Stefan Beißel

IT-Audit

Grundlagen
Prüfungsprozess
Best Practice

2., neu bearbeitete und erweiterte Auflage

ESV ERICH SCHMIDT VERLAG

ERICH
SCHMIDT
VERLAG

IT-Audit

Grundlagen
Prüfungsprozess
Best Practice

Von Dr. Stefan Beißel

2., neu bearbeitete und erweiterte Auflage

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978-3-503-19125-3

1. Auflage 2015
2. Auflage 2020

Gedrucktes Werk: ISBN 978-3-503-19124-6
eBook: ISBN 978-3-503-19125-3

Vorwort zur 2. Auflage

Das IT-Audit besitzt aufgrund der fortschreitenden Digitalisierung einen immer höheren Stellenwert. Neue technologische Fortschritte und die Zunahme an Regelwerken sind ohne ein wirksames IT-Audit nur schwer zu beherrschen. In der Folge etablieren sich auch im IT-Audit ständig neue, innovative Verfahren und Techniken. Es ist daher nicht verwunderlich, dass auch die Zertifizierungsmöglichkeiten für Auditoren immer umfangreicher werden. Die 2. Auflage dieses Buchs enthält neue Kapitel und Ergänzungen, um dieser spannenden Entwicklung im IT-Audit Rechnung zu tragen.

Moderne Unternehmen nutzen technologische Fortschritte, um ihre internen Abläufe zu optimieren – z. B. sind Cloud-Lösungen in den letzten Jahren sehr populär geworden. Das IT-Audit ist gefordert, mit dieser Entwicklung standzuhalten. Es ist ein wesentlicher Faktor, um die Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit der veränderten Abläufe zu gewährleisten. Entsprechend haben sich auch im IT-Audit neue Ansätze etabliert. Mit ihrer Hilfe können Prüfungsverfahren optimiert und mit betrieblichen Abläufen besser verknüpft werden (siehe Kapitel III Abs. 2): Integrierte Prüfstellen ermöglichen eine automatisierte Prüfung während des operativen Betriebs; eingebettete Audit-Module können in Form von integrierten Softwarekomponenten Prüfungen initiieren oder unterstützen; mit der parallelen Simulation können ausgewählte Informationsverarbeitungen simuliert und geprüft werden, ohne die produktive Umgebung zu beeinträchtigen; das agile IT-Audit bedient sich der Prinzipien aus der agilen Softwareentwicklung, um die Flexibilität und Transparenz zu erhöhen und Zwischenergebnisse schneller zu erzeugen; auch Six Sigma ist im IT-Audit nützlich – es hilft, die Qualität des Audits zu erhöhen und Prüfungsfehler zu reduzieren; sogar Ansätze aus dem Lean Management lassen sich in die Welt des IT-Audits überführen – Zeit- und Ressourceneinsatz für Prüfungen werden dadurch verringert.

Die Regelwerke für das IT-Umfeld von Unternehmen werden immer umfassender und restriktiver. Neben der Datenschutz-Grundverordnung und dem IT-Sicherheitsgesetz gibt es strenge Vorgaben im Finanz- und Versicherungssektor (siehe Kapitel II Abs. 5): Die Datenschutz-Grundverordnung soll für ein einheitliches Datenschutzrecht in Europa sorgen und ist seit Mai 2018 gültig; das IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen trat im Juli 2015 in Kraft und hat das Ziel, die Gefahr von Versorgungsstörungen zu verringern; in den Jahren 2017 und 2018 wurden detaillierte Anforderungen an die IT im Finanz- und Versicherungssektor definiert. Auch viele Standards wurden überarbeitet, z. B. der

IT-Grundschutz vom BSI im Jahr 2017. Und durch die stärkere Internationalisierung spielen Standards vom US-amerikanischen NIST eine größere Rolle.

Die zunehmende Bedeutung des IT-Audits macht sich bei Zertifizierungsorganisationen vor allem in gestiegenen Mitgliederzahlen und umfangreicheren Zertifizierungsangeboten bemerkbar (siehe Kapitel I Abs. 4.4). Beispielsweise bietet das (ISC)², das im Vergleich zum Jahr 2014 fast doppelt so viele Mitglieder besitzt, nun die Zertifizierung zum „Certified Cloud Security Professional“ an. Die GIAC hat eine ähnliche Mitgliederentwicklung zu verzeichnen und bietet sogar eine Vielzahl neuer Zertifizierungen an, sodass z. B. „Penetration Testing“ nun eine eigene Zertifizierungsdomäne darstellt.

Das IT-Audit bleibt weiterhin ein wichtiges Thema in der heutigen Industrie und ein nicht zu unterschätzender Erfolgsfaktor für fast jedes Unternehmen, bietet aber gleichzeitig auch spannende Entwicklungen gepaart mit neuen Ansätzen und Möglichkeiten für professionelle Auditoren.

Bergisch Gladbach, im Januar 2020 Stefan Beißel

Vorwort zur 1. Auflage

Informationen können einen fundamentalen Einfluss auf den Unternehmenserfolg haben. Sie sind z. B. Wettbewerbsfaktor, Machtinstrument, Alleinstellungsmerkmal oder Überlebensfaktor. Daher besitzt die IT, mit der diese Informationen gehandhabt werden, in den meisten Unternehmen einen oft unterschätzen Stellenwert.

Damit die IT wirtschaftlich effektiv genutzt wird und mit ihr verbundene Risiken reduziert werden, sollte die sichere, wirtschaftliche und ordnungsmäßige Ausübung aller IT-Aktivitäten gewährleistet werden. In vielen Unternehmen basiert die Erfüllung damit verbundener Anforderungen vornehmlich auf dem Vertrauen gegenüber zuständigen Mitarbeitern. Allerdings entstehen daraus hohe Unsicherheiten für die Stakeholder, insbesondere die Shareholder, des Unternehmens. Die Unsicherheiten ergeben sich nicht nur daraus, dass Anforderungen nicht eingehalten werden können, sondern vor allem daraus, dass sie nicht umfassend genug sind oder unbewusst und unbemerkt von ihnen abgewichen wird. Dies sollte für die Stakeholder langfristig nicht zufriedenstellend sein.

Hier kommt das IT-Audit ins Spiel, das durch die Prüfung von Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit eine hohe Transparenz für das Unternehmen und die Stakeholder schafft. Insbesondere können das Schutzniveau von Informationen und IT-Systemen, die Ausrichtung der IT am Geschäftsmodell des Unternehmens, der wirtschaftlich effiziente Umgang mit Ressourcen und die Befolgung von vorgeschriebenen Regularien oder erwünschten Standards und Best Practices überprüft werden.

Dieses Buch dient der Orientierung in die vielfältige Welt der IT-Audits und unterstützt die Wissensaufnahme durch die Verbindung von Theorien, Standards und Best Practices sowie praktisch orientierten Prüfungsinhalten.

Bergisch Gladbach, im November 2014 Stefan Beißel

Inhaltsverzeichnis

Kapitel I: Grundlagen

1 Definition des IT-Audits

Unter dem Begriff **Audit** wird im Allgemeinen ein Prozess zur Überprüfung oder Inspektion verstanden. Audits können unterschiedliche Themenbereiche betreffen, wie z. B. die Finanzberichterstattung, Sicherheit, Compliance, Governance oder Qualität mit oder ohne Schwerpunkt auf der IT. Sie haben jedoch gemein, dass die Überprüfung unabhängig und nachvollziehbar sein soll und die Ergebnisse auf angemessenen Nachweisen beruhen sollen. IT-Audits beziehen sich dabei auf den Themenbereich IT oder auf einen Ausschnitt der IT.

