Tel. +41 44 444 35 55
Fax +41 44 444 35 35
www.bdo.ch

BDO AG
Schiffbaustrasse 2
8031 Zürich

Verein Schweizerische Städte- und Gemeinde-Informatik SSGI
Herr Lukas Fässler
Zugerstrasse 76 B
6340 Baar

17. November 2020

Beurteilung der Existenz des IKS in der IT bei der Anwenderorganisation nach OR 728a/PS 890 unter Verwendung einer ISO 27001-Zertifizierung

Sehr geehrter Herr Fässler

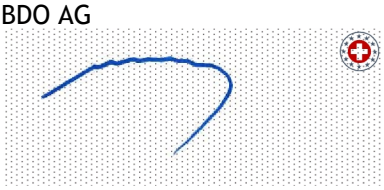
An unserem gemeinsamen Workshop vom 19. Juni 2020 haben wir die Abdeckung eines internen Kontrollsystems (IKS) in der IT nach OR Art. 728a und Schweizer Prüfungsstandard (PS) 890 durch eine ISO 27001:2013-Zertifizierung behandelt. Insbesondere ging es darum, das IKS in der IT einer Anwenderorganisation anhand einer ISO 27001:2013-Zertifizierung des IT-Dienstleistungserbringers zu beurteilen. Das Ergebnis dieses Workshops ist insbesondere in Kapitel 2 «Kontrollziele des IKS in der IT» dokumentiert.

Zusammengefasst kann für die Beurteilung der Existenz des IKS in der IT einer Anwenderorganisation unter gewissen Voraussetzungen auf eine ISO 27001:2013-Zertifizierung abgestützt werden. Diese Voraussetzungen sind in einem Leitfaden zum Umgang mit einer ISO 27001-Zertifizierung in der Beurteilung des IKS in der IT festgehalten (siehe Kapitel 3 «Vorgehen zur Beurteilung des IKS in der IT bei einer Anwenderorganisation»).

An dieser Stelle danken wir Ihnen für die Auftragserteilung und stehen Ihnen für allfällige Fragen gerne zur Verfügung.

Freundliche Grüsse

BDO AG



Martin Nay
Leiter Produktbereich Wirtschaftsprüfung

Reto S. Bürgi
Leiter IT-Prüfung (WP-Mandate)

Inhalt

1 Zusammenfassung

1.1 Ausgangslage und Ziel

Wir betrachten die Situation einer Auslagerung im Informatikbereich mit einem Dienstleistungsbezüger («Anwenderorganisation») und einem Dienstleistungserbringer, welcher die IT der Anwenderorganisation betreibt und im Bereich der Dienstleistungserbringung nach ISO/IEC 27001:2013[1] zertifiziert ist.

Dabei soll bei der Anwenderorganisation die Existenz des internen Kontrollsystems (IKS) in der IT, unter Berücksichtigung der zum Dienstleistungserbringer ausgelagerten Kontrollen, gemäss Schweizer Prüfungsstandard (PS) 890 beurteilt werden. Für die zum Dienstleistungserbringer ausgelagerten Kontrollen wird, wenn möglich, auf Kontrollen aus dessen ISO 27001-Zertifizierung abgestützt.

1.2 Ergebnis

Der Standard ISO 27001 deckt thematisch einen bedeutenden Teil der generellen IT-Kontrollen ab, die aus Sicht des Abschlussprüfers für die Beurteilung des IKS in der IT relevant sind. Für die Beurteilung des IKS nach PS 890 zur Prüfung der Existenz des IKS gemäss OR Art. 728a kann somit unter bestimmten Voraussetzungen (siehe Kapitel 3.1) auf die ISO 27001-Zertifizierung eines Dienstleistungserbringers abgestützt werden.

Zu beachten ist, dass zur Beurteilung des IKS in der IT bei einer Anwenderorganisation in aller Regel weitere Prüfungshandlungen bei der Anwenderorganisation erforderlich sind (siehe Kapitel 3.2).

