Techno Pharm Fokus IT

Regulatorische Anforderungen an die IT(IL) Prozesse

Eine Analyse verschiedener Guidelines

Dr. Eberhard Klappauf • COMLINE AG, Bad Homburg, Fachgruppe IT, APV, Mainz
Konstantin Clevermann • IDS Scheer Consulting GmbH, Düsseldorf, Fachgruppe IT, APV, Mainz

Korrespondenz: Konstantin Clevermann, IDS Scheer Consulting GmbH, Niederkasseler Lohweg 189, 40547 Düsseldorf;
e-mail: konstantin.clevermann@softwareag.com

Zusammenfassung

Der IT-Betrieb in GxP-regulierter Umgebung stellt an IT-Leitung und Mitarbeiter für viele Tätigkeiten Anforderungen, die deutlich von denen abweichen, die nicht regulierte Unternehmen berücksichtigen müssen. Ungenügende Prozesse oder Fehlverhalten im IT-Betrieb regulierter computerisierter Systeme (CS) gefährden deren qualifizierten und validierten Zustand und damit die regulatorisch zulässige produktive Nutzung. Als nützliche Hilfestellung für die Einhaltung der gesetzlichen GxP-Anforderungen im IT-Betrieb bietet sich der Anfang 2010 veröffentlichte „Good Practice Guide (GPG) IT Operations" als Companion zum „GAMP® 5" der ISPE an. Die IT ihrerseits verfügt seit 2 Jahrzehnten für „IT Service Management" (ITSM) über das immer weiter verfeinerte Best Practices Framework des Office of Government Commerce (OGC): die „IT Infrastructure Library®", kurz ITIL®, in der aktuellen Version 2011. Seitens der ISPE wird erstmalig mit GAMP® 5 dieses Framework bei der Diskussion des IT-Betriebs zitiert. In der folgenden Diskussion wird gegenübergestellt, wie die Guidelines beider Welten, also der GAMP® Good Practice Guide IT Operations und die ITIL® Best Management Practices für das regulatorische Umfeld, trotz einiger Unverträglichkeiten, nutzbringend eingesetzt werden können.

Einleitung

Im Januar 2010 hat die ISPE den „Good Practice Guide (GPG) IT Operations" als Companion zum GAMP® 5 veröffentlicht, der Vorschläge für den Betrieb von GxP-relevanten computerisierten Systemen bietet. Bisher haben Empfehlungen für den über viele Jahre aufrecht zu erhaltenden IT-Betrieb von GxP-regulierten computergestützten Systemen (CS) gefehlt. Denn alle Frameworks oder Guidelines für das IT Service Management (ITSM) waren branchenneutral und damit nur bedingt auf die Anforderungen des GxP-Umfelds abgestimmt. Die Abb. 1 gibt eine Übersicht über branchenneutrale sowie über GxP-relevante Regelwerke und Guidelines zur IT und zum ITSM. In dieser Abhandlung wird der Schwerpunkt auf die Empfehlungen für die operativen IT-Prozesse gelegt, die bereits im GAMP® 5 aufgeführt sind. Es wird exemplarisch betrachtet, wie diese sowohl durch den GPG IT Operations als auch durch das ITIL®-Framework abgedeckt werden. Die gesetzlichen GMP-Regelwerke stellen zunächst nur allgemeine regulatorische Anforderungen an den IT-Betrieb. Dazu versucht jetzt der GPG IT Operations die einzelnen Prozesse eines regulierten IT-Betriebs detailliert zu beschreiben. Er behandelt den operativen Betrieb unabhängig vom Einsatzbereich und von der GAMP-Hardware- oder Software-Kategorie. Bezogen auf den CS-Life Cycle setzt er dabei erst nach der Projektphase, also nach Qualifizierung und Validierung oder Verifikation eines Systems auf und startet mit dem Beginn des produktiven Einsatzes. Dementsprechend werden im GPG die Prozesse vom „Handover" bis zur „Stilllegung" betrachtet (Abb. 2).

Als wesentliche Ziele formuliert der GPG folgende:

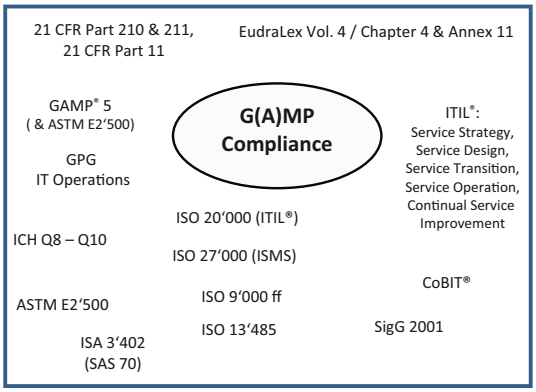

Abb. 1: Regelwerke und Guidelines für das regulierte IT-Service Management.

TechnoPharm 2, Nr. 5, 320–327 (2012)

