Topical Requirements – Praktische Anwendungstipps und Hinweise aus der Externen Qualitätsbeurteilung

Management Summary

Das Institute of Internal Auditors (IIA) hat mit der Einführung der Global Internal Audit Standards 2024 (nachfolgend «Standards») ein neues verpflichtendes Element als Bestandteil des «International Professional Practices Framework» (IPPF) geschaffen: die «Topical Requirements» (TR). Diese definieren einen verbindlichen Mindestumfang für Prüfungen in bestimmten Risikobereichen und zielen darauf ab, weltweit einheitliche Qualitätsstandards für interne Prüfungen sicherzustellen.

Im Jahr 2026 treten die ersten TR in Kraft. Interne Revisionen sind dadurch gefordert, ihre Planungs- und Prüfungsprozesse entsprechend auszurichten. Das IIA stellt hierzu mehrere offizielle Unterlagen bereit, die zentrale Fragen klären und die praktische Umsetzung unterstützen. Ein wesentlicher Punkt bei der Umsetzung ist, dass TR nur dann anzuwenden sind, wenn ein Thema im Rahmen der periodischen übergeordneten Risikoanalyse oder während der Risikoanalyse auf Engagement-Ebene als wesentlich eingestuft wird und eine Assurance-Prüfung zu diesem Thema geplant ist. Diese Wesentlichkeit wird im Kontext des Risikoappetits und der strategischen Ziele der Organisation beurteilt. Die Frage, ob ein TR anzuwenden ist, hängt vom Ergebnis der Risikoanalyse und dem daraus abgeleiteten Prüfumfang ab und erfordert das professionelle Urteilsvermögen der Internen Revision.

Das IIA betont ausdrücklich die Bedeutung eines nachvollziehbaren Begründungsprozesses. Wird ein TR nicht oder nur teilweise angewendet, obwohl ein wesentliches Risiko im Anwendungsbereich eines TR identifiziert wurde, muss dokumentiert werden, weshalb die jeweilige Anforderung nicht relevant ist oder nicht zur Ursache des Risikos passt.

Vor diesem Hintergrund hat die IIAS-Arbeitsgruppe «Professional Services Firms» dieses Whitepaper entwickelt. Es kombiniert Erkenntnisse aus ersten Anwendungspiloten im Schweizer Markt mit Perspektiven aus externen Qualitätsbeurteilungen. Ziel ist es, Revisionsleitungen bei der konsistenten, risikoorientierten und pragmatischen Umsetzung der neuen Vorgaben zu unterstützen. Das Dokument erhebt keinen Anspruch auf Vollständigkeit oder offizielle Verbindlichkeit. Es stellt die Meinung und Interpretation des Autorenteams und der Arbeitsgruppe zum Zeitpunkt der Veröffentlichung dar und soll als praktische Orientierungshilfe dienen.

Erste Schritte - Orientierung zu TR und offiziellen Quellen

Das IIA stellt sämtliche wesentlichen Informationen zu den TR zentral auf seiner Website zur Verfügung.

- Link zur Seite: https://www.theiia.org/en/standards/2024-standards/topical-requirements/

Diese Inhalte werden laufend aktualisiert und bilden die massgebliche Grundlage für die Anwendung der TR im Revisionsalltag. Dazu gehören die veröffentlichten TR, laufende Konsultationen sowie zukünftige Veröffentlichungen. Für jedes TR ist klar ausgewiesen, ab wann es verbindlich anzuwenden ist - in der Regel ein Jahr nach Veröffentlichung.

