Prüfung der generellen IT-Kontrollen

Forum "IT-Themen in der Wirtschaftsprüfung"

1. Juni 2016

Roberto Ranaldo
Manager, IT Risk and Assurance

EY Building a better working world

Agenda

- Definition IT General Controls (ITGCs)
- Prüfumfang bestimmen
- Warum brauchen wir ITGCs
- Wann testen wir ITGCs
- Beispiele von ITGCs
- Auswahl von ITGCs
- Existenz- vs. Wirksamkeitsprüfung
- Zeitliche Aspekte
- Beurteilung der ITGCs
- Fragen

Definition IT General Controls (ITGCs)

Definition IT General Controls (ITGCs)

"Generelle Informatik (IT)-Kontrollen" bilden die Grundlage für ordnungsgemäss funktionierende automatisierte IT-Anwendungskontrollen. Generelle IT-Kontrollen adressieren beispielsweise Risiken in den Bereichen Zugriffsrechte, Datenqualität, Datensicherheit oder System-Änderungen (Hardware und Software) und –unterhalt[1]

1: Schweizer Prüfungsstandard: Prüfung der Existenz des internen Kontrollsystems (PS 890)

Prüfumfang bestimmen

Für welche Anwendungen prüfen wir ITGCs

Die 8 Schritte des Vorgehensmodells[2]:

Anwendungen, welche Applikationskontrollen und IT-abhängige manuelle Kontrollen unterstützen

2: Treuhandkammer, Vorgehensmodell Anwendungsprüfung, Oktober 2010

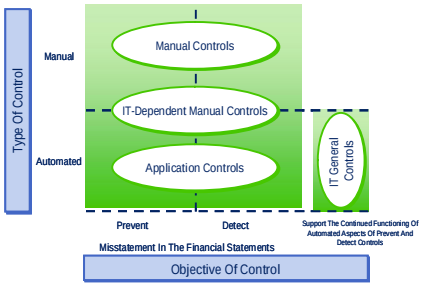
Warum brauchen wir ITGCs

Warum brauchen wir ITGCs

Durch das Testen und Beurteilen der ITGCs **unterstützen** wir die Prüfung:

- der Funktionsfähigkeit von Applikationskontrollen und IT-abhängigen manuellen Kontrollen während der Prüfungsperiode
- der Vollständigkeit und Richtigkeit von elektronischen Prüfungsnachweisen **(Information Provided by Entity, IPE)**

ITGCs sind für die verschiedenen Ebenen der IT-Umgebung relevant (Applikation, Betriebssysteme , Datenbanken)

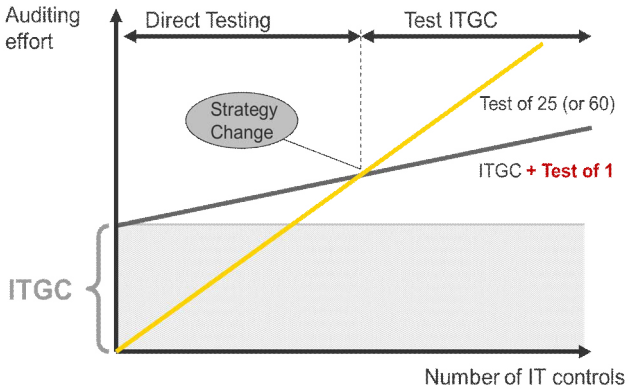


Anmerkungen zu ITGCs

- **Eine Prüfung der ITGCs alleine reicht nicht aus, um Aussagen zur Funktionsfähigkeit von Kontrollen oder zur Vollständigkeit und Richtigkeit von elektronischen Prüfungsnachweisen treffen zu können.** Nur in Verbindung mit weiteren Prüfungshandlungen (d.h. Test der Kontrollen bzw. der Elektronischen Prüfungsnachweise) ist eine Bewertung der Transaktionskontrollen oder der Elektronischen Prüfungsnachweise möglich.
- Die Prüfung der ITGCs wird dabei nicht auf Ebene der einzelnen Transaktionsklassen, sondern auf Basis von **einheitlichen IT-Prozessen** des Mandanten durchgeführt. Unterliegen die unterschiedlichen Applikationen, Schnittstellen, Datenbanken und Betriebssysteme des Mandanten einheitlichen IT-Prozessen, können die damit verbundenen ITGCs **einheitlich geprüft werden**. In diesen Fällen betreffen ITGCs die Transaktionskontrollen bzw. die IT-abhängigen manuellen Kontrollen mehrerer wesentlicher Transaktionsklassen.
- **Tests der ITGCs sind immer als „Full Test of Controls“ durchzuführen und können nicht rotiert werden.**

Wann testen wir ITGCs

Wann testen wir ITGCs



Beispiele

Beispiele von ITGCs

- Manage Change Prozess
  - Manage Change-Verfahren (Autorisierung, Test, Genehmigung)
  - Überwachung der ITGCs für die Manage Change-Kategorie
  - Funktionstrennung von unvereinbaren Funktionen für Manage Change
- Manage Access Prozess
  - Allgemeine Systemsicherheits- und Passworteinstellungen
  - Zugang zu IT-Funktionen mit weitreichenden Berechtigungen
  - Benutzerberechtigungsverwaltung
  - Überwachung der ITGCs für die Manage Access-Kategorie
  - Funktionstrennung von unvereinbaren Funktionen für Manage Access
- Manage IT Operations Prozess
  - Datensicherung und Wiederherstellung von Finanzdaten
  - Planmässige Programmverarbeitung (Scheduling)
  - Überwachung und Handhabung von Problemen und Vorfällen

