
IT-Service-Management für Hochschulrechenzentren

Inhaltsverzeichnis

1	Vorwort	1
2	Was ist IT-Servicemanagement?	3
3	Unterschied zwischen dem ITSM von Unternehmen und Hochschulen.....	5
4	How to get started?	7
5	IST-Zustand und Benchmarking.....	8
5.1	Analysetool zur strukturierten Zustandserhebung.....	8
5.2	Zielvorstellung	10
6	Anforderungen an das IT-Servicemanagement von Hochschulrechenzentren. 10	
6.1	Grundlegende Anforderungen (GR1-GR7).....	11
6.1.1	GR1: Verpflichtung der Hochschulleitung	11
6.1.2	GR2: Art und Umfang der Dokumentation.....	13
6.1.3	GR3: Definition des Anwendungsbereichs des Service Managements	15
6.1.4	GR4: PLAN: Planung.....	16
6.1.5	GR5: DO: Implementierung.....	18
6.1.6	GR6: CHECK: Überwachung und Überprüfung	18
6.1.7	GR7: ACT: Kontinuierliche Überwachung.....	19
6.2	Spezifische Anforderungen (PR1-PR14)	20
6.2.1	PR1: Service Portfolio Management.....	20
6.2.2	PR2: Service Level Management	21
6.2.3	PR3: Service Reporting Management	22
6.2.4	PR4: Service Availability & Continuity Management.....	23
6.2.5	PR5: Capacity Management.....	24

6.2.6	PR6: Information Security Management.....	24
6.2.7	PR7: Customer Relationship Management	25
6.2.8	PR8: Supplier Relationship Management	26
6.2.9	PR9: Incident and Service Request Management	26
6.2.10	PR10: Problem Management	28
6.2.11	PR11: Configuration Management.....	28
6.2.12	PR12: Change Management.....	29
6.2.13	PR13: Release & Deployment Management.....	30
6.2.14	PR14: Continual Service Improvement Management.....	31
7	Abschließende Empfehlungen.....	32
8	Danksagung.....	35
9	Literaturverzeichnis.....	36

1 Vorwort

Im heutigen digitalen Informationszeitalter sind die Hochschulrechenzentren (HRZ) eine wesentliche Säule zur Erfüllung der Aufgaben in Forschung, Lehre und Verwaltung und bilden einen zentralen Knotenpunkt innerhalb der jeweiligen Hochschule, aber auch über Hochschulgrenzen hinweg. Dabei stellen eine generell steigende Erwartungshaltung an die technische Infrastruktur (z.B. durch immer mehr WLAN-fähige Endgeräte) spezifische Anforderungen unterschiedlicher Nutzer, aber auch neue oder geänderte Nutzungsszenarien (z.B. stärkere Online-Kollaborationen) große Herausforderungen für HRZ dar. Zusätzlich spielen auch regulatorische Anforderungen (z.B. DSGVO¹, EGovG²) sowie die Gewährleistung von IT-Sicherheit und Verfügbarkeit eine immer wichtigere Rolle. Speziell durch die Zunahme von IT-Sicherheitsvorfällen oder auch Cyberattacken hat das Thema IT-Sicherheit große Aufmerksamkeit in Deutschland (Abolhassan 2017; Zwilling et al. 2020) und dadurch auch im Kontext der über 400 in Deutschland registrierten Hochschulen erhalten (Rudnicka 2020).

Aufgrund dessen werden nicht nur die internen Anforderungen an die IT-Systemlandschaft, sondern auch der Anforderungsdruck von außen, immer komplexer (Beims und Ziegenbein 2021). So zeigen die Auswirkungen der Corona-Pandemie und die damit verbundenen Maßnahmen auf, wie schlagartig der physische Lehrbetrieb an Hochschulen zurückgefahren, z.T. sogar eingestellt wird. Dies hat zur Folge, dass verstärkt alternative digitale Lehrangebote zum Einsatz kommen, sodass innerhalb kürzester Zeit neue Software und IT-Infrastrukturen zur Verfügung gestellt werden müssen, um auf diese Veränderungen flexibel reagieren zu können (Williamson et al. 2020). HRZ müssen sich stetig professionalisieren und sich weg von der bloßen Bereitstellung von IT hin zu professionellen Anbietern von IT-Services entwickeln, um den neuen Anforderungen und unterschiedlichen Nutzern in der Zukunft gerecht zu werden (Jonas et al. 2021). Dementsprechend entsteht die Notwendigkeit, sich für einen zukunftsorientierten und richtungsweisenden Betrieb der bayerischen HRZ stärker an etablierten Servicestandards, Anforderungen von hochschulinternen Nutzern sowie hochschulexternen Potentialen zu

1 Datenschutz-Grundverordnung (Link: www.dsgvo-gesetz.de)

2 E-Government-Gesetz (Link: www.gesetze-im-internet.de/egovg)

orientieren. Ein professionelles IT-Service-Management (ITSM) wird damit nicht nur in der Industrie zur essenziellen Grundlage, sondern auch für Hochschulen und deren Rechenzentren.

In diesem Zusammenhang können sich die Dienstleister und dementsprechend auch die Hochschulen nicht mehr leisten, sich ausschließlich auf die Technologie und ihre internen Prozesse zu konzentrieren. Vielmehr sind diese dazu gezwungen, auch die Qualität der von ihnen erbrachten Dienstleistungen zu berücksichtigen und den Anforderungen an Forschung und Lehre gerecht zu werden. Unternehmen und Dienstleister orientieren sich dazu an einschlägigen Referenzmodellen (z.B. ITIL®) oder Servicestandards (z.B. ISO/IEC 20000), um die eigenen IT-Services resilient und robust gegenüber den zunehmenden externen Anforderungen bereitzustellen (van Bon 2008).

Das vorliegende Booklet greift das Thema ITSM auf und bereitet die Inhalte speziell für HRZ auf. Dabei grenzt es zum einen ab, wie sich ITSM für Hochschulen von Unternehmen unterscheidet und zum anderen soll es dabei helfen schrittweise das ITSM an den Hochschulen zu verbessern.

2 Was ist IT-Service-Management?

In einer Organisation stellt das ITSM eine grundlegende Säule in der Struktur der IT-Abteilung dar und reiht sich neben Feldern wie IT-Sicherheit und der Entwicklung von Software ein. Der Begriff des ITSM wird sowohl in der Theorie als auch in der Praxis recht alltäglich verwendet. Es fällt daher schwer, eine einheitliche Begriffsdefinition zu finden, da eine große Bandbreite an Definitionen in der Literatur vorhanden ist. In der Literatur rund um die Information Technology Infrastructure Library (ITIL) wird Service Management als die Steuerung aller fachlichen Fähigkeiten der Organisation zur Bereitstellung eines Mehrwertes für den Kunden in Form von Services definiert (Beims und Ziegenbein 2021). Nach FitSM³ ist das Ziel von ITSM, Organisationen zu kunden- und serviceorientierten IT-Service-Providern zu entwickeln (Rohrer und Söllner 2017) und wird definiert als „die Gesamtheit der Aktivitäten, die von einem IT-Service-Provider durchgeführt werden, um die seinen Kunden angebotenen IT-Services zu planen, bereitzustellen, zu betreiben und zu steuern“. Im Zuge dessen verstehen wir unter dem Begriff ITSM:

ITSM ist als Ansatz für den IT-Betrieb von Service-Dienstleistern zu verstehen, der sich besonders dadurch auszeichnet, dass er den Schwerpunkt auf IT-Services, Kunden, Service Level Agreements und die Abwicklung der täglichen Aktivitäten mittels IT-Servicefunktionen legt und organisiert (Iden und Eikebrokk 2013; Tiemeyer 2020).

Wie schon an der Definition des ITSM deutlich geworden ist, stellt das ITSM Unternehmen vor eine Vielzahl von Anforderungen. In diesem Zusammenhang haben sich eine große Bandbreite an Rahmenwerken und Standards etabliert. Die Rahmenwerke versuchen Kostenminimierung und Risikominimierung bei der Umstellung der Prozesse zu gewährleisten, indem sie eine methodische Gestaltung des ITSM beim Kunden vorgeben (Hochstein et al. 2004).

Das ITSM ordnet sich thematisch zwischen den drei übergeordneten Kategorien den Rahmenwerken des Qualitätsmanagements (z.B. ISO 9000), der Informationssicherheit (z. B. ISO/IEC

3 Der Begriff FitSM setzt sich dabei aus „Fit für IT-Service-Management“ zusammen.

27001, ISIS12⁴ und BSI IT-Grundschutz⁵) und der Reifegrad- und Softwareentwicklung (z.B. ISO 15504) ein (Rohrer und Söllner 2017). Diese Rahmenwerke bedienen inhaltlich sowohl IT-sicherheitspezifische als auch regulatorische Anforderungen, unterscheiden sich jedoch in ihrer inhaltlichen Ausrichtung voneinander. Im Rahmen dieses Handbuchs steht insbesondere die Entwicklung des ITSM von Hochschulrechenzentren im Fokus. Grundlegend befassen sich Cobit® oder ITIL® ganzheitlich und sehr detailliert mit der inhaltlichen Implementierung von ITSM in beispielsweise Konzernen oder Groß- und mittelständischen Unternehmen (Beims und Ziegenbein 2021; Gaulke 2019; van Bon 2008). Dieser Detailgrad solch umfangreicher ITSM-Rahmenwerke übersteigt allerdings oftmals die Kapazitäten und die Zielsetzung für vergleichsweise kleinere HRZ, sodass eine Adaption dieser komplexeren Rahmenwerke die HRZ vor große Herausforderungen stellt. Im Vergleich dazu benötigen HRZ jedoch oftmals eine weniger komplexe Alternative zu diesen etablierten Rahmenwerken Cobit® und ITIL®. Diese leichtgewichtige Alternative finden wir in dem Rahmenwerk FitSM, welche die essentiellen Anforderungen an ein ITSM von HRZ übersichtlich bündelt und damit aus unserer Sicht für die Organisation des hochschuleigenen ITSM sehr geeignet ist (Rohrer und Söllner 2017).

Grundsätzlich ist das Ziel von FitSM speziell für klein- und mittelständische Unternehmen (KMU) einen einfachen, verständlichen und praktisch anwendbaren Ansatz für das ITSM zu schaffen. Übergeordnet bedient sich FitSM dreier Rahmenwerke und Standards (Cobit®, ITIL® und der ISO/IEC 20000 Norm). Die internationale Norm ISO/IEC 20000 beschreibt Mindestanforderungen für ein geregeltes ITSM, nach der sich Organisationen zertifizieren lassen können, während Cobit® seinen Fokus auf die IT-Governance legt und ITIL® die ITSM-spezifischen Themeninhalte adressiert (Beims und Ziegenbein 2021; Gaulke 2019; Rohrer und Söllner 2017). Gleichzeitig bedient sich FitSM aus den Bereichen des Qualitätsmanagements (ISO 9000), den Standards der Informationssicherheit (ISO/IEC 27001, ISIS12 und BSI IT-Grundschutz) sowie den Standards für Reifegrad- und Softwareentwicklung (ISO 15504). Das Zusammenspiel und die Vernetzung dieser Rahmenwerke ist in FitSM gebündelt, welches sich

4 Informationssicherheitsmanagementsystem in 12 Schritten (Link: www.isis12.it-sicherheitscluster.de)

5 Bundesamt für Sicherheit in der Informationstechnik IT-Grundschutz (Link: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html)

dadurch sowohl als ISO/IEC 20000 konforme als auch als leicht verständliche und pragmatische Option zur Implementierung in bayerischen HRZ anbietet. Die sich daraus ergebenden konkreten Anforderungen werden in Kapitel 6 im Detail vorgestellt.

3 Unterschied zwischen dem ITSM von Unternehmen und Hochschulen

Unternehmen und Hochschulen unterscheiden sich in einigen Aspekten, angefangen zum Beispiel bei der Organisationsform und Finanzierung, die auch dazu führen, dass eine Einführung des ITSM bei Hochschulen auf andere Herausforderungen als bei Unternehmen trifft. Im Folgenden möchten wir deswegen auf die Herausforderungen bei der Einführung des ITSM eingehen, welche Speziell im Hochschulkontext zu finden sind.