Eine ISO 27001-Zertifizierung stellt keine Vergangenheitsbetrachtung im Sinne einer Abschlussprüfung dar. Die Zertifizierung kann nur zur Beurteilung bzw. Bestätigung der Existenz («design effectiveness») eines IKS hinzugezogen werden und erlaubt keine Beurteilung der Wirksamkeit der Kontrollen («operating effectiveness»).

[1] Das gesamte Dokument bezieht sich auf ISO/IEC 27001:2013. Nachfolgend wird jedoch die abgekürzte Bezeichnung «ISO 27001» verwendet.

2 Kontrollziele des IKS in der IT

In Bezug auf den PS 890 zur Prüfung der Existenz des IKS gemäss OR Art. 728a betrachten wir die Bereiche Zugriffssicherheit, Änderungswesen (Programm- und Datenbankanpassungen, Programmentwicklungen) und IT-Betrieb als relevant für eine Beurteilung des IKS in der IT. In diesem Kapitel sind die Kontrollziele sowie die Schlüsselkontrollen dieser drei Bereiche aufgeführt.

In den nachfolgenden Tabellen ist jeweils der Abgleich zwischen den Schlüsselkontrollen des IKS in der IT, einerseits zu ISO 27001 in Bezug auf den Dienstleistungserbringer und andererseits in Bezug auf die Anwenderorganisation aufgeführt. Kontrollen können zwischen Dienstleistungserbringer und Anwenderorganisation aufgeteilt sein. Ein «-» bezeichnet den Teil einer Kontrolle, die entweder beim Dienstleistungserbringer oder bei der Anwenderorganisation nicht erwartet wird. Ein «●» bezeichnet den Teil einer Kontrolle, die beim Dienstleistungserbringer erwartet wird, durch ISO 27001 jedoch nicht abgedeckt ist.

2.1 Zugriffssicherheit

2.1.1 *Benutzerauthentifizierung*

Die Systemkonfigurationen stellen eine ausreichend starke Benutzerauthentifizierung sicher, welche den internen Vorgaben der Organisation entspricht.

- Eindeutige Benutzerkennung: Jeder Benutzer hat eine eindeutige Benutzerkennung. Die Verwendung unpersönlicher Konten ist angemessen eingeschränkt.
- Passwortrichtlinie: Passwortrichtlinien stellen ausreichend sichere Passwörter sicher.
- Verfahren zur Authentifizierung: Erforderliche Authentifizierungsverfahren (Benutzername/Passwort, Multi-Faktor-Authentifizierung) sind umgesetzt.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Eindeutige Benutzerkennung	-	Vorgabe (Benutzerrichtlinie) zur Verwendung persönlicher Benutzerkonten
Passwortrichtlinie	A.9.1	Vorgabe (Benutzerrichtlinie) zur Benutzerauthentifizierung
Verfahren zur Authentifizierung	A.9.2	-
Ereignisprotokollierung (Logging)	A.12.4	-

2.1.2 *Autorisierung von Benutzerberechtigungen*

Der Zugriff auf Applikationen und Daten ist auf autorisierte Personen eingeschränkt. Zugriffberechtigungen sind funktionsgerecht zugewiesen und angemessen genehmigt.

- Berechtigungsverwaltung: ein Verfahren für die Beantragung von Berechtigungen ist etabliert.
- Autorisierung von Berechtigungen: Es ist festgelegt, wer Berechtigungen autorisieren kann.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Berechtigungsverwaltung	A.9.2.2	Vorgabe für Berechtigungen (Berechtigungs- oder Rollenkonzept), Prozess zur Beantragung/Änderung von Berechtigungen
Autorisierung von Berechtigungen	A.9.2.2	Vorgabe zur Bewilligung von Berechtigungsanträgen

Kontrolle	ISO 27001	Anwenderorganisation
Ereignisprotokollierung (Logging)	A.12.4	-

2.1.3 *Entzug von Benutzerberechtigungen*

Der Zugriff auf Applikationen und Daten ist auf autorisierte Personen eingeschränkt. Bei Funktionsänderungen werden Berechtigungen zeitnah entzogen.

