, die Befragung des Personals, das Verständnis der Risiken der Anwendungskontrolle und ihrer Auswirkungen auf das Unternehmen sowie die Entwicklung von Tests zur Überprüfung der Angemessenheit und Zuverlässigkeit solcher Anwendungskontrollen umfassen.

6.6 Die Bewertung der allgemeinen und anwendungsbezogenen Kontrollen kann sich daher auf die Richtlinien, Prozesse, Personen und Systeme des geprüften Unternehmens im Einklang mit den Zielen der IS-Prüfung erstrecken.

6.7 Je nach Ziel der Prüfung können sich Wirtschaftsprüfer mit der Gestaltung, Durchführung und operativen Wirksamkeit von Kontrollen befassen. Wenn der Wirtschaftsprüfer mit der Gestaltung der Kontrolle befasst ist, kann eine Befragung

oder Inspektion der dokumentierten Geschäftsregeln ausreichend sein. Wenn der Wirtschaftsprüfer mit der Durchführung von Kontrollen befasst ist, kann es sein, dass die Untersuchung nicht ausreicht und es notwendig sein kann, eine Bestandsaufnahme oder Datenanalyse durchzuführen, um zu belegen, dass die geplante Kontrolle durchgeführt wurde. Wenn der Wirtschaftsprüfer sich mit der operativen Wirksamkeit der Kontrolle befasst, kann er/sie gegebenenfalls verpflichtet werden, eine Stichprobe von Transaktionen zu testen, um nachzuweisen, dass die Kontrolle während des betreffenden Zeitraums wirksam funktioniert hat.

6.8 Die Wirtschaftsprüfer können auch prüfen, wie sich die Nachweise über die allgemeinen Kontrollen auf Art, Zeitpunkt und Umfang der Nachweise auswirken, die erforderlich sind, um Gewissheit über den Betrieb der Anwendungskontrollen zu erhalten. Wenn der Wirtschaftsprüfer ausreichende und geeignete Prüfungsnachweise über die Wirksamkeit der allgemeinen Kontrollen zur Unterstützung des logischen Zugangs des Personals zu IT-Systemen und des Change Managements innerhalb der Produktionsumgebung erhalten hat, kann er/sie möglicherweise auf die operative Wirksamkeit von automatisierten Anwendungskontrollverfahren schließen. Dies kann durch Testen einer kleineren Stichprobe von Transaktionen erfolgen, da die Effektivität der allgemeinen IT-Umgebung dem Wirtschaftsprüfer den Nachweis über die Effektivität der Anwendungskontrolle in dem betreffenden Zeitraum liefert. Im Falle von manuellen Anwendungskontrollverfahren müssen die Wirtschaftsprüfer möglicherweise einen Stichprobenumfang prüfen, der dem gewählten Konfidenzniveau entspricht.

6.9 Basierend auf der Bewertung von IT-Kontrollen können die Wirtschaftsprüfer prioritäre Bereiche für die Aufnahme von vertieften Prüfungen identifizieren, was eine detaillierte Prüfung der IT-Kontrollen durch den Einsatz verschiedener Computer Aided Audit Techniques (CAATs) zur Abfrage, Extraktion und Analyse von Daten beinhaltet. Wirtschaftsprüfer können vertiefte Prüfungen entwerfen und durchführen, um die Prüfungsziele zu untermauern. Wirtschaftsprüfer können entsprechend ihren Anforderungen geeignete CAATs auswählen.

6.10 Wirtschaftsprüfer können CAATs verwenden, um IS-Prüfungstechniken wie Benutzeranmeldunganalyse, Ausnahmeauswertungen, Field Wise Totalling, Dateivergleich, Stratifizierung, Probenahme, Duplikatprüfungen, Lückenerkennung, Datierung, virtuelle Feldberechnungen usw. durchzuführen. Vorteile des Einsatzes von CAATs sind die Analyse großer Datenmengen, die Wiederholbarkeit von Tests

auf verschiedenen Datensätzen und mit unterschiedlichen Kriterien sowie die automatisierte Dokumentation von Prüfungstests und Ergebnissen mit Zeitstempeln.