Die größte Herausforderung, die Hochschulen zu bewältigen haben, sind die Hürden, welche sich durch ihre eigene Organisationsform ergibt. Als Expertenorganisationen und den daraus resultierenden dezentralen Strukturen gestaltet es sich für Hochschulen schwierig, Prozesse durchgängig zu etablieren. Das liegt daran, dass sich die Angestellten, insbesondere die wissenschaftlichen Mitarbeiter, sich mehr mit ihrem Fach identifizieren als mit der Hochschule als Organisation (Gröger und Schumann 2013). Dies kann unweigerlich zu Interessenkonflikten führen, die eine erfolgreiche Umsetzung von Prozessen innerhalb der Organisation verhindert.

Eine weitere Hürde, der sich Hochschulen gegenübersehen, ist, dass dort an altbewährten Verfahren und Mechanismen weiterhin vehement festgehalten wird. Das ist besonders in der Verwaltung an den Hochschulen ausgeprägt (Gröger und Schumann 2013). Daraus resultieren mehrere Probleme, die eine Veränderung der Prozesse in einer Hochschule, behindern können. Der Weg hin zu einer Entscheidung, Veränderungen überhaupt vornehmen zu wollen, folgt durch die alten oder fehlenden Prozesse zur Entscheidungsfindung in Hochschulorganisationen keinen definierten Abläufen. Die Entscheidungen finden eher unstrukturiert statt, was auf die Dezentralität der Entscheidungsorgane zurückzuführen ist (Gröger und Schumann 2013).

Nicht nur die Struktur verursacht hier Widerstände, sondern auch die Durchsetzung von Beschlüssen seitens der Hochschulleitung. Diese Verwaltungstätigkeiten, seien es Beschlüsse zur strategischen Ausrichtung der Hochschule oder Vorschriften aus der Verwaltung, werden von den wissenschaftlichen Mitarbeitenden als störend empfunden und dementsprechend schwer

angenommen. Das ist auf die in der Dezentralität beruhenden Autonomie der Hochschuleinheiten zurückzuführen (Gröger und Schumann 2013). Ein solches Problem ist in Unternehmen fast nicht vorzufinden.

Die Organisation der Prozesse kann durch die bestehenden Strukturen an den Hochschulen behindert werden. Hochschulen, die sich beispielsweise dazu entschieden haben, externe Dienstleister zu beauftragen, um Aufgaben wie den IT-Service Desk zu betreuen, sehen sich meist Zuständigkeitsproblematiken gegenüber. So kann es dazu kommen, dass das Incident Management (siehe Kapitel 6.2.9) Probleme damit bekommt, ihre Prozesse zu organisieren, da sie nur eingeschränkt Weisungsbefugnisse haben. Das liegt daran, dass die bekannte prozessorientierte Strukturierung des IT-Service Desks in 1st-Level, 2nd-Level und ggf. weitere Level aufteilt und sich nicht an den Zuständigkeiten innerhalb der Organisation orientiert. Andersherum können von dem IT-Service Desk angefragte Lösungen von Problemen an das Incident Management von den Verantwortlichen des Service Desks nur begrenzt eingefordert werden. Dies hat zur Folge, dass Anfragen langsam und teilweise gar nicht bearbeitet werden (Knittl et al. 2012). Ebenfalls in die Struktur der Gesamtorganisation der Hochschulen fällt die Aufgabe der Zielsetzung. Damit konkrete Ziele für die HRZ erarbeitet werden können und festgelegt werden kann, welche Ergebnisse unter welchen Umständen von dem HRZ zu erwarten ist, muss müssen die Unternehmensziele klar sein (Beims und Ziegenbein 2021). Durch die Struktur einer Expertenorganisation an Hochschulen kann es sich hier für die Verantwortlichen schwierig gestalten, die Ziele der Organisation klar zu sehen. Die fachlichen Ziele der Fachbereiche und Forschung reichen dafür nicht aus, da sich die Ziele, die für das HRZ abgeleitet werden sollen, auf den Unternehmensnutzen beziehen müssen.

Eine Veränderung der Prozesse und Strukturen in einer Organisation bedarf auch immer Investitionen in Menschen und Technik. Gerade bei einem so potenziell langwierigen Projekt, das Einfluss auf viele Bereiche der Organisation haben kann, wie die Umstellung oder Anpassung des ITSM, wird ein stabiles Budget benötigt. An Hochschulen findet man hier eine Sondersituation vor, da die Hochschulen, insbesondere in der Verwaltung, durch öffentliche Zuweisungen finanziert werden (Schmücker 2011). Wo Unternehmen die Möglichkeit zur Kreditfinanzierung haben, ist das an Hochschulen nur eingeschränkt möglich, kann zum Teil durch Finanzierungen aus Drittmitteln oder Studiengebühren kompensiert werden (Gröger und Schumann 2013).

Ein weiterer Faktor, der an den Hochschulen eine Rolle spielt, ist die Personalsituation. Die meisten Angestellten, insbesondere in den wissenschaftlichen Bereichen, sind befristet beschäftigt und haben zum Teil nur Projektstellen inne. Die daraus resultierende hohe Fluktuation an Mitarbeitern stellt das IT-Management vor Probleme. Es entsteht ein Verlust an Wissen und Erfahrung, wenn die Mitarbeiter die Hochschule verlassen und der dazu führt, dass keine langfristigen und verbindlichen Zusagen zu Dienstparametern abgegeben werden können (Knittl et al. 2012). Eine weitere Erschwernis ergibt sich durch die Vergütung der Mitarbeiter über das Tariffsystem des öffentlichen Dienstes. Dadurch sind beispielsweise Bereitschaftsdienste für den IT-Betrieb sehr schwer umzusetzen. Das Resultat daraus ist, dass die HRZ meist nur „best-effort“ als Qualität anbieten und garantieren können (Knittl et al. 2012). Dieser Anspruch genügt Unternehmen nicht.

Die genannten Herausforderungen haben zur Folge, dass das Thema ITSM bei Hochschulen unterschiedlich angegangen wird und nicht in allen Aspekten so vorgegangen werden kann, wie in Rahmenwerken für ITSM beschrieben. Es bedarf eine spezielle Anpassung auf den Hochschulkontext auf die wir im Folgenden eingehen wollen.

4 How to get started?

Der erste Schritt zur Etablierung von ITSM an HRZ ist das Entwickeln eines klaren Verständnisses und Bekenntnisses zu ITSM sowie das Erwerben von fachlichen Kenntnissen im Bereich ITSM gefolgt von einer strukturierten Erfassung des IST-Zustands der initialen ITSM-Umsetzung im HRZ der jeweiligen Hochschule.

Ein initialer fachlicher Überblick zum ITSM im Hochschulkontext wird im Rahmen dieses Booklets vermittelt, welcher zum Start der ITSM-Implementierung in HRZ als eine gute Basis für den initialen Kompetenzaufbau erachtet wird. Für den weiteren Implementierungsverlauf verweisen wir auf die detailliertere Primärliteratur von FitSM (Rohrer und Söllner 2017; FitSM 2021) sowie deren einschlägiger Begleitliteratur (Beims und Ziegenbein 2021; Teubner 2013).

Nach dem Gewinn eines ersten fachlichen Überblicks über ITSM und dessen Besonderheiten im Hochschulkontext sollte das HRZ im zweiten Schritt eine strukturierte Erhebung des IST-Zustands im Hinblick auf die ITSM-Ausgangslage am HRZ durchführen. Als strukturgebendes

Vorgehensmodell empfiehlt es sich, die in FitSM definierten Anforderungsdimensionen nacheinander abzuprüfen. Ein Benchmarking kann hierbei unterstützen, neben der reinen Erfassung des IST-Zustands auch eine Bewertung vorzunehmen, sodass die unterschiedlichen Reifegrade und ITSM-Ausprägungen je Anforderungsdimension sichtbar werden. Ein Überblick über das empfohlene Benchmarking erfolgt in folgenden Kapitel 5 dieses Booklets. Auf Basis der Erhebung des IST-Zustands und initialen Selbstbewertung sollte das HRZ im nächsten Schritt das Zielbild der ITSM-Implementierung definieren. Da sich die HRZ in der deutschen Hochschullandschaft mitunter deutlich in Größe, verfügbaren Ressourcen, Aufgaben, Verantwortlichkeiten, Strategien und Zielen unterscheiden, ist es wichtig ein passendes und genaues Zielbild für das künftige ITSM festzulegen. In diesem Zusammenhang sollte auch eine Vereinbarkeit des ITSM-Vorhabens und Zielbilddefinition mit der allgemeinen IT-Strategie des HRZ geprüft werden. Etwaige geplante Zertifizierung im IT-Sicherheitsbereich oder Qualitätsmanagement oder strategische Initiativen zum Enterprise Architecture Management können sollten bei der Definition des künftigen ITSM-Zielbilds berücksichtigt werden.

5 IST-Zustand und Benchmarking

5.1 Analysetool zur strukturierten Zustandserhebung

Zur Erhebung des IST-Zustands wurde auf Basis von FitSM ein Analysetool entwickelt, mit dem basierend auf sieben grundlegenden Anforderungen, die sich auf die notwendige Basis zu einem erfolgreichen Betrieb des ITSM richten, sowie 14 spezifische Anforderungen, der Status Quo des ITSM am jeweiligen HRZ erhoben werden kann. Zur Analyse und zur Bewertung des erhobenen Status Quo haben wir auf Basis dieser sieben grundlegenden und 14 spezifischen Anforderungen ein Reifegradprofil festgelegt. Dieses Anforderungsprofil wurde in Form eines Evaluierungsinstrumentes zusammengefasst und um Erläuterungen zu den Anforderungen sowie um ein Reifegradmodell mit den Reifegraden „0“ bis „3“ ergänzt. Hierbei galt die Einstufung „0“ als unbewusster oder nicht vorhandener Teil des ITSM, wohingegen „1“ das ad hoc oder initiale Bewusstsein über den Bestandteil des ITSM bedeutete. Der Reifegrad „2“ klassifizierte das Verständnis darüber, Aufgaben des ITSM wiederholbar, jedoch nicht in einem formal festgelegten Prozess durchzuführen. Der höchste Reifegrad „3“ stellte die optimale Erfassung von ITSM-Bestandteilen in definierter, dokumentierter und vollständiger Form dar. Es handelte sich bei dem Evaluierungsinstrument um ein Excel-basiertes Tool, das durch den Anwender einfach

zu benutzen ist und eine effiziente Auswertung gewährleistet. Exemplarisch sind in Abb. 1 das Evaluierungsinstrument mit den ausgeklappten Informationstexten für GR1 und PR1 abgebildet.

[ITSM] IT-Servicemanagement für bayerische Hochschulrechenzentren Evaluierungsinstrument		
Mit folgendem Evaluierungsinstrument können Sie eine Bewertung für die einzelnen Anforderungen durchführen. Weitere Informationen zu den grundlegenden sowie spezifischen Anforderungen finden Sie auf Seite 2 in der Detailsicht.		
Bewertungsumfang und Ziele	Reifegrad-Erfüllung	Kommentare
Grundlegende Anforderungen		Die Reifegradstufen für die Reifegrad-Erfüllung sind wie folgt: Stufe 0: Unbewusst / Nicht vorhanden - Es gibt kein Bewusstsein für die Aufgabenstellung. / Das erforderliche Ergebnis existiert nicht. Stufe 1: Ad-hoc / Initial - Man ist sich der Aufgabe bewusst, jedoch wird diese nicht gemanagt bzw. gesteuert. / Es existieren relevante Ergebnisse, diesen fehlen aber Kernelemente. Stufe 2: Wiederholbar / Teilweise - Aufgaben werden wiederholbar erfüllt, sind aber nicht formal festgelegt. / Ergebnisse sind nur teilweise vollständig. Stufe 3: Definiert / Vollständig - Aufgaben sind gut definiert und Ergebnisse sind vollständig, für beides sind dokumentierte Verantwortlichkeiten festgelegt.
GR1: Engagement & Verantwortung des Top-Managements	Auswählen...	
<i>Das Top-Management stellt sicher, dass die Führung, Organisationsstruktur und Prozesse des HRZ die Strategie und die Ziele des Kunden unterstützen. Es werden eine verantwortliche Person, die Ziele und eine Service-Management-Richtlinie definiert sowie Managementreviews durchgeführt.</i>		
GR2: Dokumentation	Auswählen...	
GR3: Definition des Geltungsbereichs des Service-Managements	Auswählen...	
GR4: Planung des Service-Managements (PLAN)	Auswählen...	
GR5: Implementierung des Service-Managements (DO)	Auswählen...	
GR6: Überwachung und Bewertung des Service-Managements (CHECK)	Auswählen...	
GR7: Kontinuierliche Verbesserung des Service-Managements (ACT)	Auswählen...	
Spezifische Anforderungen		Weitere Informationen zu den Stufen zu jeder Anforderung finden Sie in der Detailsicht.
PR1: Service Portfolio Management	Auswählen...	
<i>Es existiert ein aktuell und ständig gepflegtes Serviceportfolio aller Services, die vom HRZ angeboten werden. Dokumentationsrichtlinien und Vorgaben für das Serviceportfolio und die Services sind festgelegt. Die Vorgehensweise zur Planung neuer oder geänderter Services ist festgelegt. Beteiligungen und finanzielle Betrachtungen sind geklärt.</i>		
PR2: Service Level Management	Auswählen...	
PR3: Service Reporting	Auswählen...	
PR4: Service Availability & Continuity Management (SACM)	Auswählen...	
PR5: Capacity Management	Auswählen...	
PR6: Information Security Management	Auswählen...	
PR7: Customer Relationship Management	Auswählen...	
PR8: Supplier Relationship Management	Auswählen...	
PR9: Incident & Service Request Management	Auswählen...	
PR10: Problem Management	Auswählen...	
PR11: Configuration Management	Auswählen...	
PR12: Change Management	Auswählen...	
PR13: Release & Deployment Management	Auswählen...	
PR14: Continual Service Improvement Management	Auswählen...	