- Berechtigungsverwaltung: Ein Verfahren für den Entzug von Berechtigungen ist etabliert, das die zeitnahe Deaktivierung von Berechtigungen (z.B. bei Mitarbeiteraustritt, Funktionswechsel) sicherstellt.
- Autorisierung des Berechtigungsentzugs: Es ist festgelegt, wer den Entzug von Berechtigungen veranlassen kann.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Berechtigungsverwaltung	A.9.2.6	Prozess zur Beantragung/Änderung von Berechtigungen
Autorisierung des Berechtigungsentzugs	A.9.2.6	Vorgabe zur Bewilligung des Berechtigungsentzugs
Ereignisprotokollierung (Logging)	A.12.4	-

2.1.4 *Einschränkung privilegierten Berechtigungen auf angemessene Personen*

Privilegierte Benutzerberechtigungen (System- und Benutzeradministratoren, Super User etc.) sind angemessen eingeschränkt und werden überwacht.

- Berechtigungsverwaltung: Es ist festgelegt, wer unter welchen Umständen privilegierten Berechtigungen erhält. Eine angemessene Funktionentrennung wird eingehalten, damit Kontrollen (insbesondere Anwendungskontrollen) nicht umgangen werden können.
- Überwachung privilegierter Berechtigungen: Die Verwendung privilegierter Berechtigungen wird überwacht.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Berechtigungsverwaltung (Sonderzugangsrechte)	A.9.2.3	Prozess zur Verwaltung privilegierter Berechtigungen (Berechtigungs- oder Rollenkonzept); Sicherstellen der Funktionentrennung[2]
Überwachung privilegierter Berechtigungen	•	Überwachung der Aktivitäten privilegierter Berechtigungen[2]
Ereignisprotokollierung (Logging)	A.12.4	-

2.1.5 *Einschränkung des Zugangs zu Systemressourcen*

Der Zugang zu Systemressourcen (Buchungsschema, Transaktionsdaten, Direktzugriff auf Datenbanken etc.) ist angemessen eingeschränkt und wird überwacht.

- Berechtigungsverwaltung: Es ist festgelegt, wer unter welchen Umständen Zugang mit Schreib-/Änderungsberechtigung zu Systemressourcen erhält.
- Überwachung privilegierter Berechtigungen: Der Zugriff mit Schreib-/Änderungsberechtigung auf Systemressourcen wird überwacht.

[2] Falls privilegierte Berechtigungen innerhalb der Anwenderorganisation verwendet werden.

- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Berechtigungsverwaltung (Sonderzugangsrechte)	A.9.2.3, A.9.4	Prozess zur Verwaltung von Zugriffen auf Systemressourcen[3]
Überwachung privilegierter Berechtigungen	•	Überwachung der Aktivitäten privilegierter Berechtigungen
Ereignisprotokollierung (Logging)	A.12.4	-

2.1.6 *Überprüfung der Benutzerberechtigungen*

Der Zugriff auf Applikationen und Daten ist auf autorisierte Personen eingeschränkt. Die Berechtigungen werden regelmässig überprüft und bestätigt.

- Regelmässige Überprüfung: Berechtigungen werden regelmässig überprüft und bestätigt, bzw. bereinigt.
- *Optional:* Sperrung inaktiver Accounts: Accounts, die über einen bestimmten Zeitraum nicht verwendet werden, werden deaktiviert.

Kontrolle	ISO 27001	Anwenderorganisation
Regelmässige Überprüfung	A.9.2.5	Regelmässige Bestätigung bzw. Bereinigung der Benutzerberechtigungen

2.1.7 *Zutritt zur Datenverarbeitung (Rechenzentrum)*

Der Zutritt zur Datenverarbeitung (Rechenzentrum, Serverraum) ist gesichert und auf einen angemessenen Personenkreis beschränkt.

- Zutrittsschutz (Perimeter): Datenverarbeitungseinrichtungen sind durch bauliche Massnahmen vor unberechtigtem Zugang geschützt.
- Zutrittskontrolle: Vorgaben und Verfahren stellen sicher, dass nur berechtigte Personen Zutritt zu Datenverarbeitungseinrichtungen erhalten.
- Periodische Überprüfung: Zutrittsberechtigungen und Zutritte werden regelmässig überprüft.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Zutrittsschutz (Perimeter)	A.11.1.1	-
Zutrittskontrolle	A.11.1.2	-
Periodische Überprüfung	A.11.1.2	-
Ereignisprotokollierung (Logging)	A.12.4	-

2.2 Änderungswesen

Änderungen umfassen Programmentwicklungen ("Releases") und Programmänderungen, System- und Konfigurationsänderungen.

