MITTEILUNGSBLATT
DER
KARL-FRANZENS-UNIVERSITÄT GRAZ

72. SONDERNUMMER

Studienjahr 2017/18 | Ausgegeben am 19. 09. 2018 | 49.a Stück

Richtlinie
für das interne Kontrollsystem

Betrieb des an der Universität Graz eingesetzten SAP-Systems

Beschluss des Rektorats vom 13.09.2018

Impressum: Medieninhaber, Herausgeber und Hersteller: Karl-Franzens-Universität Graz, Universitätsplatz 3, 8010 Graz. Verlags- und Herstellungsort: Graz.
Anschrift der Redaktion: Rechts- und Organisationsabteilung, Universitätsplatz 3, 8010 Graz.
E-Mail: mitteilungsblatt@uni-graz.at
Internet: https://online.uni-graz.at/kfu_online/wbMitteilungsblaetter.list?pOrg=1

Offenlegung gem. § 25 MedienG
Medieninhaber: Karl-Franzens-Universität Graz, Universitätsplatz 3, 8010 Graz. Unternehmensgegenstand: Erfüllung der Ziele, leitenden Grundsätze und Aufgaben gem. §§ 1, 2 und 3 des Bundesgesetzes über die Organisation der Universitäten und ihre Studien (Universitätsgesetz 2002 - UG), BGBl. I Nr. 120/2002, in der jeweils geltenden Fassung.
Art und Höhe der Beteiligung: Eigentum 100%.
Grundlegende Richtung: Kundmachung von Informationen gem. § 20 Abs. 6 UG in der jeweils geltenden Fassung.

Richtlinie für das interne Kontrollsystem

Betrieb des an der Universität Graz eingesetzten SAP-Systems

Version 1.0	**Erstellung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer
		Mag. Manfred Ortner
	Prüfung der Richtlinie	Mag. Christa Peissl
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 2.0	**Überarbeitung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	Interne Revision
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 3.0	**Überarbeitung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	Interne Revision
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 4.0	**Überarbeitung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	Interne Revision
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 4.0, 19.09.2018

Änderungsverzeichnis

Version	Datum	Änderung	erstellt von
0.1	15.09.2005	Erstellung der IKS-Richtlinie	Mag. Andreas Doppler, Mag. Sandra Hungerländer, Mag. Manfred Ortner
0.2	13.10.2005	Endredaktion der IKS-Richtlinie	Mag. Andreas Doppler, Mag. Sandra Hungerländer, Mag. Manfred Ortner
1.0	24.10.2005	Erstellung der Endfassung der IKS-Richtlinie zur Veröffentlichung	Mag. Andreas Doppler, Mag. Sandra Hungerländer, Mag. Manfred Ortner
2.0	05.05.2011	Einarbeitung der Prüfungsergebnisse der SAP-Revision	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner
3.0	29.08.2014	Aktualisierung auf Grund der Umstellung auf den direkten SAP Einstieg und Einführung von ESS – Employee Selfservice	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner
4.0	19.09.2018	Aktualisierung auf Grund der SSO-Anmeldung für ESS-BenutzerInnen	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ACOnet	Austrian Academic Computer Network
BRZ	Bundesrechenzentrum
BuBi	Abteilung für Buchhaltung und Bilanzierung
BW	Business Warehouse
CCC	Customer Competence Center
CO	Controlling
CoRe	Abteilung für Controlling und Ressourcenplanung
ERP-System	Enterprise Resource Planning System
ESS	Employee Selfservice
FI	Finanzwesen (Finance)
FI-AA	Finanzwesen-Anlagenbuchhaltung (Finance Asset Accounting)
HR	Personalwesen (Human Resources)
ICR	Interner Change Request
IKS	Internes Kontrollsystem
LDAP	Lightweight Directory Access Protocol
MM	Materialmanagement
MSS	Management Selfservice
PeCo	Abteilung für Personalcontrolling
PIN	Persönliche Identifikationsnummer
PU1	Produktivsystem
QU1	Qualitätssicherungssystem
SAML	Security Assertion Markup Language
SAP	Systems, Applications, Products in Data Processing
SD	Verkauf (Sales and Distribution)
SLA	Service Level Agreement
SLF-System	Support Line Feedback System
SSO	Single Sign On
TU1	Entwicklungssystem
Uni-IT	Uni-IT (Informationsmanagement)
VM	Vertragsmanagement (Contract Management)
VPN	Virtual Private Network

Definitionen

Applikationsverantwortliche/r	Trägt die Verantwortung für die Entwicklungsarbeiten sowie die Konzeption und Realisierung des Weiterausbaus von SAP
BenutzerInnen- und Berechtigungsverwaltung	Ist für die gesamte Administration der SAP-Zugänge sowie für die AnwenderInnenbetreuung zuständig
Berichtsuserlizenz	Bezeichnung des Lizenztyps, mit dem definierte Berichte aus den Modulen CO und FI-AA aufgerufen werden dürfen
BetriebskoordinatorInnen	Sind für die Organisation und Sicherstellung des SAP-Betriebs verantwortlich
CCC-MitarbeiterIn	MitarbeiterInnen des BRZ, die die SLF-Meldungen der Universität annehmen und bearbeiten
CO-Kontierung	Kostenstellen und Innenaufträge
Customizing	Anpassung der Standardsoftware auf die Geschäftsprozesse des Kunden/der Kundin
Data Dictionary	Ermöglicht eine zentrale Beschreibung und Verwaltung aller im System verwendeten Daten
DateneigentümerInnen	Personen, die für bestimmte CO-Kontierungen gem. Unterschriftenprobeblatt anweisungsberechtigt sind
Debug-Modus	Ermöglicht eine Ablaufverfolgung des zu untersuchenden Programmes in einzelnen Schritten oder zwischen definierten Haltepunkten
e-Banking	Zahlungsverkehr und Bankgeschäfte werden beleglos in elektronischer Form abgewickelt
ESS-BenutzerInnen	Bezeichnung der BenutzerInnen, welche das SAP ESS - Employee Selfservice oder die Genehmigungsworkflows in SAP nutzen. ESS-BenutzerInnen werden in folgende Lizenztypen untergliedert: ESS User MSS User
ESS User Lizenz	Bezeichnung des Lizenztyps, mit dem benutzerspezifische Szenarien im ESS - Employee Selfservice aufgerufen werden dürfen
First Level Support	Erste Auskunftsstelle für die SAP-BenutzerIn bei Problemen
ITS (Internet Transaction Server)	Wandelt die Daten in eine Form um, die in Webbrowsern angezeigt werden können
Limited Professional User Lizenz	Bezeichnung des Lizenztyps, mit dem alle Transaktionen eines Modules ausgeführt werden dürfen

MM/SD Light User Lizenz	Bezeichnung des Lizenztyps, mit dem definierte Transaktionen in den Modulen MM und SD oder im Vertragsmanagement ausgeführt werden dürfen
MSS User Lizenz	Bezeichnung des Lizenztyps, mit dem benutzerspezifische Szenarien im MSS – Manager Self-service aufgerufen werden dürfen
PIN	Kennwort, das bei der Neuanlage eines/einer BenutzerIn bzw. beim Zurücksetzen eines gesperrten Kennwortes vergeben wird und das bei der erstmaligen Anmeldung im System geändert werden muss
Professional User Lizenz	Bezeichnung des Lizenztyps, mit dem alle Transaktionen aller Module ausgeführt werden dürfen
SAP Account	SAP-Zugang
SAP-BenutzerInnen	Bezeichnung der BenutzerInnen, welche im SAP-System operative Transaktionen ausführen. SAP-BenutzerInnen werden in folgende Lizenztypen untergliedert: Professional User Limited Professional User MM/SD-Light User Berichtsuser
SAP GUI	Benutzeroberfläche (Graphical User Interface), welche die Schnittstelle zwischen BenutzerInnen und dem SAP-System bildet
SAP Server	Hardware, auf der das SAP-System installiert ist
Secure Sockets Layer SSL	Secure Sockets Layer (SSL) ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet
Security Policy der Uni-IT	Regelwerk der Uni-IT, mit dem die IT-Sicherheit an der Universität gewährleistet werden soll
SLA-Report	Vom BRZ monatlich erstellter Report, in dem die Kriterien des Service Level Agreements und die durchgeführten Transporte aufgelistet sind
SLF-System	Ein Tool, mit dem alle Supportmeldungen der Key UserInnen des BRZs abgewickelt und dokumentiert werden
Support MitarbeiterIn des BRZ	Siehe CCC-MitarbeiterIn
VPN	VPN steht für "Virtual Private Network" oder "virtuelles privates Netzwerk" und bietet eine sichere und verschlüsselte Verbindung über ein öffentliches Netz

Inhaltsverzeichnis

1 Ziele und Zielgruppe, Zeitpunkt des In-Kraft-Tretens

Die vorliegende Richtlinie für das Interne Kontrollsystem (IKS) enthält die Regelungen, die einen

- sicheren,
- ordnungsmäßigen und
- wirtschaftlichen

Betrieb des an der Universität Graz eingesetzten SAP-Systems gewährleisten.

