Fachkonzept

Konzept Administration

Version:	1.0
Status:	Veröffentlichte Fassung
Vertraulichkeit:	öffentlich
Stand:	18.11.2014

Inhaltsverzeichnis

Dokumentenlenkung

Dokumenteninformationen

Dokumententyp:	Konzept
Dokumententitel:	Konzept Administration
Version:	1.0
Dateiname:	Konzept_Administration
Dokumenteneigentümer:	LAKD – Landesarchiv Mecklenburg-Vorpommern
Ablageort:	[https://teamportale.mvnet.de/pz/elamv/Projektakte%20eLA/Fachkonzepte/Konzept_Administration.docx]
Status:	Veröffentlichte Fassung
Vertraulichkeitsstufe:	**öffentlich**
Verteiler:	
Es tritt außer Kraft:	[xx/yyyy]
Nächste Prüfung:	am 30.06.2015
Ansprechpartner (opt.):	

Änderungskontrolle (ab Version 0.1)

Version	Datum	Bearbeiter	Status	Änderungsgrund	Seiten
0.1	21.10.2013	M. Marten	In Bearbeitung	Erstellung des Konzeptgerüsts	
0.4	27.03.2014	J. Lehmann, M. Marten, M. Schmitz	In Bearbeitung	Entwurf	
0.5	10.04.2014	J. Lehmann	Zur Review	Entwurf für Reviewgruppe	
0.6	30.04.2014	R. Lorenz, M. Marten, M. Schmitz	Zur Abnahme	Einarbeitung Korrekturen der QS	
1.0	20.06.2014, 07.11.2014	M. Marten	Veröffentlichte Fassung	Einarbeitung Korrekturen der LG, DVZ intern	

Referenzdokumente

Dieser Abschnitt führt alle für die Bearbeitung und das Verständnis des Produktes erforderlichen Dokumente an. Die Dokumente sollten hinsichtlich ihrer Verwendung (intern, extern) unterschieden werden. Über die referenzierten Dokumente sind folgende Informationen zu halten: Bezeichnung, Identifikation mit Versionsangabe und Art der Verwendung (z. B. Quelle, weiterführende Literatur usw.)

Dokument	Version	Ablageort
Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz – DSG M-V)	vom 28. März 2002	http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?showdoccase=1&doc.id=jlr-DSGMVrahmen
Übersicht der BSI-IT-Grundschutz-Standards		http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
Verordnung zur Schaffung barrierefreier Informations-technik nach dem Landesbe-hindertengleichstellungsgesetz (Barrierefreie Informations-technik-Verordnung Mecklenburg-Vorpommern - BITVO M-V)	vom 17. Juli 2007	http://www.regierung-mv.de/cms2/Regierungsportal_prod/Regierungsportal/de/sm/Aufgaben_und_Themen/Soziales/Referat_440__Belange_von_Menschen_mit_Behinderungen,_Soziales_Entschaedigungsrecht,_Geschaeftsstelle_des_Integrationsfoerderrates/Das_Landesbehindertengleichstellungsgesetz_und_seine_Rechtsverordnungen/Die_Barrierefreie_Informationstechnik-Verordnung_%28BITVO_M-V%29

1 EINFÜHRUNG

1.1 Gegenstand des Dokumentes

Das Konzept Administration beschreibt übergreifende Anforderungen an Software- und Hardware-Komponenten und deren Betrieb. Darüber hinaus werden im Konzept die Standards und Policies des eLA M-V dokumentiert.

1.2 Aufbau des Dokumentes

Kapitel 2 beschreibt die Einordnung der Funktionseinheit Administration in der ISO-Norm 14721 und die Ausgangssituation in M-V. Die Anforderungen an Betriebs- und Sicherheitskonzepte, Datensicherungsverfahren und die im eLA umgesetzten grafischen Oberflächen werden in Kapitel 3 dargestellt. Kapitel 4 beschäftigt sich mit den anfallenden administrativen Aufgaben im eLA und regelt die Verantwortlichkeiten. Wie geordnete Störungs-, Problembehandlungs-, Änderungs- und Release-Prozesse umgesetzt werden können, wird in Kapitel 5 beschrieben. Kapitel 0 beschäftigt sich mit der Herstellung der Funktions-, Daten- und Informationssicherheit im eLA, während Kapitel 7 Grundsätze für das eLA definiert.

2 VORAUSSETZUNGEN UND UMFELD

2.1 Funktionseinheit Administration nach ISO-14721

Die Funktionseinheit Administration stellt Dienste und Funktionen für den gesamten Betrieb des Archivsystems bereit. Die Funktionen der Administration beinhalten im Einzelnen: Übergabevereinbarungen mit Produzenten anstoßen und aushandeln; Übergaben auf die Einhaltung der Archivstandards überprüfen und das Konfigurationsmanagement von Hard- und Software aufrecht erhalten. Sie stellt außerdem Systementwicklungs-Funktionen bereit, die sowohl den Archivbetrieb überwachen und verbessern als auch Inventare und Berichte über die Inhalte des Archivs erstellen und diese Inhalte migrieren/aktualisieren. Sie ist ebenfalls zuständig für die Festlegung und Pflege von Standards und Policies des Archivs, für die Unterstützung der Kunden und für die Aktivierung gespeicherter Anfragen.