[3] Falls innerhalb der Anwenderorganisation Änderungszugriffe auf Systemressourcen möglich sind.

2.2.1 *Autorisierung der Änderung*

Alle Änderungen werden unter Einhaltung der Funktionentrennung durch die dafür zuständige Stelle genehmigt, um unberechtigte Änderungen zu verhindern.

- Beauftragung: Es ist festgelegt, wer (berechtigte Funktionen/Personen) eine Programmänderung beauftragen kann.
- Änderungsverfahren: Ein Verfahren zur Beauftragung und Genehmigung von Änderungen unter Sicherstellung angemessener Funktionentrennung ist etabliert.

Kontrolle	ISO 27001	Anwenderorganisation
Beauftragung	A.12.1.2	Vorgabe zur Beauftragung
Änderungsverfahren	A.14.2	Verfahren seitens Anwenderorganisation

2.2.2 *Testen der Änderung*

Alle Änderungen werden angemessen getestet, um unbeabsichtigte Änderungen zu verhindern.

- Getrennte Testumgebung: Eine von der Produktion und Entwicklung getrennte Testumgebung wird verwendet.
- Änderungstests: Änderungen werden anhand von Vorgaben (Testfällen) getestet. Die Durchführung und Ergebnisse der Tests werden aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Getrennte Testumgebung	A.12.1.4	-
Änderungstests	A.14.2.9	Festlegen der Testfälle, Durchführung von Anwendertests und Testprotokollierung

2.2.3 *Abnahme der Änderung*

Alle Änderungen werden von den verantwortlichen Stellen (z.B. Fachbereich) genehmigt, damit keine ungeprüften Änderungen erfolgen.

- Änderungsabnahme: Änderungen werden durch die verantwortliche Stelle abgenommen und freigegeben. Die Abnahme wird aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Änderungsabnahme	A.14.2.9	Abnahme und Freigabe durch die verantwortliche Stelle

2.2.4 *Produktivsetzung der Änderung*

Nur genehmigte Änderungen werden unter Berücksichtigung der Funktionentrennung produktiv gesetzt.

- Produktivsetzung: Ein etabliertes Verfahren stellt sicher, dass nur abgenommene Änderungen in die Produktion überführt werden.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Produktivsetzung	A.12.1.2, A.14.2.9, A.12.5.1	-

2.3 IT-Betrieb

2.3.1 *Backupdurchführung und Überwachung*

Alle finanzrelevanten Systeme und Daten werden anhand eines auf die Geschäftsanforderungen abgestimmten Planes gesichert, um ihre Wiederherstellung im Fall von Integritätsproblemen oder Systemausfällen sicherzustellen.

- Backupkonzept: Das Sicherungskonzept ist gemäss Vorgaben dokumentiert und umgesetzt.
- Überwachung der Backupdurchführung: Die Durchführung von Backups wird überwacht und Abweichungen werden zeitnah gelöst.
- Ereignisprotokollierung: Die relevanten Vorgänge werden automatisch aufgezeichnet.

Kontrolle	ISO 27001	Anwenderorganisation
Backupkonzept	A.12.3	Vorgaben (z.B. SLA, Service-Katalog)
Überwachung der Backupdurchführung	A.12.3	-

2.3.2 *Backupauslagerung*

Backupmedien werden gemäss Vorgaben regelmässig, an einen ausreichend entfernten und sicheren Ort, ausgelagert. Die Auslagerung ist auf die Geschäftsanforderungen abgestimmt.

- Regelmässige Auslagerung: Backups werden gemäss einem festgelegten Plan ausgelagert.

Kontrolle	ISO 27001	Anwenderorganisation
Regelmässige Auslagerung	A.12.3	Vorgaben (z.B. SLA, Service-Katalog)

2.3.3 *Wiederherstellungstest*

Die Wiederherstellung von Kernanwendungen (bzw. deren Datenbeständen) wird regelmässig getestet.