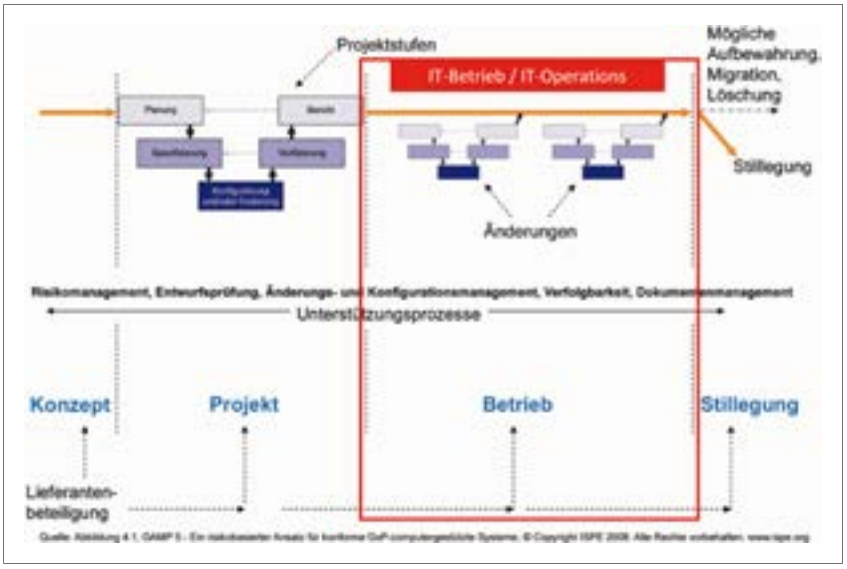

Abb. 2: Life Cycle für ein Computerisiertes System nach GAMP® 5.

- besseres Verständnis der operationellen IT-Prozesse mit ihren Beziehungen und Abhängigkeiten untereinander,
- grafisch einheitliche Darstellung der Prozesse in Prozess-Ablaufplänen, einschließlich Musterdokumenten für die Arbeitsergebnisse (control records)
- Hilfestellung, um Rollen und Verantwortungen zuzuordnen
- Überlegungen zu einem skalierbaren Risk-Based Approach.

Die Prozesse nach GAMP® 5 und GPG

Für eine bessere Übersicht werden im GPG die Prozesse einzeln identifiziert, in Ablaufdiagrammen dargestellt sowie die erforderlichen Dokumente (control records) und die Verantwortlichkeiten beschrieben. Bereits im GAMP® 5 waren im Anhang „Operation Appendices" die wichtigsten Prozesse für den operationellen Betrieb der Systeme zusammengefasst. Darüber hinaus werden im GPG zwei zusätzliche Themen (Data Migration und System Retirement) behandelt. Für einen anderen Prozess, Archiving and Retrieval, wird auf den GPG Electronic Data Archiving verwiesen. Die hier betrachteten Prozesse sind somit:

- O 1 Handover
- O 2 Establishing and Managing Support
- O 3 Performance Monitoring
- O 4 Incident Management
- O 5 Corrective and Preventive Actions
- O 6 Operational Change and Configuration Management
- O 7 Repair Activity
- O 8 Periodic Review
- O 9 Backup and Restore
- O 10 Business Continuity Management
- O 11 Security Management
- O 12 System Administration
- O 13 Archiving and Retrieval
- D 7 Data Migration
- M 10 System Retirement

Der GPG unterteilt die Prozesse in System-unabhängige und System-spezifische Prozesse. Das ITIL®-Framework hat dazu keine äquivalenten Vorschläge. Andererseits ist in ITIL® adressiert, dass Best Practices für kleinere oder größere IT-Umgebungen unterschiedlich ausfallen werden. Im Fokus von ITIL® stehen natürlich die großen IT-Infrastrukturen.

Aus Sicht der Autoren lassen sich die im GPG empfohlenen Prozesse in vier unterschiedliche Gruppen ordnen:

(I) Deployment:
- O 1 Handover
- O 2 Establishing (aus: Establishing and Managing Support)

(II) Prozesse des überwiegend kontinuierlichen regulierten IT-Betriebs:
- O 2 Managing Support (aus: Establishing and Managing Support)
- O 3 Performance Management
- O 9 Backup (aus: Backup and Restore)
- O 11 Security Management
- O 12 System Administration

(III) Prozesse des regelmäßigen regulierten IT-Betriebs, jedoch überwiegend anlassbezogenes Vorgehen:
- O 4 Incident Management
- O 5 Corrective and Preventive Actions
- O 6 Operational Change and Configuration Management
- O 7 Repair Activity
- O 9 Restore (aus: Backup and Restore)

(IV) Prozesse aus besonderem Anlass:
- O 8 Periodic Review
- O 10 Business Continuity Management
- O 13 Archiving and Retrieval
- D 7 Data Migration
- M 10 System Retirement

Verantwortlichkeiten

Im GPG IT Operations werden die Rollen und Verantwortlichkeiten der einzelnen Aktivitäten gemäß der RACI-Methode vorgeschlagen (RACI = Responsible, Accountable, Consulted, Informed (vgl. Tab. 1)). Es werden konsequent die Rollen der in den Prozessen zu beteiligenden Personen zusammengestellt. In Einzelfällen werden mehrere Rollen durch nur eine Person wahrgenommen. Die RACI-Methode zur Beschreibung der Verantwortlichkeiten bei der Geschäftsprozessmodellierung ist ein regelmäßig angewandtes Vorgehen. Auch ITIL® empfiehlt die Zuordnung von

Verantwortlichkeiten in einer RACI-Matrix, differenziert diese aber, anders als der GPG, ohne ausdrückliche Berücksichtigung einer Rolle des Bereichs Qualitätssicherung. Mit der Erstellung einer RACI-Matrix wird den regulatorischen Anforderungen nach einer verantwortlichen Person für die Aktivitäten jedenfalls Rechnung getragen. Der GPG empfiehlt, vor allem folgende Rollen zu berücksichtigen:

- Prozesseigner,
- Systemeigner,
- Subject Matter Expert (SME) (sowohl aus der IT als auch aus den Fachbereichen),
- Quality Unit,
- Enduser,
- Lieferant.

In der Praxis stellt sich heraus, dass die Zuordnung der Verantwortlichkeit bzw. der Zuständigkeit zu den beiden Rollen Prozesseigner und Systemeigner nicht immer ganz einfach und eindeutig gegeben ist. Beispiele finden sich vor allem in Laborbereichen, seltener in den „reinen" IT-Bereichen. Der GPG verweist auch darauf, dass diese beiden Rollen auch bei nur einer Person liegen können.