Die ersten TR traten bzw. treten wie folgt in Kraft:

- Cybersecurity: ab 5. Februar 2026
- Third-Party: ab 15. September 2026
- Organizational Behavior: ab 15. Dezember 2026
- Organizational Resilience: ab 30. April 2027

Neben den TR selbst stellt das IIA mehrere ergänzende Materialien bereit, die eine konsistente Anwendung unterstützen:

- Den Topical Requirements Application Guide bzw. Anwendungsleitfaden, verfügbar in mehreren Sprachen, der allgemeine und praxisnahe Anwendungshinweise liefert.
  - https://www.theiia.org/en/content/topical-requirements/topical-requirements-application-guidance
- Eine FAQ-Sektion auf der TR-Website.
- Das Dokument Assessing Topical Requirements Conformance (Insights to Quality), welches insbesondere Hinweise dazu enthält, wie TR im Kontext interner und externer Qualitätsbeurteilungen betrachtet werden und wie sich Interne Revisionsfunktionen durch sinnvolle Implementierung und transparente Dokumentation vorbereiten können.
  - https://www.theiia.org/globalassets/site/content/insights-to-quality/insights-to-quality-assessing-topical-requirements-conformance.pdf

Für Interne Revisionen empfiehlt es sich, eine strukturierte und regelmässige Überwachung aufzusetzen, um Aktualisierungen zeitnah zu berücksichtigen. Dies umfasst insbesondere:

- das frühzeitige Erkennen neuer oder überarbeiteter TR,
- die Teilnahme an Konsultationsprozessen,
- die Sicherstellung der fristgerechten Umsetzung.

Ausblick auf zu erwartende Themen

Das IIA hat weitere TR in Vorbereitung. Zum Zeitpunkt der Veröffentlichung dieses Papiers läuft der Konsultationsprozess für das TR «Anti-Corruption». Darüber hinaus ist ein TR zum Thema «Talent Management» angekündigt; der entsprechende Konsultationsprozess ist für Oktober 2026 vorgesehen. Diese beiden TR werden frühestens im Jahr 2027 anwendbar sein.

Zusätzlich stellt das IIA in Veranstaltungen und Webinaren regelmässig seinen Risiko- und Themen-Radar vor. Themen, die in der untenstehenden Grafik den Status «Mature» aufweisen (vgl. Abb. 1, blau dargestellt), gelten als etabliert; hierfür sind TR besonders wahrscheinlich.

Wichtige Themen mit hoher Dynamik, die im Radar als «Emerging» erscheinen (vgl. Abb. 1, grün dargestellt), werden derzeit nicht in TR übersetzt.

Der im vorangehenden Abschnitt empfohlene regelmässige Überwachungsprozess sollte demnach auch eine regelmässige Überprüfung der IIA-Website umfassen, um frühzeitig über neue Konsultationen sowie zukünftige TR-Themen informiert zu bleiben.