> Ein **IT-Audit** ist eine unabhängige Überprüfung der Einhaltung von Vorgaben und der Funktionalität von Kontrollmaßnahmen innerhalb der IT eines Unternehmens.

Die **Unabhängigkeit** soll sicherstellen, dass der Auditor von keinem Interessenkonflikt betroffen ist und einen objektiven Standpunkt besitzt. Interessenkonflikte bestehen, wenn der Auditor ein Interesse an den Ergebnissen des IT-Audits hat. Sollte der Auditor z. B. bei Design und Konfiguration von IT-Systemen mitgewirkt haben, ist er eher daran interessiert, dass im IT-Audit keine Abweichungen festgestellt werden, da seine Mitwirkung ansonsten nachträglich bemängelt werden könnte. Auch wenn der Auditor an der Behebung der festgestellten Abweichungen beteiligt ist, kann er ein besonderes Interesse besitzen. Eine geringe Anzahl an Abweichungen erspart ihm Arbeit, während eine hohe Anzahl an Abweichungen seine Verdienstmöglichkeiten erhöhen kann. Die Objektivität des Auditors kann beeinträchtigt werden, wenn seine Erfahrungen einen bestimmten Schwerpunkt oder eine hohe Eingrenzung besitzen, z. B. wenn derselbe Auditor ausschließlich dasselbe Unternehmen prüft.

Vorgaben können sowohl von internen als auch von externen Quellen stammen. Interne Vorgaben werden meist mithilfe von Leitlinien, Richtlinien, Arbeitsanweisungen und Verfahrensbeschreibungen definiert. Mit diesen Dokumenten kann das Personal zur Einhaltung von Vorgaben verpflichtet werden. Externe Vorgaben ergeben sich einerseits aus zwingenden Regelwerken, wie z. B. Gesetzen, und andererseits aus optionalen, wie z. B. Standards und Best Practices. Während die Abweichung von zwingenden Regelwerken zu Reputationsverlust und Strafen führen können, werden optionale lediglich aus eigenem Willen, z. B. zur Erreichung von Wettbewerbsvorteilen, umgesetzt. Da die Vielzahl interner und externer Vorgaben oft zu Überschneidungen führt, sollten sowohl bei der Umsetzung als

auch beim IT-Audit eine vollständige Identifikation und ein Abgleich aller relevanten Vorgaben stattfinden.

Kontrollmaßnahmen sind administrative, technische und physische Maßnahmen, welche die Einhaltung von Vorgaben oder die Erreichung von Zielen eines Unternehmens unterstützen. Durch diese werden Aktivitäten im Unternehmen gesteuert und überwacht. Der Zweck von Kontrollmaßnahmen liegt darin, Abweichungen von vorneherein zu verhindern oder so früh wie möglich zu erkennen oder zu korrigieren. Dadurch sollen unerwünschte Zustände, die zu Ineffizienzen, finanziellen Schäden oder Reputationsschäden führen können, vermieden werden.

Die **IT** eines Unternehmens umfasst aus institutioneller Sicht alle Mitarbeiter, die mit IT-Aktivitäten betraut sind, und aus funktioneller Sicht alle Aufgaben, die mithilfe von IT-Aktivitäten erfüllt werden. Unter IT-Aktivitäten sind alle Aktivitäten zu verstehen, die direkt oder indirekt der Speicherung, Übertragung oder Verarbeitung von Informationen unter Einbeziehung elektronischer Hilfsmittel dienen.

Ein verbreiteter Begriff im deutschen Sprachraum ist die **IT-Revision**, welche grundsätzlich dieselbe Bedeutung wie das IT-Audit besitzt. In der Praxis wird die IT-Revision jedoch eher aus institutioneller anstatt aus funktioneller Sicht betrachtet. Die institutionelle Sicht bezieht sich auf die Organisationseinheiten, die zur Ausführung von Aufgaben des IT-Audits geschaffen wurden, und die Personen, die diese Organisationseinheiten besetzten. Demgegenüber umfasst die funktionelle Sicht die eigentlichen Aufgaben des IT-Audits.

2 Kategorien des IT-Audits

2.1 Kategorisierungsansätze

Um ein IT-Audit einer Kategorie zuordnen zu können, muss man zunächst festlegen, aus welcher Perspektive man das IT-Audit betrachtet. Für jedes IT-Audit gilt es, im Vorfeld die Fragen zu beantworten, durch wen, was, worauf, wo, wann und warum geprüft wird. Daher ergeben sich fünf Betrachtungsperspektiven für die Kategorisierung von IT-Audits, und zwar Prüfungsvollzug, -umfang, -aspekt, -ort, -zeit und -anlass. Jede Perspektive kann dazu genutzt werden, um ein IT-Audit zu kategorisieren. Dabei kann ein IT-Audit bezüglich jeder Perspektive einer oder gleichzeitig mehrerer Kategorien zugeordnet werden.

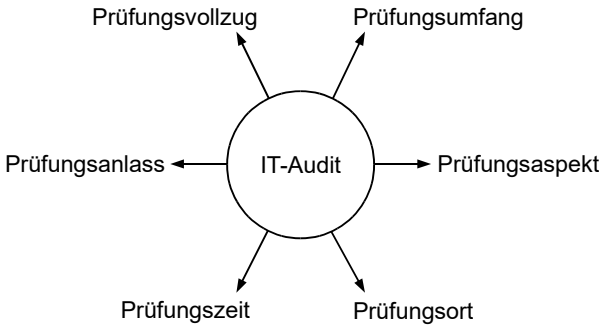

Abbildung 1: Perspektiven zur Kategorisierung von IT-Audits

2.2 Prüfungsvollzug

2.2.1 Überblick

Der **Prüfungsvollzug**, und damit die Rolle des Auditors, kann von verschiedenen Parteien wahrgenommen werden. Je nachdem welche Partei das IT-Audit vollzieht, redet man von einer 1st, 2nd und 3rd Party.

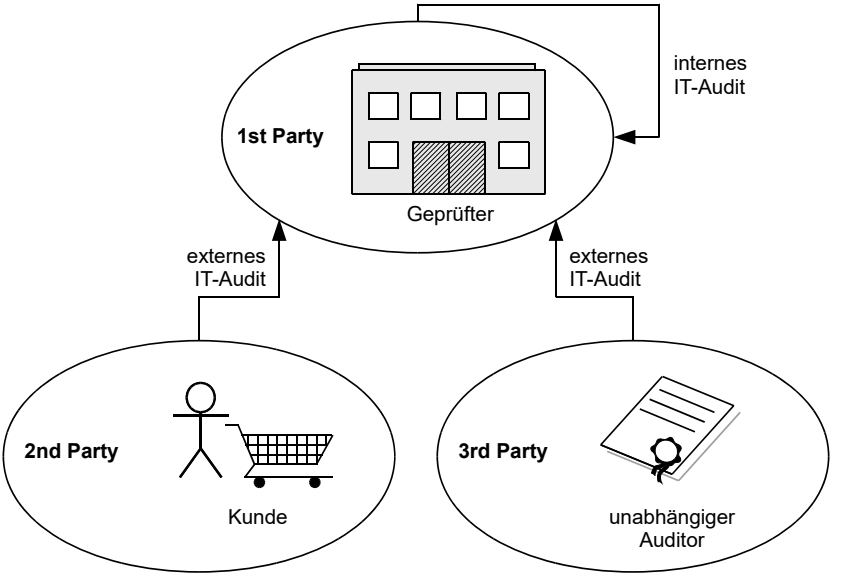

Abbildung 2: Prüfungsvollzug

2.2.2 1st Party

Die **1st Party** ist der Auditierte selbst. Das 1st Party IT-Audit wird durch den Auditierten selbst im eigenen Unternehmen durchgeführt, weshalb man auch von einem internen IT-Audit redet.