Risk-Based Approach

Der GAMP® 5 GPG IT Operations wird dem Zusatz „a risk-based approach" gerecht, indem zu allen Prozessen eine Erläuterung bzw. Anregung im Sinne der „Risk-Scaleability" enthalten ist. Dies sind entweder einzelne Hinweise oder aber eine Risikomatrix, wie die Tab. 2 illustriert. Bei den meisten Prozessen ist eine zusätzliche Risikomatrix (analog zu bisherigen Gepflogenheiten) hinterlegt. Letztlich wird damit eine Hilfe geboten, den Aufwand für Sicherheit in den Prozessen angemessen festzulegen. Als Beispiel dazu (s. Tab. 2) ist im Prozess „System Administration" illustriert, wie bei Systemen mit „Low Impact" oder „Medium Impact" Änderungen von Berechtigungen von Rollen bzw. für User (Permissioning) als normale Administrations-Prozesse zu bewerten sind. Nur bei „High Impact-Systemen" sollte diese Aktivität unter Change Control durchgeführt werden. Ähnliches ist in ITIL® nicht so stark ausgeprägt; dort wird die Risiko-Betrachtung nur allgemein oder auf die Qualität der eigenen Service-Erbringung (z. B. Service-Verfügbarkeit bzgl. Service Level Agreements (SLAs)) bezogen. Natürlich wird in den IT(IL) Prozessen (implizit) differenziert, ob es sich z. B. um ein Entwicklungssystem, Testsystem oder Produktivsystem handelt. Die formale Risikoeinschätzung bzgl. so spezifischer Risiken wie Patientengefährdung und Produktqualität findet dort keinen Nachweis. Bewertet man die oben stehenden Prozesse in der alternativen Gruppeneinteilung (I) bis (IV), so ergibt sich bezogen auf die Risikoeinschätzung folgendes:

- Die Gruppe (I) ist überwiegend durch die die letzten Schritte der Life Cycle-Phase Qualifizierung / Validierung geprägt und individuell durchzuführen. SOPs können nur einen abstrakten Rahmen vorgeben, der die Erfordernisse spezifiziert (Prüflisten zu Status, Testergebnissen und Dokumenten). Die Risiken für Produktqualität, Patientensicherheit oder Daten-Integrität sind gering einzustufen, da noch kein Eingriff an bereits produktiven CS erfolgt.

Tabelle 1

RACI Methode.

Die RACI – Methode	
Responsible / Zuständig	"Handelnde" Person, "Macher", verantwortlich für die eigentliche Durchführung, eine oder mehrere Personen
Accountable / Verantwortlich	diejenige Person, die die Aktivität (formal) zu verantworten hat; rechenschaftspflichtig aus regulatorischer und Prozess-Sicht bzw. Kostenverantwortlichkeit; es ist im Allgemeinen der Prozesseigner; es kann immer nur eine Person für einen Prozess, eine Aufgabe oder ein Projekt verantwortlich sein
Consulted / Beratend	Person(en), die die Aktivität aktiv beratend unterstützt
Informed / Informiert	Person(en), die über die Aktivität bzw. das Ergebnis zu informieren ist; die Rolle selbst ist passiv

Tabelle 2

Risk Based Approach am Beispiel „System Administration".

System Administration Task	User Account Mngmt	Permissioning	Monitoring	Data Maintenance	....
Low Impact System	...	✓	✓	✓	...
Medium Impact System	...	✓	✓	Change Request	...
High Impact System	...	Change Request	✓	Change Request	...

TechnoPharm 2, Nr. 5, 320–327 (2012)

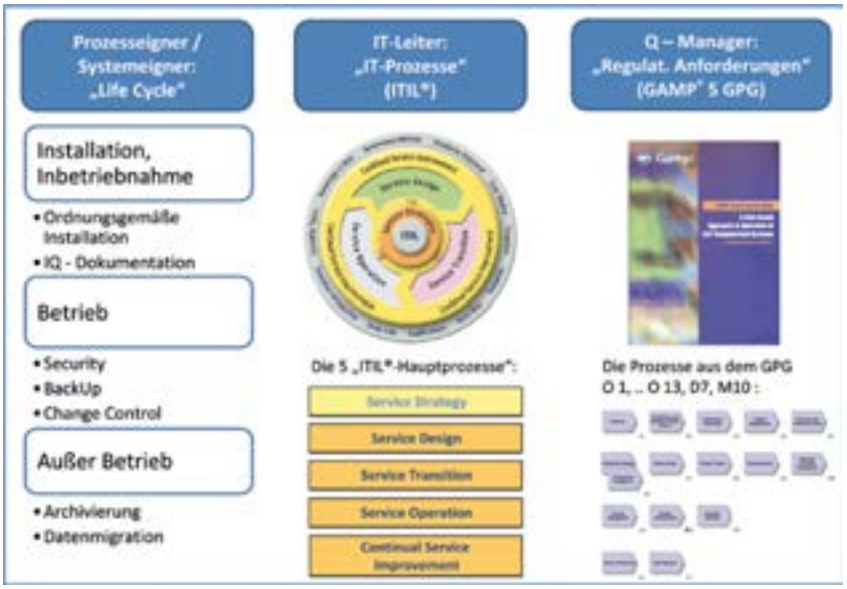

Abb. 3: Verantwortliche und ihre verschiedenen Sichten auf den Life Cycle eines CS und die IT Operations.