- Regelmässiger Wiederherstellungstest: Die Wiederherstellung der Anwendungen und Daten ab Backup wird gemäss Vorgaben regelmässig getestet.

Kontrolle	ISO 27001	Anwenderorganisation
Regelmässiger Wiederherstellungstest	A.12.3	Vorgaben (z.B. SLA, Service-Katalog); inhaltliche Überprüfung der erfolgten Wiederherstellung

2.3.4 *Planung und Überwachung der automatischen Verarbeitung*

Die automatische Verarbeitung von Daten (Batch Jobs, Schnittstellen etc.) wird geplant und überwacht. Abweichungen werden identifiziert und zeitnah behoben.

- Planung, Genehmigung automatischer Verarbeitung: Automatische Verarbeitungen sind dokumentiert. Änderungen (z.B. am Ablauf oder der Umsetzung) folgen einem kontrollierten Verfahren und werden angemessen genehmigt/abgenommen.
- Überwachung und Behandlung von Abweichungen: Die automatische Verarbeitung wird überwacht, Abweichungen werden aufgezeichnet und zeitnah behandelt.

Kontrolle	ISO 27001	Anwenderorganisation
Planung, Genehmigung automatischer Verarbeitung	•	Verfahren zur Planung und Genehmigung automatischer Verarbeitung
Überwachung und Behandlung von Abweichungen	•	Überwachung automatischer Verarbeitung und Aufzeichnung/Behandlung von Abweichungen

2.4 Zuständigkeiten

Die folgenden zwei Abschnitte fassen die Kontrollen unter deren Zuständigkeiten (Anwenderorganisation oder Dienstleistungserbringer) zusammen, wie sie in den Kapiteln 2.1, 2.2 und 2.3 aufgeführt sind.

2.4.1 *Kontrollen bei der Anwenderorganisation*

Kontrollhandlungen an der Schnittstelle zwischen Fachbereichen und der IT sind in der Regel bei der Anwenderorganisation verortet. Dies umfasst vor allem Vorgaben und Aufträge an die IT. Nachfolgend fassen wir diese Kontrollen bzw. Kontrollteile zusammen.

Zugriffssicherheit

- Vorgaben zur Benutzerauthentifizierung
- Vorgaben zur Verwendung von Benutzerkonten
- Definition und Genehmigung eines Benutzer-Berechtigungs- oder Rollenkonzepts (u.a. unter Berücksichtigung von Benutzerrollen, privilegierten Berechtigungen, Funktionentrennung)
- Prozess zur Änderung von Benutzerberechtigungen inkl. Beantragung und Bewilligung
- Einhaltung der Funktionentrennung
- Regelmässige Überprüfung der Benutzerberechtigungen

Änderungswesen

- Änderungsprozess mit Beauftragung, Benutzertests und Benutzerabnahme/-Freigabe
- Änderungsbeauftragung
- Durchführen von Benutzertests und Benutzerabnahmetests ("UAT")
- Benutzerfreigabe von Änderungen für die Produktion

IT-Betrieb

- Vorgaben für die Backupdurchführung, die Backupauslagerung und regelmässige Wiederherstellungstests
- Planung und Genehmigung automatischer Datenverarbeitung
- Vorgaben für die Überwachung und Behandlung von Fehlern der automatischen Verarbeitung oder Durchführung der Überwachung und Behandlung von Fehlern

2.4.2 *Kontrollen beim Dienstleistungserbringer*

Der Dienstleistungserbringer betreibt die IT bzw. führt die Kontrollhandlungen in der IT im Auftrag der Anwenderorganisation durch. Die nachfolgend aufgeführten Kontrollen bzw. Kontrollteile sind in der Regel beim Dienstleistungserbringer angesiedelt. Zusätzlich gekennzeichnet sind dabei Kontrollen, die nicht explizit mit ISO 27001 abgedeckt sind.