Das **1st Party IT-Audit** ist ein wichtiges Werkzeug für den Auditierten, um Kontrollmaßnahmen zu überwachen und zu beurteilen. Außerdem können die Systeme, Prozesse und das Risikomanagement des Auditierten beurteilt werden. Unzulänglichkeiten, welche z. B. die Effektivität oder Effizienz beeinträchtigen, können aufgedeckt und Empfehlungen zur Verbesserung abgeleitet werden. Dies führt insgesamt zu einer Erhöhung der Wertgenerierung beim Auditierten. Das interne IT-Audit kann dem Auditierten helfen, die Umsetzung von Regelwerken proaktiv zu überprüfen. Durch die Etablierung eines wiederkehrenden Termins für das interne IT-Audit und die Schulung von Verantwortlichen kann ein Vertrauen in die eigenen IT-Systeme geschaffen werden, das auf objektiven Nachweisen basiert. Der wiederholte Prozess des Prüfens erhöht zudem das Niveau der Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit unter dem gesamten Personal.

Die **internen Auditoren** sind häufig über einen Arbeitsvertrag als Mitarbeiter beim Auditierten beschäftigt. Organisatorisch sind sie oft einer eigenen Abteilung zugeordnet. Eine organisatorisch überlegte Zuordnung der Auditoren, z. B. als Stabstelle der Geschäftsführung, führt zu einer höheren Objektivität und Unabhängigkeit als wenn sie anderen Bereichen, z. B. der IT-Abteilung, zugeordnet werden. Objektivität und Unabhängigkeit können jedoch nicht vollständig sichergestellt werden, da die Prüfungstätigkeiten zumindest von der Geschäftsführung beeinflusst werden können. Daher haben die Prüfungsergebnisse nach außen nur eine begrenzte Aussagekraft und Akzeptanz. Folglich können z. B. keine Zertifikate ausgestellt werden, die allein auf internen IT-Audits basieren.

2.2.3 2nd Party

IT-Audits, die nicht durch den Auditierten selbst durchgeführt werden, bezeichnet man auch als externe Audits. Zu diesen zählen die 2nd und 3rd Party IT-Audits.

Die **2nd Party** ist in der Regel ein bestehender oder potenzieller Kunde des Auditierten, der Dienstleistungen erbringt, Waren bereitstellt oder dafür in Betracht gezogen wird.

Ein **2nd Party IT-Audit** wird aufgrund einer vertraglichen Vereinbarung zwischen dem Auditierten und seinem Kunden durchgeführt oder aufgrund der Absicht, neue Kunden zu gewinnen oder bestehende zu halten. Insbesondere wegen der stark verbreiteten Auslagerung von IT-Prozessen, gewinnen 2nd Party IT-Audits

zunehmend an Bedeutung. Häufig werden sie genutzt, um die initiale Auswahl des IT-Dienstleisters zu unterstützen und später kontinuierlich die Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit zu überwachen. Da der Auditierte gegenüber dem Auditor häufig die Rolle eines Lieferanten innehält, wird für das 2nd Party IT-Audit auch der Begriff Lieferantenaudit verwendet.

In der Praxis wird oft auf das 2nd Party IT-Audit verzichtet, wenn der Auditierte bereits einen Prüfungsbericht eines unabhängigen Auditors, also einer **3rd Party**, vorweisen kann. Diesen Charakter haben vor allem Zertifikate. Daher sind sie für den Auditierten nicht nur ein Werbemittel, sondern auch ein Mittel, um den Arbeitsaufwand durch IT-Audits zu reduzieren und Prozesse zu vereinfachen.

2.2.4 3rd Party

Die **3rd Party** ist eine unabhängige außenstehende Person oder Organisation, die ausschließlich für die Durchführung des IT-Audits mit dem Auditierten in Kontakt tritt und ansonsten in keiner anderen Beziehung zu ihm steht.

3rd Party IT-Audits werden häufig durch eine **Zertifizierungsstelle** durchgeführt. Das Ergebnis dieses IT-Audits ist eine nach außen vorzeigbare und anerkannte Verbriefung des Sicherheits- oder Qualitätsniveaus oder eines anderen Zustands des Auditierten, z. B. in Form eines Zertifikats.

Die 3rd Party Auditoren stellen durch die Objektivität und Unabhängigkeit ihrer Prüfungstätigkeiten das **Qualitätsniveau** ihrer Arbeit sicher, und damit die Anerkennung ihrer Professionalität im Markt. Sie vermeiden grundsätzlich jegliche Art von Interessenkonflikten. In der Regel wurden die Auditoren speziell für das IT-Audit geschult und besitzen relevante Erfahrungen oder können auf ein Netzwerk von erfahrenen Auditoren zurückgreifen. Manchmal gehen ihre Tätigkeiten über die reine Prüfung hinaus und umfassen außerdem Beratungsleistungen, die z. B. in Korrektur- und Verbesserungsvorschlägen resultieren.

2.2.5 Joint IT-Audit

Ein **Joint IT-Audit** ist ein IT-Audit, das gleichzeitig von mindestens zwei voneinander unabhängigen Parteien durchgeführt wird, um einen gemeinsamen Prüfungsbericht zu erstellen.

Die **Parteien**, die beim Joint IT-Audit die Rolle der Auditoren einnehmen, können 1st, 2nd oder 3rd Parties sein. In der Regel tendiert man jedoch zu 3rd Parties, um die **Unabhängigkeit** der Auditoren weiter zu erhöhen. Die hohe Unabhängigkeit resultiert aus Folgendem:

- Durch die Aufteilung einer **Audit-Gebühr** zwischen den Auditoren, verringert sich die wirtschaftliche Abhängigkeit des einzelnen Auditors vom Auditierten.
- **Manipulationen** durch den Auditierten werden erschwert, da es für den Auditierten schwieriger ist, zwei Auditoren anstelle nur eines Auditors zu täuschen.
- Durch den ständigen **Wechsel** der Zeitpunkte und Tätigkeiten der Auditoren, wird die Unabhängigkeit erhöht, da für den Auditierten nicht vorhersagbar ist, welcher Auditor was prüft.

Zu den **Vorteilen** des Joint IT-Audits zählen neben der höheren Unabhängigkeit auch die höhere Zuverlässigkeit und Vollständigkeit der Feststellungen. Dadurch, dass zwei Auditoren unabhängig voneinander prüfen, und damit individuell den Umfang und Inhalt der Stichproben auswählen, erhöht sich die Wahrscheinlichkeit, dass Missstände aufgedeckt werden.

Die **Nachteile** des Joint IT-Audits sind hingegen erhöhte Koordinationsaufwände und die Gefahr, dass ein Auditor zum Trittbrettfahrer des anderen Auditors wird. Andererseits kann eine zu geringe Koordination zwischen den Auditoren dazu führen, dass sie sich bei ihren Tätigkeiten gegenseitig behindern und die Qualität des Prüfungsberichts insgesamt schlechter als bei einem regulären IT-Audit ausfällt. Ein weiteres potenzielles Problem ist, dass der Auditierte die Meinung des Auditors auswählt, die ihm am günstigsten oder bequemsten erscheint. Dies wird auch als Opinion Shopping bezeichnet.