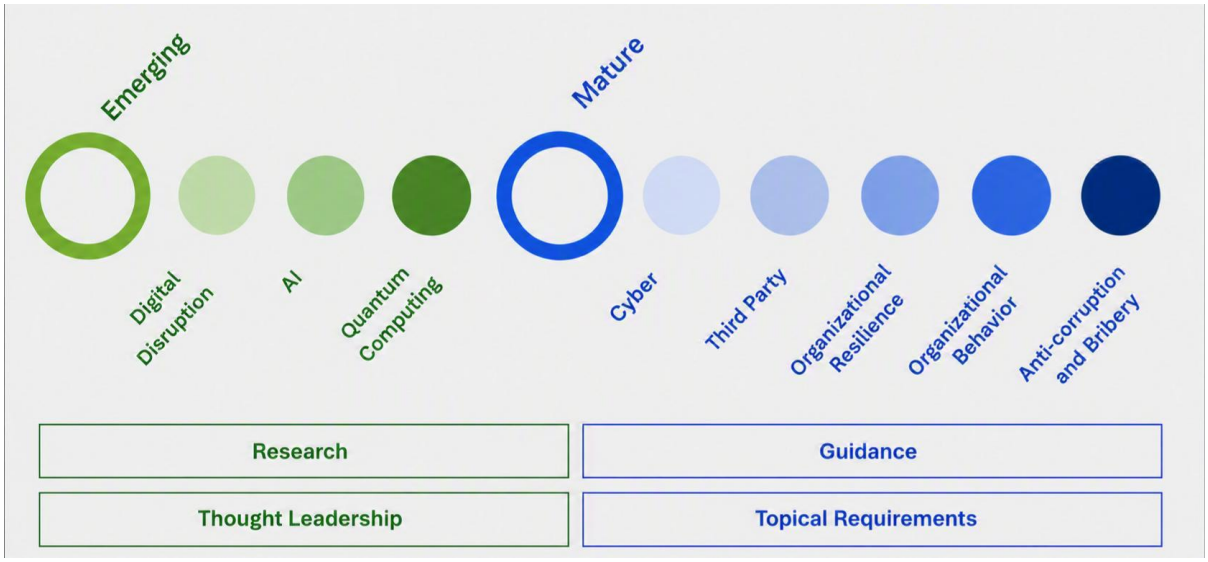

Abb. 1: Auszug aus «The IIA's risk and topics maturity radar», Quelle: IIA

Anwendung der TR

Die TR sind ein verbindlicher Bestandteil des IPPF des IIA und damit, analog zu den Standards, für Prüfungsaufträge (Assurance) verpflichtend anzuwenden. Für Beratungsaufträge in relevanten Risikobereichen wird die Anwendung empfohlen; sie ist jedoch nicht zwingend vorgeschrieben.

Der TR-Anwendungsleitfaden präzisiert, dass TR in folgenden Fällen zur Anwendung kommen:

- wenn das Thema ausdrücklich als Prüfungsauftrag im Revisionsplan enthalten ist,
- wenn das Thema während eines Prüfauftrags identifiziert wird,
- wenn das Thema in einen Prüfauftrag aufgenommen wird, auch wenn es ursprünglich nicht im Prüfungsplan vorgesehen war.

Die Identifikation von Prüfungsthemen erfolgt üblicherweise im Rahmen der periodischen Risikoanalyse (gem. Standard 9.4), während der Risikoanalyse auf Engagement-Ebene (gem. Standard 13.2) oder während der Prüfungsdurchführung. Ein TR ist anzuwenden, sobald ein entsprechendes Risiko identifiziert und als wesentlich eingeschätzt wird. Folglich sollte im Rahmen der jeweiligen Risikoanalyse geprüft werden, ob Risiken mit Bezug zu bestehenden TR vorhanden sind. Wird ein solches Thema aufgrund der Risikoanalyse, eines Stakeholder-Inputs oder während der Durchführung eines Prüfauftrags aufgenommen, ist das entsprechende TR anzuwenden.

Sobald ein Risiko als wesentlich eingestuft wird und ein TR dadurch zur Anwendung kommt, muss die Interne Revision das TR berücksichtigen. Mindestens ist eine solche Berücksichtigung auf Ebene des jeweiligen Engagements sicherzustellen. Die weiterführenden Empfehlungen des IIA legen jedoch die Basis, dass eine gesamtheitliche Betrachtung über den ganzen Prüfzyklus – von der periodischen Planung über die Engagement-Level-Planung bis zur Durchführung gemäss den entsprechenden GIAS – erfolgen kann.[1] Dies gilt auch im Falle von Co-Sourcing und Outsourcing eines Auftrags, wobei der Auftraggeber während des gesamten Lebenszyklus für die Einhaltung der Vorgaben verantwortlich bleibt.

[1] Siehe beispielsweise IIA Topical Requirements - Application Guidance, chapter 4: Applying topical requirements in the Audit Lifecycle.

Zur Unterstützung stellt die IIAS-Arbeitsgruppe einen Entscheidungsbaum zur Verfügung, der den Prozess zur Bestimmung der TR-Anwendbarkeit systematisch darstellt (vgl. Abb. 2). Er erleichtert es, die relevanten Faktoren schlüssig und konsistent zu beurteilen. Ebenso wird im Entscheidungsbaum darauf hingewiesen, in welchen Fällen eine nachvollziehbare Dokumentation des «Comply or Explain»-Ansatzes nötig ist (siehe hierzu weitere Details im nächsten Abschnitt).