6.11 Die Wirtschaftsprüfer sind möglicherweise nicht immer in der Lage, alle Instanzen, Transaktionen oder Module oder IT-Systeme zu untersuchen, da die Ressourcen begrenzt sind und die Kosten-Nutzen-Abwägungen der Prüfungsübung auftreten. In einer solchen Situation können ORKBn auf der Grundlage von Wesentlichkeitserwägungen Prüfungsstichproben zur detaillierten Prüfung einführen, um angemessene Prüfungsergebnisse zu erhalten. ORKBn können geeignete CAATs für die Durchführung verschiedener Arten von Stichproben verwenden und einen angemessenen Stichprobenumfang festlegen, abhängig von den zugrunde liegenden inhärenten und Kontrollrisiken. Es werden Prüfungsstichproben[14] entnommen, um dem Wirtschaftsprüfer eine angemessene Grundlage zu geben, auf der er Schlussfolgerungen über den gesamten Datenbestand ziehen kann, und zwar auf der Grundlage von Schlussfolgerungen aus der Anwendung von Prüfungsverfahren und Analysen in Bezug auf die Prüfungsstichprobe. Wirtschaftsprüfer können den Zweck des Prüfungsverfahrens und die Merkmale der Population, aus der die Stichprobe entnommen wird, in Betracht ziehen und einen Stichprobenumfang festlegen, der ausreicht, um das Stichprobenrisiko auf ein akzeptables Maß zu reduzieren. Die Prüfung in einer IT-Umgebung kann die Analyse von 100 Prozent der Bevölkerung erleichtern, insbesondere im Vorfeld der Bewertung. Für die Durchführung von vertieften Prüfungen können jedoch Proben erforderlich sein. Wenn die IS-Wirtschaftsprüfer eine Stichprobe im Rahmen einer Finanzkontrolle durchführen, können sie ISSAI 2530 für die Stichprobenauswahl verwenden.[15]

6.12 Wirtschaftsprüfer können sicherstellen, dass die gesammelten und dokumentierten elektronischen Beweise ausreichend, zuverlässig und genau sind, um die Prüfungsbeobachtungen aufrechtzuerhalten. Diese elektronischen Beweise können aus Datendateien, Benutzeranmeldungen, Analysemodellen, Berichten über Managementinformationssysteme usw. bestehen. und können angemessen gesammelt und so aufbewahrt werden, dass sie für die Gewährleistung der Richtigkeit und Gültigkeit des Prüfungsprozesses zur Verfügung stehen. Die während einer IS-Prüfung gesammelten Beweise können mit notwendigen Zeitstempeln und Details versehen werden, die Schritte der Datenanalyse enthalten, so dass Klarheit darüber besteht, wann die Beweise erstellt, gespeichert und zuletzt geändert wurden, um

14 ISSAI 2530, Finanzprüfung, Stichprobenprüfung, Abschnitte 6 bis 9.
15 ISSAI 2530, Finanzprüfung, Stichprobenprüfung, Abschnitte 6 bis 9.

das Risiko späterer Änderungen zu verringern.

6.13 Die IS Prüfungsunterlagen können aufbewahrt und vor jeder Änderung und unbefugten Löschung geschützt werden. ORKBn können neue Standards für die Aufbewahrung von IS-Prüfungsunterlagen entwickeln oder bestehende Standards anpassen, um die Anforderungen an die Aufbewahrung von IS-Prüfungsunterlagen zu erfüllen. Die so festgelegte Aufbewahrungsfrist hängt vom Mandat der einzelnen ORKB und der Satzung(en) ab, die ihre Tätigkeit regelt. Besondere Aufmerksamkeit kann den Medien, dem Format, der Lebenserwartung und den Speicheranforderungen an diese Daten geschenkt werden, um sicherzustellen, dass die Daten innerhalb des in der Richtlinie der jeweiligen ORKB zur Datenspeicherung und -archivierung festgelegten Zeitrahmens lesbar sind. Dies kann die Konvertierung von Daten von einem Format in ein anderes erfordern, um mit dem technologischen Fortschritt und der Veralterung Schritt zu halten.

6.14 Im Falle der Prüfung von technischen Berichten, die von externen Wirtschaftsprüfern zu technologiebezogenen Themen erstellt wurden, können die Wirtschaftsprüfer geeignete Verfahren einführen, um die Zuverlässigkeit, die finanziellen oder die Leistungsaspekte dieser Berichte zu gewährleisten[16]. Vertraut man aufgrund dieser Verfahren auf den Inhalt dieser Berichte, so kann die Tatsache des Vertrauens angemessen offengelegt werden.