- Prozesse der Gruppe (II) lassen sich standardisieren und detailliert in SOPs und zugehörige Controls fassen. Sie werden häufig durch Tools unterstützt oder sogar ausgeführt. Auch hier sind die Risiken eher gering, da kaum oder nur begrenzt Eingriffe (Change Requests) in die Systeme erfolgen.
- Die Prozesse der Gruppe (III), die überwiegend mit Systemveränderungen zusammenhängen, haben normalerweise ein höheres Risiko. Aber auch hier lohnt eine verlässliche Risikobetrachtung, weil es sich bei den Änderungen um Standardmaßnahmen (z. B. Einspielen von Security Patches) oder aber um z. B. das Einspielen komplett neuer Software-Versionen oder Funktionen handeln kann. Diese Prozesse lassen sich auf der Meta-Ebene standardisieren, müssen aber häufig individuell gelöst werden.
- Die Prozesse aus besonderen Anlässen (IV) unterscheiden sich von den anderen drei Gruppen durch den Umstand, dass sie zwar weitgehend vorauszuplanen sind und zunächst geringe Risiken bergen, doch werden sie selten ausgeführt, wodurch die Risiken in der Durchführung zunehmen.

Obwohl der GPG die Forderung nach einer Risiko-Bewertung für die meisten Prozesse beschreibt, sind doch die Verfahren der Risiko-Erhebung und -Bewertung nicht spezifiziert. Vorschläge dazu finden sich im GAMP® 5 –Guide mit einem zweistufigen Verfahren (Risiko-Klassifizierung und -Priorisierung), oder in der ICH Q9 mit Einsatz der FMEA/FMECA und ISO 14971.

Verschiedene Sichten auf die Prozesse

Nun haben verschiedene leitende Mitarbeiter in einem Unternehmen aufgrund ihres Verantwortungsbereichs unterschiedliche Sichten auf die IT Operations-Prozesse.

IT-Leiter

Der IT-Leiter hat primär die Aufgabe, für den Support aller IT-Systeme eine durchgängig hohe Qualität und Performance zu gewährleisten. Häufig hat er seine Prozesse an den Best Practices von ITIL® ausgerichtet. Darin findet er für alle Bereiche des ITSM umfangreiche Hinweise für die IT-Prozesse und ihr Management. Die speziellen Erfordernisse der Compliance-Anforderungen wird er in den meisten, aber nicht allen Fällen adressiert finden. So wird er die Prozesse Incident Management und Problem Management anders interpretieren müssen und die dem ITIL®-Framework unbekannte Anforderung der Corrective Action/Preventive Action (CAPA) neu in das Prozess-Portfolio aufnehmen müssen.

Weiterhin wird der IT-Leiter die abweichenden oder zusätzlichen Interpretationen beachten: Der Audit Trail für qualitätsrelevante Daten, sowie die Behandlung von „electronic records" ist für alle Applikationen und Tätigkeiten der IT-Administration von entscheidender Bedeutung (vgl. 21 CFR Part 11 und Annex 11).

Q-Manager

Der Qualitätsbeauftragte hat zu gewährleisten, dass für alle GxP-relevanten Systeme eine qualifizierte IT-Infrastruktur zur Verfügung steht und dass bei ihrem Betrieb der qualifizierte und validierte Zustand der computergestützten Systeme nicht gefährdet oder sogar beschädigt wird. Er wird sich, in der Kenntnis der gesetzlichen Anforderungen, auf die Empfehlungen des GAMP® 5 und des GPG stützen, damit von den Verantwortlichen für das ITSM die Serviceleistungen in der regulatorisch erforderlichen Qualität erbracht werden.

Prozesseigner/Systemeigner

Der Prozesseigner bzw. Systemeigner aus Anwendungssicht wiederum ist verantwortlich für den qualifizierten und validierten Zustand seines Systems und betrachtet daher den gesamten Life Cycle seines Systems (Abb. 3). So unterschiedlich die Sichtweisen und Herangehensweisen auch sind: letztlich sollten diese miteinander integriert werden in einheitliche Prozesse, die einen qualifizierten IT-Betrieb regeln. Laut einer Studie von IDC aus 2010 haben über 60 % der Unternehmen mit mehr als 500 Mitarbeitern ein IT-Service Management in Anlehnung an ITIL® Best Practices etabliert oder planen dies. Die Berücksichtigung jedweder regulatorischer Anforderungen werden in den Best Practices von ITIL®

bestenfalls in allgemeiner Form (regulatory compliance, z. B. SOX, ISO/IEC 27001, etc.) angesprochen. Insofern wird der Abgleich der Life Cycle Phasen des GAMP® 5 und des GPG IT Operations mit denen des ITIL®-Frameworks immer wichtiger. Es liegt primär in der Verantwortung des IT-Leiters, die GPG Good Practices zur Erfüllung der regulatorischen Anforderungen in seine nach ITIL® ausgerichteten Prozesse zu integrieren.

Life Cycle-Phasen im GPG und in ITIL®

Aus Sicht des Systemeigners müssten die Anforderungen zunächst einmal den verschiedenen Phasen des Life Cycle zugeordnet werden, wobei, wie schon zuvor erläutert, fast alle zur Betriebsphase gehören. Sie sind (mit Ausnahme von Installation und Inbetriebnahme) im ITIL®-Hauptprozess „Service Operation" abzubilden.

Das Aufsetzen des „Handover", sowie das Einführen bzw. Vorbereiten der Unterstützungsprozesse gehören noch in die Endphase der Qualifizierung bzw. Validierung eines CS vor dem Go Live. In ITIL® findet man sie im Hauptprozess „Service Transition". Die Beschaffung und Installation, die in der IQ betrachtet werden, sind nicht Bestandteil des GPG IT Operations, müssen aber im Gesamtkontext einer qualifizierten IT-Infrastruktur betrachtet werden. Das Thema Datenmigration wird – je nach System bzw. Übergabe – vor dem Produktivstart (als Übernahme aus einem Legacy-System), oder aber bei der Außerbetriebnahme – falls es von einem anderen System abgelöst wird – relevant.