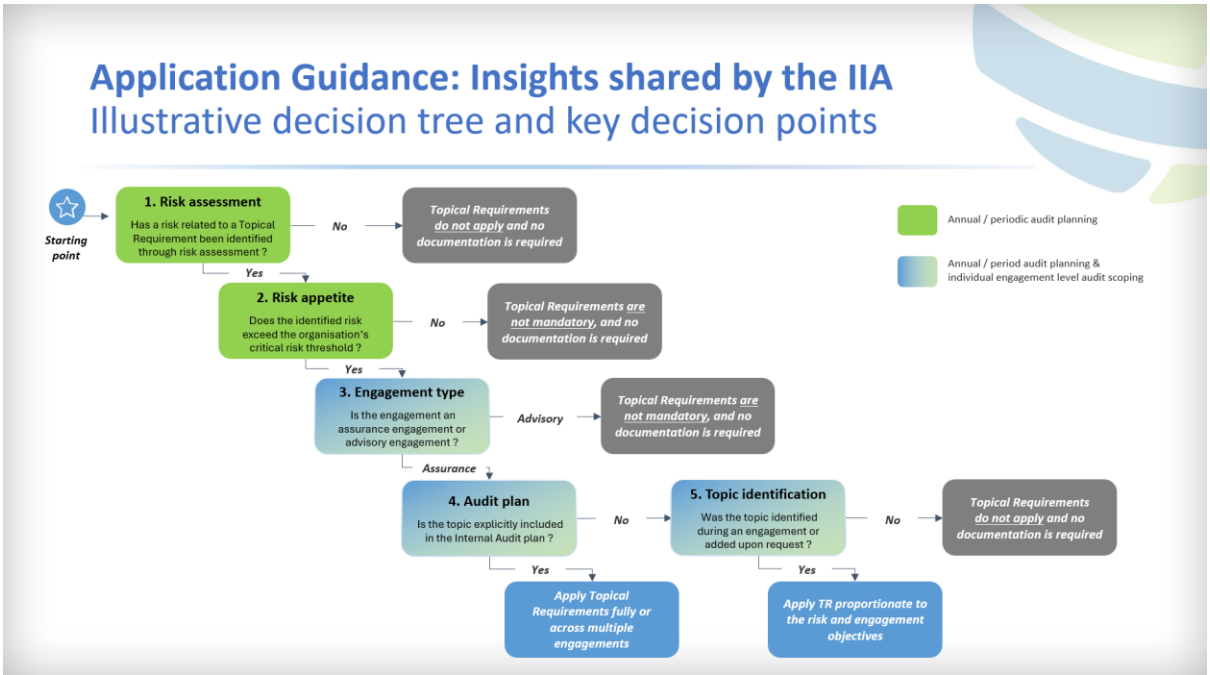

Abb. 2: Entscheidungsbaum zur Anwendung der Topical Requirements,
Quelle: IIAS-Arbeitsgruppe «Professional Services Firms»

Professionelles Urteilsvermögen bei der Anwendung

Bei allen Entscheidungen zur Anwendung der TR ist professionelles Urteilsvermögen zentral. Das IIA verweist hierbei ausdrücklich auf den «Conform or Explain»- bzw. «Comply or Explain»-Ansatz, wenn ein identifiziertes wesentliches Risiko die Anwendung eines TR obligatorisch macht und die Interne Revision dies in der Prüfung dennoch nicht berücksichtigt:

- Wenn bestimmte Anforderungen eines TR aufgrund von Art, Kontext oder Ursache eines Risikos nicht anwendbar sind, muss dies klar begründet und dokumentiert werden.
- Wenn ein Risiko beispielsweise durch eine operative Kontrollschwäche entsteht, kann es sein, dass primär kontrollspezifische Anforderungen relevant sind und bestimmte Governance-Elemente des TR nicht zur Anwendung kommen.

