IDR Prüfungsleitlinie L 135 „projektbegleitende IT-Prüfung“

Stand: 02.2021

Autor: Tim Fritsch, Revisionsamt der Stadt Frankfurt a. Main

Arbeitskreis „Digitalisierung und IT-Sicherheit“

Inhalt

I. Abbildungsverzeichnis

II. Dokumentenhistorie

Version	Datum	Verfasser	Änderung / Grund	Status
01.0	09.2020	T. Fritsch	Erstellung des Dokuments	In Arbeit
01.1	01.2021	AK DITS	REVIEW	In Arbeit
01.2	02.2021	T. Fritsch	Einarbeitung der Rückmeldungen Erstellung VORSTANDS ENTWURF	ENTWURF

1. Vorbemerkungen[1]

IT ist in sämtlichen Bereichen der Kommunen vorhanden. Eine Nutzung und Einbindung gibt es vom Computer-Arbeitsplatz über vollständige eAkten bis hin zu speziellen Fachverfahren in allen Bereichen. Eine Buchhaltung ohne digitales Buchführungssystem ist undenkbar. Der Trend der Einbindung von elektronischen Prozessen und Abläufen wird sich im Zeitalter der „digitalen Revolution“ weiter verstärken. Grund hierfür sind u.a. auch die einzelnen Gesetzgebungen (eGovernment-Gesetz, eJustice-Gesetz, Onlinezugangsgesetz, EU-Datenschutzrichtlinie u.v.m.), welche insbesondere mit ihren Regelungen den öffentlichen Dienst betreffen. Der Trend zur Digitalisierung wird darüber hinaus durch zahlreiche „Digitalisierungsoffensiven“ in einzelnen Bundesländern wirksam verstärkt.

Die zunehmende Nutzung von IT-Systemen bietet nicht nur zahlreiche Chancen, sondern birgt auch erhebliche Risiken. Mit dem ansteigenden Digitalisierungsgrad steigt auch die Abhängigkeit von technischen Systemen. Technische Störungen führen häufig im Zusammenhang mit einer unzureichenden Notfallabsicherung und fehlenden Redundanzen zu Störungen in den Arbeitsabläufen und damit zu einer Einschränkung in der Verwaltungstätigkeit. Neben persönlichen Haftungen und finanziellen Schäden besteht somit auch die Gefahr von Vertrauens- und Imageverlust in der Öffentlichkeit. Daneben können fehlerhaft konzipierte bzw. konfigurierte Elemente in der IT beispielsweise Unbefugten den Zugriff auf sensible Daten erleichtern. Durch solche Schwachstellen besteht die Möglichkeit, relevante Daten unbemerkt zu verändern oder bewusst zu manipulieren. Schlimmstenfalls stehen durch Sicherheitsvorfälle die für einen Prozess oder ein bestimmtes Produkt notwendigen kritischen IT-Anwendungen nicht zur Verfügung. Neben technischen Ursachen sorgen leider häufig auch die Mitarbeiter selbst im Umgang mit IT-Anwendungen durch fahrlässiges Verhalten oder ggf. sogar vorsätzlich falsches Handeln für eine Gefahr. Die »Awareness« für die Risiken bei Einsatz und Nutzung von IT und damit auch das Bewusstsein für die Notwendigkeit von IT-Prüfungen werden neben anderen unternehmensrelevanten Elementen zu einem der wichtigsten Handlungsfelder[2].

[1] IDR-Eckpunktepapier der IT-Prüfung vom 28.06.2018

[2] Auszüge aus dem ISACA Leitfaden „Grundlagen der IT-Revision für den Einstieg in die Praxis“ Stand Juli 2016

2. Grundlagen

2.1. IT-Prüfung

Die Anforderungen an eine IT-Prüfung sind im Verlaufe der vergangenen Jahre erheblich gestiegen. Dieser Fokus hat sich, insbesondere auf Basis der GoBD, des IT-Sicherheitsgesetzes und diverser anderer neuer gesetzlicher Normen und Standards, erweitert.