2.2.6 Selbstbewertung

Die Selbstbewertung ist eine Sonderform des 1st Party IT-Audits. Ihr hauptsächliches Merkmal ist, dass es keine speziell ausgewiesenen internen Auditoren gibt, sondern dass die regulären Mitarbeiter, die im betroffenen Bereich operativ tätig sind, die Selbstbewertung durchführen.

> Die **Selbstbewertung** (engl. Control Self Assessment) ist ein internes IT-Audit von Kontrollen, bei dem das Personal aus dem betroffenen operativen Geschäftsbetrieb die erforderlichen Prüfungsaufgaben selbst durchführt.

Das Personal prüft in der Regel die vorliegenden Dokumente und das Vorhandensein und die grundsätzliche Funktionalität von wichtigen Kontrollen. Die **Voraussetzung** dafür ist eine genaue Abgrenzung und Einteilung der Prüfungsumgebung, damit klare Zuständigkeiten für die Selbstkontrolle geschaffen werden können. Außerdem sollte das Personal mit grundlegen Techniken zur Datenerhebung und -auswertung vertraut gemacht werden. Interviews, Workshops und Fragebögen sind beliebte Techniken bei der Selbstbewertung. Die Geschäftsführung und die Führungskräfte müssen die Selbstbewertung nicht nur befürworten, sondern auch

durch die Bereitstellung angemessener Ressourcen und Befugnisse aktiv unterstützen.

Die **Vorteile** der Selbstbewertung sind:

- Im Unternehmen werden klare **Verantwortlichkeiten** für die Kontrollen geschaffen. Die verantwortlichen Personen befinden sich dauerhaft im Unternehmen, sodass sie die Kontrollen laufend überwachen und pflegen können. Die Wahrscheinlichkeit des Auftretens von Betrugsfällen, und dadurch auch das Gesamtrisiko des Unternehmens, werden merklich reduziert.
- Durch die Auseinandersetzung mit den Kontrollen und angebundenen Geschäftsprozessen wird das **Verständnis** über den Geschäftsbetrieb sowohl im operativen Bereich als auch im Management stark erhöht.
- Beim Personal steigt das **Bewusstsein** über Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit. Dadurch werden Kontrollschwächen, die aus Unwissenheit oder Unachtsamkeit entstehen, reduziert. Abweichungen werden eher bekannt gemacht, was zu einer größeren Transparenz beim Management beiträgt.
- Die **Effizienz** von 2nd und 3rd Party IT-Audits nimmt zu, da aufgrund der reduzierten Kontrollschwächen auch weniger diesbezügliche Feststellungen generiert werden müssen. Außerdem kann das Personal einen externen Auditor bei der Untersuchung von Kontrollen besser unterstützen, da bereits ein genaues Verständnis über die Kontrollen vorhanden ist.

Die **Nachteile** der Selbstbewertung sind:

- Die **Risikobewertung** basiert selten auf theoretisch fundierten Methoden oder umfangreichen Erfahrungen. Insbesondere extrem hohe Risiken werden bei der Selbstbewertung häufig unterschätzt. Sehr unwahrscheinliche Ereignisse, die jedoch katastrophale Auswirkungen haben, werden entweder nicht berücksichtigt oder nicht angemessen beachtet. Die Folge ist, dass die entsprechenden Risiken, wenn überhaupt, einen zu geringen Risikowert erhalten.
- Die **Risikobewältigung** kann sehr einseitig ausgestaltet werden, ohne dass auf ein angemessenes Kosten-Nutzen-Verhältnis geachtet wird. Das Personal tendiert meist dazu, alle Risiken zu vermindern. Zum einen bleiben dabei andere Risikobewältigungsmethoden, wie Transfer und Akzeptanz, unberücksichtigt und zum anderen werden kaum fundierte quantitative Risikobewertungsverfahren angewandt, um die Kosten und Nutzen der Gegenmaßnahmen in ausreichender Weise abzuwägen.

2.3 Prüfungsumfang

2.3.1 Überblick

Der **Prüfungsumfang** gibt vor, was geprüft werden soll. Dabei kann es sich um Themengebiete aus der virtuellen oder physischen Umgebung sowie aus der Organisation des Auditierten handeln.

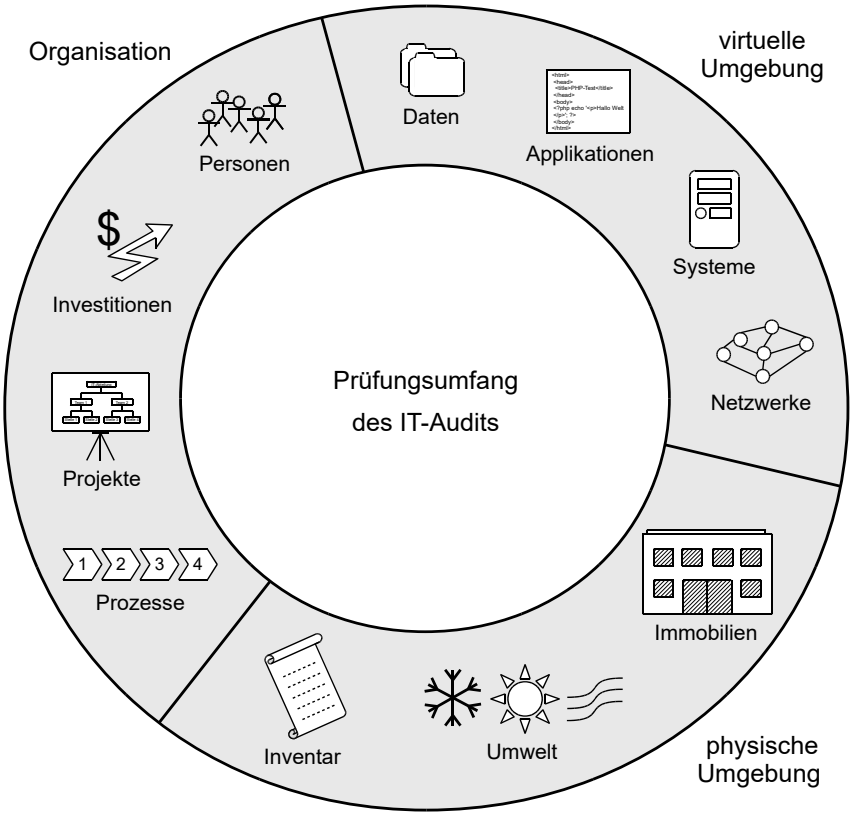

Abbildung 3: Prüfungsumfang

2.3.2 Virtuelle Umgebung

Die **virtuelle Umgebung** umfasst alle Objekte der IT, welche zwar eine konkrete und nützliche Funktionalität besitzen, jedoch in der Regel keine physische Form einnehmen.