Der Anwendungsleitfaden betont, dass aussergewöhnliche Umstände, wie Ressourcenbeschränkungen oder sektorspezifische Besonderheiten, ebenfalls zu begründeten Abweichungen führen können. In solchen Fällen sollte die Revisionsleitung alternative Massnahmen definieren, die dem Zweck der jeweiligen Anforderung entsprechen. Ebenso können Arbeiten anderer interner und externer Assurance Provider berücksichtigt werden. Eine transparente und nachvollziehbare Dokumentation ist in diesen Fällen zwingend erforderlich.

Abdeckung der TR-Anforderungen über mehrere Jahre oder Aufträge

Wenn ein Prüfthema über mehrere Jahre hinweg bearbeitet wird, ist das entsprechende TR bei jedem Prüfauftrag erneut zu berücksichtigen und dessen Anwendbarkeit zu prüfen. TR-Anforderungen können über mehrere Prüfungen hinweg, auch über mehrere Jahre, verteilt werden, sofern klar dokumentiert ist:

- welche Elemente wann abgedeckt wurden,
- welche Teile bewusst auf spätere Jahre verschoben wurden,
- und warum diese Entscheidung fachlich vertretbar ist.

In einem Prüfauftrag müssen somit nicht immer alle Anforderungen abgedeckt sein.

Der Anwendungsleitfaden fordert, dass sämtliche Ermessensentscheidungen (z. B. zur Teil- oder Nichtanwendung) in den Planungsunterlagen, Arbeitspapieren oder Anwendbarkeitsmatrizen dokumentiert und bei Qualitätsprüfungen nachvollziehbar dargestellt werden.

Erwartungen an die Dokumentation

Die Anwendung der TR sowie die teilweise oder vollständige Nichtberücksichtigung bestimmter Elemente aufgrund fachlicher Ermessensentscheide müssen so dokumentiert werden, dass eine unabhängige Drittperson die Entscheidungen nachvollziehen kann. Die Dokumentation kann direkt an den Stellen im Audit Lifecycle vorgenommen werden, an denen die Anwendbarkeit analysiert wird (vgl. hierzu den «Entscheidungsbaum zur Anwendung der TR» in Abb. 2).

Für die Dokumentation der TR-Anwendung in der Prüfung stellen die User Guides zu den jeweiligen TR im Anhang ein optionales Dokumentationstool bzw. eine Tabelle als Hilfestellung bereit.

Bei der Beurteilung, beispielsweise im Rahmen einer Externen Qualitätsbeurteilung (EQA), ist entscheidend, dass die getroffenen Entscheidungen und deren Begründungen ausreichend dokumentiert und damit für Dritte nachvollziehbar sind. TR als integraler Bestandteil des IPPF fliessen in die Bewertung der jeweiligen Prinzipien ein, insbesondere im Rahmen von Planung, Durchführung und Kommunikation von Prüfungen. Eine gesonderte Beurteilung einzelner TR findet nicht statt.

Wenn einzelne TR für bestimmte Prüfungen relevant sind, kann ein Standard im Rahmen eines EQA nur dann als «vollständig konform» eingeordnet werden, wenn alle Elemente des zugrunde liegenden Standards eingehalten wurden.

Anwendung in Verbindung mit regulatorischen Vorschriften

Wie im offiziellen Anwendungsleitfaden des IIA erläutert, gilt:

- Wenn gesetzliche Vorschriften oder externe Regelwerke strengere oder weitergehende Anforderungen stellen als die TR, bestimmen diese Vorgaben den Prüfungsumfang.

In solchen Fällen hat die Interne Revision einen risikobasierten und vergleichenden Ansatz zu wählen, bei dem regulatorische Anforderungen, TR sowie andere anerkannte Rahmenwerke miteinander abgeglichen werden.