Die Einführung und Beschaffung neuer IT-Produkte im Rahmen der Digitalisierung sowie deren Anpassung findet stetig statt. Hierfür werden grundsätzlich IT-Projekte durchgeführt.

2.2. IT-Projekte

IT-Projekte befassen sich mit der Entwicklung von Informations- und Kommunikationssystemen. Die Kernaufgabe ist dabei die Entwicklung oder Anpassung von Software, teilweise in Verbindung mit der Einführung und Anpassung der dazugehörigen Hardwarekomponenten.

Hierbei ist grundsätzlich zu beachten, dass eine Vielzahl der IT-Projekte gleichzeitig Organisationsprojekte sind.

IT-Projekte können verschiedene Ausrichtungen haben, hierzu zählen:

- Einführung neuer Software
  - Software Kauf
  - Software-Entwicklung
  - Ausrollen von Standardsoftware
- Einführung neuer Infrastruktur (Hardware)
  - Clients
  - Server
  - Netzwerk
  - Serverräume
  - Mobile Devices
  - Netzwerkfähige Elektronik (Peripherie, Fernseher …. Kaffemaschine usw.)
- Einführung neuer Software in Verbindung mit neuer Infrastruktur
  - Kombination der oben genannten Themen
- Anpassung / Änderung bestehender IT-Systeme
  - Migration
  - Neuausrichtung
  - Erweiterung
  - Re-Design

Die Größe eines IT-Projektes spielt hierbei eine entscheidende Rolle. Durch die Veränderung der jeweiligen Arbeitsgrundlage ist eine Organistations- und Prozessbetrachtung sowie ggf. Anpassung dieser unerlässlich.

2.3. Agiles Projektmanagement / Softwareentwicklung

Durch die Inanspruchnahme externer Projektdienstleister und Softwarehersteller hält der Ansatz des agilen Projektmanagements bzw. der agilen Softwareentwicklung Einzug in die Arbeitswelt des öffentlichen Dienstes. Die innovativen und sehr dynamischen Ansätze dieser Arbeitsweise wirken für den meist sehr strukturierten öffentlichen Dienst - insbesondere bei der ersten Berührung - befremdlich.

Grundsätzlich beinhaltet eine agile Softwareentwicklung Ansätze im Softwareentwicklungsprozess, die die Transparenz und Veränderungsgeschwindigkeit erhöhen und zu einem schnelleren Einsatz des entwickelten Systems führen sollen, um so Risiken und Fehlentwicklungen im Entwicklungsprozess zu minimieren. Dazu wird versucht, die Entwurfsphase auf ein Mindestmaß zu reduzieren und im Entwicklungsprozess so früh wie möglich zu ausführbarer Software zu gelangen. Diese wird in regelmäßigen, kurzen Abständen mit dem Kunden abgestimmt. So soll es möglich sein, flexibel auf Kundenwünsche einzugehen, um so die Kundenzufriedenheit insgesamt zu erhöhen. Agile Softwareentwicklung zeichnet sich durch selbstorganisierende Teams sowie eine iterative und inkrementelle Vorgehensweise aus.

Ein agiler Entwicklungsprozess bedeutet, dass in fest abgesteckten Zyklen - sogenannten Sprints - die Arbeitspakete fertiggestellt werden und im Anschluss zur fertigen Integration und Abnahme zur Verfügung stehen. Eine agile Arbeitsweise bedeutet, dass auf Veränderungen und insbesondere auf neue Anforderungen eingegangen wird. Ein Vorurteil ist, dass hierbei nicht (ordentlich) dokumentiert wird. Auch bei einer agilen Arbeitsweise gehört Dokumentation aller Schritte / Ziele und Ergebnisse zu einer ordnungsgemäßen und zweckmäßigen Arbeitsweise.

Innerhalb der Prüfung sollte bei einem agilen Ansatz die grundsätzliche Zweckmäßigkeit der Projekt- / Entwicklungsorganisation betrachtet werden. Eine Prüfung der einzelnen Sprints bzw. deren Ergebnisse sind besonders durch eine begleitende Prüfung gut möglich und lassen ein direktes Prüfurteil zu. Insbesondere das agile Projektmanagement kann auf die Beratung und Hinweise während der begleitenden Prüfung gut eingehen und auf die Empfehlungen der Rechnungsprüfer_innen (Hinweis auf die notwendige Erfüllung gesetzlicher Vorgaben und Anforderungen) zeitnah reagieren.