Abgleich einiger Prozesse des GPG mit ITIL®

Die Prozesse des GPG IT Operations finden Entsprechungen in vier von fünf Hauptprozessen des ITIL®-Framework. Der GPG verzichtet berechtigter Weise darauf, Konzepte und Strukturen für den Aufbau einer IT-Abteilung zu begleiten. So kann aus Sicht der GxP-Regulierung der erste ITIL®-Hauptprozess „Service Strategie" (die erste Phase des ITIL®-Life Cycles) weitgehend unbeachtet bleiben. Für die kontinuierliche Qualitätssteigerung wurde ein eigener Hauptprozess „Continual Service Improvement" (CSI) etabliert. Damit kann das ITSM an das Qualitätsmanagement-System des Unternehmens (QMS) angeschlossen werden. Unterstützt wird er in „Service Operation" von ITIL®, indem dort für eine Reihe administrativer IT-Tätigkeiten ein Audit Trail empfohlen wird, in Anerkennung der Eingriffsmöglichkeiten durch Personen mit Administrationsrechten. Im Folgenden (vgl. Abb. 4) soll auszugsweise der zentrale ITIL®-Hauptprozess Service Operations mit den teilweise übereinstimmenden Prozessen des GPG verglichen werden: Incident Management, Repair Activity und Preventive Action (als Teil von CAPA). Die beiden hier zugeordneten ITIL®-Prozesse sind besonders auffällige Kandidaten für eine abweichende Implementierung im regulierten Umfeld:

- Incident Management und
- Problem Management.

Aus dem regulierten Umfeld stehen ihnen die nur eingeschränkt entsprechenden GPG-Prozesse Incident Management, Preventive Action (als Teil von CAPA) und Repair Activity gegenüber. Im nicht regulierten Umfeld besteht die Aufgabe des Incident Managements in der schnellstmöglichen Störungsbeseitigung und Wiederherstellung eines Services, orientiert an den SLAs. Die Initiierung (ITIL®: Event) zur Erfassung und Bearbeitung des Incident erfolgt über den Service Desk als Single Point of Contact (SPOC). Die zur Lösung des Incident erforderlichen Maßnahmen greifen bei bekannten Störungen auf Workarounds zurück, andernfalls wird im Rahmen der Bearbeitung eine Maßnahme gesucht, die die Störung behebt. Dazu wird ggf. zur fachlichen Unterstützung an den 2nd Level Support oder den 3rd Level Support eskaliert. Die Störungsursache grundsätzlich zu beheben wird innerhalb ITIL® an einen anderen Prozess delegiert: das Problem Management. Erst in diesem Prozess werden, ohne direkten zeitlichen Zusammenhang, die Fehlerursache ermittelt, Lösungen für die Beseitigung der Fehlerursache erarbeitet und ein Request for Change (RfC) gestellt. Für die im Incident Management des GPG zu CAPA alternativ empfohlenen Aktivitäten, die unter Repair Activity ablaufen, können mit „predefined standard incident models" (ITIL®) identifiziert werden. In ihnen werden nach ITIL® bereits bekannte Störungen, hier Austausch defekter Hardware-Komponenten, behoben. Ansonsten müssen derartige „Repair Aktivitäten" bei ITIL® in einem Change abgewickelt werden. Alle anderen Störungsarten, seien es Funktionen der Software, Daten-Verfügbarkeit oder Daten-Integrität, werden ebenfalls im Incident Management von ITIL® bearbeitet und behoben, z. B. durch bekannte Work-

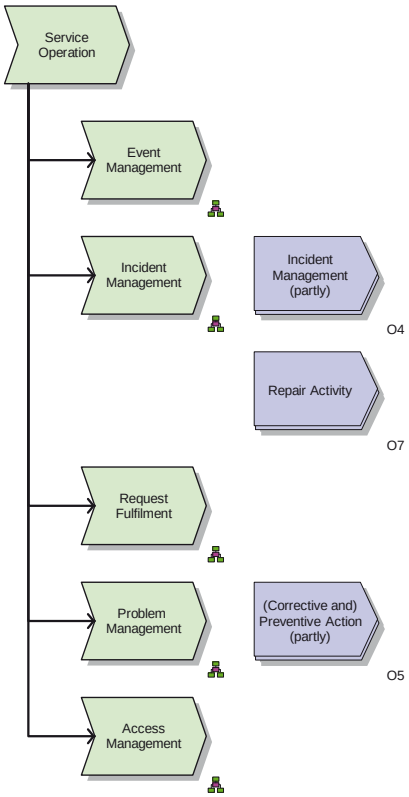

Abb. 4: Gegenüberstellung einiger Prozesse aus ITIL® Service Operations vs GPG bei streng ausgelegter Korrelation der Aktivitäten (Interpretation der Autoren).