Zu beachten ist, dass TR keine Vorgaben zur organisatorischen Ausgestaltung der geprüften Themen machen, sondern den Prüfungsansatz definieren. Ihr Zweck besteht darin, in kritischen Prüfbereichen ein konsistentes Vorgehen sicherzustellen und die verbindliche Einhaltung grundlegender Qualitätsanforderungen zu fördern.

Berichterstattung von TR-Aspekten

Die Einhaltung der TR muss im Rahmen der Prüfungsplanung und -durchführung dokumentiert werden und wird zusätzlich durch das Quality Assurance and Improvement Program (QAIP) der Internen Revision überwacht.

Eine gesonderte Berichterstattung zur TR-Konformität (bspw. an die Geschäftsleitung und/oder den Verwaltungsrat) ist nicht notwendig. Diese Aspekte sind vielmehr implizit in der allgemeinen Berichterstattung zum QAIP zu berücksichtigen.

Hilfestellung für EQA-Assessoren

Für EQA-Assessoren stellen die offiziellen Inhalte des IIA - insbesondere die auf der Website verfügbaren Materialien - zentrale Orientierungspunkte dar. Sie definieren die Erwartungshaltung des IIA zur Implementierung der TR sowie zur Beurteilung der Konformität im Rahmen von Qualitätsprüfungen. Besonders hervorzuheben ist das Dokument «Assessing Topical Requirements Conformance» (Insights to Quality), das detaillierte Hinweise zur TR-Anwendung bereitstellt.

Topical Requirements sind eine verpflichtende Komponente des IPPF und werden deshalb im Rahmen interner wie externer Qualitätsbeurteilungen analog zu anderen Elementen des IPPF, etwa den Standards, beurteilt. Das Quality Assessment Manual 2024 des IIA hält fest, dass Assessoren den risikobasierten Prüfungsplan dahingehend überprüfen sollen, ob TR, die im Prüfungszeitraum in Kraft waren, korrekt berücksichtigt wurden. Diese Prüfung erfolgt typischerweise unter anderem durch Einsicht in die Arbeitspapiere auf Ebene der einzelnen Prüfungen.

Das Dokument «Assessing Topical Requirements Conformance» verdeutlicht, wie interne Revisionsfunktionen und Assessoren bei der Bewertung der TR-Konformität vorgehen sollten. Für Interne Revisionen empfiehlt das IIA in diesem Kontext insbesondere:

- Integration der TR in Planungs- und Prüfprozesse,
- Transparente Dokumentation der Anwendbarkeit sowie Begründungen für Fälle der Nichtanwendung,
- Sicherstellung, dass Prozesse, Arbeitspapiere und Dokumente auf Ebene der Prüfaufträge die TR-Konformität nachvollziehbar widerspiegeln.

So werden Assessoren – je nach Umsetzung der TR in den einzelnen Revisionsfunktionen – die verschiedenen Elemente im Audit-Prozess bei der Analyse des Audit-Universums, der Risikoanalyse sowie des IR-Planungsprozesses berücksichtigen und beurteilen, ob Themen vorliegen, die durch TR abgedeckt werden.

Zu den massgeblichen Dokumenten, die Assessoren heranziehen, gehören unter anderem:

- Risikoanalyse und Prüfplan (periodische Planung sowie auf Prüfauftrag-Ebene),
- Planungsmemos und Arbeitspapiere auf Prüfauftrag-Ebene,
- Risiko-Kontroll-Matrizen,
- TR-User-Guide «Documentation Tool» bzw. die entsprechende Checkliste,
- Abdeckung der TR im QAIP.