Bei der Arbeitsweise sollte insbesondere darauf geachtet werden dass die einzelnen Ist- und Soll-Prozesse und/oder die einzelnen Ziele und Anforderungen und Arbeitspakete ordnungsgemäß konzeptioniert und dokumentiert werden.

2.4. Ziel und Umfang

Ziel der Prüfung ist die Festellung der Zweckmäßigkeit, Ordnungsmäßigkeit und Wirtschaftlichkeit des Projektes sowie der aus dem Projekt resultierenden Ergebnisse (der eingeführten IT-Systeme). Der Umfang der erforderlichen Prüfung hängt nicht von der Größe der Kommune ab, sondern von der Komplexität der eingesetzten und prüfungsrelevanten IT-Systeme.

Daraus resultieren drei zur prüfende Projektbereiche

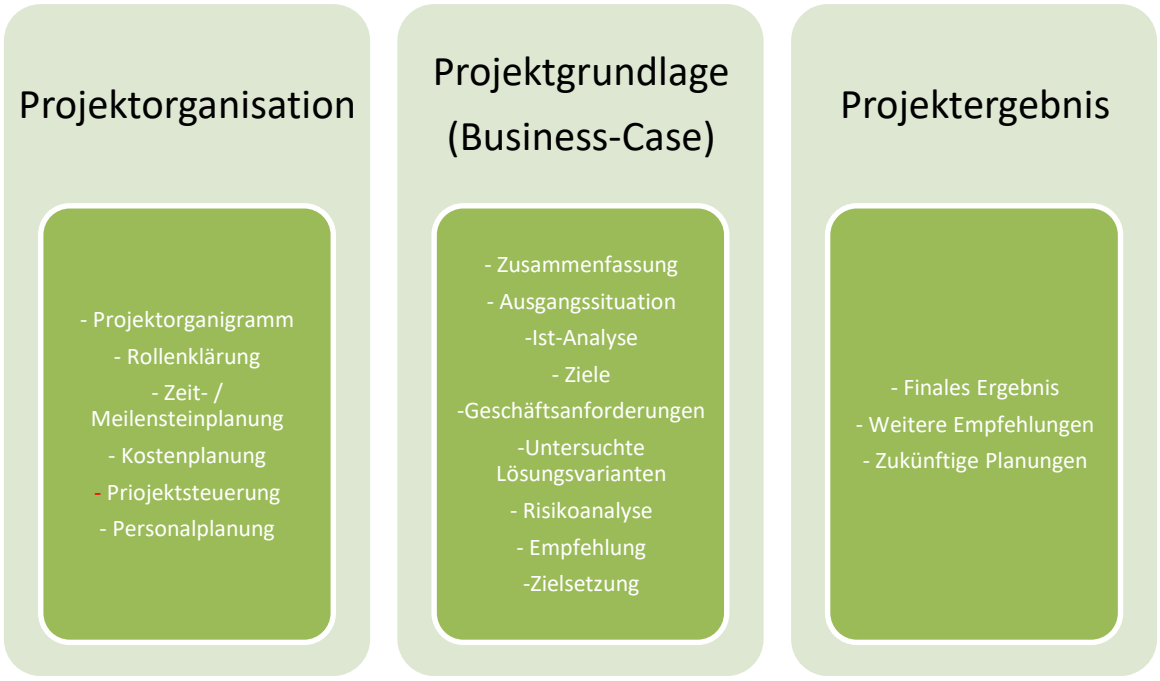

Abbildung 1 - Zu prüfende Projektbereiche

3. Grundsätze zur Prüfungsdurchführung

3.1. Prüfungsplanung

Zur Prüfungsplanung ist insbesondere die Information zum Start bzw. der grundsätzlichen Information über die Durchführung eines Projektes wichtig.