Auswahl von ITGCs

Auswahl von ITGCs

- Bei der Festlegung des Prüfungsumfanges kann risikoorientiert vorgegangen werden und die Prüfungsschwerpunkte auf diejenigen Bereiche legen, in denen die Risiken für die Rechnungslegung am grössten sind
- Es liegt im Ermessen des Abschlussprüfers, welche Prüfungen in Bezug auf generelle IT-Kontrollen durchzuführen sind
- Der Prüfungsumfang soll der Grösse, Komplexität sowie dem Risikoprofil des Unternehmens Rechnung tragen

Existenz- vs. Wirksamkeitsprüfung

Existenzprüfung

Existenzprüfung (”Design and Implementation Effectiveness”): Zur Prüfung, ob eine Kontrolle existiert, stehen dem Abschlussprüfer folgende Prüfungsverfahren zur Verfügung:

- Durchsicht der Dokumentation der Ausgestaltung
- Befragung
- Beobachtung
- Überprüfung
- Walkthrough Test (Wurzelstichprobe)

Wirksamkeitsprüfung

Wirksamkeitsprüfung (”Operating Effectiveness”): Die Wirksamkeit der Kontrollen umfasst die Beurteilung, ob eine Kontrolle gemäss ihrem Design funktioniert, ob sie tatsächlich durchgeführt wurde, ob die Kontrolle vollständig durchgeführt wurde und ob die Kontrolle durch eine qualifizierte und berechtigte Person ausgeführt wurde.

Frequenz der Kontrolldurchführung	Minimale Stichprobengrösse
Täglich (mehrere Male) durchgeführt	25
Wöchentlich durchgeführt	5
Monatlich durchgeführt	2
Quartalsweise durchgeführt	2
Jährlich durchgeführt	1
Für unperiodische Kontrolldurchführungen wählen wir 10% falls die Anzahl zwischen 50 und 250 liegt, 25 falls die Anzahl bei 250 oder höher liegt und 5 falls die Anzahl bei 50 oder darunter liegt	

Zeitliche Aspekte

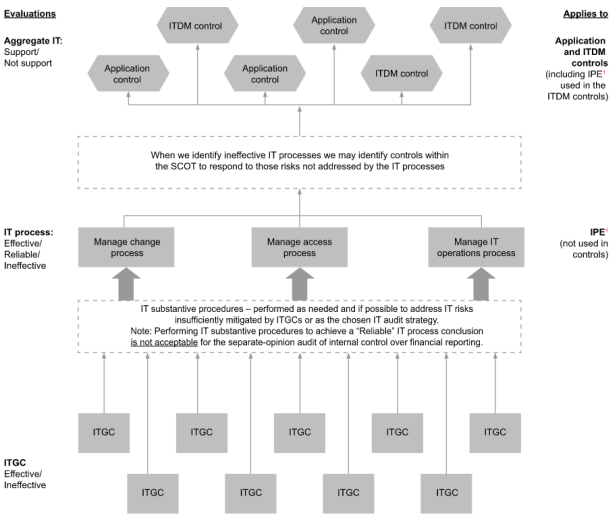
Zeitliche Aspekte

Die Berichterstattung ist auf den Stichtag der Jahresrechnung ausgerichtet. Das heisst jedoch nicht, dass die Prüfungshandlungen unmittelbar vor dem Bilanzstichtag erfolgen müssen. Es muss jedoch sichergestellt werden, dass fundamentale Änderungen zwischen dem Zeitpunkt der Prüfungshandlungen und dem Bilanzstichtag angemessen in die Beurteilung einfliessen.

Tests of Controls Completed…	Procedures to Update our Evaluation
Within 3 months of year end	▸ Inquiry. We interview appropriate officers and employees and look for evidence of reassignments of duties; changes in key personnel; the introduction of new systems, procedures, or programs; and other changes that may affect our conclusion about the continued effectiveness of specific controls. If changes are identified, we consider the effects of such changes on our evaluation and whether there is a need for additional tests of controls. ▸ Observation ▸ Additional walkthroughs not required unless evidence from our inquiries and observation indicates otherwise (e.g., significant changes in the process or key personnel)
3-6 months before year end	▸ Inquiry (see above) ▸ Observation ▸ Consider additional walkthroughs of controls (e.g., certain key controls based on the materiality and risk of a significant account and/or relevant assertions)
More than 6 months before year end	▸ Inquiry (see above) ▸ Observation ▸ Perform additional walkthroughs of controls or some additional tests of controls

Beurteilung von ITGCs

Beurteilung der ITGCs



Fragen

Thank you

Roberto Ranaldo
Ernst & Young AG
Maagplatz 1
Postfach
CH-8010 Zürich
Tel.: +41 58 286 37 10
Mobile: +41 58 289 37 10
Email: roberto.ranaldo@ch.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ey.com