Abb. 1: Ausschnitt aus dem Evaluierungsinstrument

Ergänzend dazu, sind im Folgenden die Erklärungen für die drei Reifestufen aufgeführt:

- **Stufe 0:** Unbewusst / Nicht vorhanden - Es gibt kein Bewusstsein für die Aufgabenstellung. / Das erforderliche Ergebnis existiert nicht.
- **Stufe 1:** Ad-hoc / Initial - Man ist sich der Aufgabe bewusst, jedoch wird diese nicht gemanagt bzw. gesteuert. / Es existieren relevante Ergebnisse, diesen fehlen aber Kernelemente.
- **Stufe 2:** Wiederholbar / Teilweise - Aufgaben werden wiederholbar erfüllt, sind aber nicht formal festgelegt. / Ergebnisse sind nur teilweise vollständig.
- **Stufe 3:** Definiert / Vollständig - Aufgaben sind gut definiert und Ergebnisse sind vollständig, für beides sind dokumentierte Verantwortlichkeiten festgelegt.

5.2 Zielvorstellung

Nach Erhebung bzw. Analyse des IST-Zustands muss der SOLL-Zustand definiert werden. Also mit anderen Worten muss ein Zielzustand erarbeitet werden, welcher erreicht werden soll. Dieser kann sich an bekannten Richtlinien orientieren, z.B. das Erreichen von Stufe 3 bei den Anforderungen von FitSM oder eine offizielle Zertifizierung nach ISO 20000. Dabei sollte aber darauf geachtet werden, ob diese Ziele auch realistisch umgesetzt werden können bzw. sinnvoll für die Größe des jeweiligen HRZ sind. Gerade eine offizielle Zertifizierung nach ISO 20000, welches sicherlich der höchste SOLL-Zustand ist, ist mit sehr viel Aufwand und Maßnahmen verbunden, die nicht für jedes HRZ sinnvoll sind. Deswegen sollte vor einer Einführung oder Weiterentwicklung des ITSM ein klares Ziel und ggf. auch ein Zeitplan definiert werden, welcher sowohl von der HRZ-Leitung, dem HRZ-Team als auch der Hochschulleitung unterstützt wird, da ein funktionierendes Team, welches hinter den Zielen steht, essenziell für die darauffolgende Umsetzung ist. Zum Beispiel kann man sich auch kleinere Ziele stecken, wie die Erstellung eines vollständigen Servicekatalogs, den Ausbau des Incident Managements oder auch das Etablieren von systematischen Service-Verträgen. Auch im Zusammenhang mit einer gewünschten offiziellen Zertifizierung kann auch erst eine Zertifizierung nur für IT-Sicherheit nach ISO 27001 angestrebt werden bevor man sich auf eine Zertifizierung nach ISO 20000 konzentriert. Abschließend lässt sich zusammenfassen, dass die Ziele zu der Größe und Ambition des jeweiligen HRZ passen sollten.

6 Anforderungen an das IT-Service-Management von Hochschulrechenzentren

Im Folgenden wird anhand des Rahmenwerks FitSM auf die einzelnen Anforderungen an das ITSM eines HRZ eingegangen. Das Rahmenwerk FitSM gliedert die Anforderungen in sieben grundlegende Anforderungen (GR 1-7) und 14 spezifische Anforderungen (PR 1-14), welche in abgewandelter Form auch in der ISO/IEC 20000 Norm und in den ITIL®-Rahmenwerken wiederzufinden sind. Während die grundlegenden Anforderungen vor allem die Rahmenbedingungen für eine kontinuierliche Entwicklung des generellen ITSM schaffen (z.B. Verpflichtung der Hochschulleitung, Art und Weise der Dokumentation sowie die fortlaufende Entwicklung

des ITSM durch einen iterativen PDCA-Zyklus)⁶, erstreckt sich das inhaltliche Profil der spezifischen Anforderungen über die unterschiedlichen Bereiche des Service-Portfolios (z.B. Service Portfolio Management, Information Security Management oder Customer Relationship Management). Abb. 2 gibt einen Überblick über die Anforderungen des FitSM-Rahmenwerks an das ITSM bayerischer HRZ (Rohrer und Söllner 2017).

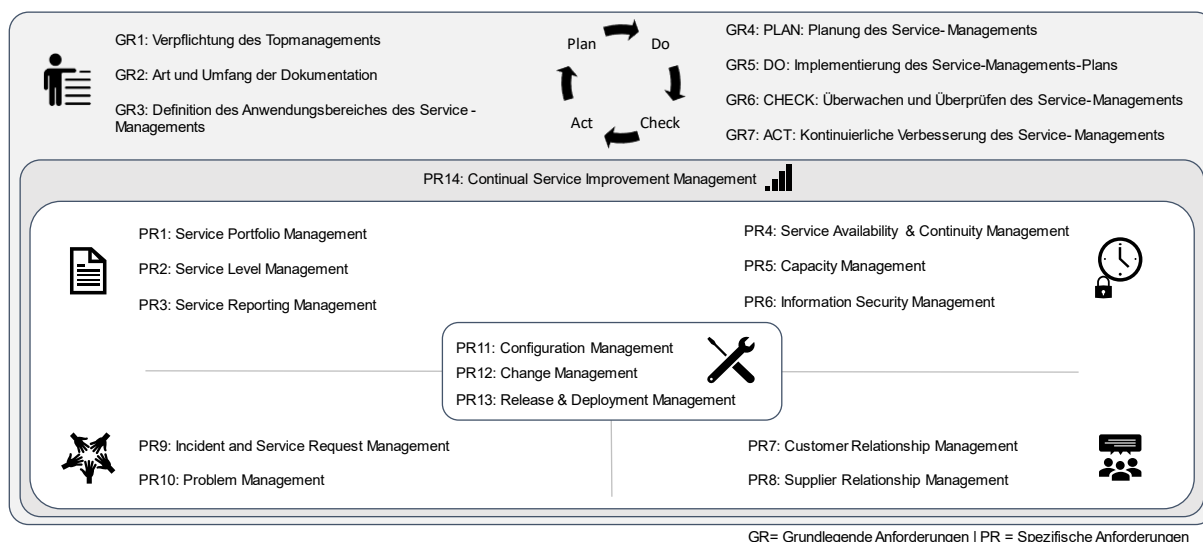


Abb. 2: Übersicht der FitSM-Anforderungen (in Anlehnung an Rohrer und Söllner 2017)

Im Folgenden möchten wir Ihnen im Detail erläutern, welche Bereiche die jeweiligen Anforderungen beinhalten und insbesondere transparent erklären in welcher Form diese in HRZ umgesetzt werden (können). Dazu erklären wir zunächst die grundlegende Beschaffenheit jeder einzelnen Anforderung und geben dann konkrete Empfehlungen in Form von Umsetzungsbeispielen, die Sie in der Praxis heranziehen können.

6.1 Grundlegende Anforderungen (GR1-GR7)

6.1.1 GR1: Verpflichtung der Hochschulleitung

Die Verpflichtung und Verantwortung der Leitung eines HRZ als grundlegende Anforderung kann in zwei Aspekte untergliedert werden. Zum einen ist es zwingend erforderlich, dass die Hochschulleitung ein Qualitätsmanagement in Form eines Service-Management-Systems

⁶ Der PDCA-Zyklus ist eine methodische Vorgehensweise mit dem Ziel, den Umfang, Detailgrad als auch Anforderungen an ein ITSM zu planen., diese umzusetzen und nachhaltig weiterzuentwickeln (Rohrer und Söllner 2017).

(SMS) integriert und unterstützt. Zum anderen ist im Einklang mit dem Qualitätsmanagement eine Service-Management-Richtlinie einzuführen.

Die Integration eines Qualitätsmanagements durch die Leitung des HRZ kann signalisiert werden, indem zur Planung, Einführung, Umsetzung, Kontrolle, Überprüfung und Verbesserung des SMS beigetragen wird. In diesem Zusammenhang sollte darüber nachgedacht werden, für die operative Umsetzung neben dem Chief Information Officer (CIO) einen verantwortlichen Leiter für das SMS zu bestimmen. Im Hochschulkontext handelt es sich bei dem CIO oftmals um einen Professor bzw. Professorin der Hochschule, die diese Aufgaben neben ihrer Lehr- und Forschungstätigkeit übernimmt. Durch die Tätigkeit als CIO wird der zuständige Professor bzw. Professorin Mitglied der Hochschulleitung. Sofern die Position des Informationssicherheitsbeauftragten besetzt ist, werden die Aufgaben bezüglich Informationssicherheit koordiniert. Darüber hinaus erscheint es aus strategischer Sicht sinnvoll, dass der CIO der Hochschule zeitgleich ebenfalls für den Grad und die Fortschrittlichkeit der Digitalisierung an der Hochschule zuständig ist. Aufgrund der detaillierten Einblicke bezüglich der IT-Sicherheit der Hochschule kann so die Digitalisierung unter Einhaltung von IT-Sicherheitsaspekten umgesetzt werden. Auf der anderen Seite können ebenso Verbesserungen bezüglich bestehender Sicherheitsvorkehrungen vorgenommen werden, um so für neue Digitalisierungsprojekte ausreichend geschützt zu sein. Des Weiteren ist es wichtig, klare Ziele in Bezug auf das IT-Service Management zu definieren und zu kommunizieren. Diese könnten beispielsweise sein: Zertifizierung der Hochschule und Vereinheitlichung des Service-Angebots. Mit einer einheitlichen Darstellung und Umsetzung des Service-Angebots geht ein weiterer zentraler Punkt einher. Die Verantwortung des HRZ ist eindeutig von anderen Bereichen abzugrenzen. Darüber hinaus soll eine Service-Management-Richtlinie ausgearbeitet werden, deren Inhalte in dem zweiten Punkt dieser grundlegenden Anforderung näher thematisiert werden. Abschließend wird zur Sicherstellung der Qualitätsanforderungen an das Service-Management empfohlen, in regelmäßigen Abständen (empfohlen werden diese im Abstand von etwa 2 Jahren) interne Evaluationen durchzuführen.

Die inhaltliche Ausgestaltung der Service-Management-Richtlinie erfordert einige Kriterien, die es zu beachten gilt. In Zusammenhang mit einer serviceorientierten Ausrichtung des Service-Managements sollte eine Verpflichtung zur Erfüllung der Service-Anforderungen aller

Hochschulangehörigen bzw. Nutzer des HRZ einhergehen. Darüber hinaus sollte eine prozessorientierte Umsetzung angestrebt werden, wobei der Anwendungsbereich alle Service-Angebote des HRZ miteinschließt. Die Verpflichtung zur kontinuierlichen Verbesserung kann mit den regelmäßig durchgeführten internen Evaluationen erfüllt werden.