TechnoPharm 2, Nr. 5, 320–327 (2012)

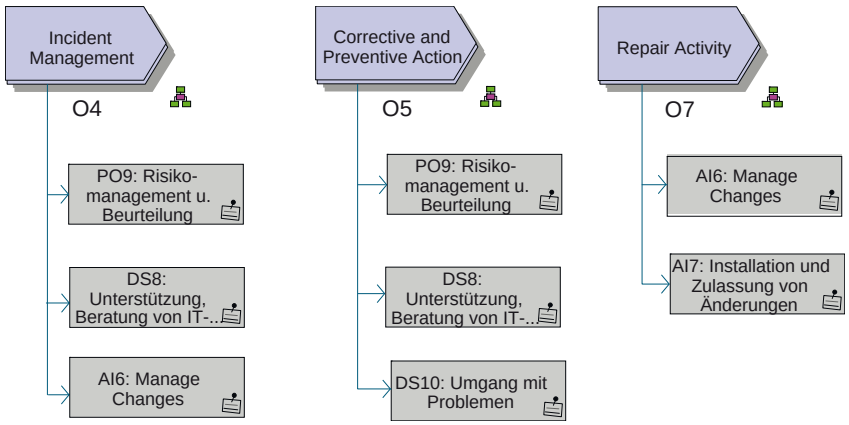

Abb. 5: Zuordnung einiger Controls aus CObIT® zu GPG IT Operations Prozessen.

arounds. Der GPG sieht demgegenüber neben den beiden genannten Abläufen CAPA und Repair Activity keine Alternative vor. Für die ITIL®-Prozesse Event Management, Request Fulfilment und Access Management finden sich im GPG keine eigenen Prozess-Modelle. Dies ist im Fall ITIL®-Event Management unerheblich, da dieser Prozess als erstes nur eine Erfassungsfunktion ausführen lässt. Ziel dieses Prozesses ist, alle „Vorkommnisse" in der Umgebung der IT Operations zu erfassen. Dieser Aspekt (ein „Logbuch" der Vorkommnisse) wiederum ist teilweise im GPG als Bestandteil des Incident Management (GPG) eingestuft. Das Event Management führt darüber hinaus ggf. Aktionen durch, die Reaktionen automatisierter Monitoring-Systeme beinhalten. Hier ist unbedingt zu prüfen, wie diese Aktionen regulatorisch zu behandeln sind. Nach der Protokollierung erbringt das Event Management noch eine Filter- und Zuweisungsfunktion. Jedes Event ist einer der folgenden vier Weiterbearbeitungen zu unterwerfen:

- Incident Management (wie zuvor diskutiert)
- Problem Management (wie zuvor diskutiert)
- Access Management (Security)
- Request Fulfilment

ITIL® lässt in dem separaten Prozess Access Management alle Vorfälle bearbeiten, die mit jeder Art Änderungen von Anwender-Berechtigungen verbunden sind. Einige wenige Hinweise zu derartigen Aktivitäten finden sich im GPG unter Establishing and Managing Support Service. Die grundsätzlichen Verfahren zur Security werden im GPG-Prozess Security Management behandelt, und die Änderungen von Anwender-Rechten werden im Teilprozess „Starter, Leavers and Movers Processes". Im Request Fulfilment werden Anfragen jedweder Art erledigt. Kennzeichnend ist, dass sie keinerlei Auswirkungen auf die IT-Infrastruktur haben. Im GPG IT Operations findet sich keine direkte Entsprechung.

Trotz der divergenten Zielsetzungen und der oben dargestellten Unterschiede stellt sich eine hohe Überdeckung zwischen den Empfehlungen des GPG und der ITIL® Best Practices ein. Es lassen sich viele Synergien identifizieren und letztlich in einer integrierten Vorgehensweise zusammenfassen.

Update ITIL® v3 auf ITIL® 2011

In 2011 wurde durch die OGC eine aktualisierte Version ITIL® 2011 veröffentlicht. Dazu wurde die Version v3 (inzwischen auch ITIL® 2007) in vielen Punkten überarbeitet und ergänzt. Dies trifft für alle 5 Hauptprozesse zu. So wurden u.a. die Schnittstellen der Prozesse verfeinert (Input/Output), Prozesse detaillierter beschrieben, weitere Rollen spezifiziert und Begriffe präziser gefasst (Glossar) und konsistenter eingesetzt. Die Grundprozesse sind unverändert geblieben, doch ist im Service Design der Prozess Design Coordination neu hinzugekommen. Das Incident Management enthält im Incident-Abschluss die Prüfung, ob Problems, Workarounds oder Known Errors an das Problem Management zu melden sind.

In Summe ist festzuhalten, dass die Änderungen der Version ITIL® 2011 weitgehend unbeachtlich sind für die Nutzung des ITIL®-Frameworks für den regulierten IT-Betrieb unter Beachtung des GPG IT Operations.

Abgleich zu CObIT®

Aus IT-Sicht ist neben ITIL® ein weiteres Framework für die Ordnungsmäßigkeit relevant: Control Objectives for Information and Related Technology, kurz CObIT®. CObIT® enthält, ähnlich wie ITIL®, Empfehlungen für IT-Prozesse. Darüber hinaus wird von CObIT® ein umfangreicher Katalog an Controls angeboten, um die Angemessenheit und Wirksamkeit der eingeführten Verfahren zu beurteilen. Dies erfolgt insbesondere im Rahmen von auf CObIT® basierenden Audits, internen wie externen. Die Controls sind in vier Domänen gruppiert:

- PO Plan and Organize
- AI Acquire and Implement
- DS Deliver and Support
- ME Monitor and Evaluate

Die ISPE hat im Anhang zum GPG eine tabellarische Cross-Referenz erstellt, in der die betroffene CObIT® Controls aufgeführt sind. Auch sie bietet zwar eine erste gute Orientierungshilfe, muss jedoch im jeweiligen Einzelfall genau analysiert werden. Es ist nachvollziehbar, dass die Prozesse des GAMP® 5 Companion am stärksten die CObIT® Controls in den Bereichen „Acquire and Implement" und „Deliver and Support" beeinflussen. Interessanterweise ist in CObIT® wieder stärker die Risikobeurteilung thematisiert. Zum Vergleich ist in Abb. 4 der Zusammenhang zwischen den drei GPG-Prozessen und ITIL®-Prozessen dargestellt und in Abb. 5 zwischen den gleichen drei GPG-Prozessen und den CObIT®-Controls, die in diesen drei exemplarisch ausgewählten GPG-Prozessen relevant sind.