Die Richtlinie gilt für alle Personen, für deren Tätigkeit ein Zugriff auf das SAP- und/oder ESS-System erforderlich ist.

Die Richtlinie trat am 7. November 2005 in Kraft und galt bis zur Veröffentlichung der Version 2.0.

Die Version 2.0 trat am 25.05.2011 mit der Veröffentlichung im Mitteilungsblatt in Kraft und galt bis zur Veröffentlichung der Version 3.0.

Die Version 3.0 trat am 24.09.2014 mit der Veröffentlichung im Mitteilungsblatt in Kraft und galt bis zur Veröffentlichung der Version 4.0.

Die Version 4.0 tritt mit der Veröffentlichung im Mitteilungsblatt in Kraft und gilt bis auf Widerruf.

2 Produktivsystem (PU1)

2.1 IKS-Bereich: Sicherheit

Im IKS-Bereich Sicherheit können insbesondere folgende Risiken auftreten:

- **Zugriff auf SAP-Daten durch unberechtigte Personen**
  Der unberechtigte Zugriff auf SAP-Daten kann sowohl durch MitarbeiterInnen der Universität als auch durch externe Personen erfolgen. Ursachen für den unberechtigten Zugriff auf SAP-Daten sind zu weit gefasste Berechtigungen eines/r SAP-BenutzerIn oder Angriffe auf das Netzwerk und einzelne PCs. Mögliche Gefahrenquellen befinden sich daher innerhalb und außerhalb der Universität.

- **Datenschutzverletzungen**
  Da im SAP-System personenbezogene Daten verarbeitet werden, besteht die Gefahr von Datenschutzverletzungen.

Die im IKS-Bereich Sicherheit definierten Regelungen zur

- Netzwerksicherheit,
- Anmeldesicherheit und
- Berechtigungsverwaltung

sollen diesen Risiken entgegenwirken.

2.1.1 Netzwerksicherheit

Die Regelungen zur Netzwerksicherheit legen die Abläufe hinsichtlich

- Kommunikation zwischen Arbeitsplatzrechner und SAP-Server sowie die
- Einhaltung der Security Policy für Computer und Netze

fest.

2.1.1.1 Kommunikation zwischen Arbeitsplatzrechner und SAP-Server

Die Kommunikation zwischen den Arbeitsplatzrechnern an der Universität Graz und den SAP-Servern im BRZ erfolgt über das ACOnet. Die Verbindung zwischen Arbeitsplatzrechner und VPN-Appliances und im ACOnet muss verschlüsselt erfolgen. Die Verschlüsselung im ACOnet wird hierzu über eine Lan-To-Lan-Verbindung hergestellt. Dazu stellt das BRZ zwei Lan-To-Lan-Router für die Kommunikation zwischen der Universität Graz und dem BRZ zur Verfügung. Die Verschlüsselung von den SAP-Clients in die Rechenzentren der Universität erfolgt über Cisco SSL VPN Clients zu redundanten VPN Appliances der Universität.

Die Herstellung einer gesicherten Verbindung über Lan-To-Lan bis inkl. der Lan-To-Lan Router an der Universität ist Aufgabe des Bundesrechenzentrums.[1] Für den Teil nach den Lan-To-Lan Routern bis zu den Clients ist die Uni-IT zuständig. Aufgabe des SAP-Betriebskoordinatorenteams an der Universität ist es, einmal wöchentlich das Vorhandensein der gesicherten Verbindung zu überprüfen. Die Überprüfung erfolgt, indem versucht wird, sich ohne gesicherte Verbindung am System anzumelden.

Der sichere Zugang zum ITS und NetWeaver Business Client erfolgt über Secure Sockets Layer (SSL).

2.1.1.2 Einhaltung der Security Policy der Uni-IT

Um den Zugriff auf SAP-Daten durch unberechtigte Personen zu verhindern, ist die Security Policy der Uni-IT einzuhalten. Die Security Policy der Uni-IT ist unter https://online.uni-graz.at/kfu_online/wbMitteilungsblaetter.display?pNr=75196 einsehbar. Für den Inhalt und die Umsetzung der Security Policy sind die dafür zuständigen MitarbeiterInnen der Uni-IT verantwortlich.

2.1.2 Anmeldesicherheit[2]

Die Regelungen zur Anmeldesicherheit legen die Abläufe hinsichtlich

- Anlage der SAP-BenutzerInnenstammdaten,
- Anlage der ESS-BenutzerInnenstammdaten,
- Kennwortregelung für SAP-BenutzerInnen,
- Kennwortregelung für ESS-BenutzerInnen,
- Sperren, Freischalten und Löschen von SAP-Zugängen,
- Sperren, Freischalten und Löschen von ESS-Zugängen,
- SAP-Zugänge für MitarbeiterInnen des BRZ,
- SAP-Zugänge für MitarbeiterInnen von Beratungsfirmen und sonstigen externen Stellen

fest.

Im Bereich Anmeldesicherheit wird zwischen SAP- und ESS-BenutzerInnen unterschieden, da sich die Prozesse zum Anlegen, Sperren und Löschen bei diesen beiden BenutzerInnengruppen unterscheiden.
SAP-BenutzerInnen sind jene BenutzerInnen, welche im SAP-System operative Transaktionen ausführen.
ESS-BenutzerInnen hingegen nutzen in SAP die Employee Selfservices, Manager Selfservices und die Genehmigungsworkflows. Das heißt, diese BenutzerInnen sind mit keinen individuellen Berechtigungsrollen ausgestattet.

---

[1] vgl. Anhang, Kapitel 5.3, Seite 40: Auszug aus Angebot „VPN-Anbindung“

[2] vgl. Anhang Kapitel 5.2.2.1, Seite 32: Prozess IKS1 – Neue/r SAP-UserIn
vgl. Anhang Kapitel 5.2.2.2, Seite 33: Prozess IKS2 – Neue/r ESS-UserIn
vgl. Anhang Kapitel 5.2.2.3, Seite 34: Prozess IKS3 – Passwort zurücksetzen
vgl. Anhang Kapitel 5.2.2.4, Seite 35: Prozess IKS4 – Sperren, Freischalten und Löschen eines SAP-Zugangs

2.1.2.1 Anlage der SAP-BenutzerInnenstammdaten

Die Vergabe von SAP-Accounts erfolgt ausschließlich auf Basis des Antragsprozesses.
Für Berichts- und InstitutsuserInnen ist der Antrag durch eine/einen DateneigentümerIn zu genehmigen, auf deren/dessen Daten durch die einzurichtenden Berechtigungen der Zugriff ermöglicht wird. DateneigentümerInnen sind Anweisungsberechtigte lt. Unterschriftenprobenblatt.
Der Antrag für Professional und Limited-Professional UserInnen ist durch den/die fachlich Vorgesetzten des/der AntragstellerIn sowie durch die DateneigentümerInnen zu genehmigen.

Die Genehmigung des/der DateneigentümerIn ist notwendig, um den Datenschutz zu gewährleisten.

Von der Genehmigungspflicht durch die DateneigentümerInnen ausgenommen sind Limited-Professional und Professional UserInnen der BuBi, der CoRe, der PeCo, der Wirtschaftsabteilung, des Personalressorts, der Abteilung für Gebäude und Technik, der Uni-IT (Abt. f. Business Applications), der Internen Revision, des Forschungsmanagement und -service sowie das Competence Center SAP, da diese Personen ändernden oder anzeigenden Zugriff auf alle Kostenstellen und Innenaufträge der Universität im Rahmen der ihnen zugeordneten Rollen benötigen.

Der/die AntragstellerIn muss ein bestehendes Dienstverhältnis zur Universität Graz haben.