Einzelne Objekte aus der virtuellen Umgebung können durchaus fest mit einer konkreten physischen Form verbunden sein, z. B. kann ein System nicht nur virtuell, sondern auch in Form eines Computergehäuses inklusive Hardware existieren. Im vorliegenden Themenbereich wird der Prüfungsumfang jedoch auf die virtuelle Gestalt der Objekte fokussiert:

- **Daten** sind das fundamentale Hilfsmittel, um Informationen zu speichern, zu übertragen oder zu verarbeiten. Sie bestehen aus mehreren Zeichen, die unter Berücksichtigung von Regeln der Syntax zusammengesetzt wurden. Die Zeichen stammen aus einem existierenden Zeichenvorrat, der sich meist aus Buchstaben, Ziffern und Sonderzeichen zusammensetzt und auch Zeichensatz genannt wird. Daten können durch eine Person oder ein System interpretiert werden, und dadurch Informationen vermitteln. Besonders schützenswerte Daten gehören zu den drei Kategorien Leib und Leben, Privatsphäre und Fortbestand des Unternehmens:
  - **Leib und Leben** können durch Daten beeinflusst werden, wenn sie Einfluss auf die Gesundheit oder das Leben von Menschen haben. Dazu zählen z. B. aktuelle Krankendaten und Steuerungsdaten für kritische Systeme.
  - Die **Privatsphäre** wird durch Daten beeinflusst, die Informationen über die informationelle Selbstbestimmung und private Interessen beinhalten, z. B. Politik und Religion.
  - Der **Fortbestand des Unternehmens** ist von Daten abhängig, die sich auf Wettbewerbsvorteile, Finanzlage oder Reputation auswirken können. Sie beinhalten z. B. geheime Forschungsergebnisse oder Baupläne.
- **Applikationen** sind Computerprogramme, die im Unternehmen eingesetzt werden, da sie für die Funktionalität von Prozessen oder Dienstleistungen benötigt werden. In erster Linie wandeln sie Eingabedaten in Ausgabedaten so effizient um, wie es manuell kaum möglich wäre. Dazu wird eine Abfolge von Maschinenbefehlen – der Maschinencode – ausgeführt, welcher wiederum von einem menschenlesbaren Quellcode abgeleitet wurde. Applikationen können lokal auf einem Arbeitsplatzcomputer oder zentral auf einem Server betrieben werden. In den meisten Unternehmen ist der Betrieb von Applikationen essenziell für ein profitables Geschäftsmodell. Sie sind entweder direkter Bestandteil von Kernprozessen, z. B. bei der computergestützten Herstellung von Waren oder bei elektronischen Dienstleistungen, oder sie sind für die effiziente Durchführung von Unterstützungsprozessen unabdingbar, z. B. bei der Lohn- und Gehaltsbuchhaltung oder der Einsatzplanung. Grundsätzlich ist zwischen Applikationen zu unterscheiden, die durch Fremdfirmen entwickelt wurden, z. B. Standardsoftware, oder durch das Unternehmen selbst.
- **Systeme** bilden die Grundlage zur Ausführung von Applikationen und stellen ihnen ausreichende Kapazitäten zur Verfügung, wie Speicher, Rechenleistung und eine Netzwerkanbindung zu anderen Systemen. Aus softwareseitiger Sicht

steuern Systeme alle Prozesse zum Betrieb eines Computers und regeln die Kommunikation zwischen Software und Hardware. Für die anforderungsgerechte Ausführung von Applikationen spielen die Konfiguration und die verfügbare Leistung des Systems eine große Rolle.

– **Netzwerke** ermöglichen die Übertragung von Daten zwischen Systemen, und damit den Austausch von Informationen und den Fernzugriff darauf. Netzwerkkomponenten steuern die Datenübertragung über ein lokales Netzwerk (engl. Local Area Network) oder über geographisch verteilte Netze, z. B. das Internet. Neben einer Verkabelung sind für die zielgerichtete Übertragung der Daten auch Switches, Router und Firewalls erforderlich. Ein Switch leitet Datenpakete innerhalb eines Netzwerks oder zwischen Netzwerksegmenten weiter und ein Router zwischen Netzwerken mit verschiedenen Adressbereichen oder Architekturen. Eine Firewall kann hingegen den Datenverkehr filtern und Verbindungsversuche bei Bedarf blockieren.

2.3.3 Physische Umgebung

Die **physische Umgebung** besteht aus allen Objekten, die eine physische Form besitzen, und den Umweltfaktoren, die deren Zustand beeinflussen können.

Im IT-Bereich handelt es sich dabei zum einen um Immobilien, in denen die IT-Systeme betrieben werden, und zum anderen um IT-Systeme selbst, also die Hardware. Die Umweltfaktoren können zu einer äußeren Einwirkung auf diese Objekte führen.

– **Immobilien** umfassen alle Räumlichkeiten, also Gebäude und Büros, in denen IT-Systeme betrieben oder aufbewahrt werden. Dabei handelt es sich auch um Rechenzentren, die speziell für den Betrieb von Servern vorgesehen sind, und um die Arbeitsräume des Personals.

– **Umwelt** ist ein Oberbegriff für alle Umweltfaktoren, die von außen auf IT-Systeme, Datenträger und andere Objekte einwirken, und dadurch die Funktionalität beeinträchtigen können. Dazu gehören zum einen das Raumklima und zum anderen diverse Umweltbedrohungen, z. B. durch Feuer, Hochwasser, Erdbeben und extreme Wettersituationen.

– **Inventar** bezieht sich nicht nur auf die Pflege des Bestandsverzeichnisses aller IT-Objekte, sondern auch auf die Bewahrung ihrer Funktionsfähigkeit. Sie sollten also nicht nur nachvollziehbar verwaltet, sondern auch gepflegt und gesichert werden.

2.3.4 Organisation

Die **Organisation** ist notwendig, damit die geschäftlichen Aktivitäten im Unternehmen verteilt, koordiniert und strukturiert abgewickelt werden können.

Sie kann institutionell und funktionell gedeutet werden. Aus **institutioneller** Sicht umfasst sie alle Regelungen des Unternehmens, die der Zuordnung und Abwicklung von geschäftlichen Aktivitäten dienen. Aus **funktioneller** Sicht umfasst sie die Aktivitäten zur Koordinierung und Arbeitsteilung selbst. Fundamentale Bestandteile der Organisation sind:

- **Prozesse** sind eine Abfolge von geschäftlich relevanten Ereignissen und Tätigkeiten, die ein Eingabeobjekt in ein Ausgabeobjekt umwandeln. Sie haben das übergeordnete Ziel, einen direkten oder indirekten Nutzen für den Kunden, und dadurch einen Wert für das Unternehmen, zu erzeugen. Meistens wirken mehrere Personen oder Systeme bei der Ausführung eines Prozesses mit.
- **Projekte** sind Vorhaben, bei denen innerhalb einer definierten Zeitspanne ein definiertes Ziel erreicht werden soll und die sich dadurch auszeichnen, dass sie im Wesentlichen durch die Einmaligkeit der Bedingungen und der Vorgaben in ihrer Gesamtheit gekennzeichnet sind. Beispiele sind die Schaffung eines speziellen Sachguts oder einer Dienstleistung. Der Erfolg von Projekten kann essenziell für das Fortbestehen eines Unternehmens sein. Daher ist der Umgang mit Projekten im Unternehmen von großer Bedeutung.
- **Investitionen** ermöglichen nicht nur ein Wachstum des Unternehmens, sondern sind auch eine potenzielle Gefahrenquelle. Daher wird vor einer Investitionsentscheidung der finanzielle Nutzen der Investition abgewogen. Auch die Frage, ob die neue Investition in das bisherige Portfolio passt, ist eine wichtige Entscheidungshilfe. Investitionen sollten der Wertschöpfung dienen und über ihren gesamten Lebenszyklus gesteuert werden.
- **Personen** stellen dem Unternehmen im Rahmen eines Arbeitsverhältnisses ihre Arbeitskraft entgeltlich zur Verfügung. Sie besetzen die Stellen in der Organisation des Unternehmens und führen damit verbundene Aufgaben und Weisungen aus. Weisungsbefugnisse bestehen in der Regel gegenüber Mitarbeitern aus untergeordneten Organisationseinheiten. Die wichtigsten Verantwortlichkeiten im Unternehmen sind die Koordination und Durchführung von Aufgaben, die Übernahme der Kostenverantwortung, die Konsultierung von Kollegen und die Berichterstattung an Interessenspersonen.