6.15 Die ISSAI sehen vor, dass die Wirtschaftsprüfer während des gesamten Prüfungsprozesses eine wirksame Kommunikation herstellen und das geprüfte Unternehmen über alle Fragen im Zusammenhang mit der Prüfung auf dem Laufenden halten sollten (vgl. ISSAI 100 Absatz 43). Bei Prüfungen, die IS-Prüfungsarbeiten beinhalten, kann das Ergebnis der IS-Prüfung in einigen Fällen dem Unternehmen durch ein separates Schreiben mitgeteilt werden. In diesen Fällen kann es wichtig sein, zu erläutern, wie sich das Ergebnis der Prüfungsarbeit auf andere Mitteilungen bezieht, die Teil derselben Finanz-, Leistungs- oder Konformitätsprüfung sind, und wie die Ergebnisse der IS-Prüfungsarbeit für den daraus resultierenden ORKB-Prüfbericht relevant sein können.

16 Wenn der Umfang im Rahmen der Finanzprüfung liegt, können die Wirtschaftsprüfer die ISSAI 2402 Prüfungsüberlegungen in Bezug auf ein Unternehmen unter Verwendung einer Serviceorganisation verwenden

7 BERICHTERSTATTUNG ÜBER DIE IS-PRÜFUNG

7.1 Da es sich bei einem Prüfungsauftrag entweder um eine Finanzprüfung (ISSAI 200), eine Wirtschaftlichkeitsprüfung (ISSAI 300) oder eine Konformitätsprüfung (ISSAI 400) handeln würde, können Wirtschaftsprüfer die Berichtspflichten entsprechend berücksichtigen. Dies wäre ORKB-spezifisch. Ebenso kann jede ORKB ihre eigenen Meldeschwellen haben, die auf der Wesentlichkeit der Prüfungsergebnisse basieren. Ebenso kann ein Wirtschaftsprüfer bei der Berichterstattung über einen IS-Prüfungsauftrag die gesetzlichen und internen Beschränkungen für die Offenlegung finanzieller und technischer Informationen berücksichtigen.

7.2 Wirtschaftsprüfer sind sich möglicherweise der Notwendigkeit, die Verwendung von Fachjargon zu beschränken, und der Sensibilität der im Bericht enthaltenen Informationen (z.B. Passwörter, Benutzernamen, Ausweis und persönliche Daten) bewusst. Trotz des technischen Charakters einer IS-Prüfung können die Wirtschaftsprüfer sicherstellen, dass der Bericht für die Geschäftsleitung des geprüften Unternehmens, die Interessenvertreter und die breite Öffentlichkeit vollständig verständlich ist. Die Wirtschaftsprüfer können ein entsprechend detailliertes Glossar der Begriffe in Berichte aufnehmen, das auf die Definition eines Akronyms oder eines Begriffs mit einer szenariobasierten Erklärung, wie dies in einer kontrollierten Umgebung funktioniert, verweist.

7.3 Wirtschaftsprüfer können die potenziellen negativen Auswirkungen des Berichts berücksichtigen, sobald der IS-Prüfbericht veröffentlicht ist. Wenn beispielsweise der IS-Prüfbericht einige Sicherheitsrisiken im Informationssystem eines geprüften Unternehmens feststellt und diese gemeldet werden, bevor notwendige Kontrollen zur Minderung der Risiken ergriffen wurden, kann die

Schwachstelle des Informationssystems der Öffentlichkeit zugänglich gemacht werden. In einem solchen Szenario können Wirtschaftsprüfer Optionen wie die Berichterstattung erst nach der Verabschiedung der erforderlichen Kontrollen oder die unvollständige Berichterstattung über das genaue Sicherheitsrisiko in Betracht ziehen, um mögliche nachteilige Auswirkungen auf das geprüfte Unternehmen zu vermeiden.

8 FOLLOW UP

8.1 Da ein Prüfungsauftrag für Informationssysteme aus einer oder mehreren der Hauptarten der Prüfung stammt, können Wirtschaftsprüfer die Folgeanforderungen für solche Prüfungsaufträge als gleichwertig mit denen für die Finanzprüfung (ISSAI 200), die Wirtschaftlichkeitsprüfung (ISSAI 300) und die Konformitätsprüfung (ISSAI 400) betrachten.