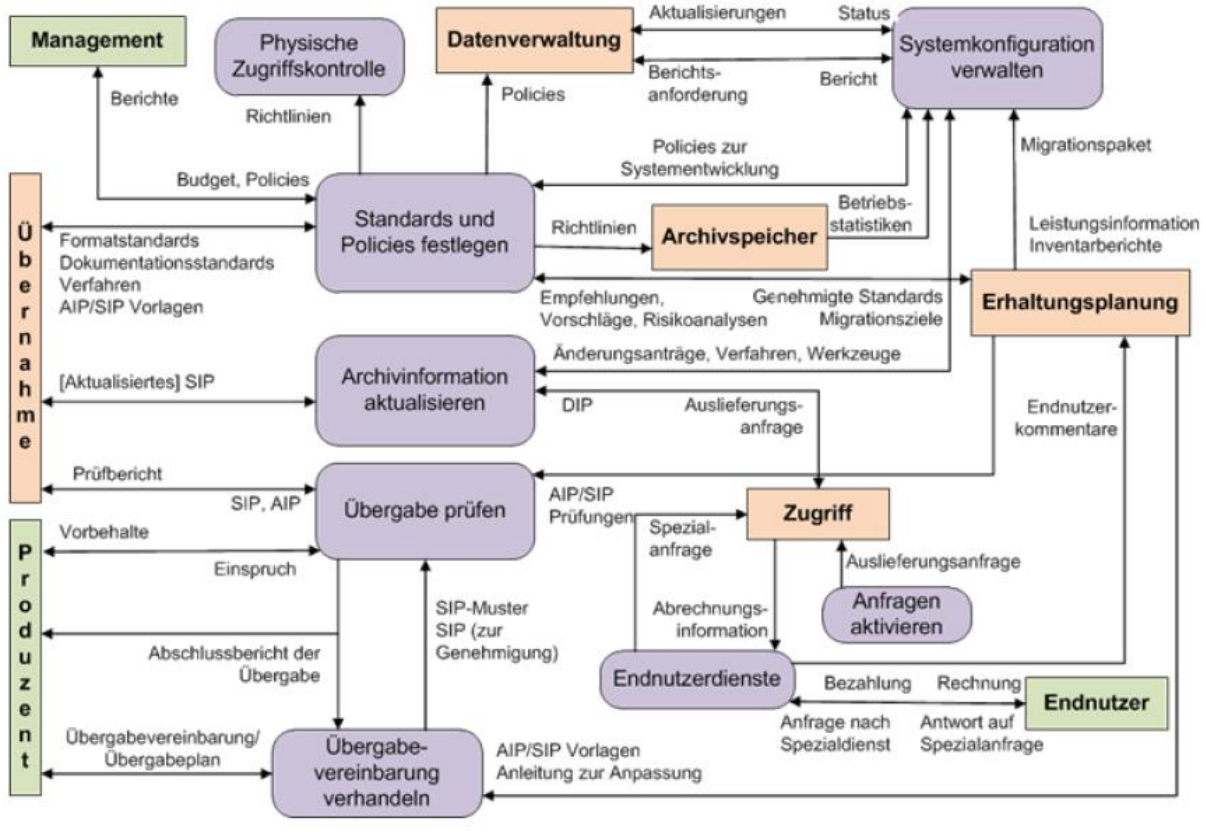

Abbildung 1 Funktionen der Funktionseinheit Administration nach ISO-14721

2.2 Ausgangssituation und Voraussetzungen in M-V

Es existieren keine vergleichbaren technisch-organisatorischen Maßnahmen und Konzepte im LA M-V. Es fließen aber Erfahrungen aus anderen IT-Verfahren der Landesverwaltung M-V

in das vorliegende Konzept ein.

3 ANFORDERUNGEN

3.1 Anforderungen an die Betriebs- und Sicherheitskonzepte

Die Anforderungen an Betriebs- und Sicherheitskonzepte leiten sich aus dem Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz – DSG M-V), den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Best-Practice-Erfahrungen der DVZ M-V GmbH ab. Die Betriebskonzepte sollten alle Informationen für den Betrieb der technischen Systeme des eLA enthalten, so dass in der täglichen Arbeit keine zusätzlichen Dokumente erforderlich sind.

ID	Art	Anforderungsbeschreibung	MSK	Quellen	Kommentar
Req-6.5-001	nfA	In einem Sicherheitskonzept ist für jedes automatisierte Verfahren festzulegen, in welcher Form die Anforderungen des DSG M-V § 21 und des §22, Absätze 1 bis 4 umzusetzen sind. Da es sich beim eLA um ein automatisiertes Verfahren handelt, ist ein Sicherheitskonzept zu erstellen	M	DSG M-V, §22, Abs. 4	
Req-6.5-002	nfA	Das Sicherheitskonzept sollte nach BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, erstellt werden. Folgende Aktivitäten müssen durchgeführt werden: ■ Erstellung einer Strukturanalyse auf Basis eines Netzplans der im Informationsverbund befindlichen Komponenten ■ Erstellung der Schutzbedarfskategorien, soweit diese noch nicht vorhanden sind oder Bereitstellung vorhandener Schutzbedarfskategorien der Landesverwaltung M-V ■ Feststellung des allgemeinen Schutzbedarfs auf Basis der Schutzbedarfskategorien ■ Modellierung der Objekte in einer geeigneten Software (z.B. GSTOOL), Überprüfen der Modellierungsvorgaben des Tools anhand des Schichtenmodells ■ Prüfung der Bausteine (Basis-Sicherheits-Check) des zuvor modellierten Informationsverbundes ■ Dokumentation der Ergebnisse des Basis-Sicherheitschecks ■ ergänzende Sicherheitsanalyse	S	DVZ M-V GmbH	

		■ Erstellung eines Umsetzungskonzeptes			
Req-6.5-003	nfA	Sofern in der Schutzbedarfsfeststellung ein hoher oder sehr hoher Schutzbedarf festgelegt wird, sollte eine Risikoanalyse auf der Basis von IT-Grundschutz nach BSI-Standard 100-3 durchgeführt werden.	S	BSI	
Req-6.5-004	nfA	Für alle technischen Komponenten des eLA sollte zur Gewährleistung der Funktions-, Informations- und Datensicherheit ein Betriebshandbuch erstellt werden. Das Betriebshandbuch sollte folgende Inhalte umfassen: ■ Einleitung □ Kurzbeschreibung des Funktion □ Zielsetzung des Dokumentes und Abgrenzung □ Zielgruppe des Dokumentes ■ Verantwortlichkeiten und Ansprechpartner □ Ansprechpartner - Ansprechpartner beim Kunden - Ansprechpartner für die angeschlossenen Komponenten - Weitere Ansprechpartner □ Verantwortlichkeiten ■ VERTRAGSINFORMATIONEN □ Vereinbarte Service Level Agreements und Messkritieren - Servicezeiten - Reaktionszeiten - Maximale Ausfallzeiten - Nutzung außerhalb der Servicezeit □ Zeittafel der Komponente(n) für Betrieb und Wartung ■ KOMMUNIKATIONSWEGE □ Berichtswege □ Meldewege □ Eskalationswege ■ SYSTEMBESCHREIBUNG	S	DVZ M-V GmbH	