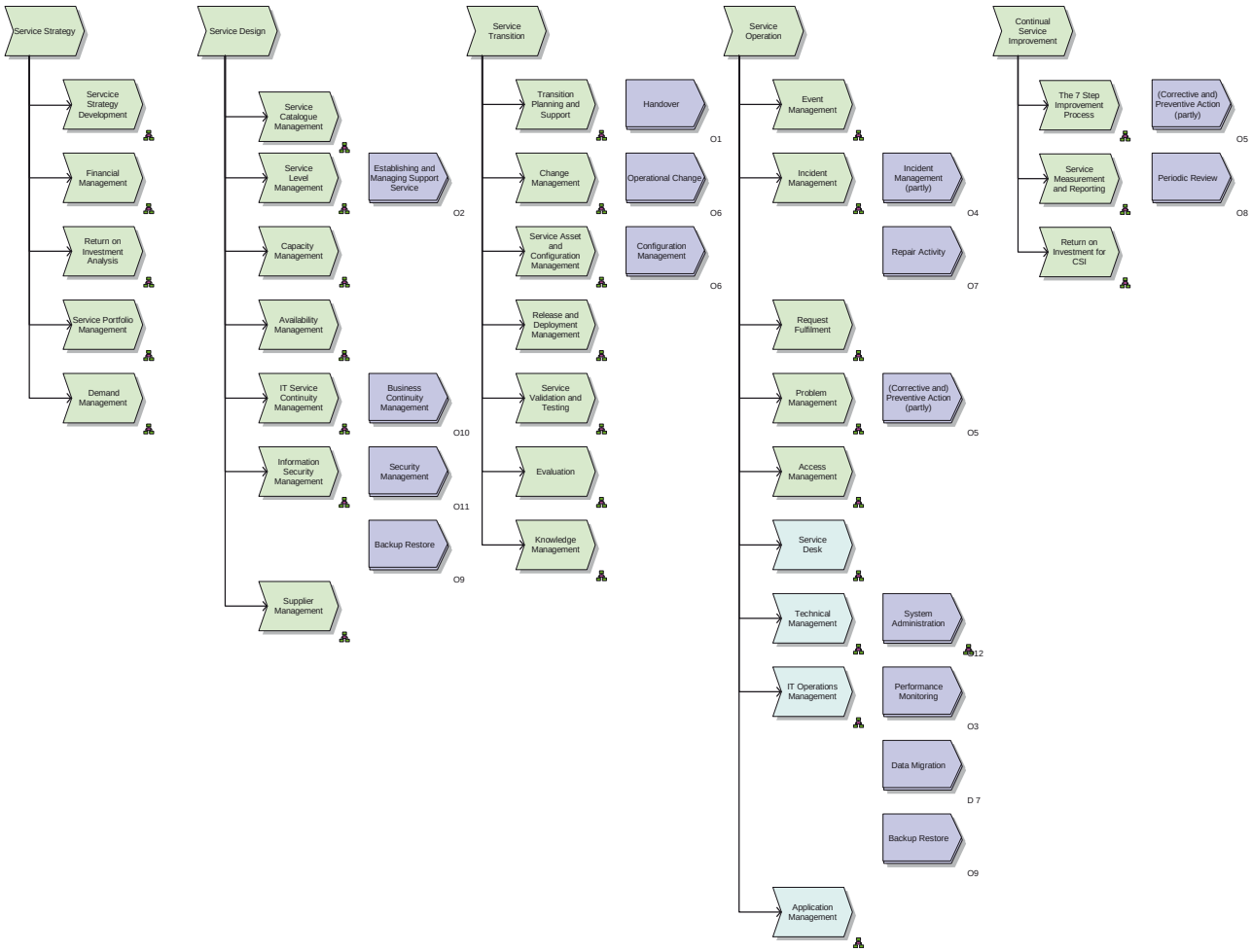

Abb. 6: Gegenüberstellung GPG IT Operations vs ITIL®-Framework. Sie gibt einen Überblick der Zuordnung von GAMP® 5-Prozessen (violett markiert) zu ITIL®-Prozessen (grün markiert). Die fünf Spalten repräsentieren die fünf ITIL®-Hauptprozesse „Service Strategy", „Service Design", „Service Transition", „Service Operation" und „Continual Service Improvement". Es war zu erwarten, dass aufgrund der unterschiedlichen Zielsetzung von ITIL® und GAMP® 5 und seinem GPG eine Zuordnung der Prozesse nicht 1:1 möglich ist, sondern dass dies einiger Interpretation bzw. detaillierter Analyse der Prozesse bedarf. Das heißt, die nachfolgende Sicht ist zunächst ein Einstieg, um anschließend in einer detaillierten Analyse die IT-Prozesse zu optimieren.

Zusammenfassung

Der GAMP® 5 GPG IT Operations ist ein deutlicher Schritt zur Prozessoptimierung der IT-Prozesse im regulierten Umfeld. Erstmalig sind damit „qualitative" Anforderungen prozessorientiert dargestellt worden. Dies wird verstärkt durch die konsequente Zuordnung der Rollen und Verantwortungen nach dem RACI-Konzept. Die Zuordnung zu den Prozessen des ITIL®-Frameworks, die aufgrund der unterschiedlichen Ansätze nicht eindeutig sein kann, gibt trotzdem eine große Hilfestellung für IT-Manager, diese Anforderungen in ihre internen IT-Prozesse zu integrieren. Die Gegenüberstellung der GPG-Prozesse zu denen des ITIL®-Frameworks bedürfen einer detaillierten Betrachtung. Vor allem größere IT-Organisationen, die ihr ITSM bereits in Anlehnung an ITIL® organisiert haben, werden von dort ausgehend die regulatorischen Anforderungen integrieren. Ebenfalls sind die notwendigen Controls, die in CObIT® beschrieben sind, zugeordnet und aufbereitet worden. Werden mit Hilfe der Prozessdarstellungen die Anforderungen aus dem GPG als „Requirements" und die „Controls" aus CObIT in die ITIL® Prozesse integriert, gewinnt man eine integrierte Sicht auf die IT Operations für eine regulierte Umgebung. Diese Prozesse können (und sollten!) in einem integrierten Prozessmodell zusammengeführt werden, um IT-intern globale GxP-compliant Prozesse für das IT Service Management zu erreichen.