6.1.2 GR2: Art und Umfang der Dokumentation

Eine weitere zentrale grundlegende Anforderung stellt die Dokumentation in Bezug auf Art und Umfang dar. Die Dokumentation beläuft sich sowohl auf das SMS als auch die entsprechenden Prozesse. Darüber hinaus sind eine Ergebnisdokumentation sowie eine geeignete Vorgehensweise und Struktur wichtig. Der Dokumentationsgrad orientiert sich an den definierten Zielen des HRZ. Je höher der Dokumentationsgrad, desto höher der damit verbundene Aufwand und desto geringer die Flexibilität und der Interpretationsspielraum. Die Dokumentation beinhaltet die grundlegenden Bestandteile des SMS: Definition des Anwendungsbereichs des SMS, Beschreibung der Service-Management-Richtlinie und Service-Management-Planung. Die Service-Management Richtlinie des HRZ wird bereits in GR1 festgelegt, wohingegen der Anwendungsbereich sowie die Service-Management-Planung erst in den nächsten Anforderungen (GR3 und GR4) konkretisiert werden. Die Prozessdokumentation sollte folgende Aspekte beinhalten: Beschreibung der Prozessziele, Beschreibung Ein- und Ausgaben sowie der Aktivitäten des Prozesses, Beschreibung prozessspezifische Rollen und Verantwortlichkeiten, Beschreibung Schnittstellen zu jeweils anderen Prozessen. Bei der Dokumentation der Prozesse ist es wichtig zunächst die übergeordneten Prozessbereiche sowie deren Prozessverantwortliche zu definieren. Bei der anschließenden Erhebung des IST-Prozesse, welche eine wichtige Grundlage für die Service-Management-Planung darstellen, ist eine Dokumentation nach klaren Standards wichtig. Hierfür sollten sich die Prozessverantwortlichen und der Leiter des SMS am HRZ auf einen einheitlichen Prozessmodellierungsstand sowie ein Dokumentationsmedium verständigen. Ein im IT-Management verbreiteter Prozessmodellierungsstandard, welcher für die Dokumentation von IT-Services gut geeignet ist, ist die Business Process Model and Notation (BPMN). Durch den grafischen Fokus von BPMN, können Stakeholder einen schnellen Überblick über den Services erhalten und auch die Abhängigkeiten und Zusammenhänge zu anderen Services einfach nachvollziehen. Ergänzend zur reinen Erhebung von IST-Prozessen, ist es zudem sinnvoll, die jeweiligen Ergebnisse der Prozessdurchführung zu dokumentieren.

Hierdurch lässt sich zum einen die Transparenz durchgeführter Services erhöhen und gleichzeitig mögliche Serviceprobleme nachvollziehen.

Neben der grafischen und durchführungsorientierten Dokumentation der Serviceprozesse ist es zudem sinnvoll, die zentralen Metainformationen der Services strukturiert zu erfassen. Dies kann beispielsweise umgesetzt werden, indem das HRZ einen Servicekatalog führt und diesen regelmäßig aktualisiert. Der Servicekatalog kann hierbei in öffentliche und nicht-öffentliche Serviceleistungen unterteilt werden. Relevante Informationen, welche in einem solchen Service-Katalog dokumentiert werden können, sind unter anderem folgende:

Servicebezeichnung, Kurzbeschreibung, Servicezeiten, Voraussetzung für die Servicenutzung, Servicenutzer, Wartungszeiten, Serviceverantwortlicher, Servicekritikalität

Die öffentlichen Serviceleistungen inklusive ihrer Beschreibungen können in HRZ-Newslettern oder dem Jahresbericht des HRZ mitaufgenommen werden, um so den Umfang des Serviceangebot des HRZ zu verdeutlichen beziehungsweise transparent zu kommunizieren. Tab.1 zeigt eine exemplarische Darstellung eines Eintrages für einen Servicekatalog.

Tab. 1 Eintrag aus einem Servicekatalog für den Service Eduroam

Name des Services	Eduroam
URL des Dienstes	/
Kurzbeschreibung des Leistungsumfangs	Eduroam (education roaming) ermöglicht allen Angehörigen einer Hochschule und Mitgliedern teilnehmender Institutionen den drahtlosen Internetzugang (verschlüsselt) einerseits an der Heimatinstitution, andererseits international beim Besuch einer anderen teilnehmenden Institution.
Zusätzliche Angaben zum Leistungsumfang (optional)	keine
Nutzungszeiten und ggf. Öffnungszeiten	24/7
Voraussetzung für die Nutzung	Benutzerkennung
Nutzende	Beschäftigte, Studierende, Angehörige des Eduroam-Verbundes
Ansprechpartner	Anlaufstelle innerhalb der Sprechzeiten persönlich oder unter Telefon XYZ und per E-Mail: XYZ

Zusätzliches Leistungsangebot	/
URL für weitere Informationen	XYZ.de
Wartungszeiten	keine
Servicestatus (gemäß Servicelebenszyklus)	Im Betrieb
Klassifikation des Eintrags gemäß der Betriebsrichtlinie (erscheint nicht im Dienstleistungskatalog)	öffentlich

6.1.3 GR3: Definition des Anwendungsbereichs des Service Managements

Grundsätzlich ist es bei der Implementierung und beim Einsatz eines Service-Management-Systems wichtig, den zugrundeliegenden Anwendungsbereich zu definieren, in welchem ein systematisches Service-Management betrieben werden soll. Der Anwendungsbereich kann dabei entlang einer oder mehrerer Dimensionen abgesteckt werden. Im klassischen Unternehmenskontext wird der Anwendungsbereich häufig anhand von Servicetypen, Kundenarten oder auch Standorten aufgespannt. Eine Definition des Anwendungsbereichs im Hochschulkontext auf Basis dieser Dimensionen ist zwar grundsätzlich möglich, allerdings sollte die Definition, aufgrund der besondere Strukturen und Rahmenbedingungen an Hochschulen entsprechend angepasst vorgenommen werden (siehe Abb. 3). Beispielsweise hängt die Definition des Anwendungsbereichs signifikant von der Größe der Hochschule und des HRZ ab sowie von den Zielen in Bezug auf das angestrebte Service-Management. Hinsichtlich der verschiedenen Servicetypen und Kundenarten lassen sich an der Hochschule vier größere Kundengruppen identifizieren, für die typischerweise Services erbracht werden: Studierende, akademisches Lehrpersonal, Hochschulverwaltungspersonal, Dritte. Zur Identifikation des Anwendungsbereichs kann es insbesondere für kleine HRZ hilfreich sein, den Anwendungsbereich zunächst auf Servicetypen zu beschränken, welche sich an die gemeinsamen Kernprozesse aller Kundengruppen – mit Ausnahme derer von Dritten – gleichzeitig richten. Größere HRZ oder HRZ mit fortgeschrittenen Zertifizierungsplänen hingegen können den Anwendungsbereich entlang der Services breiter fassen. Bezüglich der Eingrenzungsdimension des Anwendungsbereichs anhand von Standorten empfiehlt es sich im Hochschulkontext nur bedingt eine dedizierte Eingrenzung vorzunehmen. Hochschulen sind durch das allgemeine Wachstum in den letzten Jahrzehnten zwar häufig auf mehrere Standorte verteilt, allerdings haben sie an den jeweiligen Standorten meist

identische Kundengruppen und Services. Eine Beschränkung des SMS auf einen bestimmten Standort ist entsprechend nur selten als sinnvoll zu erachten.

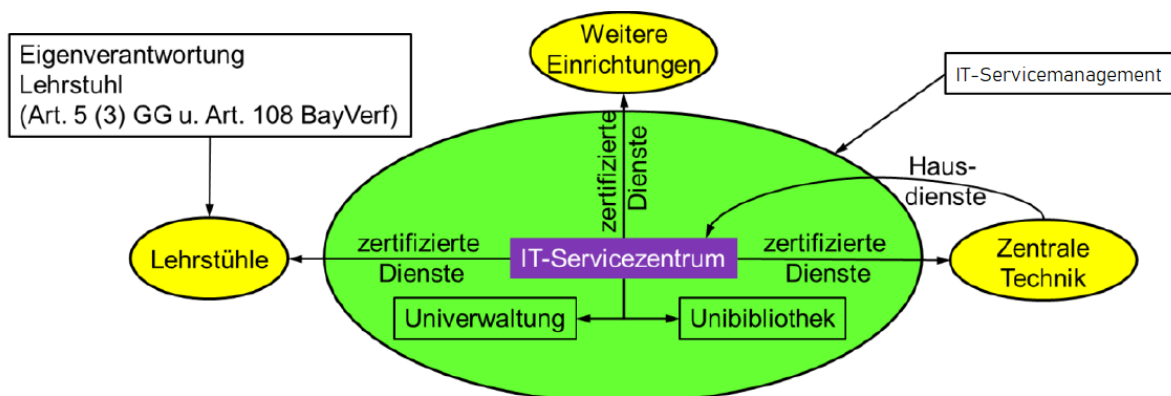


Abb. 3: Anwendungsbereich vom IT-Servicemanagement in einem exemplarischen HRZ

6.1.4 GR4: PLAN: Planung

Die Implementierung und der Einsatz eines SMS an Hochschulen ist eine umfangreiche und mitunter anspruchsvolle Aufgabe, bei dem der initiale Zielzustand von späteren Zielzuständen oftmals abweicht. Dies ist zum einen dem Umstand geschuldet, dass bei der initialen Implementierung eines SMS in der Regel ein zunächst engerer Anwendungsbereich und Zielerreichungsgrad definiert wird, gegenüber dem langfristigen Zielzustand. Ferner ändern sich in der Praxis die angebotenen Services, Prozesse, Technologien, sowie Anforderungen und sonstige Rahmenbedingungen, wodurch sich die Notwendigkeit einer kontinuierlichen Anpassung und Optimierung des SMS ergibt. Zur Erreichung eines fortgeschrittenen Zielerreichungsgrads sowie dem Begegnen von Umweltveränderungen bietet der Ansatz eines inkrementellen, kontinuierlichen Verbesserungsprozesses (KVP) ein strukturiertes Vorgehen für die Optimierung des Reifegrads des SMS. FitSM nutzt als KVP den bekannten PDCA-Zyklus, welcher den Verbesserungsprozess in die vier Phasen *Plan, Do, Check, Act* unterteilt (siehe Abb.4). Diese werden in den GR4 bis GR7 näher spezifiziert.

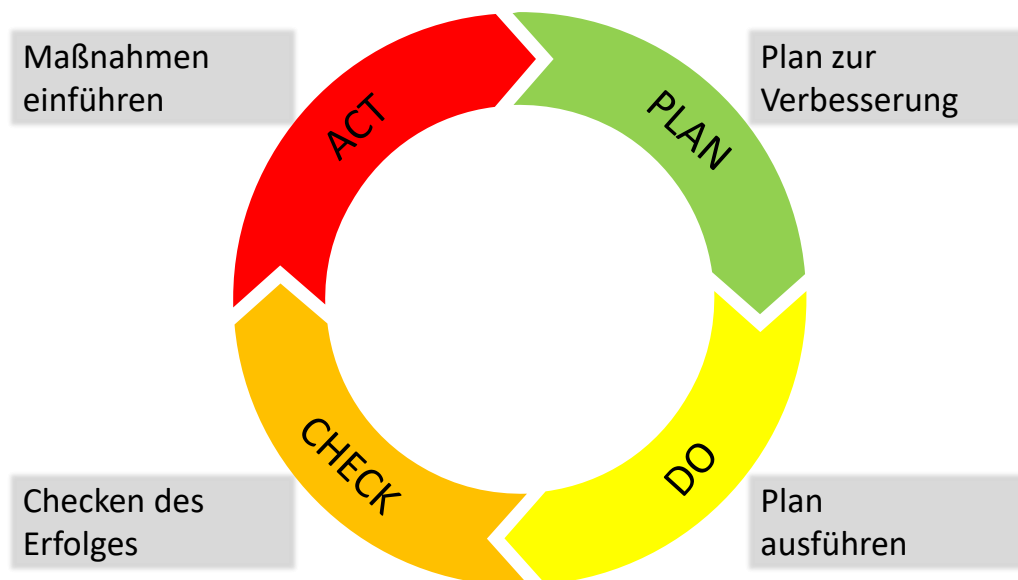


Abb. 4: Phasen des PDCA-Zyklus

In der Phase *Plan* sollen zunächst konkrete Maßnahmen zur Verbesserung des gegenwärtigen Status Quo des SMS definiert und in Form eines sogenannten Service Management Plans festgehalten werden. Oftmals gestaltet es sich für HRZ schwierig konkrete Maßnahmen zu planen, da Informationen über den Status Quo sowie den zugehörigen Optimierungspotentiale, gegenwärtige Fehlerquellen oder sonstige Unreife nicht in ausreichend strukturierter Form vorliegen. Entsprechend ist es zur Planung von Verbesserungsmaßnahmen zunächst wichtig, den gegenwärtigen Reifegrad des SMS zu definieren. Zur Bewertung des aktuellen Reifegrads stellt das in Kapitel 5 vorgestellte ITSM-Evaluierungsinstrument eine wertvolle Grundlage dar. Die Ergebnisse aus der Evaluierung zeigen dem Serviceverantwortlichen die Schwächen und Optimierungspotentiale des jeweiligen Anwendungsbereichs. Als nächstes sollte eine Festlegung von Zielen, welche im Zuge des Verbesserungsprozesses erreicht werden sollen. Die Ziele können sowohl strategischer als auch operativer Natur sein und sollten top-down durch den Leiter des HRZ oder CIO der Hochschule vorgegeben werden. Aus der Diskrepanz zwischen dem Status Quo auf Basis des ITSM-Evaluierungsinstruments und den definierten Zielen ergibt sich nun ein Delta, welche systematisch zu schließen ist. Da die formalisierten Ziele häufig qualitativer Natur sind, deren objektive Überprüfung meist Interpretationsspielraum aufweist, empfiehlt es sich die Ziele, um spezifische quantitative Leistungsindikatoren zu ergänzen. Sollte das HRZ beispielsweise eine große Diskrepanz zwischen der IST- und Soll-Servicequalität bei der Registrierung für das Gast-WLAN am Campus identifiziert haben und diese verbessern