Zugriffssicherheit

- Umsetzung der Benutzerauthentifizierung gemäss Vorgaben der Anwenderorganisation
- Verfahren zur Umsetzung von Berechtigungsanträgen der Anwenderorganisation
- Verfahren zur Beantragung, Bewilligung und Umsetzung von Berechtigungen seitens des Dienstleistungserbringers (z.B. Systemkonten, Support User)
- Ereignisprotokollierung
- Regelmässige Überprüfung der Berechtigungen des Dienstleistungserbringers (Support User, Administratoren etc.)
- *Nicht im ISO 27001*: Verfahren zur Überwachung privilegierter Berechtigungen (z.B. Administratoren, Direktzugriffe auf Datenbanken)

Änderungswesen

- Umsetzung von Änderungsanträgen der Anwenderorganisation
- Bereitstellen von der Produktion getrennter Testumgebung
- Durchführung technischer Tests (u.a. Integrationstests) und Freigabe aus Sicht IT-Betrieb
- Produktivsetzen einer Änderung nach erfolgter Freigabe durch die Anwenderorganisation

IT-Betrieb

- Umsetzung des Backupkonzepts gemäss Vorgaben der Anwenderorganisation
- Überwachung der Backupdurchführung
- Auslagerung der Backups gemäss Vorgaben der Anwenderorganisation
- Durchführung von Wiederherstellungstests gemäss Vorgaben der Anwenderorganisation
- *Nicht im ISO 27001*: Konfiguration der automatischen Verarbeitung gemäss Vorgaben der Anwenderorganisation
- *Nicht im ISO 27001*: Überwachung der automatischen Verarbeitung und Fehlerbehandlung gemäss Vorgaben der Anwenderorganisation

3 Vorgehen zur Beurteilung des IKS in der IT bei einer Anwenderorganisation

Für die Beurteilung der Existenz des IKS in der IT einer Anwenderorganisation müssen sowohl die Kontrollen bei der Anwenderorganisation selbst als auch die Kontrollen beim Dienstleistungserbringer beurteilt werden. Dabei muss beachtet werden, dass Kontrollen häufig organisationsübergreifend sind und somit gewisse Teile einer Kontrolle bei der Anwenderorganisation und andere Teile beim Dienstleistungserbringer lokalisiert sind - siehe Tabellen in Kapitel 2. Diese Tabellen geben eine gemäss unserer Erfahrung typische Aufteilung der Kontrollen wieder. Im Einzelfall kann diese Aufteilung zwischen Anwenderorganisation und Dienstleistungserbringer von der obigen Darstellung abweichen.

Im vorliegenden Fall wird die bestehende ISO 27001-Zertifizierung des Dienstleistungserbringers berücksichtigt.

3.1 Kontrollen beim Dienstleistungserbringer

3.1.1 *Durch ISO 27001 abgedeckte Kontrollen*

Damit für die Beurteilung der Existenz des IKS in der IT bei der Anwenderorganisation auf eine ISO 27001-Zertifizierung des Dienstleisters abgestützt werden kann, müssen zwingend folgende Voraussetzungen erfüllt sein:

- Ein gültiges ISO 27001-Zertifikat liegt vor.
- Das ISO 27001-Zertifikat deckt die für die Dienstleistungserbringung relevanten Unternehmensbereiche[4] ab.
- Das zur ISO 27001-Zertifizierung gehörende «Statement of Applicability»[5] (Anwendbarkeitserklärung) liegt vor.
- Seit der (Re-)Zertifizierung sind keine wesentlichen Änderungen an relevanten Kontrollen erfolgt.

Für die Beurteilung des IKS in der IT bei der Anwenderorganisation muss das oben erwähnte «Statement of Applicability» konsultiert werden. Dieses gibt Aufschluss darüber, welche Kontrollen Bestandteil der ISO 27001-Zertifizierung sind. Relevante Kontrollen, die von der Zertifizierung ausgenommen sind, müssen zusätzlich geprüft werden.