		◻ Funktionsübersicht ◻ Systemarchitektur - Ressourcen • Produktionsumgebung • Referenzumgebung • Testumgebung ◻ Hardware ◻ Software ■ Installation und Konfiguration ◻ Server - Logins - Lokale Firewall - Dienste ◻ Software ◻ Datenbank ◻ Client ◻ Netzwerk ◻ Weitere Komponenten ■ BETRIEB ◻ Fehlerzustände und Behebung ◻ Normales Starten und Stoppen ◻ Wiederanlauf der Komponente ◻ Berechtigungsverwaltung ◻ Datensicherung ◻ Datenrücksicherung ◻ Log-Dateien und Systemüberwachung ■ Systemmanagement-Prozesse ◻ Change Management ◻ Patch Management ◻ Release Management ◻ Incident Management ◻ Config Management ◻ Capacity Management ■ Systemwartung ◻ Wartungszyklen ◻ Wartungsablauf ◻ Externe Wartung ■ Notfallvorsorge ◻ Kenndaten			

		◻ Kontinuitätsstrategie ◻ Herstellung des Notbetriebs - Ressourceneinschränkung im Notbetrieb - Vorbereitungen auf den Notbetrieb ◻ Wiederherstellung Normalbetrieb - Voraussetzungen - Handlungsanweisungen ◻ Tests und Übungen - Geplante Tests und Übungen - Ergebnisse von durchgeführten Tests und Übungen ■ Sicherheitskonzept ◻ Verweis auf das Sicherheitskonzept ◻ Rollenkonzept			

3.2 Anforderungen an das Datensicherungsverfahren

Nachfolgend werden die Anforderungen an die Datensicherung für das elektronische Archivgut dokumentiert. Ein Generationenbackup wird nicht als notwendig erachtet.

ID	Art	Anforderungsbeschreibung	MSK	Quellen	Kommentar
Req-6.5-004	fA	Die Sicherung der Daten muss dateibasiert erfolgen.	M	LA	
Req-6.5-005	nfA	Zur Sicherung der Daten müssen zwei unterschiedliche Verfahren genutzt werden.	M	LA	
Req-6.5-006	nfA	Die Sicherung der Daten muss auf zwei unterschiedlichen Backup-Medien erfolgen.	M	LA	
Req-6.5-007	nfA	Die Daten müssen täglich inkrementell gesichert werden.	M	LA	
Req-6.5-008	nfA	Die Sicherungsverfahren müssen an zwei geographisch getrennten Standorten betrieben werden.	M	LA	

Req-6.5-009	fA	Das Sicherungsverfahren muss fähig sein den Schutzbedarf „hoch“ nach BSI Standard 100-2 für die Vertraulichkeit des elektronischen Archivguts zu gewährleisten.	M	LA, BSI Standard 100-2 S. 51	
Req-6.5-010	fA	Das Sicherungsverfahren muss fähig sein, den Schutzbedarf „hoch“ nach BSI Standard 100-2 für die Integrität des elektronischen Archivguts zu gewährleisten.	M	LA, BSI Standard 100-2 S. 51	
Req-6.5-011	fA	Das Sicherungsverfahren sollte fähig sein, den Schutzbedarf „normal“ nach BSI Standard 100-2 für die Verfügbarkeit des elektronischen Archivguts zu gewährleisten.	S	LA, BSI Standard 100-2 S. 51	
Req-6.5-012	fA	Die Daten müssen wöchentlich vollständig gesichert werden.	M	LA	

3.3 Anforderungen an grafische Oberflächen

Die nachfolgenden Anforderungen sind für alle grafischen Oberflächen im eLA gültig. Sie adressieren primär die Software-Ergonomie, um die Anwender möglichst gut zu unterstützen. Dafür sind überflüssige Arbeiten, wie zum Beispiel die mehrfache Eingabe gleicher Daten, zu vermeiden. Die Nutzerführung ist so zu gestalten, dass Fehler sowie inkonsistente Zustände möglichst nicht auftreten und sich die Handhabung der Software selbsterklärend gestaltet, damit Handbücher in der täglichen Arbeit wenig genutzt werden müssen.

ID	Art	Anforderungsbeschreibung	MSK	Quellen	Kommentar
Req-6.1-001	nfA	DAS SYSTEM MUSS folgenden Teilen der Software-Ergonomie-Normen ISO 9241 genügen: ■ 9241-3 (Anforderungen an visuelle Anzeigen) ■ 9241-8 (Anforderungen an Farbdarstellungen) ■ 9241-10/110 (Grundsätze der Dialoggestaltung) ■ 9241-12 (Ergonomische Anforderungen) ■ 9241-13 (Nutzerführung/Fehlerbehandlung und Hilfefunktionen) ■ 9241-14 (Dialogführung mittels Menüs) ■ 9241-16 (Dialogführung mittels direkter Manipulation) ■ 9241-17/143 (Dialogführung mittels Bildschirmformularen/Formulardialoge)	M	LA	

		■ 9241-20 (Leitlinien für die Zugänglichkeit der Geräte und Dienste in der Informations- und Kommunikationstechnologie) ■ 9241-151 (Leitlinien zur Gestaltung von Benutzungsschnittstellen für das World Wide Web)			

In der folgenden Tabelle werden spezifische Anforderungen für die einzelnen im eLA konzipierten grafischen Oberflächen aufgeführt.