wollen, so wäre ein geeigneter quantitativer Leistungsindikator beispielsweise der Quotient aus benötigter Registrierungszeit für Gäste gegenüber der benötigten Zeit für Hochschulangehörige.

Die im Zuge der Planungsphase erarbeiteten Informationen über den IST- und SOLL-Zustand, die daraus abgeleiteten Ziele sowie Leistungsindikatoren werden je nach Größe des Anwendungsbereichs umfangreich ausfallen und steuerungsintensiv. Aus diesem Grund empfiehlt es sich, sämtliche Planungsinhalte in Form eines Service-Management-Plans (SMP) zusammenzufassen. Der SMP sollte neben den Zielen insbesondere eine zeitliche Planung deren Umsetzung enthalten sowie dafür zuständige Rollen und Verantwortlichkeiten zuweisen. Häufig sind mit der Zielerreichung auch Schulungs- und Sensibilisierungsaktivitäten mit relevanten Stakeholdern verbunden. Diese können ebenfalls im SMP erfasst werden.

6.1.5 GR5: DO: Implementierung

In der *Do*-Phase des PDCA-Zyklus erfolgt die Umsetzung des in der *Plan*-Phase definierten Service-Management-Plans. Gemäß FitSM sind hierbei die Prozessbeschreibung, Mitarbeiter-schulung sowie eine Abstimmung zwischen Prozessschnittstellen vorzunehmen. Bei der Implementierung ist es wichtig, dass sämtliche involvierten Rollen und Verantwortlichen die für die Serviceprozesse definierten Service-Richtlinien und -Prozeduren von Beginn an auch in der Praxis einhalten. Nicht prozesskonformes Verhalten sollte durch das HRZ wahrgenommen werden können, und Reaktionen auf solche Prozessabweichungen erarbeitet werden. Die Reaktionen können von einfachen informationellen Hinweisen und Warnungen im Serviceprozess bis hin zu größeren Eskalationen mit disziplinarischen Maßnahmen reichen.

6.1.6 GR6: CHECK: Überwachung und Überprüfung

Sobald die im Service-Management-Plan definierten Maßnahmen implementiert und umgesetzt sind, sollten diese in der *Check*-Phase auf deren Effektivität und Effizienz hin überprüft werden. Die im SMP definierten Leistungsindikatoren stellen hierbei eine belastbare Grundlage für die Überprüfung des Maßnahmen Erfolgs dar. Im Zuge der *Check*-Phase werden zunächst die für die Leistungsindikatoren benötigten Daten erhoben und anschließend analysiert und ausgewertet. Die HRZ sollten den Überwachungsphase so strukturiert wie möglich angehen und Ergebnisse transparent für spätere, nachgelagerte Analysen dokumentieren. Für jede Messung sollten

HRZ zum Vergleich quantifizierte Zielgrößen definieren, um den Grad der Zielerreichung beschreiben zu können. FitSM empfiehlt bei der Definition der Zielgrößen die Beachtung des SMART-Prinzips. Dem SMART-Prinzip nach sollen Ziele spezifisch, messbar, erreichbar, angemessen, und terminiert sein. Sofern aus dem Leistungsindikator der Mitteleinsatz nicht unmittelbar hervorgeht, sollten zudem für den Leistungszustand benötigte Ressourcen erhoben werden, um diese ins Verhältnis zur Zielgröße setzen zu können. Zielerreichungen sind nur als sinnvoll zu erachten, wenn der Servicenutzen die dafür benötigten Mittel überwiegt.

Zudem sollte das HRZ klare Regeln definieren, wie die Überwachung organisational eingebettet wird und welche Teilbereiche des SMP in welchen zeitlichen Abständen durch welche verantwortliche Rolle überprüft werden sollen. Die Definition eines Auditplans kann für größere oder komplexere HRZ notwendig und von großem Nutzen sein.

6.1.7 GR7: ACT: Kontinuierliche Überwachung

In der *Act*-Phase werden die während der vorangehenden Phase gemessenen Daten der Leistungsindikatoren bewertet und das mögliche Verbesserungspotential daraus abgeleitet. Durch die aus der *Check*-Phase bekannten Ressourcenaufwände lassen sich die Verbesserungsmöglichkeiten priorisieren und strukturiert gemäß der spezifischen Ressourcenverfügbarkeit umsetzen. Falls das HRZ durch die Auswertung der Leistungsdaten nichtkonforme Abweichungen von definierten Zielen vorliegen feststellt, sollten korrigierende je nach Schwere der Abweichung unmittelbar Maßnahmen zur Verbesserung eingeleitet werden. Die Nichtkonformitäten sollten zunächst strukturiert dokumentiert und zugehörige Reaktionen durch spezifische Rollen definiert werden. Sofern in der *Plan*-Phase inkrementelle Prozess- und Serviceverbesserungen definiert wurden, fällt das Ableiten von Reaktionen in der *Act*-Phase in der Regel leichter und fördert die inkrementelle, aber kontinuierliche Verbesserung der Servicequalität des HRZ.

6.2 Spezifische Anforderungen (PR1-PR14)

6.2.1 PR1: Service Portfolio Management

Das Ziel des Service Portfolio Management ist einerseits die initiale Definition als auch kontinuierliche Pflege eines Serviceportfolios. Im Serviceportfolio sind die Informationen aller Services strukturiert zusammengeführt. Das Serviceportfolio beschränkt sich dabei nicht nur auf Informationen zu aktiven Services, sondern umfasst auch in der Entwicklung befindliche Services und temporär nicht angebotene Services. Der für den Kunden zur Verfügung stehende Satz an beziehbaren Services wird im Servicekatalog dargestellt. Im Zuge der Umstellung auf digitale Lehre während der Corona-Pandemie mussten HRZ kurzfristig zahlreiche neue digitale Services anbieten und bestehende temporär außer Betrieb nehmen. Beispielfähig ist hier der an vielen Hochschulen existierende Raumbuchungsservice für Lernräume am Campus zu nennen. Durch den temporären Charakter der pandemischen Restriktionen für den Präsenzlehrbetrieb war bei Außerbetriebnahme des Raumbuchungssystems dennoch mit einer späteren Wiederaufnahme zu rechnen. Ein temporäres Entfernen des Raumbuchungsservice aus dem für Hochschulangehörige zugänglichen Servicekatalog war entsprechend folgerichtig, ein Entfernen aus dem Service Portfolio allerdings nicht.

Für die strukturierte Erfassung sowie einer effizienten späteren Verwaltung und Handhabung der Services empfiehlt FitSM die Dokumentierung eines Service in Form eines Service Design & Transition Package, welches unter anderem folgende Informationen beinhaltet:

- **Serviceanforderungen, Projektplanung, Kommunikation- und Schulungsplanung, Technische Pläne und Spezifikationen, Ressourcenplänen, Terminpläne für die Entwicklung und Produktivsetzung**
- **Funktionale und nicht-funktionale Serviceabnahmekriterien, die ein Service erfüllen muss, bevor er den relevanten Stakeholdern zur Verfügung gestellt wird**

Neben der Konzeption und Definition von Wissensartefakten in Form des Service-Portfolios sowie der Service Design & Transition Packages werden im Rahmen des Service Portfolio Management ferner Anforderungen bezüglich Vorgehensweisen zur Serviceplanung, -änderung und -pflege aus strategischer und operativer Perspektive gestellt.

Bei der Implementierung eines SMS müssen gemäß FitSM folgende initiale und regelmäßige

Aktivitäten prozessual definiert und durchgeführt werden:

- **Initiale Aktivitäten:** Dokumentationsnormen und -standards für das Service Portfolio Management definieren, Servicespezifikationen definieren, erstmaliges Serviceportfolio definieren, Übersicht über relevante Beteiligte an der Serviceerbringung entwerfen
- **Wiederkehrende Aktivitäten:** Pflege des Service Portfolios, Gestaltung und Einbindung von neuen und geänderten Services, Gestaltung der Organisation zur Serviceerbringung

Die Gesamtverantwortung und strategische Steuerung des Serviceportfolios sollte dem IT-Service Manager obliegen. Operative Tätigkeiten können an die jeweiligen Prozessmanager delegiert werden. Die Aufgaben des Prozessmanagers umfassen:

- **Wiederkehrende Aktivitäten:** Aufrechterhaltung, Überprüfung und Aktualisierung des Serviceportfolios, Konformität neuer Services im Einklang mit den definierten Prozessen des Service Portfolio Management

Da allerdings die meisten kleineren HRZ die Aufgaben nur bedingt auf mehrere Rollen aufteilen können, sondern diese eher in Personalunion durchführen, ist es wichtig, dass die operativen Tätigkeiten auf der Ebene des Prozessmanagers immer auch aus einer strategischen High-level-Perspektive evaluiert und kritisch hinterfragt werden.

6.2.2 PR2: Service Level Management

Die Kernaufgabe des Service Level Management ist die Pflege des Servicekatalogs. Zudem werden im Rahmen der PR2 die Services Levels zu den angebotenen Services definiert und überwacht. Die Service Levels werden zwischen dem HRZ und den Servicenutzern durch sogenannte Service Level Agreements (SLA) formalisiert und dokumentiert (Abb. 5). Neben SLAs existieren ergänzende Operational Level Agreements (OLA), die die Beziehung zwischen HRZ-internen Teams bei der Serviceerbringung formalisieren. Underpinning Agreements (UA) formalisieren die umgekehrte Perspektive aus Sicht des HRZ – sie definieren die Rahmenbedingungen der Services von externen Lieferanten.

Ausgangslage für das Service Level Management bildet das Servicekatalog, welcher alle aktiven und beziehbaren Services des HRZ enthält. Typische Inhalte und Einträge des Servicekatalog sind in Tabelle 1 im Kapitel 6.1.2 dargestellt. Zu jedem Service im Servicekatalog sollte

das HRZ ein zugehöriges SLA definieren. Bei ähnlichen oder gar identisch anwendbaren SLAs auf mehrere Services im Servicekatalog können auch Standard-SLAs angewendet werden.