2.4 Prüfungsaspekt

2.4.1 Überblick

Beim **Prüfungsaspekt** eines IT-Audits handelt es sich primär um die Sicherheit, Wirtschaftlichkeit oder Ordnungsmäßigkeit der IT in einem Unternehmen. Sekundär lassen sich außerdem noch weitere Prüfungsaspekte nennen, die durch Konkretisierung aus den primären abgeleitet werden können.

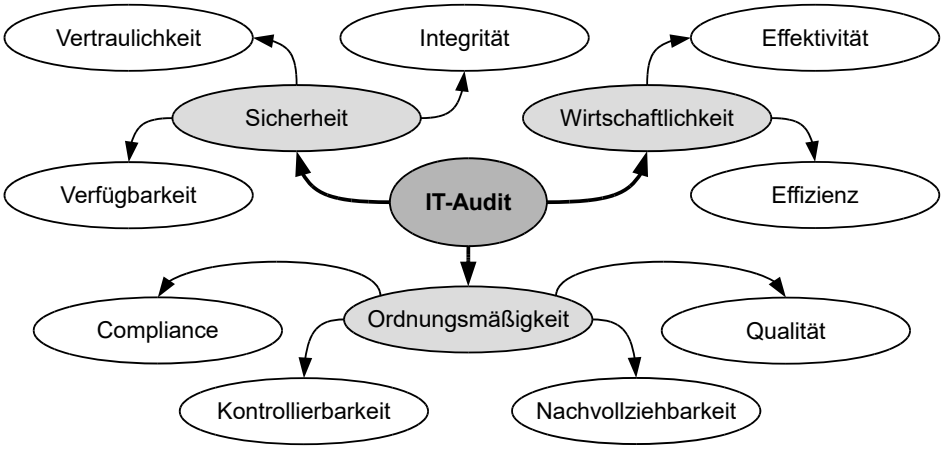

Abbildung 4: Prüfungsaspekte

2.4.2 Sicherheit

Die **Sicherheit** sieht vor, dass Informationen und IT-Systeme nicht kompromittiert, manipuliert oder beschädigt werden.

Die **Schutzziele** Vertraulichkeit, Integrität und Verfügbarkeit müssen möglichst gut erfüllt werden. In Anlehnung an diese Schutzziele lassen sich die entsprechenden Prüfungsaspekte konkretisieren:

- Die **Vertraulichkeit** ist vorhanden, wenn keine unbefugte Informationsgewinnung stattgefunden hat. Sie wird dadurch gewährleistet, dass kompromittierende Aktivitäten unberechtigter Personen und Systeme verhindert werden.
- Die **Integrität** ist vorhanden, wenn keine unbefugte Manipulation stattgefunden hat. Die Maßnahmen, die zum Schutz der Vertraulichkeit genutzt werden, dienen oft auch zum Schutz der Integrität. Denn wenn Daten nicht kompromittiert werden können, können sie in der Regel auch nicht beschädigt oder manipuliert werden.

– Die **Verfügbarkeit** ist vorhanden, wenn keine unerwünschte Beeinträchtigung der Funktionalität stattgefunden hat. Sie wird gewährleistet, indem die Objekte und die Infrastruktur, die zur Ausübung des Geschäftsbetriebs notwendig sind, zur Nutzung bereitstehen und genügend Kapazitäten besitzen, um alle Aufgaben schnell genug abzuarbeiten.

2.4.3 Wirtschaftlichkeit

Die **Wirtschaftlichkeit** orientiert sich an der Profitabilität des Unternehmens und der Aufrechterhaltung eines wirtschaftlich effizienten Geschäftsbetriebs.

Wenn die Kosten für die eingesetzten Ressourcen höher sind als der erzielte Umsatz, kann kein Gewinn erwirtschaftet werden und das Unternehmen ist langfristig nicht überlebensfähig. Aus Sicht der IT müssen daher stets eine Ausrichtung der IT-Tätigkeiten am Geschäftsbetrieb und eine möglichst hohe Wertgenerierung durch diese erfolgen. Von der Wirtschaftlichkeit lassen sich die Effektivität und Effizienz ableiten:

– Die **Effektivität** der Organisation ist Bestandteil der Wirtschaftlichkeit, da der Aufbau und die Abläufe in der Organisation zur Erwirtschaftung eines Gewinns zweckmäßig sein müssen.
– Die **Effizienz** ist ebenfalls fundamental für die Wirtschaftlichkeit, da nur der effiziente Umgang mit Arbeitsleistung, Betriebsmitteln und Rohstoffen zur Realisierung einer Gewinnspanne, und somit zur Profitabilität des Unternehmens, führt.

2.4.4 Ordnungsmäßigkeit

Die **Ordnungsmäßigkeit** beinhaltet die Konformität der IT zu allen vorgeschriebenen Regeln, z. B. aus Gesetzen und Verträgen.

Diese Regeln können auch vom Unternehmen selbst vorgegeben worden sein, z. B. durch interne Richtlinien. Für die Ordnungsmäßigkeit ist sowohl ein konformes Vorgehen als auch die Einhaltung inhaltlicher Vorgaben von Bedeutung. Von der Ordnungsmäßigkeit lassen sich die Compliance, Kontrollierbarkeit, Nachvollziehbarkeit und Qualität ableiten:

– Die **Compliance** leitet sich von der Ordnungsmäßigkeit ab, da ordnungsmäßige IT-Aktivitäten konform zu vorgeschrieben Regeln sein müssen. Die Compliance befasst sich genau mit der Einhaltung von Regeln, die zumeist aus externen Quellen stammen, z. B. Gesetzen und Standards.

- Die **Kontrollierbarkeit** ist Bestandteil der Ordnungsmäßigkeit, da ordnungsmäßige IT-Aktivitäten so gestaltet werden müssen, dass sie z. B. durch organisatorische Vorgesetzte und mithilfe von Fortschrittsberichten kontrolliert werden können.
- Die **Nachvollziehbarkeit** ist ebenfalls mit der Ordnungsmäßigkeit verbunden, da ordnungsmäßige IT-Aktivitäten in der Regel protokolliert und dokumentiert werden müssen, sodass sie für Kollegen und Außenstehende nachvollziehbar sind.
- Die **Qualität** ist die Summe aller Eigenschaften eines Betrachtungsobjekts und das Ausmaß, wie es vorgegebene Anforderungen erfüllt. Die Qualität steht mit der Ordnungsmäßigkeit im Zusammenhang, da ordnungsmäßige Betrachtungsobjekte unter anderem Qualitätsanforderungen genügen müssen. Nicht nur das Ergebnis der IT-Aktivitäten ist für eine hohe Qualität ausschlaggebend, sondern auch die Gestaltung effizienter Prozesse und die überlegte Nutzung von Ressourcen innerhalb der IT. Eine hohe Qualität schützt die IT vor nachgelagerten Aufwänden zur Fehlerbehebung und Nachbesserung.

2.5 Prüfungsort

2.5.1 Überblick

Der **Prüfungsort** bezeichnet den Ort, an dem sich der Auditor während der Prüfung des Auditierten befindet. Der Standort des Auditierten wird im Englischen auch als Site bezeichnet. On-Site bedeutet demnach der Aufenthalt des Auditors am Standort das Auditierten und Off-Site außerhalb des Standorts.