ID	Art	grafische Oberfläche	Anforderungsbeschreibung	MSK	Quellen
Req-6.1-002	nfA	**Steuerung der Übernahme**	DAS SYSTEM MUSS FÄHIG SEIN, einen intuitiven Zugriff auf den Steuerungsprozess zu ermöglichen.	M	LA
Req-6.1-003	fA		DAS SYSTEM MUSS FÄHIG SEIN, den Zugriff auf den Steuerungsprozess von unterschiedlichen Standorten zu ermöglichen.	M	LA
Req-6.1-004	nfA		DAS SYSTEM MUSS FÄHIG SEIN, den Übernahmeprozess effektiv zu unterstützen.	M	LA
Req-6.1-005	nfA	**Archivspeicher-administration**	DAS SYSTEM MUSS FÄHIG SEIN, einen intuitiven Zugriff auf den Steuerungsprozess zu ermöglichen.	M	LA
Req-6.1-006	fA		DAS SYSTEM MUSS FÄHIG SEIN, den Zugriff auf den Steuerungsprozess von unterschiedlichen Standorten zu ermöglichen.	M	LA
Req-6.1-007	nfA		DAS SYSTEM MUSS FÄHIG SEIN, die Administration des Archivspeichers effektiv zu unterstützen.	M	LA
Req-6.1-008	fA	**Bearbeitung des DIPs**	DAS SYSTEM MUSS FÄHIG SEIN, dem Archivar die Möglichkeit zu bieten, Passagen zu schwärzen. Die	M	LA

			Schwärzungen dürfen durch einen externen Nutzer nicht mehr rückgängig gemacht werden.		
Req-6.1-009	fA		DAS SYSTEM MUSS FÄHIG SEIN, Primärdatenobjekte zu konvertieren.	M	LA
Req-6.1-010	fA		DAS SYSTEM MUSS FÄHIG, sein Primärdatenobjekte aus dem DIP zu löschen.	M	LA
Req-6.1-011	nfA	**Steuerung des Zugriffsprozesses**	DAS SYSTEM MUSS FÄHIG SEIN, einen intuitiven Zugriff auf den Steuerungsprozess zu ermöglichen.	M	LA
Req-6.1-012	nfA		DAS SYSTEM MUSS FÄHIG SEIN, den Zugriffsprozess effektiv zu unterstützen.	M	LA
Req-6.1-013	fA	**Steuerung des Nutzerzugriffs**	DAS SYSTEM MUSS FÄHIG SEIN, Inhalte und Informationen gemäß den Anforderungen der Verordnung zur Schaffung barrierefreier Informations-technik nach dem Landes-behindertengleichstellungs-gesetz M-V zugänglich zu machen.	M	BITVO M-V Anlage 1 Priorität I, Priorität II
Req-6.1-014	nfA		DAS SYSTEM SOLLTE zusätzlich zu den o.g. Teilen der Software-Ergonomie-Normen ISO 9241 dem Teil 9241-171 (Leitlinien für die Zugänglichkeit von Software) genügen.	S	LA
Req-6.1-015	fA		DAS SYSTEM MUSS FÄHIG SEIN, elektronisches Archivgut in unterschiedlichen Formaten und Auflösungen zu präsentieren.	M	LA
Req-6.1-016	fA		DAS SYSTEM MUSS FÄHIG SEIN, den Zugriff auf das DIP zu reglementieren.	M	LA

Req-6.1-017	fA		DAS SYSTEM MUSS FÄHIG SEIN, das Kopieren, Löschen oder Drucken des DIPs durch externe Benutzer zu verhindern.	M	LA
Req-6.1-018	fA		DAS SYSTEM MUSS FÄHIG SEIN, Kopier-, Lösch- und Druckrechte personalisiert umzusetzen.	M	LA
Req-6.1-019	fA		DAS SYSTEM MUSS FÄHIG SEIN, den Archivar den Druckschutz für das DIP individuell aufheben zu lassen.	M	LA
Req-6.1-020	nfA		DAS SYSTEM MUSS FÄHIG SEIN, einen intuitiven Zugriff auf den Steuerungsprozess zu ermöglichen	M	LA

4 BESCHREIBUNG DER ADMINISTRATIVEN AUFGABEN

In der folgenden Tabelle werden die anfallenden administrativen Aufgaben benannt und die Verantwortlichkeit für die Aufgabe zugeordnet.

Fachadministrator	**Archivar**	**IT-Administrator**	**Externer Dienstleister**
Datenübergabeplan vereinbaren	Übergabe-vereinbarung verhandeln	Entgegennahme von AIP-/SIP-Vorlagen	Physische Zugriffskontrolle (vgl. Kapitel 6.1)
Zeitplan der Datenübergabesitzungen überwachen	Prüfung der Umsetzung der Übergabe-vereinbarung (Verstehbarkeit in der Zielgruppe, ggf. SIP-Neuanforderung)	Entgegennahme von Anleitungen zur Anpassung	Policies zur Speicher- und Datenbank-verwaltung sowie Sicherheit erstellen
Prüfung Systembetrieb		Angepasste SIP- und AIP-Muster senden	
Prüfung Systemnutzung		Bereitstellung von Systemanalysen	
Berichtsanforderungen stellen		Systemüberwachung (Funktionalitäten)	
Leistungsinformationen und Inventarlisten erstellen		Systematische Ver-änderungen in der Konfiguration kon-trollieren	
Organisatorische Vorbereitung der Migration und Initiierung		Prüfung Systemleistung	
Planung Weiterentwickl-ung des Systems		Planung Weiterent-wicklung des Systems	
Festlegung und Pflege der Standards (Format- und Dokumentationsstandards,		Technische Vorbereitung der Migration	