Alle Anträge auf einen SAP-Zugang sind von der BenutzerInnen- und Berechtigungsverwaltung hinsichtlich Vollständigkeit und Freigaben zu prüfen. Anträge, die eine SAP-Professional bzw. Limited Professional User Lizenz erfordern, sind zusätzlich vom Betriebskoordinatorenteam in Hinblick auf die Vereinbarkeit mit den in dieser Richtlinie genannten Regelungen und das Auftreten von kritischen Berechtigungen zu prüfen. Erst nach Freigabe des Antrags durch den/die Applikationsverantwortliche/n darf der SAP-Zugang im System angelegt werden.

Bevor der/dem neu angelegten UserIn die Zugangsdaten übermittelt werden, ist im Sinne des 4-Augen-Prinzips von einer/einem weiteren MitarbeiterIn der BenutzerInnen- und Berechtigungsverwaltung zu prüfen, ob die beantragten Berechtigungen im SAP-System richtig vergeben wurden und die Richtigkeit ist zu bestätigen.

2.1.2.2 Anlage der ESS-BenutzerInnenstammdaten

Ab dem Zeitpunkt, an welchem

- ein neuer Personalstammsatz im HR angelegt wurde
- die Emailadresse im IT 0105 (Subtyp 0010) gepflegt wurde
- das Beginndatum des Dienstverhältnisses <= Tagesdatum ist
- das Endedatum des Dienstverhältnisses > Tagesdatum ist
- das Dienstverhältnis nicht in einer Z-Tabelle (Mitarbeitergruppe, Mitarbeiterkreis, Anstellungsverhältnis) als Ausnahme definiert ist und
- der Abrechnungskreis ungleich 99 ist

wird ein ESS-Zugang für die/den MitarbeiterIn angelegt.

2.1.2.3 Kennwortregelung für SAP-BenutzerInnen

Wenn ein(e) BenutzerIn in SAP Tätigkeiten ausführen soll, die über das ESS und MSS hinausgehen, wird der ESS-Zugang in einen SAP-Zugang umgewandelt.
Für jede/n neue/n SAP-BenutzerIn muss ein eigener PIN generiert werden. Ansonsten besteht die Gefahr, dass mit einem allgemein bekannten PIN Anmeldungen unter dem neu angelegten Benutzernamen von nicht berechtigten Personen vorgenommen werden.

Verfahren zur Vergabe des PINs
Der PIN ist immer achtstellig und besteht aus einer Buchstaben-Zahlenkombination. Wird ein/e neue/r SAP-BenutzerIn angelegt, wird von der BenutzerInnen- und Berechtigungsverwaltung der PIN generiert. Dieser wird in einer SAP-Datenbanktabelle mit dem SAP-Benutzernamen verschlüsselt gespeichert. Die Speicherung des PIN ist notwendig, weil beim Freischalten eines gesperrten Kennwortes per Telefon der PIN die eindeutige Identifikation des/der SAP-BenutzerIn sicherstellt.
Die BenutzerInnen erhalten den PIN per E-Mail mitgeteilt. Der PIN muss von den BenutzerInnen bei der erstmaligen Anmeldung geändert werden.

BenutzerInnenkennwort
Das von der/dem BenutzerIn verwendete Kennwort muss aus mind. 8 Zeichen bestehen, wobei mind. 2 Buchstaben und mind. 2 Ziffern vorkommen müssen. Vom System wird nach 120 Tagen eine Kennwortänderung verlangt.

2.1.2.4 Kennwortregelung für ESS-BenutzerInnen

ESS-BenutzerInnen melden sich im System über Single Sign On mittels SAML mit den LDAP-Zugangsdaten dh mit ihrem Uni-Graz-Account an. Somit gelten für ESS-BenutzerInnen die Kennwortregelungen (Mindestanforderungen, Kennwortänderung, usw.) welche für die SSO-Systeme der Uni-IT gelten.

2.1.2.5 Sperren, Freischalten und Löschen von Zugängen der SAP-BenutzerInnen

Falscheingabe des Kennworts
Der SAP-Zugang wird durch das System automatisch gesperrt, wenn bei der Anmeldung von der/dem BenutzerIn das Passwort dreimal falsch eingegeben wurde.

In diesem Fall ist von der/dem gesperrten UserIn Kontakt mit der BenutzerInnen- und Berechtigungsverwaltung aufzunehmen, die das Passwort entsperrt, wenn der/die UserIn die ersten vier Zeichen des ursprünglich vergebenen PINs bekannt gibt (schriftlich oder telefonisch).

Sind auch die ersten vier Zeichen des PINs nicht mehr bekannt, kann das Kennwort nur nach einem schriftlichen Antrag des/der BenutzerIn an die BenutzerInnen- und Berechtigungsverwaltung entsperrt werden.

Kennwort ist der/dem UserIn nicht mehr bekannt
Von der/dem UserIn ist Kontakt mit der BenutzerInnen- und Berechtigungsverwaltung aufzunehmen, die das Passwort zurücksetzt, wenn der/die UserIn sich an das Kennwort nicht mehr erinnern kann. Dabei sind die ersten vier Zeichen des ursprünglich vergebenen PINs bekannt zu geben (schriftlich oder telefonisch). Sind auch die ersten

vier Zeichen des PINs nicht mehr bekannt, kann das Kennwort nur nach einem schriftlichen Antrag des/der BenutzerIn an die BenutzerInnen- und Berechtigungsverwaltung entsperrt werden.

Beendigung des Dienstverhältnisses, organisatorische Änderungen
Bei der Beendigung des Dienstverhältnisses darf auch der SAP-Zugang des/der jeweiligen MitarbeiterIn nicht mehr möglich sein. Ändert sich der Aufgabenbereich des/der SAP-BenutzerIn derart, dass kein SAP-Zugang mehr benötigt wird, ist der SAP-Zugang zu löschen. Daher ist in diesen Fällen die SAP-BenutzerInnen- und Berechtigungsverwaltung von der/dem jeweiligen Vorgesetzten mittels Formular zu verständigen.

Von der BenutzerInnen- und Berechtigungsverwaltung muss monatlich geprüft werden, ob ein SAP-Zugang an eine Person vergeben ist, deren Beschäftigungsverhältnis geendet hat, oder deren organisatorische Zuordnung sich geändert hat.
Bei der Änderung der organisatorischen Zuordnung ist mit dem/der bisherigen Vorgesetzten abzuklären, was mit dem SAP-Zugang geschehen soll, falls noch kein Formular bei der BenutzerInnen- und Berechtigungsverwaltung eingelangt ist.

Für die beiden oben angeführten Prüfungen werden jeweils eigenentwickelte SAP-Reports eingesetzt.

Keine Anmeldung in SAP über einen längeren Zeitraum hinweg
Von der BenutzerInnen- und Berechtigungsverwaltung ist monatlich zu prüfen, ob SAP-BenutzerInnen seit 60 Tagen nicht mehr angemeldet waren. Diese BenutzerInnen sind darauf hin zu sperren. Es ist dann zu klären, ob diese SAP-BenutzerInnen im System gelöscht werden sollen. BenutzerInnen, deren letzte Anmeldung 6 Monate zurückliegt, sind zu löschen. Der/die gelöschte SAP-BenutzerIn erhält eine Verständigung per Email, das sein/ihr Zugang gelöscht wurde und dass er/sie einen Antrag auf Neuanlage eines SAP-Zugangs stellen muss, falls er/sie den Zugang wieder benötigt.

2.1.2.6 Sperren, Freischalten und Löschen von Zugängen der ESS-BenutzerInnen

Da die ESS-BenutzerInnen das LDAP-Kennwort zur Anmeldung in ESS verwenden, gelten für das Sperren und Freischalten der LDAP-Kennwörter die entsprechenden Regelungen der Uni-IT[3].

Wenn ein Dienstverhältnis endet, ist eine Anmeldung über Single Sign On nicht mehr möglich. Ein Dienstverhältnis gilt als beendet, wenn das Endedatum des Dienstverhältnisses < Tagesdatum ist.

Die Zugänge werden regelmäßig nach Ablauf eines definierten Zeitfensters gelöscht.

[3] siehe https://intranet.uni-graz.at/einheiten/715/services/Pages/SEC_benutzungsordnung.aspx

2.1.2.7 SAP-Zugänge für MitarbeiterInnen des BRZ

Die SAP-Zugänge von Support-MitarbeiterInnen des BRZ werden vom BRZ verwaltet. Die Richtlinien für die Vergabe und den Umfang der Berechtigungen von Support-MitarbeiterInnen müssen in einem Sicherheitskonzept des BRZ enthalten sein.[4]

Die BenutzerInnen- und Berechtigungsverwaltung der Universität muss vom BRZ benachrichtigt werden, wenn wesentliche Veränderungen an den Berechtigungen von Support-MitarbeiterInnen des BRZ vorgenommen werden.
Die BetriebskoodinatorInnen prüfen monatlich die Einhaltung der in der Richtlinie festgelegten Namenskonventionen für die MitarbeiterInnen des BRZ und deren Rollenzuordnung.