Fokus Cyber-TR: Überblick über zu prüfende Gebiete

- **Governance:** Beurteilung der strategischen Steuerung und strukturellen Verankerung. Geprüft wird:
  - Existenz einer formellen Cybersicherheitsstrategie, die regelmässig aktualisiert und vom Verwaltungsrat (inkl. Budgetfreigabe) auditiert wird.
  - Etablierung klarer Richtlinien sowie die Definition von Rollen und Verantwortlichkeiten innerhalb der Organisation.
  - Sicherstellung und Beurteilung der notwendigen Fachkenntnisse und Fähigkeiten der zuständigen Mitarbeitenden.
  - Stakeholder-Management: aktive Einbindung der Anspruchsgruppen (GL, HR, Legal, Compliance und Lieferanten) in den Dialog über Bedrohungen und Schwachstellen.
- **Risikomanagement:** Überprüfung der Prozesse zur Beherrschung von Cyberrisiken. Geprüft wird:
  - Systematische Identifikation, Analyse, Minderung und Überwachung von Cyberbedrohungen über alle Organisationseinheiten hinweg.
  - Klare Zuweisung von Zuständigkeiten für die laufende Überwachung und das Reporting der Risikosituation.
  - Etablierte Prozesse zur schnellen Eskalation bei Schwellenwertüberschreitungen sowie Massnahmen zur Förderung des allgemeinen Risikobewusstseins.
  - Validierung eines Reaktions- und Wiederherstellungsprozesses (Erkennung, Eindämmung, Nachbereitung), der regelmässig beübt wird.
- **Kontrollprozesse:** Es wird geprüft, ob interne sowie lieferantenbasierte Kontrollen bestehen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten zu schützen. Dies umfasst unter anderem:
  - Ein Lebenszyklusmanagement aller IT-Assets (Hardware, Software, externe Dienstleistungen) von der Auswahl bis zur Ausserbetriebnahme.
  - Eine kontinuierliche Überwachung von Schwachstellen sowie Talentmanagement zur Förderung technischer Kompetenzen.
  - Prozesse zur Stärkung der IT-Sicherheit, einschliesslich Verschlüsselung, Patch-Management, Zugriffsverwaltung, Softwareentwicklung (DevSecOps) sowie Konfiguration.
  - Netzwerkkontrollen, wie Netzwerksegmentierung, Firewalls, VPN/Zero-Trust-Zugänge (ZTNA), IoT-Kontrollen und Angriffserkennungs- sowie Abwehrsysteme (IDS/IPS).
  - Endpunkt-Sicherheit für Dienste wie E-Mail, Browser, Videokonferenzen und Cloud-Anwendungen.

Organisation und Planung einer Prüfung am Beispiel der Cyber-TR

Auslöser für die Prüfung

Die TR-Anforderungen müssen grundsätzlich angewendet werden, sobald das Thema Cybersecurity im Rahmen der periodischen Risikoanalyse als wesentliches Risiko identifiziert wird und hierfür eine Assurance-Prüfung geplant ist. Dies gilt, wenn das Thema ausdrücklich im Revisionsplan enthalten ist, wenn es im Rahmen eines anderen Prüfauftrags als wesentliches Risiko auftritt oder wenn ein zusätzlicher, nicht geplanter Prüfauftrag von Anspruchsgruppen angefragt wird.

Bei der Detailplanung des Prüfungsauftrags muss zwingend belegt werden, dass die einzelnen Anforderungen des TR auf ihre Anwendbarkeit geprüft wurden. Wird entschieden, gewisse Elemente nicht oder nur teilweise in den Prüfungsumfang aufzunehmen, muss diese Abweichung begründet und dokumentiert werden. Diese Begründung kann auch zusammenfassend, beispielsweise für einen der drei Bereiche des TR - Governance, Risikomanagement, Kontrollprozesse - erfolgen, wenn etwa Governance-Aspekte aus einem nachvollziehbaren Grund (z. B. Prüfung durch einen anderen Assurance Provider, Aufnahme in die Mehrjahresplanung o. Ä.) nicht Bestandteil der geplanten Prüfung sein sollen.