Fachliteratur

GAMP® 5, A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008
GAMP, A Risk-Based Approach to Operation of GxP Computerized Systems, Companion Volume to GAMP® 5 ISPE 2009
ITIL® 2011 Core Publications (Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement), Cabinet Office part of HM Government, former Office Government Commerce (OGC), 07/2011
Aligning CObIT® 4.1, ITIL® v3 and ISO/IEC 27002 for Business Benefit, IT Governance Institut, 2008

TechnoPharm 2, Nr. 5, 320–327 (2012)

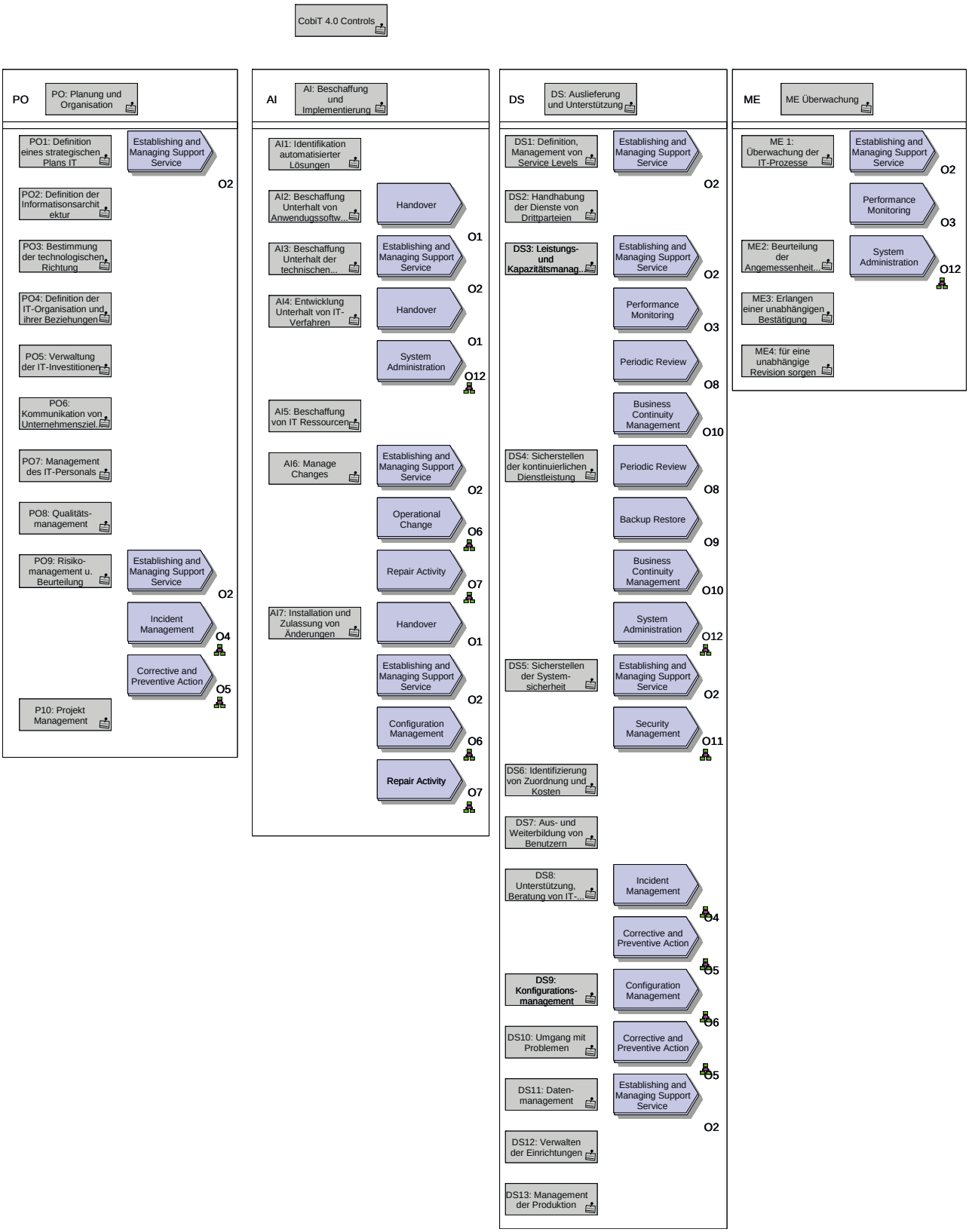

Abb. 7: Gegenüberstellung GPG IT Operations vs CObIT®. Sie zeigt im Überblick die Beziehung von GAMP® 5-Prozessen (violett markiert) zu CObIT® Controls (grün markiert). Die vier Spalten repräsentieren die Domänen „Plan and Organize" (PO), „Acquire and Implement" (AI), „Deliver and Support" (DS) und „Monitor and Evaluate" (ME) (noch CObIT Version 4.0). Es ist naheliegend, dass die Prozesse des GAMP® 5 Companion am stärksten die CObIT® Controls in den Bereichen „Acquire and Implement" und „Deliver and Support" beeinflussen.