Von den BetriebskoordinatorInnen wird monatlich geprüft, ob von MitarbeiterInnen des BRZ im Produktivsystem schreibende Zugriffe auf Applikationsdaten vorgenommen wurden.

2.1.2.8 SAP-Zugänge für MitarbeiterInnen von Beratungsfirmen und sonstigen externen Stellen

Die SAP-Zugänge für MitarbeiterInnen von Beratungsfirmen und sonstigen externen Stellen werden von der BenutzerInnen- und Berechtigungsverwaltung der Universität verwaltet. Diese Zugänge werden nach folgender Namenskonvention im System angelegt: B_EXT_*NACHNAME*. Der Benutzername ist maximal 12 Zeichen lang.

2.1.3 Berechtigungsverwaltung

Berechtigungen werden an der Universität über Rollen vergeben.

2.1.3.1 Berechtigungsverwaltung für SAP-BenutzerInnen

Die Rollen müssen funktional/organisatorisch so gestaltet sein, dass der/die InhaberIn dieser Rolle alle in seinem Aufgaben- und/oder Verantwortungsbereich liegenden Tätigkeiten durchführen kann. Es ist bei der Definition der Rollen aber auch sicherzustellen, dass von der/dem RolleninhaberIn jene Funktionen des Systems, die nicht für seine/ihre Arbeit benötigt werden, nicht ausgeführt werden können. Daher muss durch das Rollenkonzept verhindert werden, dass von RolleninhaberInnen auf Daten zugegriffen werden kann, für die sie nicht berechtigt sind.

Die Regelungen zur Berechtigungsverwaltung legen die Abläufe hinsichtlich

- Detaillierungsgrad der Berechtigungen,
- Kritische Berechtigungen,
- Berechtigungsänderungen und
- Rollenänderungen

fest.

[4] vgl. BRZ UNISAP-Sicherheitskonzept V7.71, Seite 22 und UNISAP-Berechtigungskonzept V2.2 (Diese liegen bei den SAP-BetriebskoordinatorInnen auf. Das Sicherheitskonzept und UNISAP-Berechtigungskonzept wird aufgrund von Vertraulichkeitserfordernissen dieser Richtlinie nicht beigelegt.)

2.1.3.1.1 Detaillierungsgrad der Berechtigungen

Das Berechtigungskonzept ist in SAP technisch so umzusetzen, dass Berechtigungen hierarchisch bis auf einzelne Transaktionen sowie Berechtigungsobjekte vergeben werden können.

2.1.3.1.2 Kritische Berechtigungen

Vom Betriebskoordinatorenteam sind Transaktionen und die entsprechenden Berechtigungsobjekte zu berücksichtigen, die nicht zusammen an eine Person vergeben werden dürfen, da sie zu kritischen Kombinationen von Berechtigungen führen würden.

Bei der Definition von kritischen Kombinationen von Berechtigungen sind auch Berechtigungen des/der SAP-AnwenderIn zu berücksichtigen, die diese/r in Non-SAP-Systemen hat (zB e-Banking).

2.1.3.1.3 Berechtigungsänderungen[5]

Bei der Änderung von Berechtigungen sind zwei Fälle zu unterscheiden:

- Änderung der Zugriffsberechtigung auf Kostenstellen und Innenaufträge und
- Änderungen der Rollenzuordnung von Professional und Limited Professional UserInnen.

Änderung der Zugriffsberechtigung auf Kostenstellen und Innenaufträge

Änderungen der Berechtigungen eines/r AnwenderIn zur Bearbeitung oder Anzeige von Kostenstellen oder Innenaufträgen dürfen nur vorgenommen werden, wenn ein Antrag entsprechend des Berechtigungsänderungsprozesses vorliegt, der von allen betroffenen DateneigentümerInnen genehmigt ist. Ergeben sich Berechtigungsänderungen durch einen organisatorischen Wechsel der/des SAP-BenutzerIn, so ist im Antragsformular anzugeben, ob die bisherigen Berechtigungen belassen werden können.[6]

Von der BenutzerInnen- und Berechtigungsverwaltung ist monatlich zu überprüfen, ob für alle organisatorischen Änderungen, die SAP-BenutzerInnen betreffen, die entsprechende Änderung der Zugriffsberechtigung beantragt wurde. Dies geschieht mittels eines eigenentwickelten SAP-Reports.

Änderungen der Rollenzuordnung von Professional und Limited Professional UserInnen

Bei der Zuordnung der Rollen ist darauf zu achten, dass es zu keiner Funktionshäufung kommt, die zu kritischen Berechtigungen des/der einzelnen AnwenderIn führt. Alle Anträge auf Berechtigungsänderungen, die Professional und Limited Professional User-Lizenzen betreffen, sind daher vom Betriebskoordinatorenteam zu prüfen und von der/dem Applikationsverantwortlichen zu genehmigen.

Bevor die/der UserIn über die Berechtigungsänderung informiert wird, ist im Sinne des 4-Augen-Prinzips von einer/einem weiteren MitarbeiterIn der BenutzerInnen- und Berechtigungsverwaltung zu prüfen, ob die beantragte Berechtigungsänderung im SAP-System richtig umgesetzt wurde und die Richtigkeit ist zu bestätigen.

---

[5] vgl. Anhang Kapitel 5.2.2.6, Seite 37: Prozess IKS6 – Berechtigungsänderung
[6] vgl. Anhang Kapitel 5.2.2.5, Seite 36: Prozess IKS5 – Übertragung eines SAP-Zugangs

2.1.3.1.4 Rollenänderungen[7]

Das Betriebskoordinatorenteam muss vor der technischen Umsetzung der Rollenänderung die Änderung des Funktionsumfangs einer Rolle prüfen. Es muss geprüft werden, ob kritische Kombinationen von Berechtigungen innerhalb der Rolle oder in Kombination mit anderen Rollen auftreten können.

Nach der Prüfung der Rollenänderung durch das Betriebskoordinatorenteam muss der/die Applikationsverantwortliche die Änderung schriftlich genehmigen.

Bevor die geänderte Rolle in das Produktivsystem transportiert wird, ist im Sinne des 4-Augen-Prinzips von einer/einem weiteren MitarbeiterIn der BenutzerInnen- und Berechtigungsverwaltung zu prüfen, ob die beantragte Rollenänderung im SAP-System richtig umgesetzt wurde, und die Richtigkeit ist zu bestätigen.

2.1.3.1.5 Vergabe erweiterter Rollen in SAP-Projekten

Ergibt sich aus dem Inhalt eines SAP-Projektes, dass bestimmte Projektteammitglieder erweiterte, modulübergreifende Berechtigungen benötigen, können Sonderrollen vergeben werden, die die Berechtigung für alle Module beinhalten. Die Personen, die diese Rollen erhalten (Key UserInnen), müssen im Projektauftrag genannt werden.

Key UserInnen sind

- AnsprechpartnerInnen für laufende SAP Anwendungsfragen, welche durch den First Level Support nicht gelöst werden konnten,
- zuständig für die Weiterentwicklung und Optimierung – entsprechend des auftretenden Bedarfs – von SAP,
- zentrale AnsprechpartnerInnen zur Funktionsweise der einzelnen Module für die reibungslose Integration von SAP in Bezug auf organisatorische Änderungen (zB Veränderung von organisatorischen Prozessen mit SAP-Bezug),
- SchlüsselbenutzerInnen, die mit den Abläufen in SAP und den Prozessen, welche mit SAP in Zusammenhang stehen, bestens vertraut sind.

Dadurch ist sichergestellt, dass bei den RolleninhaberInnen das notwendige umfangreiche Wissen über die modulübergreifenden Abläufe im SAP-System vorhanden ist.

Die Rollenzuordnung ist von der/dem Applikationsverantwortlichen zu genehmigen. Die Rollen dürfen nur für die Zeitdauer des SAP-Projekts zugeordnet bleiben.