Typischer Inhalt eines Service Level Agreements:

- Zweck des SLA
 - Änderungshistorie des SLA
- Ausführliche Servicebeschreibung
 - Verantwortlichkeiten des HRZ
 - Rolle des Serviceempfängers
- Zugesagte Serviceverfügbarkeit und Servicezeit
 - Supportzeiten und -vereinbarungen
 - Reaktionszeiten
 - Umgang bei Serviceanpassungen und Änderungen
 - Kontinuität und Sicherheit
 - Preisgestaltung des Services
- Art der Service-Überprüfung und des Reportings
 - Konsequenzen bei Verletzung des SLA
 - Information über Art und Häufigkeit der Überprüfung

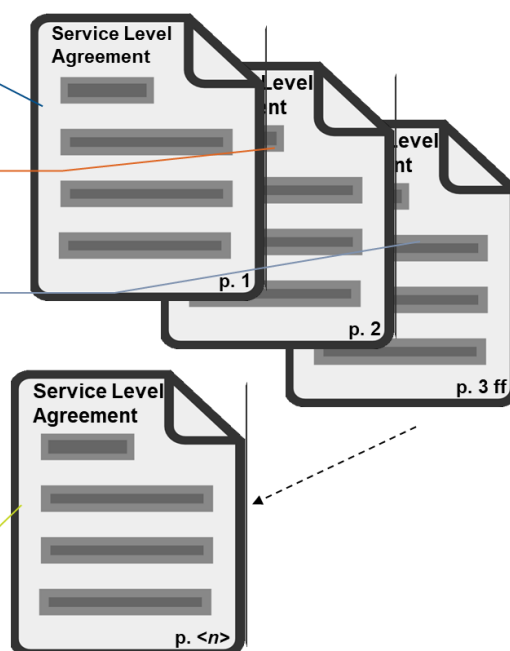


Abb. 5: Typische Inhalte von Service Level Agreements

Nicht zu vernachlässigen im Kontext von HRZ ist zudem die Definition und Erstellung von UAs. Durch oftmals hochschulübergreifende Prozesse (z.B. IT-Beschaffungsprozesse) spielen UAs eine ebenso wichtige Rolle für den späteren erfolgreichen Betrieb durch das HRZ angebotener Services wie die direkten Service Level Agreements selbst.

6.2.3 PR3: Service Reporting Management

Im Rahmen der PR3 „Service Reporting Management“ werden die Inhalte sowie der Struktur von Serviceberichten näher definiert. Das Service Reporting selbst dient insbesondere der Kommunikation der Qualität der Services. Die Services sollten regelmäßig auf ihre grundsätzliche Funktionserfüllung untersucht werden, und auf die Einhaltung der in den SLAs (aber auch OLAs und UAs) definierten Rahmenbedingungen bei der Serviceerbringung. Daneben können auch sonstige für einen Service vereinbarte Ziele untersucht werden. Das Ergebnis aus solchen Serviceprüfungen sollte anschließend in Form von Service Reports zusammengefasst und an einen ebenfalls zu definierenden Empfängerkreis versandt werden. Ein Service Report von ein und demselben Service kann je nach Empfängerkreis anders gestaltet sein, da diese mitunter

unterschiedliche Zwecke erfüllen. Service Reports an einen internen Empfängerkreis dienen beispielsweise primär der Kontrolle aber auch der gezielten Identifikation bis dato latenter Serviceprobleme, welche bisher nicht durch andere Kontrollprozesse entdeckt wurden. Die Berichterstattung kann sowohl in Umfang als auch zeitlicher Häufigkeit von Service zu Service abweichen. Inhaltlich sollten Service Reports stets eine eindeutige Bezeichnung des Berichts, einen Zweck, einen Empfängerkreis, einer Berichtshäufigkeit, ein definierter Inhalt, sowie die Art und Weise der Bereitstellung des Berichts umfassen. Die genauen Spezifikationen sind stets mit dem Empfängerkreis des jeweiligen Service Reports abgestimmt werden. Verantwortlich für den Inhalt des Service Reports ist in der Regel der Service Owner.

6.2.4 PR4: Service Availability & Continuity Management

Ziel und Zweck des Service Availability & Continuity Managements ist die Sicherstellung der Serviceverfügbarkeiten im täglichen Betrieb. Durch die mittlerweile zunehmend virtualisierte IT-Anwendungslandschaft von HRZ ist das Risiko von Serviceausfällen durch Hardware-Defekte in den letzten Jahren merklich zurückgegangen. Nichtsdestotrotz hat sich das Ausfallrisiko bestimmter Services durch die Einbindung extern verwalteter Service zunehmend erhöht. Fällt beispielsweise eine extern in der Cloud gehostete Videokonferenz-Software betreiberseitig aus, lassen sich daraus resultierende Störungen nur schwer beheben. Durch die heterogene Servicestruktur und zugrundeliegende IT-Landschaft müssen HRZ umfassende Maßnahmen zur Sicherstellung der Serviceverfügbarkeit (Availability Management) sowie zur Vorbeugung und Auflösung von außerordentlichen Störereignissen (Continuity Management) ergreifen. Beispielhaft für solche außerordentlichen Störereignisse sind Krisen, Notfälle oder Katastrophen in Form von Stromausfällen oder Pandemien.

Die grundsätzlichen Anforderungen an die Serviceverfügbarkeit ergibt sich aus den SLAs. Die dort formalisierten Anforderungen stellen die Mindestanforderungen an das Service Availability & Continuity Management. Die dort definierten messbaren Zielgrößen beziehen sich meist auf die grundsätzliche Verfügbarkeit des Service, die Zeit zwischen zwei Störungen oder die Ausfallzeit. Ferner existieren häufig auch lösungsorientierte Kenngrößen wie die Entdeckungszeit, Reaktionszeit, Reparaturzeit oder Wiederherstellzeit.

Wichtig bei der Beurteilung möglicher Störereignisse ist das Risiko der Störung. Das Risiko ergibt sich aus der Multiplikation zweier relevanter Kenngrößen: Eintrittswahrscheinlichkeit (0

bis 100%) und Schadensauswirkung (z.B. quantifiziert in monetären Kosten). Eine gründliche Risikobewertung ist gleichzeitig auch der erste Schritt zu Erarbeitung von vorbeugenden Maßnahmen. Je höher das Risiko eines Serviceausfalls, desto wichtiger die Vorbereitung entsprechender Notfallmaßnahmen, welche in strukturierten Notfallpläne überführt werden können. Ein bewährtes Artefakt aus der Service Availability & Continuity Management stellt die Erstellung eines Notfallhandbuchs da, welches umfangreiche Informationen zu erwarteten Störeeignissen und empfohlenen Lösungsstrategien definiert. Ein gutes, umfassendes Notfallhandbuch ermöglicht im Störfall die schnelle Wiederherstellung von ausgefallenen Services.

6.2.5 PR5: Capacity Management

Bei der Anforderung des Capacity Management geht es darum, dass sichergestellt wird, dass ausreichend Kapazitäten für die Erfüllung der Anforderungen bereitgestellt werden. Dabei bezieht sich der Begriff Kapazität nicht nur auf die technische Perspektive (Speicherplatz, Serverleistungen, Webseitenzugriffe) sondern auch auf finanzielle oder personelle Aspekte. Die Anforderungen der Kapazitäten können aus den jeweiligen Service-Level-Agreements oder Vereinbarungen entnommen werden, aber auch individuell aus Antwortzeiten für Anfragen oder Tickets.

Um einen Soll- und Ist-Vergleich für Kapazitäten zu ermöglichen, macht es Sinn einen Kapazitätsplan aufzusetzen, um diese zu überwachen. Dies ermöglicht es auch auf Kapazitätsengpässe zu reagieren. So können aber auch neue Services eingepflegt werden und der benötigte Bedarf an neuen Kapazitäten schnell eingepflegt werden. Das Aufsetzen, die Pflege und die Überwachung der Kapazitäten obliegt dabei dem jeweiligen Service Owner.

6.2.6 PR6: Information Security Management

Auch beim IT-Servicemanagement spielt die Informationssicherheit auch eine wichtige Rolle. Dabei ergeben sich auch viele Parallelen zur ISO 27001 Norm oder verwandten IT-Sicherheitsstandards. Das Information Security Management umfasst dabei die Schutzziele Vertraulichkeit, Integrität und Zugreifbarkeit von Informationen, welches für die Serviceerbringung gehalten werden soll. Dabei wird unter den Schutzziele folgendes verstanden:

- **Vertraulichkeit:** Nur berechtigte Personen dürfen in der Lage sein, Informationen einzusehen.

- **Integrität:** Die Integrität von Informationen ist gewahrt, wenn diese nicht unberechtigt geändert, dupliziert oder gelöscht wurden.
- **Zugreifbarkeit:** Informationen sind für autorisierte Personen zugreifbar und nutzbar.

Für die jeweiligen Services macht es Sinn den Schutzbedarf zu erfassen, also wie hoch ein Schadensfall in Bezug auf die Informationen sein kann. Dabei kann nach den Schutzbedarfskategorien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nach Normal, Hoch und Sehr hoch unterschieden werden (BSI 2017). Nach identifizieren des jeweiligen Sicherheitsniveaus sollte dann entsprechende Risiken identifiziert und reduziert werden. Dabei sind Risiken nicht nur Phishing-E-Mails oder Ransomware, sondern auch versehentliches Löschen von Dateien durch Mitarbeiter. Entsprechend der Risiken sollten Maßnahmen vorbereitet werden, um diesen entgegenzuwirken. Dabei können Maßnahmen sowohl technischer Natur (Virens Scanner, Firewall), organisatorisch (Richtlinien für den Arbeitsplatz) oder Awareness steigend (Schulungen) sein. Ein Mix unterschiedlicher Maßnahmen ist dabei sehr zu empfehlen.

Um die Informationssicherheit im Rechenzentrum zu gewährleisten, sollte dabei ein Informationssicherheitsbeauftragter bestimmt werden, welcher zentraler Ansprechpartner für das Thema ist. Zum Aufgabenfeld der Informationssicherheit gehört dabei neben den Informationssicherheits-Richtlinien und Maßnahmen auch die regelmäßige Überprüfung und das koordinierte Bearbeiten von Informationssicherheitsereignissen. Für die wichtigsten schützenswerten Informationen sollte es zudem einen jeweiligen Eigentümer der Daten geben, welcher für diese der primäre Ansprechpartner ist und bei der Ermittlung und Analyse von Informationssicherheitsrisiken unterstützt.

6.2.7 PR7: Customer Relationship Management

Beim Customer Relationship Management ist am Anfang wichtig zu erklären was mit „Customer“ (Kunde) gemeint ist. Wichtig dabei ist die Unterscheidung zwischen Kunden und Anwendern. Dabei meint der Begriff Kunde „eine Organisation oder einen Teil einer Organisation, die einen Service-Provider mit der Bereitstellung eines oder mehrerer Services beauftragt.“ (Quelle FitSM) und der Begriff Anwender bezeichnet die direkten Nutzer eines Service. Diese Unterscheidung ist wichtig, da Anwender Störungen oder Anfragen direkt beim Servicedesk melden, während Kunden einen Kundenbetreuer haben, auf den sie zugehen können.

Für den Hochschulkontext bedeutet das, dass ein Großteil der beteiligten Parteien als Anwender eingestuft werden können, wie z.B. Studierende oder wissenschaftliche Mitarbeitende. Kunden sind nur die Parteien mit denen Service Level Agreements (SLAs) unterschrieben werden. Das kann zum Beispiel der Fall sein, wenn ein Rechenzentrum seine Dienste auch externen anbietet. Für diese Fälle muss ein entsprechendes Customer Relationship Management aufgebaut werden. Dies bedeutet konkret, dass entsprechende Kundenbetreuer bereitgestellt werden, welche dem Kunden zur Verfügung stehen. Dieser bildet den Kontaktpunkt für entsprechende Kunden. Der Kundenbetreuer ist dann verantwortlich für die Erfüllung der Anforderungen des Kunden, aufgetretene Beschwerden, aber auch die Kundenzufriedenheit. Dabei sollten die Kunden übergreifend in einer Kundendatenbank gemanagt werden.

6.2.8 PR8: Supplier Relationship Management

Sowie sich das Customer Relationship Management mit den Kunden auseinandersetzt, beschäftigt sich das Supplier Relationship Management mit den „Suppliern“ (Lieferanten). Dabei sollte entsprechend wie für die Kunden eine Lieferantendatenbank angelegt werden, in welcher alle externen Zulieferer von Produkten und Dienstleistungen zusammengeführt werden. Auch gibt es für jeden Lieferanten einen entsprechenden Lieferantenbetreuer, welcher zentraler Ansprechpartner für die Lieferanten ist und die Kommunikation übernimmt. Diese Person überwacht auch die Leistungen der Lieferanten.