Verfahren) und Policies (Migrationsstrategie, Notfallplanung, Sicherheit)			
Berichterstattung an die Archivleitung			
Risikoanalysen erstellen			
Prüfung der Umsetzung der Übergabevereinbarung			
Einhaltung der Migrations-ziele prüfen (Benutzbarkeit, Authentizität etc.)			
SIP-Neuanforderung			
Abschließenden Übernahmebericht erstellen			

5 INCIDENT-, PROBLEM-, CHANGE- UND RELEASEMANAGEMENT

Zu einer reibungslosen Bereitstellung des eLA M-V IT-Systems gehört neben dem eigentlichen Betrieb auch die Bearbeitung von Änderungen und Störungen. Notwendige Änderungen oder Anpassungen werden im Prozess Change-Management bearbeitet und dort gesondert beschrieben. Störungen oder weitere Abweichungen vom Normalbetrieb werden im Incident-Management behoben. Wiederkehrend auftretende Incidents werden im Problem-Management behandelt. Das Release-Management koordiniert Änderungen an den IT-Systemen für das eLA, sichert die Dokumentation des Umfanges von Änderungen, insbesondere die Beschreibung der für die Rückwärtskompatibilität relevanten Eigenschaften und verwaltet die Versionshistorie und stellt dadurch Reproduzierbarkeit sicher.

5.1 Incident-Management

Das Ziel des Incident-Mangement ist die schnellstmögliche Wiederherstellung eines Service bei Auftreten einer Störung. Dabei sollen bei der Behebung von Störungen mögliche nachteilige Auswirkungen auf den Betrieb des eLA auf ein Minimum reduziert werden. Die Grundlange hierfür ist in den vereinbarten Service-Level-Agreements (SLA) mit dem IT-Dienstleister verankert.

Das Incident Management umfasst die Behebung von Störungen und die Bearbeitung von Service-Anfragen (Service Requests). Diese definieren sich wie folgt:

- Eine Störung wird definiert als ein Ereignis, das nicht Teil des standardmäßigen Betriebes eines Service ist und das eine Unterbrechung oder eine Minderung seiner Qualität verursacht oder zu verursachen droht.
- Als Service Request werden Anfragen zur Änderung oder Erweiterung des eLA sowie Anfragen nach Informationen, Dokumentationen oder Hilfestellungen bezeichnet. Hierunter fallen z.B. Anfragen zur Anpassung der Infrastruktur, das Rücksetzen eines Passworts oder eine Frage zur Handhabung einer Anwendung.

Im Vordergrund des Incident-Managements steht die Qualität der Service-Wiederherstellung und nicht die Qualität der Lösungsermittlung. Abbildung 2 stellt den allgemeinen Incident-Management-Prozess dar.

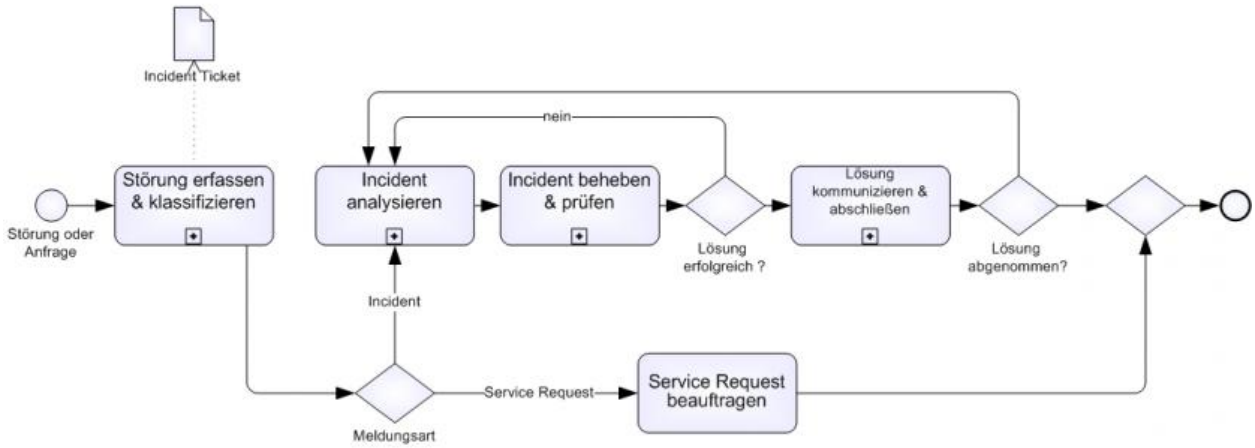

Abbildung 2 Incident-Management-Prozess

5.2 Problem-Management

Das Ziel des Problem-Managements ist die Minimierung negativer Auswirkungen von Incidents und Problemen, die durch Störungen in der IT-Infrastruktur verursacht werden. Um dieses Ziel zu erreichen, versucht das Problem-Management die Ursache von Störungen und Ausfällen zu bestimmen und Maßnahmen zur Verbesserung/Korrektur einzuleiten. Wiederkehrende Ausfälle aufgrund der gleichen Ursache sollen somit vermieden werden. Weiterhin bietet das Problem-Management die Möglichkeit, intensiv nach Lösungen für Incidents zu suchen, welche mittels einer Umgehungslösung gelöst wurden und bei denen eine endgültige Fehlerbeseitigung noch aussteht.

Innerhalb des Problem-Management-Prozesses werden Incidents, die von längerer Dauer sind oder auf einen notwendigen Change warten, bearbeitet und gepflegt. Hierzu wird ein Problem-Ticket mit dem Inhalt des Incident-Tickets erstellt und der Incident mit dem Verweis auf das Problem-Ticket geschlossen. Im Problem-Ticket werden zur Lösung notwendige Analysen und Diagnosen sowie Absprachen und Arbeitsfortschritte dokumentiert. Die Korrektur bzw. Behebung wird durchgeführt und nach erfolgreicher Behebung das Problem-Ticket geschlossen. Der Problem-Management-Prozess ist in Abbildung 3 dargestellt.