2.1.3.1.6 Periodische Autorisierung der Rollenvergabe

Um sicherstellen zu können, dass die Rollenvergabe noch den tatsächlichen Aufgabenbereichen der Professional und der Limited Professional UserInnen entspricht, wird den LeiterInnen jener Einheiten, in denen MitarbeiterInnen einen Professional oder Limited Professional Zugang haben, in periodischen Abständen (halbjährlich) die Information, welche MitarbeiterIn welche Rollen zugeordnet hat und welche Transaktionen in den einzelnen Rollen enthalten sind, zur Verfügung gestellt.

Diese Zuordnungen sind von den LeiterInnen zu bestätigen und der BenutzerInnen- und Berechtigungsverwaltung zu übermitteln.

[7] vgl. Anhang Kapitel 5.2.2.7, Seite 38: Prozess IKS7 – Rollenänderung

2.1.3.2 Berechtigungsverwaltung für ESS-BenutzerInnen

ESS-BenutzerInnen erhalten einheitliche, nicht benutzerspezifisch ausgeprägte Rollen je nach Art des Dienstverhältnisses. In den Rollen sind das Menü und die Berechtigungen für die einzelnen Applikationen für ESS - Employee Selfservice, MSS – Manager Selfservice und für Genehmigungsprozesse abgebildet.

Die Einschränkung der Berechtigungen in den einzelnen Applikationen von ESS und MSS erfolgt über die Zuordnung der jeweiligen Person im Organisationsmanagement im Modul HR. Das heißt, über diese Zuordnungen ist gewährleistet, dass die ESS-BenutzerInnen nur die für sie vorgesehenen Aktivitäten ausführen bzw. Daten einsehen können.

Für die Genehmigungsprozesse sind keine benutzerspezifischen Berechtigungseinschränkungen in den Rollen notwendig, da die BenutzerInnenfindung auf Grund des im jeweiligen Workflow festgelegten Regelwerkes erfolgt[8].

2.2 IKS-Bereich: Ordnungsmäßigkeit

Im IKS-Bereich Ordnungsmäßigkeit können insbesondere folgende Risiken auftreten:

- **Die Nachvollziehbarkeit von Aktivitäten im SAP-System ist nicht gegeben.** Eine Ursache für die mangelnde Nachvollziehbarkeit kann das Fehlen einer Dokumentation von Eigenentwicklungen oder die fehlende Weitergabe von Informationen über vorgenommene Systemeinstellungen durch das BRZ sein.

- **Fehlerhaft arbeitende Schnittstellen**
  Daten aus Vorsystemen werden unvollständig, redundant oder nicht zeitnah in SAP übernommen

- **Fehler im Ablauf der Anwendungsentwicklung**
  Eigenentwicklungen werden ohne Freigabeverfahren ins Produktivsystem transportiert oder die Anwendungsentwicklung erfolgt direkt im Produktivsystem. Es besteht weiters das Risiko, dass das Freigabeverfahren durch Änderung der Entwicklung auf QU1 beeinflusst wird. Wenn diese Änderungen nicht auf TU1 1:1 nachgezogen werden, entstehen Inkonsistenzen zwischen der freigegebenen und der auf die PU1 transportierten Eigenentwicklung.

Die im IKS-Bereich Ordnungsmäßigkeit definierten Regelungen zur

- Nachvollziehbarkeit,
- Anwendungsentwicklung,
- Transportsystem und zur
- Vornahme von Systemeinstellungen durch das BRZ

sollen diesen Risiken entgegenwirken.

[8] siehe „Rahmenbetriebsvereinbarung über den Einsatz der Informations- und Kommunikationstechnologie im Arbeitsprozess an der Universität Graz (RBV IKT): Anhang SAP"

2.2.1 Nachvollziehbarkeit

2.2.1.1 Tabellenprotokollierung

Im Produktivsystem muss die Tabellenprotokollierung aktiviert sein. Es sind alle von SAP standardmäßig vorgesehenen Tabellen sowie die Tabellen aus dem SAP-Hinweis 112388 - Protokollierungspflichtige Tabellen zu protokollieren. Der SAP-Hinweis mit den zu protokollierenden Tabellen liegt bei.[9] Im Transportmanagement sind alle Transporte zu protokollieren.[10] Die Verantwortung für die Durchführung der Tabellen- und Transportprotokollierung liegt gemäß Betriebsvertrag beim BRZ.

Die Umsetzung im SAP-System ist von den BetriebskoordinatorInnen in halbjährlichen Abständen zu prüfen.

2.2.1.2 Dokumentation des Anlegens und Löschens von BenutzerInnenstammsätzen sowie der Rollenzuordnungen

Die Anträge zu den Administrationstätigkeiten in der BenutzerInnen- und Berechtigungsverwaltung müssen aufbewahrt werden, damit die Nachvollziehbarkeit von Änderungen gewährleistet ist. Hierbei ist die gesetzliche Aufbewahrungsfrist zu beachten. Durch die Aufbewahrung der Anträge wird das Risiko vermieden, dass BenutzerInnen unberechtigt im System angelegt werden oder unberechtigt Rollen an BenutzerInnen vergeben werden.

2.2.1.3 Namenskonvention für den SAP-Benutzerstammsatz

Als Benutzerkennung ist ein Benutzername zu generieren, der folgendem Muster entspricht: B_NACHNAME. Der Benutzername ist maximal 12 Zeichen lang. Um die Nachvollziehbarkeit sicherzustellen, sind auch die Adressdaten (Vorname, Nachname, E-Mailadresse) im SAP-Benutzerstammsatz zu pflegen. Dies ist für die Nachvollziehbarkeit von Systemaktivitäten notwendig, die von BenutzerInnen mit gleichem Vor- und Nachnamen durchgeführt wurden.
SAP-Zugänge für MitarbeiterInnen von Beratungsfirmen und sonstigen externen Stellen sind nach folgender Namenskonvention: B_EXT_*NACHNAME* einzurichten.

2.2.1.4 Unzulässigkeit von Sammelbenutzern

Jede Aktion im SAP-System muss eindeutig einer Person zugeordnet werden können. Daher muss es eine 1:1-Beziehung zwischen SAP-Benutzerkennung und einer physischen Person geben. SammelbenutzerInnen (zB ABRECHNUNG oder INVENTUR), sind daher nicht zulässig. Von dieser Richtlinie ausgenommen sind nur die SAP-Standardbenutzer sowie der Notfallbenutzer. Die Verantwortung für die Dokumentation des Einsatzes dieser Benutzer liegt beim BRZ. [11]

Die Weitergabe des Passworts für den SAP-Zugang ist ebenfalls nicht zulässig, da bei einer Passwort-Weitergabe nicht mehr eindeutig nachvollzogen werden kann, wer mit dieser Benutzerkennung im System gearbeitet hat.

---

[9] vgl. Anhang, Kapitel 5.4, Seite 41: Auszug aus dem SAP Hinweis 112388 – Protokollierungspflichtige Tabellen

[10] vgl. BRZ UNISAP-Sicherheitskonzept V7.71, Seite 20 (Dieses liegt bei den SAP-Betriebskoordinator-Innen auf. Das Sicherheitskonzept wird aufgrund von Vertraulichkeitserfordernissen dieser Richtlinie nicht beigelegt.)

[11] vgl. BRZ UNISAP Berechtigungskonzept V2.2, Seite 13 (Dieses liegt bei den SAP-Betriebsko-ordinatorInnen auf. Das Sicherheitskonzept wird aufgrund von Vertraulichkeitserfordernissen dieser Richtlinie nicht beigelegt.)

2.2.2 Anwendungsentwicklung

2.2.2.1 Anforderung einer Eigenentwicklung – Interner Change Request (ICR)[12]

Die Anforderung einer Eigenentwicklung muss mittels Formulars zur Beantragung eines Internen Change Requests (ICR) erfolgen. Anforderungsberechtigt ist jede/r Professional UserIn. Das Formular für den ICR muss eine detaillierte Definition der Anforderungen enthalten. Nach der Beantragung eines ICR wird dieser von der/dem organisatorischen oder technischen BetriebskoordinatorIn überprüft und bei positiver Prüfung ein Umsetzungsvorschlag inkl. Pflichtenheft erstellt. Der Umsetzungsvorschlag und das Pflichtenheft müssen von der/dem AuftraggeberIn des ICR unterschrieben werden. Im Umsetzungsvorschlag wird auch festgelegt, ob die Umsetzung des ICR intern erfolgt oder extern beauftragt wird. Nach erfolgter Durchführung des ICR, unabhängig davon, ob die Umsetzung intern oder extern erfolgte, muss dieser durch den/die AuftraggeberInnen abgenommen werden.