Grundsätzlich sollten innerhalb der jeweiligen Organisationen die Information über neue IT-Projekte mithilfe eines einheitlichen Prozesses (bspw. eines Projekt-Maßnahmen- oder Stellungsnahmeverfahren) den zentralen Organen (Finanzen / Personal / Datenschutz / IT-Sicherheit / Revision / Personalrat) zur Verfügung gestellt werden. Somit können alle Bereiche mit Grundsatzfunktionen vorab über neue Projekte informiert werden.

Auf Grundlage dieser Informationen kann die Prüfung eines Projektes im Zuge der risikoorientierten Prüfplanung durchgeführt werden.

3.2. Prüfteam

Bei der Einführung der meisten IT-Systeme werden technische und fachliche Aspekte behandelt. Hierdurch ist es sinnvoll, bei der begleitenden Prüfung von IT-Projekten ein Prüfteam aus fachlichen und informationstechnischen Prüfer_innen zusammen zu stellen. Handelt es sich um größere IT-Projekte einhergehend mit Bauprojekten sind zusätzliche die bautechnischen Prüfer zu involvieren.

Je nach Größe und Dauer des Projektes ist die Einbindung der jeweiligen Leitung der Rechnungsprüfer im Lenkungsausschuss zu etablieren.

3.3. Methode

Auf Grundlage des Status der jeweiligen Projekte stehen ggf. viele Informationen (noch) nicht zur Verfügung und werden auf Grundlage der jeweiligen Anforderungen im Laufe des Projektes erarbeitet.

Hierbei ist es nicht immer sofort möglich, IST gegen SOLL zu prüfen.

Als Prüfer_in besteht die schwierige Aufgabe, der geprüften Stelle prüfend und beratend zur Seite zu stehen. Ansprechpartner_in hierfür ist die Projektleitung. Es besteht die Aufgabe darauf zu achten, dass gesetzliche Vorgaben eingehalten sowie die einzelnen Schritte und Konzepte dokumentiert werden, damit nach / während der Einführung ein IST-SOLL-Verglich des Projektes möglich ist. Hierauf ist bereits bei der Durchführung der Beschaffung im Rahmen des Leistungsverzeichnisses zu achten.

Während des Projektes sind den Prüfern alle Informationen zur Projektorganisation und Projektinhalt zur Verfügung zu stellen. Es ist an den Projektveranstaltungen teilzunehmen bzw. deren Protokolle und Ergebnisse hierzu zu sichten. Ein lesender Zugriff auf die Projektunterlagen (bspw. SharePoint) ist einzufordern.

Die Hauptmethode der begleitenden Prüfung ist Beobachtung durch Teilnahme der Projektveranstaltungen, Sichtung und Beurteilung der Dokumentationen und Konzepte sowie der Interviews im Austausch mit den Projektverantwortlichen. Einen weiteren guten Einblick, insbesondere bzgl. der tatsächlichen Zweckmäßigkeit, ergibt ein Interview mit der späteren Zielgruppe des Projektes.

Bei längeren IT-Projekten bietet sich die Erstellung von Zwischenberichten an.

3.4. Risikoanalyse

Grundsätzlich werden Prüfungen risikoorientiert durchgeführt. Zusätzlich zur Beurteilung des Risikos - wie in den anderen Leitlinien beschrieben (Risikobeurteilung / Prüfplanung / Prüfung von IT) - gelten zur Risikobewertung der Prüfung eines IT-Projektes u.a. folgende Kriterien:

- **Strategische Bedeutung des Projekts**
  Budget des Projekts
  Relative Größe des Projekts im Verhältnis zur Organisationseinheit
  Bedeutung für Gesamtverwaltung nimmt analog der Größe zu
  Bevor kleinere Projekte geprüft werden:
  Prüfung, ob überhaupt wirtschaftlich gerechtfertigt?
  Prüfungsstunden in Relation zur Größe des Projekts?