6.2.9 PR9: Incident and Service Request Management

Das Incident and Service Request Management setzt sich mit der Behebung und Beantwortung von Incidents (Störungen) und Service-Requests (Anfragen von Anwendern) auseinander. Dabei bezeichnet eine Störung den Fall, dass ein Service nicht nach seinen versprochenen Zielen angeboten werden kann, und die Anfragen bezeichnen die Nachfrage nach von Anwendern nach IT-Unterstützung. Beide Arten von Fällen laufen in der Regel im Rechenzentrum über einen Service-Desk. Störungen können dabei sowohl vorliegen, wenn ein Serviceangebot nicht mehr verfügbar ist, aber auch wenn ein Service nicht in seiner vereinbarten Qualität angeboten wird. Dabei muss es auch nicht unbedingt der Fall sein, dass der Anwender die Störung mitbekommt.

Wichtig ist, dass alle Incidents und Service-Requests müssen auf konsistente Art und Weise

erfasst, klassifiziert und priorisiert werden. Klassifikation bedeutet in dem Fall das Anfragen nach gewissen Kriterien in Kategorien gebündelt werden. So können ähnliche Anfragen vom gleichen Verantwortlichen beantwortet werden bzw. kann auch auf die bisherigen Anfragen zurückgegriffen werden. Personen, die mit der Bearbeitung von Anfragen und Störungen beauftragt sind, müssen Zugang zu relevanten Informationen sowie bekannten Fehlern und Workarounds erhalten, damit eine Bearbeitung erfolgen kann. Zudem ist es durch eine Klassifikation möglich, Statistiken darüber zu erstellen, in welchen Bereichen verstärkt Vorfälle auftreten bzw. vice versa. Ergänzend zu Klassifikation sollte auch eine Priorisierung der Anfragen vorgenommen werden, da die Kapazitäten des Rechenzentrums nur begrenzt zur Verfügung stehen. Hier hat es sich bewährt Anfragen nach Auswirkung und Dringlichkeit zu klassifizieren. Grundsätzlich sind so vier Fälle zu unterscheiden:

- **Auswirkung niedrig, Dringlichkeit niedrig:** Drucker ist nicht mehr eingerichtet nach Update für eine Person
- **Auswirkung hoch, Dringlichkeit niedrig:** Ein automatisches Anmelden im Eduroam ist nicht mehr möglich, sondern nur noch manuell möglich.
- **Auswirkung niedrig, Dringlichkeit hoch:** Drucker ist nicht mehr eingerichtet nach Update für eine Person und es sollen bspw. Uniklausuren gedruckt werden.
- **Auswirkung hoch, Dringlichkeit hoch:** Das Internet an der Hochschule ist ausgefallen.

Wichtig dabei ist, dass eine Klassifikation und Priorisierung auf strukturierte und konsistente Art erfolgt. Gleichzeitig muss es Prozesse bzw. Regelungen dafür geben wann bei einer Anfrage eine Eskalation erfolgt. Dies kann der Falls ein, wenn z.B. eine gewisse Zeit bei der Beantwortung überschritten wurde aber auch, wenn zusätzliches Know-how hinzugezogen werden muss bzw. eine Anfrage nicht von der zugeteilten Person beantwortet werden kann.

Des Weiteren hat sich aus Praxiserfahrungen gezeigt, dass eine hohe Transparenz bei Anfragen sinnvoll ist und eine zusätzliche Klassifikation nach Major Incidents sinnvoll ist. Ersteres lässt sich über ein simples Tracking bei der Beantwortung von Anfragen erreichen, sodass Anwender sich jederzeit über den aktuellen Bearbeitungsstand erkundigen können. Die Einteilung nach Major Incidents sollte für den Fall notwendig sein, dass eine Störung hohe Auswirkungen be-

sitzt, z.B. ein Ausfall der kompletten Netzwerk-Infrastruktur. Häufig bedarf es bei solchen Störungen einer Zusammenstellung eines speziellen Teams und eine stetige Abstimmung mit verantwortlichen Führungspersonen.

Zusammenfassend ist beim Incident and Service Request Management wichtig, dass es klare Regelungen dazu gibt, wie Störungen und Anfragen klassifiziert, priorisiert und abgearbeitet werden.

6.2.10 PR10: Problem Management

Das Problem Management ist eng mit dem Incident Management verknüpft, und zwar beschäftigt sich dieses mit dem Erarbeiten von langfristigen Lösungen, damit wiederkehrende Störungen vermieden werden können. Anders formuliert, geht es darum dauerhafte Lösungen für Workarounds zu schaffen. Dabei verfolgt das Problem Management eine Ursachenanalyse bzw. Trendanalyse für Störungen. Eine Ursachenanalyse sollte dabei durchgeführt werden, wenn eine Störung häufiger auftritt oder eine Störung nicht ohne Ursachenanalyse gelöst werden kann.

Vergleichend wie bei Störungen sollten Probleme klassifiziert und priorisiert werden, damit diese der Reihenfolge nach abgearbeitet werden können. Für die priorisierten Probleme sollte dann eine Lösung gefunden werden, welche dann im Sinne des Change Managements (siehe Kapitel 4.5.12) implementiert werden. Dabei ist es wichtig, dass das Finden und Ausarbeiten einer Lösung grundsätzlich nicht mehr Aufwand als die Workarounds bedeuten sollte. Dabei kann natürlich auch der Fall auftreten, dass ein Problem nicht dauerhaft beseitigt werden kann, in so einem Fall sollten effektiven Workarounds oder Umgehungslösungen systematisch erfasst und bereitgestellt und auch gepflegt werden.

6.2.11 PR11: Configuration Management

Das Configuration Management beschäftigt sich mit den Elementen bzw. Objekten, welche zur Erbringung von Services erforderlich sind. Diese Verknüpfungen und Elemente sollten dabei in einer Datenbank erfasst und gemanagt werden. Diese Elemente können dabei unterschiedlicher Natur sein: Hardware, Software, Dokumentationen/Leitfäden und Services selbst. Die Erfassung der Beziehungen untereinander ist dabei wichtig, um zu erkennen welche Abhängigkeiten gegeben sind, und was vielleicht ein Ausfall von einem Hardware-Element für welche

Services bedeutet bzw. auch andersrum gedacht, wenn man gewisse Reaktionszeiten oder Up-time für Services garantiert, was dies auch für die einzelnen Elemente bedeutet.

Wichtig für die praktische Umsetzung sind zwei Aspekte. Erstens, dass eine geeigneter Detaillierungsgrad für die Datenbank gewählt wird, also welche Granularität gewählt wird. Ein zu geringer Grad kann dazu führen, dass wichtige Elemente nicht genug Aufmerksamkeit bekommen, ein zu hoher Grad kann dazu führen, dass Elemente nicht mehr aktuell gehalten werden können durch den zu hohen Aufwand. Dies leitet auch zum zweiten Punkt über, dass eine Datenbank aktuell gehalten werden muss, hierfür müssen Strukturen und Prozesse geschaffen werden, dass ein regelmäßiger Soll-Ist-Abgleich durchgeführt wird. Ebenfalls muss bei einem neuen Service oder Element zum Release eine erste Version dazu in der Datenbank angelegt werden.

6.2.12 PR12: Change Management

Das Change Management befasst sich mit dem koordinierten Einführen neuer Services bzw. Anpassen bestehender Services. Der Hintergrund hierbei ist, dass es einheitlich Prozesse und Abläufe zur Einführung/Anpassung von Services gibt, so dass auch dieser Bereich strukturiert angegangen werden kann. Als Change kann dabei eine Veränderung (wie das Hinzufügen, Entfernen, Modifizieren oder Ersetzen) an einem Configuration Item (siehe Kapitel 4.5.11) verstanden werden.

Wichtig für die Implementierung von Changes ist, dass auch diese klassifiziert und priorisiert werden, unterschieden nach Standard-Changes, Nicht-Standard-Changes und Notfall-Changes.

- **Standard-Change:** Hierunter fallen alle Changes mit geringem Risiko, welche auch schon Mal den Change-Prozess durchlaufen haben, z.B. Bereitstellung von Grundausstattung, Austausch eines Geräts, usw. Für diese Changes ist keine Autorisierung oder Change-Prozess erforderlich.
- **Nicht-Standard-Change:** Nicht-Standard-Changes bedürfen eines Änderungsantrags, da sie mit einem gewissen Risiko verbunden sind. Das kann zum Beispiel der Fall sein, wenn Infrastruktur (z.B. Server) ausgetauscht werden muss, welche für Kernservices verantwortlich sind.

- **Notfall-Change:** Ergänzend bei Notfall-Changes kommt bei Notfall-Changes ein Zeitfaktor hinzu, der dafür sorgt, dass der Standard-Change-Prozess nicht durchlaufen werden kann, z.B. bei einem neuen Sicherheitspatch. In diesem Fall müssen separate Verfahren und Abläufe definiert werden, um weiterhin die Qualität zu gewährleisten.

Für den Change-Prozess ist es wichtig, dass für die Changes bzw. als Genehmigungsgrundlage Angaben zu dem Nutzen, den Risiken, potenziellen Auswirkungen auf Services und Kunden sowie der technischen Realisierbarkeit gemacht werden, so dass anschließend die Changes genehmigt werden können. Die Genehmigung erfolgt dann durch das definierte Leitungsgremium des Change Managements, was meistens auch einer Kombination aus mindestens Rechenzentrumsleitung und Stellvertreter besteht. Ergänzend ist wichtig, dass für Changes mit hohem Maß an Auswirkungen und Risiken Abläufe geplant sind, was im Falle eines Fehlschlages passiert, also wie die Changes wieder rückabgewickelt werden können.

6.2.13 PR13: Release & Deployment Management

Eng verknüpft mit dem Change Management ist das Release & Deployment Management, welches sich damit befasst einzelne, genehmigte Changes zu bündeln und als gebündelter Release zu testen und live zu setzen. Den Rahmen sowie den Ablauf eines Release von der Planung über die Implementierung bis zum Abschluss bildet eine Release-Richtlinie. Diese sollte die folgenden Schritte enthalten:

- **Releaseplanung:** Der Bedarf an Ressourcen (Personal, finanzielle Mittel) für einen neuen Release wird zusammengestellt.
- **Releasezusammenstellung:** Einzelne Changes werden zu einem Release zusammengestellt und gebündelt
- **Abnahmetest:** Der Release wird anhand vorher gewählter Kriterien getestet, sowohl durch Kunden als auch andere relevante Beteiligte. Auf Basis der Abnahmetests wird entschieden, ob der Release ausgerollt wird. Die Abnahmekriterien für einen Release sollten vorher soweit möglich einheitlich festgelegt werden
- **Rollout-Planung:** Der Zeitpunkt und die Form des Rollouts werden festgelegt. Zum Beispiel kann es bei einem umfassenden betriebssystemupdate Sinn machen, nicht alle Rechner auf einmal upzudaten, sondern abteilungsweise vorzugehen.

- **Rollout-(Vorbereitung):** Entsprechende Software und Hardware für den Rollout wird bereitgestellt und anschließend am Tag des Rollouts ausgerollt und der Release implementiert

Für jeden Release sollten zudem Fehlerkorrekturpläne vorliegen, was passiert, wenn ein Release fehlschlägt bzw. angepasst werden muss. Zudem sollte nach einem Release geprüft und überwacht werden, ob es zu Fehlermeldungen kommt.

6.2.14 PR14: Continual Service Improvement Management

Das Continual Service Improvement Management hat den Grundgedanken im IT-Service-Management kontinuierlich Verbesserungsmöglichkeiten zu erkennen, diese zu priorisieren und strukturiert umzusetzen. Verbesserung bedeutet, dass das Niveau an Konformität, Effektivität oder Effizienz optimiert werden soll (Quelle FitSM).

- **Konformität:** Werden die Anforderungen erfüllt oder gibt es Abweichungen?
- **Effektivität:** Welcher Zielerreichungsgrad wird erreicht bzw. wie wirksam sind spezielle Aktivitäten?
- **Konformität:** Wie wirtschaftlich sind die Aktivitäten?

Die Verbesserung eines Service soll die Qualität oder die Leistung eines gesamten Service oder auch nur einer einzelnen Servicekomponente optimieren. Dabei werden die Qualitäts- und Leistungsziele aus den entsprechenden Anforderungen abgeleitet. Ist eine potentielle Verbesserung identifiziert worden, wird das Verbesserungspotential erfasst und bewertet. Dazu werden Leistungsindikatoren (Key Performance Indicator, KPI) abgeleitet, die auch klar definieren, wie eine Verbesserung zu bewerten ist. Bei einer positiven Einschätzung wird die Verbesserung implementiert und umgesetzt im Einklang mit dem Change Management.