2.2.2.2 Freigabeverfahren für Eigenentwicklungen

Anwendungsentwicklung darf ausschließlich im Entwicklungssystem TU1 durchgeführt werden. Nach einem ersten funktionalen Test im Entwicklungssystem wird die Eigenentwicklung auf das Qualitätssicherungssystem QU1 transportiert und durch die jeweils fachlich zuständige Abteilung getestet. Änderungen an der Eigenentwicklung, die aufgrund dieser Tests notwendig werden, dürfen nur auf TU1 vorgenommen werden, anschließend ist die Eigenentwicklung wieder zum Testen nach QU1 zu transportieren. Erst nach der Freigabe durch den/die AntragstellerIn wird die Entwicklung auf das Produktivsystem PU1 transportiert. Sollten bei einer Eigenentwicklung Objekte geändert werden müssen, die im SAP-Namensraum liegen, so ist dies ausführlich zu dokumentieren.

Die Transporte werden vom BRZ durchgeführt. Die Abwicklung und Dokumentation der Transporte erfolgt über das SLF-System.

2.2.2.3 Sperrkonzept

Der Sperrmechanismus wird nicht automatisch vom SAP-System bei jedem ändernden Zugriff auf einen Datensatz aktiviert, sondern muss explizit programmiert werden. In jedem eigenentwickelten Programm, das ändernd auf SAP-Daten zugreift, muss daher von dem/der EntwicklerIn dafür gesorgt werden, dass keine Inkonsistenzen entstehen.

2.2.2.4 Berechtigungsprüfungen

In eigenentwickelten Programmen müssen Berechtigungsprüfungen implementiert werden. Wenn die Berechtigungsprüfung nicht explizit programmiert wurde, kann das Programm von jedem/r SAP-BenutzerIn ausgeführt werden. Die relevanten Berechtigungsprüfungen sind in den Programmiervorgaben festzulegen.

[12] vgl. Anhang, Kapitel 5.2.2.8, Seite 39: Prozess IKS8 – Abwicklung Interner Change Request (ICR)

2.2.2.5 Dokumentation

Jedes Programm ist ausführlich zu dokumentieren. Die Dokumentation muss aus einer Dokumentation für die AnwenderInnen und einer technischen Dokumentation für andere EntwicklerInnen bestehen.

2.2.2.6 Direkter Datenbankzugriff

Zugriffe auf die Datenbank dürfen grundsätzlich nur über das Data Dictionary stattfinden. Der direkte Datenbankzugriff unter Umgehung der R/3 Datenbankschnittstelle darf in Anwendungsprogrammen nicht verwendet werden, da dadurch die Sicherheit und Konsistenz der Daten nicht gewährleistet ist.

2.2.2.7 Versionierung

Alle Versionen von Programmen sind aufbewahrungspflichtig. Das Löschen der Versionshistorie ist nicht zulässig. Die Aufbewahrungspflicht wird auch erfüllt, wenn die Versionen von eigenentwickelten Programmen im Entwicklungssystem archiviert werden.

2.2.2.8 Datenänderungen im Debug-Modus

Änderungen von Hauptspeicherinhalten im Debug-Modus werden nicht protokolliert. Da im Debug-Modus jedoch betriebswirtschaftliche Werte während des Ablaufs eines Programms verändert werden können, darf dieses Zugriffsrecht im Produktivsystem niemandem zugeordnet werden.

2.2.3 Transportsystem

Um zu verhindern, dass EntwicklerInnen ihre Eigenentwicklungen ohne Freigabeverfahren ins Produktivsystem transportieren können, ist eine Funktionstrennung zwischen Entwicklung und Transporten zu realisieren. Daraus folgt, dass die Berechtigungen für die Entwicklung und das Transportsystem nicht gemeinsam an eine Person der Karl-Franzens-Universität Graz vergeben werden dürfen. Da die Trennung der Berechtigungen für die Entwicklung und den Transport bei MitarbeiterInnen des BRZ aus organisatorischen Gründen nicht möglich ist, wurde vom BRZ technisch sichergestellt, dass die/der EntwicklerIn die eigenen Entwicklungen nicht transportieren kann.

2.2.4 Vornahme von Systemeinstellungen durch das BRZ

Die Universität ist von sämtlichen geplanten Eingriffen in das System zu informieren. Dies gilt insbesondere für Customizing-Einstellungen und Entwicklungen. Die durchgeführten Tätigkeiten sind vom BRZ zu dokumentieren und den BetriebskoordinatorInnen der Universität zur Verfügung zu stellen.

Von den BetriebskoordinatorInnen ist anhand der im SLA-Report angeführten Transporte monatlich zu prüfen, welche vom BRZ am Mandanten der Karl-Franzens-Universität Graz durchgeführten Eingriffe (Customizing-Einstellungen und Entwicklungen) transportiert wurden.

2.3 IKS-Bereich: Wirtschaftlichkeit

Im IKS-Bereich Wirtschaftlichkeit kann insbesondere folgendes Risiko auftreten:

- **Bezahlung zu hoher Lizenzkosten**
  Zu hohe Lizenzkosten können anfallen, wenn seitens des BRZ fehlerhafte Lizenzverrechnungen erfolgen oder seitens der Universität gegen Lizenzbestimmungen verstoßen wird. Das mit SAP vereinbarte Lizenzvolumen kann auch überschritten werden, wenn die BenutzerInnen falschen Nutzertypen zugeordnet werden.

Die im IKS-Bereich Sicherheit definierten Regelungen zur

- Verrechnung von Lizenzkosten,
- Einhaltung der SAP-Lizenzbestimmungen,
- Vergabe von Nutzertypen und zum
- Lizenzvolumen

sollen dem Eintreten dieses Risikos entgegenwirken.

2.3.1 Verrechnung von Lizenzkosten

Die vom BRZ in Rechnung gestellten Lizenzgebühren werden von den BetriebskoordinatorInnen geprüft.

Die Aufstellung über die zu verrechnenden Lizenzkosten muss von der BenutzerInnen- und Berechtigungsverwaltung halbjährlich an die Abteilung für Buchhaltung und Bilanzierung übermittelt werden. Den LizenzinhaberInnen werden aufgrund dieser Aufstellung die einmaligen Lizenzkosten und die jährliche Wartungsgebühr in Höhe von 17 % des Lizenzwertes verrechnet.

SAP-Lizenzen, die von LeiterInnen bzw. MitarbeiterInnen von Projekten gem. §§26, 27 und 28 UG 2002 beantragt werden, müssen weiterverrechnet werden. Lizenzen, die das festgelegte Lizenzkontingent einer Organisationseinheit, Akademischen Einheit bzw. Verwaltungseinheit übersteigen, müssen ebenfalls weiterverrechnet werden.

Die SAP-Lizenzkosten für ESS-UserInnen werden nicht an die Einheiten weiterverrechnet.

Die Modalitäten der Weiterverrechnung sind in gesonderten Regelungen enthalten.

2.3.2 Einhaltung der SAP-Lizenzbestimmungen

Mehrfachanmeldungen im Produktivsystem verstoßen gegen das Lizenzabkommen mit SAP und sind daher nicht erlaubt.[13]

[13] vgl. Anhang, Kapitel 5.5., Seite 42: Auszug aus der Preis- und Konditionenliste für die Überlassung und Pflege von mySAP.com, Version 4.0a;

2.3.3 Vergabe von Nutzertypen

Von SAP wird in regelmäßigen Abständen eine Systemvermessung durchgeführt[14]. Bei der Systemvermessung wird die Zahl der zu einem bestimmten Zeitpunkt auf dem SAP-System vorhandenen BenutzerInnen ermittelt. Da die Kosten einer Lizenz vom jeweiligen Nutzertyp abhängen, ist bei der Anlage der BenutzerInnen darauf zu achten, dass der richtige Nutzertyp im Benutzerstammsatz hinterlegt wird.

2.3.4 Lizenzvolumen

Von der BenutzerInnen- und Berechtigungsverwaltung ist die Anzahl der vergebenen Lizenzen anhand einer ständig aktuell gehaltenen Liste mit dem Lizenzvolumen der Universität abzugleichen. Sollte das Lizenzvolumen überschritten werden, ist das weitere Vorgehen zu klären, da in diesem Fall bei einer Systemvermessung Lizenzen nachzukaufen sind.