- **Komplexität – Anzahl der Beteiligten**
  Art des Projekts
  Zahl der Restriktionen
  Zahl beteiligter Auftraggeber
  Zahl beteiligter Auftragnehmer
  Zahl beteiligter Verwaltungsbereiche
  Zahl (einzubindender) technischer Systeme und Verfahren

- **Faktor Zeit – Dauer des Projekts**
  Projektrisiko (und damit die Kosten) nimmt mit zunehmender Zeitdauer zu; die Möglichkeiten zur Beeinflussung nehmen hingegen ab.
  Zeitliche Vorgaben zur Realisierung einhaltbar?
  Zeitdruck kann Projektrisiko erhöhen.

- **Neue Thematik**
  Neue Thematik? - Wenn ja, höheres Risiko?
  Gibt es Vorprojekte? - Wenn nicht, höheres Risiko!
  Projektleitung mit Erfahrung? - Wenn nicht, höheres Risiko!

4. Prüffelder

Für die projektbegleitende Prüfung sind folgende Prüffelder zu betrachten und individuell zu beurteilen.

4.1. Rahmenbedingungen / Rechtliche Vorgaben

Alle Beteiligten, insbesondere die Projektleitung, sollte vor / mit Start des Projektes die Rahmenbedingungen der rechtlichen Vorgaben geklärt haben. Hierzu zählen neben den Vorgaben zur Projektorganisation und Durchführung die jeweiligen Gesetze, welche für die einzuführenden Prozesse und Werkzeuge (Software / Hardware) gelten.

Diese gliedern sich in Gesetze aus den vielfältigen Themengebieten:

Finanzsysteme (Hessen / Frankfurt am Main) • GemKVO, GemHVO -> GoBD • Interne Geschäftsanweisungen • …
IT-Verfahren • IT-Grundschutz Kompendium des BSI (früher IT-Grundschutzkataloge) • eGovernment-Gesetz • eJustice-Gesetz • Onlinezugangsgesetz • EU-Datenschutzrichtlinie • etc.
Fachbereich / Prozesse (exemplarisch) • StVG, • StVO, • WaffVwV, • PStG, • HGastG • u.v.m

Tabelle 1 - Beispiele für die Vielfältigkeit maßgeblichen Rechtgrundlagen.

Im Zuge dieser Klärung ist auch zu ermitteln, ob alle Rollen und alle zu involvierenden Stellen in das Projekt eingebunden sind. Hierbei ist zu beachten, dass in manchen Ländern für Soft- oder Hardware bestimmte übergeordnete und gesetzliche Regelungen als Voraussetzungen zur Nutzung gibt (beispielweise die übergeordneten Programmprüfungen).

4.2. Rollenklärung (Projekt)

Innerhalb eines Projektes gibt es viele Beteiligte. Insbesondere bei einem organistationsübergreifenden IT-Projekt arbeiten viele Personen unterschiedlichster Funktionen und Hierachien miteinander.

Folgende Rollen müssen klar definiert sein:

- Auftraggeber / Lenkungskreis
- Projektleiter_in (intern / extern)
- Teilprojektleiter_in
- Projektmitarbeiter_in
- Zielgruppe

Hierzu kommen bei einem IT-Projekt zusätzliche Rollen, welche fest definiert und allen Projektbeteiligten bekannt sein müssen. Diese sind ergänzend zu den oben genannten Positionen notwendig und bestehen ggf. über das Projekt hinaus (Doppelfunktionen hierbei sind möglich.).

- Verfahrensverantwortliche_r
- IT-Betrieb (Server / Datenbank etc.) – ggf. mehrere Personen
- Prozessverantwortliche_r
- DataOwner (Datenbesitzer_in)
- Endnutzende

Die wichtigsten oben genannten Rollen sind die Prozessverantwortlichen und Datenbesitzer. Die Prozessverantwortlichen haben für Umsetzung und Einsatz des Prozesses in/mit dem IT-System die vollständige Prozessverantwortung, die Datenbesitzer bestimmen über den Umgang mit den Daten. Alle anderen Beteiligten sind Dienstleister für diese Rollen.