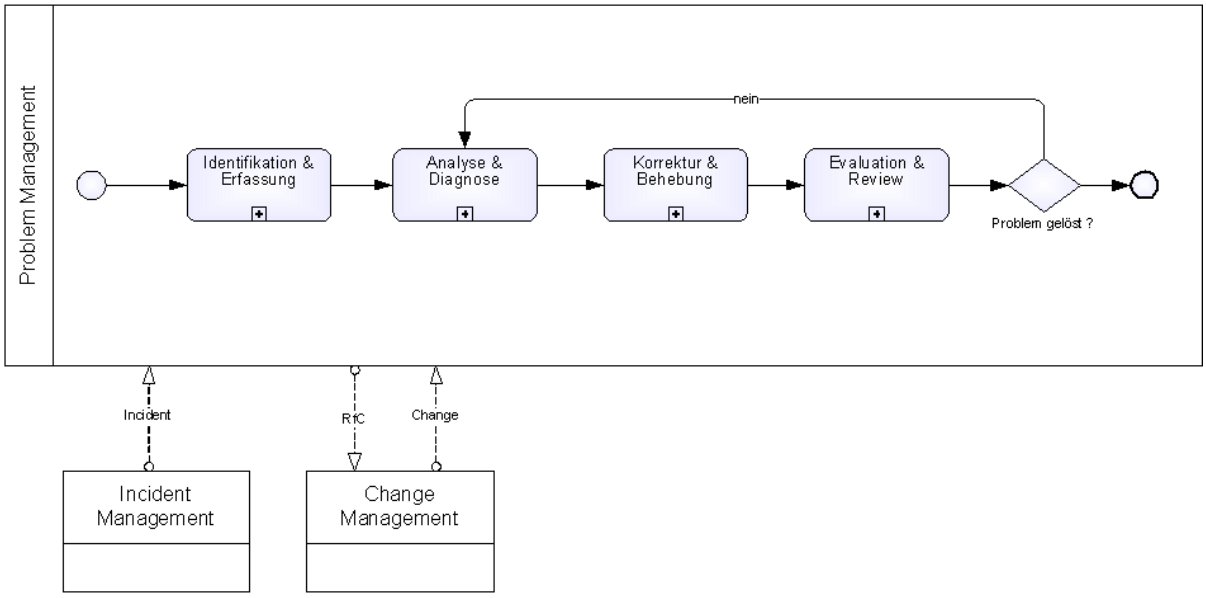

Abbildung 3 Problem-Management-Prozess

5.3 Change-Management

Das Change-Management ist verantwortlich für die Steuerung von Änderungsabläufen im Zusammenhang mit:

- den betroffenen Hardware-Komponenten
- der verwendeten Systemsoftware
- den Komponenten des produktiven Anwendungsprogramms
- allen Dokumentationen und Verfahren, die mit dem Betrieb, der Betreuung und der Wartung von Systemen in der Produktionsumgebung betroffen sind.

Das Change-Management stellt sicher, dass standardisierte Methoden und Verfahren verwendet werden, damit Änderungen termingerecht durchgeführt werden können und sich so wenig wie möglich auf die Bereitstellung des IT-Systems für das eLA im laufenden Betrieb auswirken.

Dadurch ist es möglich:

- negative Auswirkungen auf den Betrieb zu verhindern und eine hohe Verlässlichkeit beim Umgang mit notwendigen Änderungen am IT-System zu gewährleisten,
- mit einer generellen Vorgehensweise unterschiedlichste Änderungen am eLA nach abgestimmten Kriterien sinnvoll zu strukturieren,
- die notwendige Koordination zwischen Archiv und IT-Dienstleister beim Umgang mit Änderungen zu erleichtern,
- eine bessere Übersicht über Änderungen und deren Auswirkungen auf das eLA zu erhalten.

Es werden folgende Change-Typen unterschiedenen:

- Standard Change
  - Der Change muss mindestens einmal erfolgreich als Normal Change gemäß Prozess durchgeführt worden sein, bevor der zentrale Change Manager diesen zum Standard Change freigibt.
  - Der Change ist wiederholbar und endet immer mit dem gleichen Ergebnis.
  - Es sind gleichbleibende Implementierungsschritte beschrieben, die nicht verändert werden dürfen.
  - Der Change hat kein oder ein sehr geringes Risiko.
  - Es besteht keine Abhängigkeit zu anderen Changes.
  - Der Zeitpunkt der Durchführung ist frei wählbar, da keine Abhängigkeiten zu anderen Komponenten bestehen und kein oder ein sehr geringes Risiko vorhanden ist.
  - Für Standard Changes können entsprechend der Priorität gestaffelte SLAs definiert sein.
- Normal Change
  - Ein Normal Change bedarf immer der Genehmigung (zur Durchführung und zur Implementierung) durch den betroffenen lokalen bzw. den zentralen Change Manager.
  - Ab einer hohen Priorität und einem mittleren Risiko ist der Change in Form eines Änderungsantrages im Betriebsgremium abzustimmen.
  - Ein Rollbackverfahren ist definiert, beschrieben und getestet.
- Notfall Change
  - Der Change ist notwendig, um eine akute Störung am eLA zu beheben.
  - Der Change ist notwendig, um eine unmittelbar drohende Störung an eLA abzuwenden.
  - Der Change ist notwendig, um eine akute oder unmittelbar drohende Sicherheitslücke an einem oder mehreren IT-Systemen des eLA zu beseitigen, welche die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Daten im eLA in hohem Maße bedrohen.
  - Ein Notfall Change kann im Nachhinein dokumentiert werden. Die Freigaben können persönlich eingeholt werden.

Abbildung 4 stellt den Change-Management-Prozess dar.