[14] vgl. Anhang, Kapitel 5.6., Seite 43: Auszug aus der Beilage ./1 zum Betriebsvertrag uni.verse, S. 50

3 Nicht-Produktivsysteme

3.1 Qualitätssicherungssystem (QU1-102)

Im Qualitätssicherungssystem finden die Produktionsvorbereitung sowie die Abnahme von Entwicklungen aus dem Entwicklungssystem statt. Das QU1-System ist an der Universität Graz einer gesondert definierten Gruppe von BenutzerInnen zugänglich, die für die Weiterentwicklung und Optimierung des SAP-Systems verantwortlich ist. Für diese Arbeiten sind umfangreiche Berechtigungen notwendig.

Die Vergabe der Berechtigungen erfolgt durch die BenutzerInnen- und Berechtigungsverwaltung.

3.2 Entwicklungssystem (TU1)

Das Entwicklungssystem ist der Ausgangspunkt für Eigenentwicklungen und alle Customizing-Einstellungen. Hinsichtlich der Berechtigungen und der Zugangsbestimmungen gelten die gleichen Regelungen wie für das Qualitätssicherungssystem, da auf TU1 erste funktionale Tests durchgeführt werden müssen.

Die Vergabe der Berechtigungen erfolgt durch das Betriebskoordinatorenteam.

3.3 Schulungsmandant (QU1-502)

Das Schulungssystem steht allen AnwenderInnen zur Verfügung. Da der Schulungsmandant eine Kopie des Produktivsystems ist, müssen die Berechtigungen am Schulungsmandanten den Berechtigungen auf dem Produktivsystem entsprechen.

Die Vergabe der Berechtigungen erfolgt durch die BenutzerInnen- und Berechtigungsverwaltung.

4 Ausgelagerte Bereiche des SAP-Systems

4.1 ERP-System

Der Betrieb der SAP-Basiskomponenten ist an das BRZ ausgelagert. Das BRZ ist dafür verantwortlich, dass der Betrieb der ausgelagerten Bereiche den Anforderungen einer Revision bzw. Wirtschaftsprüfung entspricht.

Das Sicherheitskonzept des BRZ liegt bei den SAP-BetriebskoordinatorInnen auf.

Der Nachweis der Zertifizierung des Sicherheitsmanagements des BRZ gem. ISO 27001 liegt dieser Richtlinie bei.[15]

4.2 SAP Business Warehouse (SAP BW)

Neben dem SAP ERP wird von der Universität auch noch ein SAP Business Warehouse eingesetzt. Das SAP Business Warehouse der Universität wird von der Axians ICT Austria GmbH betrieben.

Die in den vorangegangenen Kapiteln dieser Richtlinie enthaltenen Regelungen gelten mit Ausnahme der im Folgenden angeführten Punkte auch für das SAP Business Warehouse.

Tätigkeiten, die für das SAP ERP lt. dieser Richtlinie vom BRZ durchgeführt werden, werden für das SAP Business Warehouse durch die Axians ICT Austria GmbH durchgeführt.

Die Nachweise der Zertifizierung der Axians ICT Austria GmbH gem. ISO 27001 liegt dieser Richtlinie bei[16]. Der Report gem. SAS70 bzw. ISAE3402 liegt bei den SAP-BetriebskoordinatorInnen auf.

4.2.1 Für das SAP BW nicht relevante Regelungen dieser Richtlinie

Kapitel	Seite	Begründung
2.2.1.1 Tabellenprotokollierung	17	Die im SAP Hinweis 112388 genannten Tabellen beziehen sich auf Tabellen des ERP und nicht auf das BW; für das BW gibt es keine entsprechenden Protokollierungsrichtlinien

[15] vgl. Anhang Kapitel 5.7, Seite 44: Sicherheitszertifikat gem. ISO 27001 (BRZ)
[16] vgl. Anhang Kapitel 5.8, Seite 45: Sicherheitszertifikat gem. ISO 27001 und SAS70 bzw. ISAE3402 (Axians ICT Austria GmbH)

4.2.2 Für das SAP BW in geänderter Form relevante Regelungen

Kapitel	Seite	Begründung
2.1.2.4 Kennwortregelung	11	Bei der Vergabe des Initialkennwortes in SAP BW ist nach denselben Regeln wie in Kapitel 2.1.2.4 angeführt, vorzugehen. Falls der BW-Zugang gleichzeitig mit dem ERP-Zugang angelegt wird, ist als Initialpasswort in SAP BW der gleiche PIN wie für den SAP-Zugang zu verwenden.
2.2.1.3 Namenskonvention für den SAP-Benutzerstammsatz	17	Der Benutzername im BW lautet gleich wie jener für den SAP-Zugang.
2.2.2.1 Anforderung einer Eigenentwicklung	18	Zu den Eigenentwicklungen zählen im SAP BW auch Änderungen am Datenmodell und an Objekten des BW (zB InfoAreas, InfoPackages, InfoSources, DataStoreObjects und Infocubes) sowie die Änderung von Prozessketten
2.2.2.2 Freigabeverfahren für Eigenentwicklungen	18	Entwicklungs- und Qualitätssicherungssystem sind in der BW-Systemlandschaft zu einem System zusammengefasst. Daher erfolgen alle Tests für den Freigabeprozess auf dem BW-Entwicklungssystem. Die Transporte für die Produktivsetzung der Eigenentwicklung werden von der Imtech durchgeführt, sobald der Auftrag im Transportmanagement freigegeben wurde.
2.2.2.4 Berechtigungsprüfungen	18	Falls BW-Queries BenutzerInnen ohne Gesamtberechtigung auf alle CO-Kontierungen der Universität zur Verfügung gestellt werden, ist entweder beim Erstellen der Query selbst oder durch geeignete Berechtigungsvergabe in den Rollen (zB mittels Analyseobjekten) sicherzustellen, dass nur Daten von CO-Kontierungen eingesehen werden können, für die der bzw. die BW-BenutzerIn berechtigt sind.
2.3.3 Vergabe von Nutzertypen	21	Ein SAP BW-Zugang erfordert eine Professional User Lizenz. Personen, die bereits als Professional User im ERP lizenziert sind, sind im BW-Benutzerstamm als Multimandant/Multisystem-NutzerIn einzutragen.

4.2.3 Für das SAP BW zusätzlich geltende Regelungen

Kapitel	Seite	Begründung
Entwicklungs- und Qualitätssicherungssystem SAP BW	22	Die BW-Systemlandschaft ist zweistufig aufgebaut. Entwicklungs- und Qualitätssicherungssystem sind zu einem System zusammengefasst. Für das BW-Entwicklungssystem gelten dieselben Regelungen wie für das Entwicklungs- und Qualitätssicherungssystem des ERP.

5 Anhang

5.1 Zusammenfassung der Verantwortlichkeiten aus der IKS-Richtlinie

Die sich aus dieser Richtlinie ergebenden Verantwortlichkeiten sind in der folgenden Matrix nochmals zusammengefasst.

5.1.1 BenutzerInnen- und Berechtigungsverwaltung, SAP-Betriebskoordination, Applikationsverantwortliche/r

IKS-Bereich		Richtlinie	BenutzerInnen- und Berechtigungs-verwaltung	SAP-Betriebskoordination	Applikationsverantwortliche/r
2 Produktivsystem (PU1)					
2.1 Sicherheit					
	2.1.1 Netzwerksicherheit	Seite 8f		➢ Überprüfung des Vorhandenseins einer gesicherten Verbindung Uni <=> BRZ	
	2.1.2 Anmeldesicherheit	Seite 9ff	➢ Vergabe des PINs ➢ Anlegen, Sperren, Freischalten, Löschen von SAP-Zugängen ➢ Überprüfung der Umsetzung im System i.S.d. Vier-Augen-Prinzips	➢ Prüfung der SAP-Professional User-Anträge auf Vereinbarkeit mit den IKS-Regelungen ➢ Prüfung der Einhaltung der in der Richtlinie festgelegten Namenskonventionen und Rollenzuordnungen für MitarbeiterInnen des BRZ ➢ Prüfung, ob von MitarbeiterInnen des BRZ schreibende Zugriffe auf Applikationsdaten vorgenommen wurden (monatlich)	➢ Genehmigung von SAP-Professional und Limited Professional User-Anträgen
	2.1.3 Berechtigungsverwaltung	Seite 13ff	➢ Technische Umsetzung Berechtigungskonzept; ➢ Vergabe von Rollen an BenutzerInnen ➢ technische Umsetzung Rollenänderungen ➢ Überprüfung der Umsetzung im System i.S.d. Vier-Augen-Prinzips	➢ Berücksichtigung von kritischen Berechtigungen ➢ Erstellung der Information der Rollenzuordnung für Professional und Limited Professional UserInnen	➢ Genehmigung von erweiterten Berechtigungen für ProjektmitarbeiterInnen ➢ Genehmigung von Berechtigungsänderungen bei Professional und Limited Professional UserInnen