Weitere Personen, die maßgeblich zu dem Erfolg des Projektes beitragen sind die Endbenutzenden sprich die Zielgruppe. Diese muss mitgenommen, gehört und verstanden werden. Mit Ihr entscheidet sich der zweckmäßige Einsatz nach Abschluß des Projektes.

Zusätzlich einzubeziehende Gremien sind ggf.:

- Personalrat
- Gleichstellungsbeauftragte_r
- Schwerbehindertenvertrettung
- IT-Sicherheitsbeauftragte_r / Informationssicherheitsbeauftragte_r
- Datenschützer_in
- Rechnungsprüfungsamt
- Übergeordnete Freigabe / Prüfungsinstanzen (bspw. GPA)

4.3. Projektorganisation

Zur ordnungsgemäßen Projektorganisation gehören min. folgende Punkte:

- Projektziel (s. gesonderter Punkt)
- Projektorganigramm
- Projektzeitplan
- Projektressourcen
    - Budget
    - Personal
    - Ausstattung
- Risikomanagement
- Projektende

4.4. (richtiges) Projektziel

Grundlage für den Erfolg jeden Projektes ist das Projektziel. Hierbei gilt für jedes Projektziel der Grundsatz es muss:

Spezifisch,
Messbar,
Akzeptiert,
Realistisch,
Terminiert

sein. Die KGST spricht bei der Steuerung mit Zielen sogar von der Definition von Wirkungszielen, Program-/Produktzielen, Prozessstruktuzielen und Ressourcenzielen. Dies sollte man auch bei der Formulierung von Projektzielen im Hinterkopf haben.

Bsp. Projektziel: *Die Aussage „Ziel ist die Einführung der Software XYZ" ist kein Projektziel.* *„Eine Reduzierung der Vorsprachen vor Ort um 20%" / „Eine Erhöhung der Online-Anträge um 20% bis zum 31.12.XX (mit Hilfe der Einführung der Software XY)." Sind konkrete Projektziele.* *Beide Ziele können für das gleiche Projekt sein. Mit dem ersten Ziel liegt der Fokus einzig auf der Einführung. Mit dem zweiten Ziel ist unabängig der genauen Definitionen von „20%" sowie der zeitlichen Begrenzung ein völlig anderer (besserer) Fokus zur Einführung eines IT-Systems gesetzt. Mit diesem Ziel wird die Umsetzung wesentlich zweckmäßiger. Das Erste Ziel könnte auch erreicht werden, ohne dass sich etwas im Bürger_innen/Kunden - Verhalten verändert. Die Software wäre eingeführt und hätte keinerlei Nutzen. Das Projek wäre weder zweckmäßig noch wirtschaftlich.*

Tabelle 2 - Beispiel Projektziel

Die Zielsetzung wird auch heute noch sehr unterschätzt. Es empfiehlt sich, insbesondere die Definition sowie die Aussage des Projektziels zu prüfen sowie diese ggf. gezielt zu hinterfragen.

Das Projektziel ist ein erstes messbares Kriterium für den IST-SOLL-Vergleich im Bezug auf den Erfolg (Zweckmäßigkeit/Ordnungsmäßigkeit/Wirtschaftlichkeit) des Projektes.

4.5. Beschaffung / Ausschreibung

Die Beschaffung steht am Anfang, ggf. vor dem Projekt. Teilweise gibt es (Vor-) Projekte zur Ermittlung des grundsätzlichen Bedarfs und die Erstellung der jeweiligen (komplexen) Leistungsverzeichnisse.

Die Beschaffung und Ausschreibung muss ggf. gesondert zum Projekt betrachtet werden.

Das Ergebniss der Beschaffung hat einen maßgeblichen Einfluss auf die Wirtschaftlichkeit und Zweckmäßigkeit des Projektes, da die hierdurch geschaffenen Grundlagen anschließend als gegeben feststehen und nur schwer zu widerrufen sind.

Je nach Projektgröße und geschätzter Kosten ist eine Vorab-/Machbarkeitsstudie empfehlenswert. Hierbei ist bei Softwareprojekten insbesondere darauf zu achten, dass eine Kompatiblität zur bestehenden Infrastruktur gewährleistet ist.