3.1.2 *Kontrollen, die nicht durch ISO 27001 abgedeckt sind*

Gewisse Teile von Kontrollen des IKS in der IT einer Anwenderorganisation, die grundsätzlich beim Dienstleistungserbringer erwartet werden, werden durch ISO 27001 nicht oder nicht explizit abgedeckt (in den Tabellen in Kapitel 2 mit «●» bezeichnet). Falls diese Kontrollen relevant sind für das IKS der Anwenderorganisation, müssen diese zusätzlich beurteilt werden:

- Überwachung privilegierter Berechtigungen (siehe Kapitel 2.1.4, 2.1.5): Es soll beurteilt werden, wie der Dienstleistungserbringer seinerseits die Verwendung privilegierter Zugriffe (z.B. von System- und Benutzeradministratoren oder Zugang zu Systemressourcen) überwacht.
- Planung und Überwachung der automatischen Verarbeitung (siehe Kapitel 2.3.4): Falls relevante, automatische Verarbeitung stattfindet, z.B. Wertflüsse von Nebenbuch zu Haupt-

[4] Relevante Unternehmensbereiche zur Dienstleistungserbringung beziehen sich auf die Umgebung der für die Anwenderorganisation finanzrelevanten Anwendungen. Dies umfasst z.B. Rechenzentrumsbetrieb, Betrieb und Unterhalt der Anwendungen, Benutzeradministration für die Anwenderorganisation, Konfiguration und Entwicklung der Anwendungen.

[5] Das «Statement of Applicability» (SoA) ist eine Voraussetzung für die ISO 27001-Zertifizierung. Darin beschreibt die zertifizierte Organisation nach ISO 27001 Anhang A, welche dieser Kontrollen umgesetzt sind, nicht umgesetzt sind oder nicht anwendbar sind inkl. allfälliger Begründungen.

buch, müssen Teile der Kontrollen, die beim Dienstleistungserbringer laufen, ebenfalls beurteilt werden. Dies kann die Planung, Änderung oder Überwachung der automatischen Verarbeitung betreffen.

3.2 Kontrollen bei der Anwenderorganisation

Wesentliche Teile der im Kapitel 2 aufgeführten Kontrollen können in der Regel nicht an den Dienstleistungserbringer ausgelagert werden und müssen durch die Anwenderorganisation durchgeführt und nachgewiesen werden. Diese Kontrollen bzw. Kontrollteile sind in den Tabellen in Kapitel 2 jeweils unter «Anwenderorganisation» aufgeführt. Bei der Beurteilung des IKS in der IT einer Anwenderorganisation müssen diese Kontrollen somit bei der Anwenderorganisation selbst geprüft werden.

Die Aufstellung der Kontrollen in Kapitel 2 basiert auf einer typischen Auslagerungssituation. Zur Beurteilung des IKS in der IT bei einer Anwenderorganisation muss im Einzelfall verifiziert werden, ob Kontrollen oder Kontrollteile, die mit «-» bezeichnet sind, trotzdem für die Anwenderorganisation relevant sind und somit dort geprüft werden sollen.

Ebenso können Kontrollen oder Kontrollteile, die hier der Anwenderorganisation zugerechnet werden, im Einzelfall ebenfalls ausgelagert sein und müssen dementsprechend beim Dienstleistungserbringer geprüft werden. Dieser Fall kann z.B. auftreten, wenn nicht nur die Informatik, sondern ein ganzer Geschäftsbereich ausgelagert wird.

4 Schlussfolgerung

Das Ergebnis der vorliegenden Betrachtung ist, dass der Standard ISO 27001 thematisch einen bedeutenden Teil der generellen IT-Kontrollen abdeckt, die aus Sicht des Abschlussprüfers für die Beurteilung des IKS in der IT relevant sind. Für die Beurteilung des IKS in der IT nach PS 890 kann somit unter bestimmten Voraussetzungen auf eine ISO 27001-Zertifizierung abgestützt werden.

Eine ISO 27001-Zertifizierung stellt keine Vergangenheitsbetrachtung im Sinne einer Abschlussprüfung dar. Die Zertifizierung kann nur bei der Beurteilung bzw. Bestätigung der Existenz («design effectiveness») eines IKS hinzugezogen werden und erlaubt keine Beurteilung der Wirksamkeit der Kontrollen («operating effectiveness»).