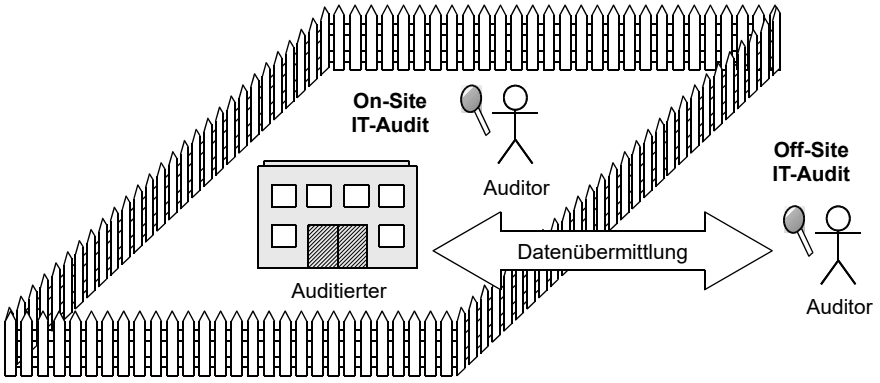

Abbildung 5: Prüfungsort

2.5.2 On-Site IT-Audit

Ein **On-Site IT-Audit** wird in den Geschäftsräumen des Auditierten durchgeführt und umfasst ein systematisches Durchlaufen von prüfungsrelevanten physischen Bereichen durch den Auditor.

Beim On-Site IT-Audit folgt der Auditor einem Plan zum Besuchen physischer Bereiche, die sich in den **Geschäftsräumen** des Auditierten befinden, z. B. Lager- oder IT-Räume, Büros, Konferenzräume für Interviews und Zutrittspunkte zum Gelände des Auditierten. Zur besseren Vorbereitung beim Auditierten übergibt der Auditor vorher einen Zeitplan mit einer Auflistung der zu besuchenden physischen Bereiche und relevanten Interviewpartner.

Eine adäquate **Vorbereitung** ist essenziell für das On-Site IT-Audit und sollte Folgendes umfassen:

- Alle benötigten Mitarbeiter sollten beim Auditierten vor Ort sein. Dazu gehören z. B. Administratoren zur Gewährung von lesendem Zugriff auf Daten, Interviewpartner zur Beantwortung von Fragen und Manager zur Koordination des IT-Audits und kurzfristigen Entscheidung zu auftretenden Problemen.
- Alle benötigten Mitarbeiter sollten vorher darüber informiert und angewiesen werden, in welcher Weise sie den Auditor unterstützen sollen.
- Die Verfügbarkeit von Dokumenten, die für das IT-Audit relevant sein können, und der Zugriff darauf sollten sichergestellt werden.
- Der Auditor sollte einen privaten Raum für die Durchführung vertraulicher Interviews und den Zugang zu üblichen Bürohilfsmitteln, wie Fotokopierer und Telefon erhalten.

Der **Ablauf** des On-Site IT-Audits kann folgende Aktivitäten umfassen:

1. Ein Begrüßungsgespräch des Auditors mit dem Management dient dazu, den Umfang des IT-Audits und den Zeitplan zu bestätigen sowie sich gegenseitig vorzustellen.
2. Ein Mitarbeiter des Auditierten führt den Auditor durch die Geschäftsräume, um ihn mit der räumlichen Anordnung vertraut zu machen.
3. Der Auditor wird anschließend die eigentliche Prüfung durchführen, unter anderem Interviews, Diskussionen, Beobachtungen, physische Untersuchungen und Datensammlungen und -auswertungen.
4. Der Auditor wird die gesammelten Daten auswerten, Beweise identifizieren und Feststellungen dokumentieren. Diesen Schritt wird der Auditor in einem privaten Raum durchführen.

5. Der Auditor präsentiert dem Management in einem Abschlussmeeting seine Feststellungen. Hier werden ein gemeinsames Verständnis über die Feststellungen geschaffen und eventuelle Missverständnisse aufgeklärt.
6. Der Auditor übergibt dem Auditierten den Prüfungsbericht.

2.5.3 Off-Site IT-Audit

Ein **Off-Site IT-Audit** wird außerhalb der Geschäftsräume des Auditierten durchgeführt und umfasst die Prüfung von übermittelten Daten des Auditierten durch den Auditor aus der Ferne.

Durch die Nutzung moderner **Kommunikationstechniken**, wie Videokonferenzen, Web-Meetings, Fernzugriffe auf IT-Systeme und breitbandige Internetzugänge, können durch den Auditor große Mengen an Informationen über den Auditierten aus der Ferne gesammelt und geprüft werden, ohne dass er physisch beim Auditierten präsent ist. So kann theoretisch ein vollständiges IT-Audit durchgeführt werden, ohne dass der Auditor sein Büro verlässt.

Durch das Off-Site IT-Audit vermeidet der Auditor langwierige Anreisen zu eventuell schwer erreichbaren Orten. Er kann **Unterstützung** vom Personal vor Ort erhalten, um z. B. mit einer Webcam einen Eindruck über die physischen Gegebenheiten oder Geschäftsabläufe zu erhalten.

Auch das Off-Site IT-Audit sollte **vorbereitet** werden. Die Rollen der beteiligten Personen beim IT-Audit sollten zuvor festgelegt werden, z. B. welche Mitarbeiter den Auditor unterstützen und wer die Übermittlung von Daten an den Auditor koordinieren soll. Außerdem sollte ein Notfallplan erarbeitet werden, der beschreibt, wie bei einem Abbruch der Kommunikationsverbindung oder anderen Störungen mit dem Auditor umzugehen ist.

In der Praxis findet häufig eine **Kombination** von On- und Off-Site IT-Audit statt. So prüft der Auditor in erster Linie Dokumente und leicht zu erhebende Daten aus der Ferne und führt Interviews und komplexere Datenerhebungen in den Geschäftsräumen des Auditierten durch. Dadurch kann der Auditor seine Ressourcen insbesondere in der Planungsphase effizienter einsetzen.

2.6 Prüfungszeit

2.6.1 Überblick

Die **Prüfungszeit** ist der Zeitpunkt der Durchführung des IT-Audits in Bezug auf ein bestimmtes Ereignis. Das IT-Audit kann vor einem Ereignis (engl. Pre), gleichzeitig dazu, danach (engl. Post) oder kontinuierlich durchgeführt werden.

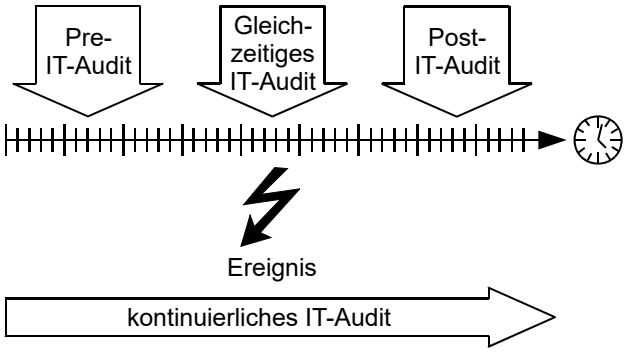

Abbildung 6: Prüfungszeit

2.6.2 Pre-IT-Audit

Ein **Pre-IT-Audit** ist ein IT-Audit, das vor einem Ereignis stattfindet, um den Zustand der Objekte zu prüfen, die von diesem Ereignis potenziell betroffenen sind, und damit die Auswirkungen dieses Ereignisses beurteilen zu können.