Für die Entwicklung von Webanwendungen stellt bspw. der BSI Leitfäden zur Entwicklung sicherer Webanwendungen (zwei Leitfäden, Empfehlung für Auftraggeber und Auftragnehmer) inkl. Anforderungen etc. zur Verfügung.

4.6. Standardisierung / Kompatibilität des IT-Verfahrens

Bei der Durchführung und insbesondere bei der Beschaffung (neuer) IT-Systeme sind die Standardisierung sowie Kompatiblität der neuen Systeme zur bestehenden IT-Infrastruktur eine große Herausforderung. Die Kompatiblität der neuen Produkte hat eine direkte Auswirkung auf die Wirtschaftlichkeit und Zweckmäßigkeit des späteren Einsatzes.

Hierbei sollte min. darauf geachtet werden, dass die neuen Komponenten folgende Anforderungen erfüllen:

- Kompatiblität zu den IT-Standards der Organistation
    - Vohandene (Standard) Hardwarevorrausetzungen werden unterstützt.
        - Netzwerk
        - Serversysteme

        - Client
        - Ggf. Peripherie (Drucker / Scanner etc.)
    - Eine Kombatitblität zur bestehenden (standardisierten) Softwarelandschaft besteht.
        - (Server-/Client)Betriebssystem
        - Browserstrategie
        - Konfigurations-/Sicherheitseinstellungen
        - Vor- / Folgesystemen
- Vorhandene notwendige Schnittstellen zum
    - ERP/Finanz- und Buchhaltungssystem
    - eAkte-System
    - ISMS / Personalmanagement-System
    - Weiterer wichtiger Querschnttsverfahren

  (Oder die Möglichkeit zur späteren Anbindung bestehen.)
- Einhaltung standardisierter Programmier / Softwareentwicklungs-Richtlinien

Die allgemeinen Anforderungen der jeweiligen internen Vorgaben und Richtlinien der Organistation sollten durch die Einführung weiterhin erfüllt werden.

Sofern es keine standardisierten Vorgaben und Prozesse bspw. IT-Richtlinien, Anforderungen an finanzrelevante Verfahren, Projekthandbücher, Programmierrichtlinien, Aktenpläne, Anforderungen an Schriftgutverwaltung, IT-Sicherheitsrichtlinien etc. gibt, sind diese grundsätzlich zu erstellen und für die Organistation und für die Durchführung von Projekten anzuwenden.

4.7. Prozessanalyse / Prozessprüfung

Dreh- und Angelpunkt der Einführung eines IT-Projektes sind die einzelnen Prozesse. Hierzu zählen auch die jeweiligen Organistationseinheiten. Ein IT-Projekt ist ein Organisationsprojekt.

Die einzelnen Prozesse müssen vorab bestehen und beschrieben sein.

Dennoch wird oft bei Einführung eines IT-Systems (vermeintlich zum ersten Mal) der Prozess betrachtet. Hierbei gilt:

Digitaler Unsinn, bleibt Unsinn!!

Losgelöst der späteren Digitalisierung der einzelnen Prozesse müssen diese klar beschrieben und definiert sein. Die Aufnahme der Prozesse muss **vor** der Digitaliserung stattfinden. Erst wenn der Prozess beschrieben und abgenommen ist, kann dieser digitalisert werden.

Hierfür sind ggf. die Stellen zur Prozessorganisation einzubeziehen, welche mit dem jeweiligen Fachbereich vorab die Prozesse erstellen oder redesigenen. Eine

Prozessprüfung kann an dieser Stelle oder ggf. schon vor dem eigentlichen Projekt durchgeführt werden. Eine Prozessprüfung zeigt Schwachstellen klar auf. Durch eine gute Prozessprüfung werden ggf. spätere Einzefallprüfungen obsolet.

4.8. Konzeption / Dokumentation

Am Anfang eines Projektes gibt es wenige Grundlagen (Dokumentationen / Konzepte). Diese werden erst im Laufe des Projektes erstellt. Zum Start des jeweiligen Projektes sollten alle Informationen bzgl. der Projektorganistation sowie die Ergebnisse der Projektgrundlage (Vorstudien etc.) vorliegen.