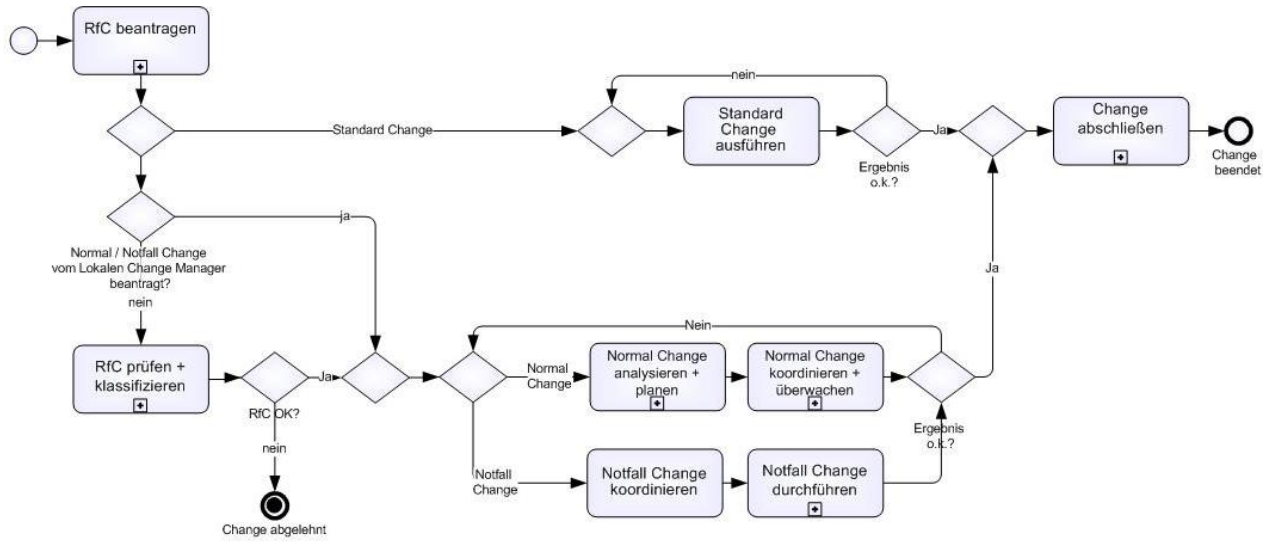

Abbildung 4 Change-Management-Prozess

5.4 Release-Management

Das Release-Management hat das Ziel, einen oder mehrere Changes in einem Release in die produktive Umgebung auszuliefern, zu verteilen und zu verfolgen. Eine wesentliche Aufgabe dabei ist die Koordination aller beteiligten Ressourcen, um ein Release in eine verteilte Umgebung zu übergeben. Eine gute Planung ist Grundvoraussetzung für eine erfolgreiche Verteilung sowie die Minimierung der zugehörigen Auswirkungen und Risiken auf das eLA.

Alle Release-Elemente müssen zurückverfolgbar und sicher gegen Veränderungen sein, um so Nachvollziehbarkeit zu gewährleisten. Nur geprüfte und freigegebene Releases dürfen in der Produktionsumgebung akzeptiert werden.

Die Aufgaben des Release-Managements sind also die Festlegung des funktionellen Umfangs sowie des genauen Zeitplans einer Release-Freigabe in Abstimmung mit dem Change- bzw. Produkt-Management. Weiterhin sichert es die Dokumentation des Umfanges von Änderungen, insbesondere die Beschreibung der für die Rückwärtskompatibilität relevanten Eigenschaften und verwaltet die Versionshistorie und stellt dadurch Reproduzierbarkeit sicher.

Der Release-Management-Prozess sollte in die Change-Management-Prozesse integriert werden, um sicher zu stellen, dass Releases und ausgeführte Changes aufeinander abgestimmt sind. Beim Release-Management erfolgt die Koordination der Aktivitäten des IT-Dienstleisters und der Lieferanten von Bestandteilen des eLA-Systems. Das Ergebnis ist eine Planung zur Bereitstellung eines Releases in die produktive IT-Umgebung.

Die folgende Darstellung bietet als Einstieg einen Gesamtüberblick über die notwendigen Aktivitäten.

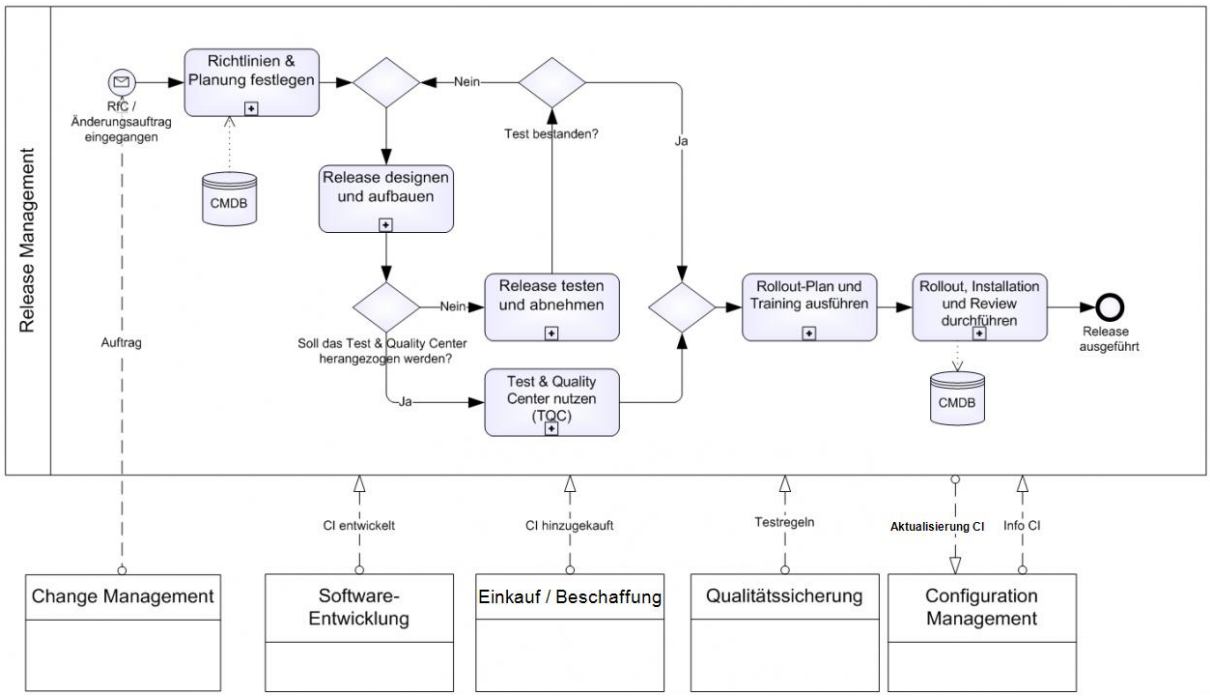

Abbildung 5 Release-Management

Ergänzende Erläuterung zur Abbildung 5:

- Configuration Item (CI): Konfigurationselemente, z.B. Hard- und Softwarekomponenten, Dokumentation, Verfahrensanweisungen, die für die Erbringung eines IT-Services überwacht und gesteuert werden müssen.
- Configuration Management Database (CMDB): System, welches alle Informationen zu einem Configuration Item sowie den Beziehungen und Abhängigkeiten zwischen den Configuration Items speichert und verwaltet.

6 SICHERHEITSMANAGEMENT

6.1 Funktionssicherheit, Informationssicherheit und Datenschutz

6.1.1 Rechtliche Regelungen

Das Landesarchivgesetz M-V ist die maßgebliche rechtliche Regelung für die Errichtung, den Betrieb und die Nutzung des elektronischen Landesarchivs M-V (weitere Regelungen sind dem Betrieborganisationskonzept Kap. 6.1 zu entnehmen). Es verbindet datenschutzrechtliche Interessen (Schutz des Persönlichkeitsrechts) mit dem im Grundgesetz verankerten Recht der Informations- und Wissenschaftsfreiheit. Dem Nutzer ermöglicht es ungehinderten Zugang zu archivierten Informationen, Betroffene bewahrt es mittels Schutzfristen vor dem unbefugten Zugriff auf persönliche Daten.

6.1.2 Organisatorische Regelungen

Mit dem im Betriebsorganisationskonzept beschriebenen Rechte- und Rollenkonzept (Kap. 6.3) wird der Zugriff (lesen, schreiben, löschen) auf das System und folglich auf das Archivgut geregelt. Analoge Unterlagen, die im Regelbetrieb nur durch den zuständigen Bestandsreferenten (Verschlusssachen) eingesehen und bearbeitet werden können, werden auch elektronisch zunächst nur der verantwortlichen Person zugänglich sein. Der Nutzer kann lediglich auf den Nutzungsspeicher zugreifen.

6.1.3 Technische Regelungen

Ein Zugriff des Nutzers auf den Archivspeicher wird nicht nur organisatorisch (Rechte- und Rollenkonzept), sondern auch technisch verhindert. Der Nutzungsspeicher wird als eigenständiges Speichermedium eingesetzt. Hier werden die DIPs für die anschließende Nutzung aufbewahrt. Die Erzeugung des AIPs und des DIPs erfolgt innerhalb eines vom Nutzungsspeicher getrennten Zwischenspeichers, die Ablage im separaten Archivspeicher.

7 STANDARDS UND POLICIES FÜR DAS ELA M-V

7.1 Zusammenfassung Grundsätze und Richtlinien

- Die Speicherung der ausgesonderten Unterlagen hat vollständig zu erfolgen. Kein digitales Archivale darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Inhaltsinformationen des digitalen Archivale müssen mit Integritätsnachweis gespeichert werden.
- Erhaltungsmetadaten des digitalen Archivale werden fortgeschrieben, dürfen aber nicht nicht undokumentiert verändert werden.
- Jedes Archivale darf nur von entsprechend berechtigten Benutzern eingesehen werden.
- Jedes Archivale muss in angemessener Zeit wiedergefunden und reproduziert werden können.
- Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden.
- Das gesamte organisatorische und technische Verfahren der Archivierung kann von einem sachverständigen Dritten jederzeit geprüft werden.
- Bei allen Migrationen und Änderungen am Archivspeicher muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein.
- Für das eLA M-V gelten folgende Standards und Normen in ihrer aktuellen Version: ISO 14721, DIN 31644, DIN 31645, DIN 31646, DIN 31647.

7.2 Grundaufbau AIP

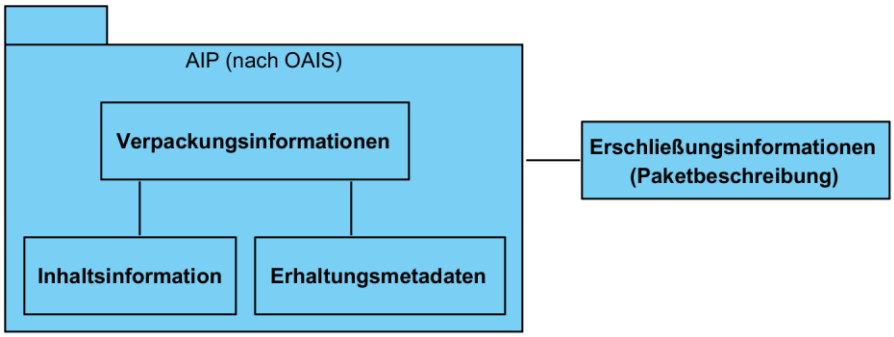

Abbildung 6 Grundaufbau des AIP

Das AIP ist gemäß OAIS selbst Informationsobjekt und zugleich Container für andere Informationsobjekte, und zwar Inhaltsinformation und dazu gehörende Erhaltungsmetadaten sowie Verpackungsinformationen. Die einzelnen Bestandteile des AIPs werden im hiesigen Fall als zusammengehörig gedacht und durch die Verpackungsinformation logisch in Beziehung gesetzt.

Abbildungsverzeichnis