7 Abschließende Empfehlungen

Im Folgenden haben wir noch Empfehlungen gesammelt, welche sich im Rahmen der Befragung und Auswertung einzelner HRZ ergeben haben.

Empfehlung 1: Die Einführung von ITSM erfordert freie Mitarbeiterkapazität(-en)

Die Einführung und Etablierung von ITSM-Strukturen ist ein langwieriger Prozess und erfordert Mitarbeitende, die für das Thema abgestellt werden und die Einführung koordinieren. In diesem Zusammenhang sollte auch die komplette Mitarbeiterschaft des HRZ informiert und abgeholt werden, da eine Einführung vom kompletten Team getragen werden sollte. Dabei sollte am Anfang klar ein Ziel (siehe Kapitel 5.2) definiert werden, welches erreicht werden soll, um darauf basierend einen Plan für die Umsetzung zu entwickeln. Zum Beispiel kann bei einer Einführung eines ITSMs nach ISO 20000 Standard je nach aktuellem IST-Zustand von einem Zeitraum von 2-3 Jahren ausgegangen werden.

Empfehlung 2: Eine ITSM-Strategie für das jeweilige HRZ muss ausgehend von unterschiedlichen Reifegradstufen individualisiert gestaltet werden.

Durch die Analyse und Evaluierung der einzelnen HRZ hat sich ergeben, dass das Thema ITSM unterschiedlich stark in den jeweiligen HRZ verankert ist. Zum einen gibt es HRZ, die sich im Rahmen von IT-Sicherheitsthemen auch gleichzeitig mit ITSM auseinandergesetzt haben und somit erste Grundpfeiler für ITSM-Strukturen gelegt wurden, zum anderen gibt es auch HRZ, die sich mit dem ITSM noch gar nicht beziehungsweise sehr wenig auseinandergesetzt haben und wodurch noch keine Strukturen vorhanden sind. Für eine mögliche Vorgehensweise bedeutet dies, dass man kein pauschales Integrationskonzept zur Vereinheitlichung des hochschuleigenen ITSM aller HRZ entwickeln kann, sondern je nach Reifegrad individuell eine Strategie entwickeln muss. Beispielsweise kann ein HRZ, welches sich auf einem niedrigeren Reifegrad einordnet, mit der Erstellung eines Serviceportfolios beginnen, um initial den Status Quo und den Umfang des aktuellen Service Angebots abzustecken. Im Kontrast dazu identifiziert ein HRZ, welches sich tendenziell bei den höheren Reifegraden einordnet, konkrete Punkte zur Umsetzung einer professionellen (ITSM-)Zertifizierung (vgl. Kapitel 5).

Empfehlung 3: Eine Involvierung der Hochschulleitung ist unabdingbar.

Gerade durch die individuelle Selbstevaluierung der einzelnen HRZ ließ sich feststellen, dass

das Thema ITSM durch einen „top-down“-Ansatz geprägt ist. Zum einen konnte im Rahmen der Interviews festgestellt werden, dass das Thema ITSM vom Topmanagement beziehungsweise im Hochschulkontext, der Hochschulleitung, getrieben wird, um ITSM fokussiert anzugehen. Zum anderen ließ sich über die Länge des Bearbeitungszeitraums zur Beantwortung der Fragestellungen des Evaluierungsinstruments, zwischen drei Werktagen bis über 60 Werktage, feststellen, dass eine Motivation und eine Verpflichtung der Hochschulleitung für das Thema unabdingbar sind. Dies ist auch dadurch zu begründen, dass für eine Integration des ITSM in bestehende HRZ sowohl finanzielle als auch organisatorische Mittel notwendig sind, sei es über Prozesse, welche zu definieren, oder durch Stellen für Mitarbeitende, welche speziell für ITSM geschaffen und integriert werden müssen. Des Weiteren liegt das Thema ITSM nicht allein bei einem HRZ, sondern ist auch übergreifend für andere Abteilungen, zum Beispiel der Verwaltung, der Lehrstühle, der Bibliotheksdienste, relevant und muss auch bei diesen Organisationseinheiten, welche nicht mehr nur dem HRZ zugeordnet sind, in gewissem Maße integriert und umgesetzt werden, wofür eine Unterstützung der Hochschulleitung unabdingbar ist.

Empfehlung 4: Betrachtung der eigenen Leistungen als Service-Portfolio.

Ein Aspekt, der im Rahmen der Evaluierung der HRZ aufgefallen und auch Teil der Anforderungen von FitSM, ITIL® und ISO/IEC 20000 ist, ist das Service-Portfolio. Basierend auf der Datenerhebung konnte die Erstellung einer trennscharfen Definition der angebotenen Services im Rahmen eines Service-Portfolios als essenzieller Teilaspekt eines professionellen ITSM abgeleitet werden. Dies bietet eine effiziente Möglichkeit, sich einen Überblick über die eigenen Leistungen des HRZ zu verschaffen und darüber hinaus auch die Verantwortlichkeiten des HRZ abzustecken. Dieser Überblick über die angebotenen Leistungen, ergänzt durch Informationen, wie zum Beispiel Verantwortung, Anlaufstelle, Verfügbarkeit und Umfang ergeben dann auch ein entsprechendes Service-Portfolio beziehungsweise Servicekataloge, welche unter anderem für eine ISO/IEC 20000 Zertifizierung gefordert sind. Die Erstellung ist deswegen ein fundamentaler Baustein zum Ausbau des ITSM, da basierend auf diesem Portfolio dann weitere Anforderungen, wie zum Beispiel Change-Management oder Service-Reporting, geprüft und integriert werden können.

Empfehlung 5: Die Thematik der IT-Sicherheit eignet sich als Einstieg für die Vertiefung des ITSM.

Im Rahmen der Ergebnisanalyse unserer Datenerhebungen mit den einzelnen HRZ hat sich ergeben, dass die Thematik der IT-Sicherheit ein sinnvoller Einstieg für die ITSM-Strategie bietet. Dies liegt unserer Meinung nach an zwei Aspekten. Zum einen ist das Thema IT-Sicherheit wie in Kapitel 6.2.6 beschrieben durch spezifische Auflagen in Deutschland auch in HRZ bereits rechtlich gefordert und deswegen schon sehr stark verbreitet. Zum anderen können sich IT-Organisationen sowohl nach ISO/IEC 20000 (ITSM) als auch nach ISO/IEC 27000 (IT-Sicherheit) voneinander unabhängig zertifizieren lassen. Im Zuge dessen wird die Thematik der IT-Sicherheit häufig höher priorisiert, auch aufgrund gesetzlicher Anforderungen, und eignet sich daher als idealer Einstiegspunkt für einer Vertiefung des hochschuleigenen ITSM. Es kann in einem späteren Schritt für eine Zertifizierung nach ISO/IEC 20000 (ITSM) weiter ausgebaut werden. ITSM und IT-Sicherheit bieten aufgrund einer thematisch hohen Schnittmenge einen idealen Anknüpfungspunkt, um beginnend mit der IT-Sicherheit entsprechende Anforderungen gebündelt anzugehen.

8 Danksagung

Die Autoren bedanken sich herzlich beim Staatsministerium für Wissenschaft und Kunst (StMWK) für die finanzielle Unterstützung als Fördergeber des Forschungsprojekts „*IT-Servicemanagement für bayerische Hochschulrechenzentren*“. Des Weiteren gilt der Dank den beteiligten Hochschulen bzw. Hochschulrechenzentren, die an der Datenerhebung, Analyse und Evaluierung als Grundlage für dieses Booklet beteiligt waren.

9 Literaturverzeichnis

Abolhassan, Ferri (2017): *The Drivers of Digital Transformation*. Cham: Springer International Publishing.

Beims, Martin; Ziegenbein, Michael (2021): *IT-Service-Management in der Praxis mit ITIL: Zusammenarbeit systematisieren und relevante Ergebnisse erzielen*. 5. Aufl. München: Hanser.

BSI (2017): *BSI-Standard200-2 IT-Grundschutz-Methodik*. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html;jsessionid=9A9F21F2EF05E747755CDFC572991E31.internet082.

FitSM (2021): *FitSM - Standards for lightweight IT service management*. Online verfügbar unter <https://www.fitsm.eu/>, zuletzt geprüft am 01.12.2021.

Gaulke, Markus (2019): *Praxiswissen COBIT: Grundlagen und praktische Anwendung in der Unternehmens-IT. Geeignet als Vorbereitung auf die ISACA-Prüfungen: COBIT Foundation, IT-Governance & IT-Compliance Practitioner, IT-Governance-Manager, IT-Compliance-Manager, CGEIT*. 3., aktualisierte und überarbeitete. Heidelberg: dpunkt.Verlag.

Gröger, S.; Schumann, M. (2013): *IT-Unterstützung Zur Verbesserung Der Dritt- Und Sondermittelbewirtschaftung an Hochschulen – State of the Art*. Arbeitsbericht Nr. 3, Arbeitsbericht. Hg. v. Georg-August-Universität Göttingen. Göttingen.

Hochstein, Axel; Zarnekow, Rüdiger; Brenner, Walter (2004): *Serviceorientiertes IT-Management nach ITIL: Möglichkeiten und Grenzen*. In: *HMD - Praxis der Wirtschaftsinformatik*, Bd. 239.

Iden, Jon; Eikebrokk, Tom Roar (2013): *Implementing IT Service Management: A systematic literature review*. In: *International Journal of Information Management* 33 (3), S. 512–523. DOI: 10.1016/j.ijinfomgt.2013.01.004.

Jonas, Claudius; Lautenschlager, Jonathan; Eymann, Torsten (2021): *Die Entwicklung bayerischer Hochschulrechenzentren – Handlungsempfehlungen aus einer Fallstudie für ein professionelles IT-Service-Management*. In: *HMD* 58 (5), S. 1004–1019. DOI: 10.1365/s40702-021-00763-7.

Knittl, Silvia; Grindler, Achim; Vellguth, Karmela (2012): IT-Service-Management Rahmenwerke – wie sie sinnvoll in Universitäten einsetzbar sind. Hg. v. P. Müller, B. Neumair, H. Reiser und G. D. Rodosek. Gesellschaft für Informatik e.V. Bonn (5. DFN-Forum Kommunikationstechnologien – Verteilte Systeme im Wissenschaftsbereich).

Rohrer, Anselm; Söllner, Dierk (2017): IT-Service Management mit FitSM: Ein praxisorientiertes und leichtgewichtiges Framework für die IT. Heidelberg: dpunkt.Verlag.

Rudnicka, J. (2020): Anzahl der Hochschulen in Deutschland in den Wintersemestern 2015/2016 bis 2019/2020 nach Hochschulart. Hg. v. Statista. Online verfügbar unter <https://de.statista.com/statistik/daten/studie/247238/umfrage/hochschulen-in-deutschland-nach-hochschulart/#professional>, zuletzt geprüft am 18.11.2021.

Schmücker, Stefanie (2011): Universitätsprofile – Konzeption, Komponenten sowie empirische Umsetzung an deutschen Universitäten. Bayerisches Staatsinstitut für Hochschulforschung und Hochschulplanung, München.

Teubner, Alexander (2013): IT-Service Management in Wissenschaft und Praxis: VDM Verlag Dr. Müller.

Tiemeyer, Ernst (2020): Handbuch IT-Management; Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 7., überarbeitete. München: Hanser.

van Bon, JAn (2008): Foundations of IT Service Management Based on ITIL®. Vol. 3. 3. Aufl. Zaltbommel: Van Haren Publishing.

Williamson, Ben; Eynon, Rebecca; Potter, John (2020): Pandemic Politics, Pedagogies and Practices: Digital Technologies and Distance Education during the Coronavirus Emergency. In: *Learning, Media and Technology* 45 (2), S. 107–114. DOI: 10.1080/17439884.2020.1761641.

Zwilling, Moti; Klien, Galit; Lesjak, Dušan; Wiechetek, Łukasz; Cetin, Fatih; Basim, Hamdullah Nejat (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. In: *Journal of Computer Information Systems*, S. 1–16. DOI: 10.1080/08874417.2020.1712269.