Missstände, die im Pre-IT-Audit auffallen, haben oft noch keinen Schaden verursacht, da das relevante Ereignis in der Zukunft liegt. Pre-IT-Audits verhelfen dazu, bereits im Vorfeld die notwendigen Kontrollmaßnahmen und deren Implementierungsaufwände abzuschätzen oder Möglichkeiten zu identifizieren, um das Auftreten von unerwünschten Ereignissen sogar zu verhindern. Häufige Anlässe für Pre-IT-Audits sind Fusionen, Akquisitionen, Outsourcing, Investitionen und ebenfalls Audits:

– Vor der Durchführung von **Fusionen** besitzen die Fusionspartner ein gegenseitiges Interesse an bestehenden Vorgaben zur Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit und am Ausmaß, wie diese Vorgaben eingehalten werden. Dadurch sollen vor allem Risiken transparent gemacht werden, von denen die Fusionspartner nach der Fusion betroffen sind.
– Vor **Akquisitionen** besitzt der Käufer ein Interesse am käuflichen Unternehmen. Die Ergebnisse des Pre-IT-Audits beeinflussen zum einen den geschätzten Unternehmenswert und dienen zum anderen auch der Beurteilung von Risiken.

In diesen Fällen ist das Pre-IT-Audit meist Bestandteil einer Due-Diligence-Prüfung.

– Bevor ein Dienstleister beim **Outsourcing** unter Vertrag genommen wird, wird oft die Sicherheit bei ihm geprüft. Obwohl die meisten Risiken durch vertragliche Vereinbarungen transferiert werden können, darf die Sicherheit durch den Auftraggeber nicht vollständig vernachlässigt werden. Eventuelle Sicherheitsvorfälle haben meist starken Einfluss auf die Reputation des Dienstleisters und ebenfalls seiner Auftraggeber. Daher werden Pre-IT-Audits genutzt, um die Sicherheit des Dienstleisters vorab zu beurteilen.
– **Investitionen** können vorgenommen werden, um z. B. Hardware oder Software anzuschaffen. Damit sie für das Unternehmen lohnenswert sind, sollen sie einen Wert generieren oder die Wertgenerierung unterstützen. Eine nicht hinreichende Sicherheit, Wirtschaftlichkeit oder Ordnungsmäßigkeit beeinflusst die Wertgenerierung negativ, da z. B. Störungen oder Schäden auftreten können. Durch das Pre-IT-Audit kann also besser abgeschätzt werden, ob Investitionen lohnenswert sind.
– Ein internes Pre-IT-Audit vor einem **Audit** gibt dem Auditierten die Chance, Fehler und Missstände selbst aufzudecken und zu beheben. Auf diese Weise kann er die späteren Prüfungsaufwände und Nacharbeiten reduzieren. Außerdem wird insbesondere vor 2nd und 3rd Party IT-Audits gewährleistet, dass potenziell reputationsschädigende Abweichungen im Voraus identifiziert und beseitigt werden können.

2.6.3 Gleichzeitiges IT-Audit

Ein **gleichzeitiges IT-Audit** ist ein IT-Audit, das zur selben Zeit wie ein bestimmtes, eingegrenztes Ereignis stattfindet. In der Regel steht dieses Ereignis im Zusammenhang mit einer erwarteten Abweichung.

Das gleichzeitige IT-Audit ist in solchen Fällen sehr hilfreich, in denen zum **Zeitpunkt** eines Ereignisses bestimmte Informationen oder Zustände entstehen, die sich direkt im Anschluss wieder verflüchtigen oder nachträglich nur sehr schwer nachvollziehen lassen. Durch die Einbettung eines gleichzeitigen IT-Audits in die technischen Abläufe eines Unternehmens können ereignisbezogene Daten langfristig gespeichert und zur Identifikation eventueller Abweichungen genutzt werden.

Die **Ereignisse**, die bei einem gleichzeitigen IT-Audit häufig im Mittelpunkt stehen, sind das Verhalten einer Applikation, die Zustandsänderung eines Systems und die Verarbeitung einer Transaktion:

– Wenn eine **Applikation** geprüft werden soll, wird in der Regel betrachtet, wie sie sich im Rahmen eines speziellen Ereignisses verhält: Werden Daten so ver-

arbeitet, gespeichert und übermittelt wie vorgesehen? Entspricht das Ergebnis den Vorgaben und Erwartungen?

- Der Zustand eines **Systems** sollte zu jeder Zeit sicher und ordnungsmäßig sein. Bestimmte Ereignisse (z. B. ein Speicherüberlauf) können allerdings einen unerwünschten Systemzustand herbeiführen. Mit einem IT-Audit, das zur selben Zeit wie ein solches Ereignis stattfindet, kann der Systemzustand unverzüglich in Bezug auf mögliche Abweichungen untersucht werden.
- Die Prüfung einer **Transaktion** ist vor allem dann interessant, wenn Transaktionen mit bestimmten Attributen im Verdacht stehen, nicht erwartungsgemäß verarbeitet zu werden. Derartige Transaktionen können z. B. zu ungünstigen Wechselwirkungen (z. B. ein Deadlock zwischen mehreren Prozessen) oder Kompatibilitätsproblemen (z. B. aufgrund unterschiedlicher, länderspezifischer Schreibweisen – wie bei verschiedenen Datumsformaten) führen.

Ein Ereignis zur selben Zeit wie dessen Auftreten zu prüfen, ist nicht immer leicht – insbesondere wenn ein Ereignis schwer vorherzusehen ist und sich auch nicht in irgendeiner Weise ankündigt (z. B. durch den Empfang bestimmter Daten oder durch Indizien für einen bevorstehenden Hacker-Angriff). Um ein derartiges Ereignis manuell zu erzeugen oder möglichst präzise herbeizuführen, ist oft viel Aufwand erforderlich. Trotzdem gibt es einige **Gründe** dafür, ein IT-Audit gleichzeitig zu einem Ereignis durchzuführen und nicht erst nachträglich die verdächtigen Ereignisse zu prüfen. Die Gründe liegen unter anderem in folgenden Punkten:

- Trotz der vielfältigen Protokollierungsmöglichkeiten von IT-Systemen sind einzelne Ereignisse oft nur **schwer nachvollziehbar**. Viele Protokollierungsmöglichkeiten werden nämlich aufgrund begrenzter Speicherkapazitäten, einer generellen Datensparsamkeit und möglicher Performance-Beeinträchtigungen der Systeme nicht genutzt. Die nachträgliche Prüfung eines vergangenen Ereignisses ist entsprechend schwierig.
- Selbst wenn Daten in ausreichender Weise protokolliert wurden, sind sie aufgrund von großen, unstrukturierten Datenmengen nur **schwer auffindbar**. Die Strukturierung und Filterung von Protokolldaten sind oft mit viel Aufwand verbunden, eine manuelle Sichtung der Daten ist kaum machbar. Vor allem wenn das fragliche Ereignis zeitlich nicht eingegrenzt werden kann, sind eine nachträgliche Identifikation und Auswertung schwierig.
- Der technische Fortschritt führt zu einer immer stärkeren **Integration** von IT-Systemen und -Abläufen. Diese Integration ist nicht nur auf die Geschäftsprozesse ausgerichtet, sondern auch auf eine wechselseitige Zusammenführung von Systemen. In der Folge existieren vielen Schnittstellen und Standards, die auch zur Integration eines gleichzeitigen IT-Audits genutzt werden können. Spezialisierte IT-Audit-Lösungen sind in der Regel mit standardisierten Da-