Es ist nicht zwingend erforderlich, dass eine einzelne Prüfung alle Cybersicherheitsanforderungen auf einmal abdeckt. Eine fokussierte Prüfung kann aus verschiedenen Gründen ratsam sein, da insbesondere im Fall der Cyber-TR eine allumfassende Prüfung logistisch und technisch nur schwer darstellbar ist. Die Interne Revision kann die Anforderungen auf mehrere Prüfungen und über mehrere Jahre verteilen. Voraussetzung hierfür ist jedoch, dass dokumentiert wird, welche Themen wann abgedeckt wurden, welche Aspekte bewusst auf spätere Zeitpunkte verschoben wurden und warum dies fachlich vertretbar ist. Die Anwendung der Anforderungen muss zudem in den Planungsunterlagen und Arbeitspapieren für Dritte transparent und nachvollziehbar dargestellt werden.

Prüfplanung

Das IIA orientiert sich in den Cyber-TR inhaltlich stark an etablierten Standards. Das TR für Cybersecurity verweist gleich zu Beginn direkt auf das National Institute of Standards and Technology (NIST), um die grundlegenden Definitionen von Cybersicherheit und Informationssicherheit festzulegen. Zudem fordern die TR, dass die Interne Revision einen vergleichenden Ansatz wählen sollte, insbesondere wenn bereits regulatorische Anforderungen bestehen bzw. Prüfungen in Anlehnung an international anerkannte Frameworks durchgeführt werden. Eine Ausrichtung der Prüfplanung am NIST-Framework entspricht somit genau diesem Gedanken.

Beispiel einer Prüfplanung über einen Drei-Jahres-Zeitraum entlang der Mindestanforderungen:

Jahr	NIST-Kernfunktion	Fokus gemäss TR-Cybersecurity	Konkrete Prüfungsziele und TR-Anforderungen
Jahr 1	Identify (Identifizieren)	Governance und Fundament (Teile des Risikomanagements und der Kontrollen)	Strategie und Rollen: Vorhandensein einer formellen Strategie, Definition von Verantwortlichkeiten und Einbezug von Anspruchsgruppen.

			Risikoidentifikation: Prozesse zur Analyse von Cyberbedrohungen quer durch die Organisation. Asset Management: Cybersecurity im Lebenszyklus aller IT-Assets (Hardware, Software, Vendoren).
Jahr 2	Protect (Schützen)	Präventive Kontrollprozesse (Kontrollen & spezifisches Risikomanagement)	System- und Netzwerksicherheit: Zugriffsverwaltung, Verschlüsselung, Patch-Management, DevSecOps. Infrastruktur: Netzwerkkontrollen (Firewalls, ZTNA, Segmentierung) und Endpunkt-Sicherheit (E-Mail, Cloud, Browser). Menschlicher Faktor: Talentmanagement zur Erhaltung technischer Kompetenzen und Sensibilisierung der Mitarbeitenden.
Jahr 3	Detect, Respond, Recover (Erkennen, Reagieren, Wiederherstellen)	Überwachung und Ereignisbewältigung (verbleibende Kontrollen und Risikomanagement)	Überwachung: Kontinuierliche Überwachung von Schwachstellen sowie Einsatz von Intrusion-Detection-/Prevention-Systemen (IDS/IPS). Eskalation: Prozesse zur schnellen Meldung inakzeptabler Risiken an das Management. Vorfallsbewältigung: Implementierter und regelmässig getesteter Incident-Response- und Recovery-Prozess (Erkennung, Eindämmung, Wiederherstellung, Nachbereitung).

Dieses Whitepaper wurde durch die Arbeitsgruppe der Professional Services Firms des IIA Switzerland erarbeitet. Die Co-Autoren Urgent Azizi, Markus Berger, Christian Jung und Markus Pfeiler haben dabei Meinungen weiterer Personen und des IIA Switzerland abgeholt und einfliessen lassen. Das Whitepaper hat zum Ziel, Interne Revisor:innen bei der Umsetzung der Topical Requirements zu unterstützen und soll als Orientierungshilfe dienen.