4.1 Fazit für die Anwenderorganisation

Das IKS in der IT bei einer Anwenderorganisation erstreckt sich über Kontrollen innerhalb der Anwenderorganisation und Kontrollen beim IT-Dienstleistungserbringer. Für die Beurteilung der Existenz des IKS nach PS 890 kann für die zum Dienstleistungserbringer ausgelagerten Kontrollen auf dessen ISO 27001-Zertifizierung abgestützt werden. Eine ISO 27001-Zertifizierung deckt nicht zwingend alle relevanten, ausgelagerten Kontrollen des IKS in der IT der Anwenderorganisation ab. Daher muss der Anwendungsbereich der ISO 27001-Zertifizierung beurteilt werden und gegebenenfalls sind ergänzende Prüfungshandlungen zur Beurteilung von Kontrollen erforderlich, die nicht durch die Zertifizierung abgedeckt sind.

4.2 Fazit für den Dienstleistungserbringer

Die ISO 27001-Zertifizierung des Dienstleistungserbringers kann grundsätzlich für die Beurteilung des IKS in der IT einer Anwenderorganisation verwendet werden - natürlich unter der Voraussetzung, dass die für das IKS der Anwenderorganisation relevanten Bereiche durch die Zertifizierung abgedeckt sind.

Eine ISO 27001-Zertifizierung deckt jedoch nicht zwingend alle für das IKS der Anwenderorganisation relevanten Kontrollen beim Dienstleistungserbringer ab. Der Dienstleistungserbringer kann die Beurteilung des IKS in der IT bei der Anwenderorganisation durch das Bereitstellen von Informationen über die Ausgestaltung und Implementierung dieser Kontrollen unterstützen. Aus Kapitel 2 geht hervor, welche relevanten Kontrollen nicht explizit durch ISO 27001 abgedeckt sind; folgende Aufstellung zeigt beispielhaft, wie diese seitens des Dienstleistungserbringers nachgewiesen werden könnten - vorausgesetzt, dass die Kontrollen tatsächlich für die Anwenderorganisation relevant sind und durch den Dienstleistungserbringer durchgeführt werden:

- *Überwachung privilegierter Berechtigungen*: Das Verfahren zur Überwachung der Verwendung privilegierter Berechtigungen (Administratoren etc.) kann in einem Zugriffsschutzkonzept beschrieben sein. Die Implementierung der Kontrolle kann z.B. durch dokumentierte Überprüfung von Logdaten, durch manuelle Protokollierung, durch «Session Monitoring» nachgewiesen werden.
- *Konfiguration der automatischen Verarbeitung*: Das Verfahren zur Konfiguration der automatischen Verarbeitung kann z.B. im Änderungsverfahren dokumentiert sein; dies kann auch Teil der Dienstleistungsvereinbarung (SLA) sein. Nachgewiesen kann eine solche Kontrolle z.B. durch Änderungs-Tickets, mit Test- und Abnahmeprotokollen.
- *Überwachung der automatischen Verarbeitung und Fehlerbehandlung*: Das Verfahren zur Überwachung und Fehlerbehandlung der automatischen Verarbeitung ist typischerweise in einer Betriebsdokumentation festgehalten, auch als Teil eines SLA. Der Nachweis der Kontrolle kann über Verarbeitungs-Logs und die dokumentierte Fehlerbehandlung (z.B. in Ticket-System) erbracht werden.

Das IKS in der IT des Dienstleistungserbringers

Die in dieser Betrachtung aufgeführten Kriterien zur Beurteilung des IKS in der IT einer Anwenderorganisation anhand einer ISO 27001-Zertifizierung gelten analog für die Beurteilung des IKS in der IT des Dienstleistungserbringers selbst.

Berücksichtigt werden muss dabei, ob die finanzrelevanten Prozesse und Systeme des Dienstleistungserbringers ebenfalls unter seine ISO 27001-Zertifizierung fallen - dies ist üblicherweise nicht der Fall, falls die ISO 27001-Zertifizierung auf die dienstleistungsbezogenen Unternehmensbereiche beschränkt ist.

Falls die ISO 27001-Zertifizierung auch das IKS in der IT des Dienstleistungserbringers abdeckt, sind typischerweise (im Unterschied zur Situation mit einer Anwenderorganisation und einem Dienstleistungserbringer) auch die Kontrollen, welche in Kapitel 2.4 der Anwenderorganisation zugeordnet werden, weitgehend durch die Zertifizierung abgedeckt.