Im Laufe des Projektes sind weitere fachliche und technische Dokumentationen zu erarbeiten, welche den IST-/SOLL-Zustand beschreiben. In vielen Projekten wird die Priorität für Dokumenation grob vernachlässigt. In manchen Projekten werden keine Konzepte und Dokumentationen angefertigt. Hierbei ist auf die jeweiligen Dokumentationspflichten hinzuweisen und deren Einhaltung zu fordern.

Vor Umsetzung einzelner Maßnahmen müssen Soll-Konzepte erstellt werden. Diese Soll-Konzepte sind von den jeweiligen Verantwortlichen (Projektleitung / Verfahrensbetreuung / Prozessverantwortlichen) abzunehmen und freizugeben. Erst nach Freigabe eines Kozeptes kann dies umgesetzt werden.

Weiterhin sind für alle Module und Prozesse vollständige (Verfahrens-) Dokumentationen zu erstellen. Bestenfalls ensteht daraus eine vollumfängliche Verfahrensdokumentation, die alle Bereiche abdeckt.

Folgende Dokumentation sollten in den jeweiligen Phasen erstellt werden:

Projektstart	Doumentation der Projektorganisation
Projektdurchführung	Erestellung Dokumentation Erstellung und Abnahme Konzepte
Projektabschluss	Fertigstellung der vollumfänglichen (Verfahrens-) Dokumentation Projektabschlussbericht

Tabelle 3 - Dokumentationen der einzelnen Projektphasen

Grundlagen für die Erstellung der Dokumentation sind u.a. die Ziffern 6 und 10.1 GoBD sowie das IT-Grundschutz-Kompendium des BSI.

4.9. Prüfung des (umzusetzenden / fertigen) IT-Systems

Das Ergebniss des jeweiligen Projektes muss die gesetzlichen und internen Vorgaben vollumfänglich abbilden.

Im Gegensatz zur ex post Prüfung ist die projektbegleitende Prüfung eine ex ante Prüfung. Die Entwicklung und Konzeption des jeweiligen IT-Systems wird zeitnah verfolgt. Innerhalb der einzelnen Projektsitzungen und zu den einzelnen Konzepten können direkte Empfehlungen und Anmerkungen ausgesprochen werden. Der Inhalt der jeweiligen Anforderungen basiert auf den gesetzlichen Grundlagen und entspricht hierbei den gleichen Anforderungen wie für bereits bestehende IT-Systeme.

Als Grundlage hierfür können die Checklisten und Leitlinien zur Prüfung von IT-Verfahren herangezogen werden.

4.10. Projektabschluss und Empfehlungen

Nach Abschluss des Projektes ist von der Projektleitung ein Projektabschlussbericht zu erstellen. Aus dem Projektabschlussbericht sind die weiteren Handlungsempfehlungen des Projektes an den Auftraggeber / Lenkungsauschuss ersichtlich.

Im Zuge der Projektprüfung ist nach Abschluss des Projektes ein Prüfbericht zu erstellen. Dieser sollte alle Prüffestellungen beinhalten. Hierzu zählen:

- Prüffestellungen zur Projektorganistation
- Prüffestellungen zur Projektgrundlage (sofern nicht bereits vorab erstellt)
- Prüffestellungen zum Projektergebnis (dem fertigen IT-System)

Des Weiteren sollte der Bericht der Revision eine Prüffestellung bzgl. der weiteren Maßnahmen und Empfehlungen unter Bezugnahme auf den Abschlusbericht beinhalten.

5. Literatur und Hilfen

5.1. Allgemein

- IDW PS 850 - Projektbegleitende Prüfung bei Einsatz von Informationstechnologie
- DIIR Prüfungsstandard Nr. 4 STANDARD ZUR PRÜFUNG VON PROJEKTEN DEFINITIONEN UND GRUNDSÄTZE
- BSI-Leitfäden zur Entwicklung sicherer Webanwendungen (www.bsi.de)
- IDR Prüfleitlinien