IKS-Bereich		Richtlinie	BenutzerInnen- und Berechtigungs-verwaltung	SAP-Betriebskoordination	Applikationsverantwortliche/r
2.2 Ordnungsmäßigkeit					
	2.2.1 Nachvollziehbarkeit	Seite 17f	➢ Dokumentation der Administrationstätigkeiten; ➢ Einhaltung der Namenskonvention	➢ Prüfung der Einstellungen zu protokollierungspflichtigen Tabellen (halbjährlich)	
	2.2.2. Anwendungsentwicklung	Seite 18ff		➢ Prüfung von ICRs; ➢ Erarbeitung von Umsetzungsvorschlägen für ICRs	➢ Genehmigung von ICRs
	2.2.3 Transportsystem	Seite 19	➢ Rollenmäßige Trennung zwischen Entwicklungs- und Transportberechtigung		
	2.2.4 Systemeinstellungen durch das BRZ	Seite 19		➢ Prüfung, welche vom BRZ durchgeführten Eingriffe transportiert wurden	
2.3 Wirtschaftlichkeit					
	2.3.1 Verrechnung von Lizenzkosten	Seite 20	➢ Prüfung, Weitergabe und Dokumentation der zu verrechnenden Lizenzkosten	➢ Prüfung, der vom BRZ in Rechnung gestellten Lizenzkosten	
	2.3.2 Einhaltung der SAP-Lizenzbestimmungen	Seite 20f			
	2.3.3. Vergabe von Nutzertypen	Seite 21	➢ Hinterlegen des richtigen Nutzertyps in den SAP-Stammdaten		
	2.3.4 Lizenzvolumen	Seite 21	➢ Klärung des Vorgehens bei Überschreitung des Lizenzvolumens		
3 Nicht-Produktivsysteme					
3.1 Qualitätssicherungssystem (QU1-102)		Seite 22	➢ Vergabe von Berechtigungen für QU1-102		
3.2 Entwicklungssystem (TU1)		Seite 22		➢ Vergabe von Berechtigungen für TU1	
3.3 Schulungsmandant (QU1-502)		Seite 22	➢ Vergabe von Berechtigungen für QU1-502		

5.1.2 Buchhaltung und Bilanzierung, Uni-IT, BRZ

IKS-Bereich		Richtlinie	Buchhaltung und Bilanzierung	Uni-IT	BRZ
2 Produktivsystem (PU1)					
2.1 Sicherheit					
	2.1.1 Netzwerksicherheit	Seite 8f		➢ Inhalt und Umsetzung Security Policy	➢ Herstellung einer gesicherten Verbindung Uni <=> BRZ
	2.1.2 Anmeldesicherheit	Seite 9ff			➢ Verwaltung der SAP-Zugänge von CCC-Mitarbeiterlnnen, ➢ Informieren der Uni, wenn wesentliche Ver-änderungen an den Berechtigungen von Support-Mitarbeiterlnnen des BRZ vorgenommen werden
	2.1.3 Berechtigungsverwaltung	Seite 13ff			
2.2 Ordnungsmäßigkeit					
	2.2.1 Nachvollziehbarkeit	Seite 17f			➢ Tabellen- und Transportprotokollierung
	2.2.2 Anwendungsentwicklung	Seite 18ff			➢ Transporte der Eigenentwicklungen durchführen
	2.2.3 Transportsystem	Seite 19			
	2.2.4 Systemeinstellungen durch das BRZ	Seite 19			➢ Weitergabe detaillierter Informationen über geplante und vorgenommene Systemeinstellungen
2.3 Wirtschaftlichkeit					
	2.3.1 Verrechnung von Lizenzkosten	Seite 20	➢ Verrechnung einmaliger und laufender Lizenzkosten an die LizenzinhaberInnen		➢ Verrechnung der Lizenzgebühren
	2.3.2 Einhaltung der SAP-Lizenzbestimmungen	Seite 20f			
	2.3.3 Vergabe von Nutzertypen	Seite 21			
	2.3.4 Lizenzvolumen	Seite 21			

IKS-Bereich	Richtlinie	Buchhaltung und Bilanzierung	Uni-IT	BRZ
3 Nicht-Produktivsysteme				
3.1 Qualitätssicherungssystem (QU1-102)	Seite 22			
3.2 Entwicklungssystem (TU1)	Seite 22			
3.3 Schulungssystem (QU1-502)	Seite 22			
4 Ausgelagerte Bereiche des SAP-Systems	Seite 23			➢ Betrieb der SAP-Basiskomponenten, der den Anforderungen einer Revision bzw. Wirtschafts-prüfung entspricht

5.1.3 BRZ, SAP-Betriebskoordination, BenutzerInnen- und Berechtigungsverwaltung

IKS-Bereich	Richtlinie	BRZ	SAP-Betriebskoordination	BenutzerInnen- und Berechtigungs-verwaltung
2 Produktivsystem (PU1)				
2.1 Sicherheit				
2.1.1 Netzwerksicherheit	Seite 8f	➢ Herstellung einer gesicherten Verbindung Uni <=> BRZ	➢ Überprüfung des Vorhandenseins einer gesicherten Verbindung Uni <=> BRZ (wöchentlich)	
2.1.2 Anmeldesicherheit	Seite 9ff	➢ Verwaltung der SAP-Zugänge von CCC-MitarbeiterInnen ➢ Informieren der Uni, wenn wesentliche Veränderungen an den Berechtigungen von MitarbeiterInnen des BRZ vorgenommen werden	➢ Prüfung der Einhaltung der in der Richtlinie festgelegten Namenskonventionen und Rollenzuordnungen für MitarbeiterInnen des BRZ (monatlich) ➢ Prüfung, ob von MitarbeiterInnen des BRZ schreibende Zugriffe auf Appli-kationsdaten vorgenommen wurden (monatlich)	
2.1.3 Berechtigungsverwaltung	Seite 13ff			
2.2 Ordnungsmäßigkeit				
2.2.1 Nachvollziehbarkeit	Seite 17f	➢ Tabellen- und Transportprotokollierung	➢ Prüfung der Einstellungen zu protokollierungspflichtigen Tabellen (halbjährlich)	
2.2.2. Anwendungsentwicklung	Seite 18ff	➢ Transporte der Eigenentwicklungen durchführen		
2.2.3 Transportsystem	Seite 19			
2.2.4 Systemeinstellungen durch das BRZ	Seite 19	➢ Weitergabe detaillierter Informationen über geplante und vorgenommene Systemeinstellungen	➢ Prüfung, welche vom BRZ durchgeführten Eingriffe transportiert wurden (monatlich)	

IKS-Bereich		Richtlinie	BRZ	SAP-Betriebskoordination	BenutzerInnen- und Berechtigungs-verwaltung
2.3 Wirtschaftlichkeit					
	2.3.1 Verrechnung von Lizenzkosten	Seite 20	➢ Verrechnung der Lizenzgebühren	➢ Prüfung, der vom BRZ in Rechnung gestellten Lizenzkosten	➢ Prüfung, Weitergabe und Dokumentation der zu verrechnenden Lizenzkosten
	2.3.2 Einhaltung der SAP-Lizenzbestimmungen	Seite 20ff			
	2.3.3 Vergabe von Nutzertypen	Seite 21			➢ Hinterlegen des richtigen Nutzertyps in den SAP-Stammdaten
	2.3.4 Lizenzvolumen	Seite 21			➢ Klärung des Vorgehens bei Überschreitung des Lizenzvolumens
3 Nicht-Produktivsysteme					
3.1 Qualitätssicherungssystem (QU1-102)		Seite 22		➢ Vergabe von Berechtigungen für QU1-102	
3.2 Entwicklungssystem (TU1)		Seite 22		➢ Vergabe von Berechtigungen für TU1	
3.3 Schulungsmandant (QU1-502)		Seite 22			➢ Vergabe von Berechtigungen für QU1-502
4 Ausgelagerte Bereiche des SAP-Systems		Seite 23	➢ Betrieb der SAP-Basiskomponenten, der den Anforderungen einer Revision bzw. Wirtschaftsprüfung entspricht		➢

5.2 Geschäftsprozesse, die sich aus der IKS-Richtlinie ergeben

Die sich aus der Richtlinie ergebenden Geschäftsprozesse sind im Folgenden grafisch dargestellt.

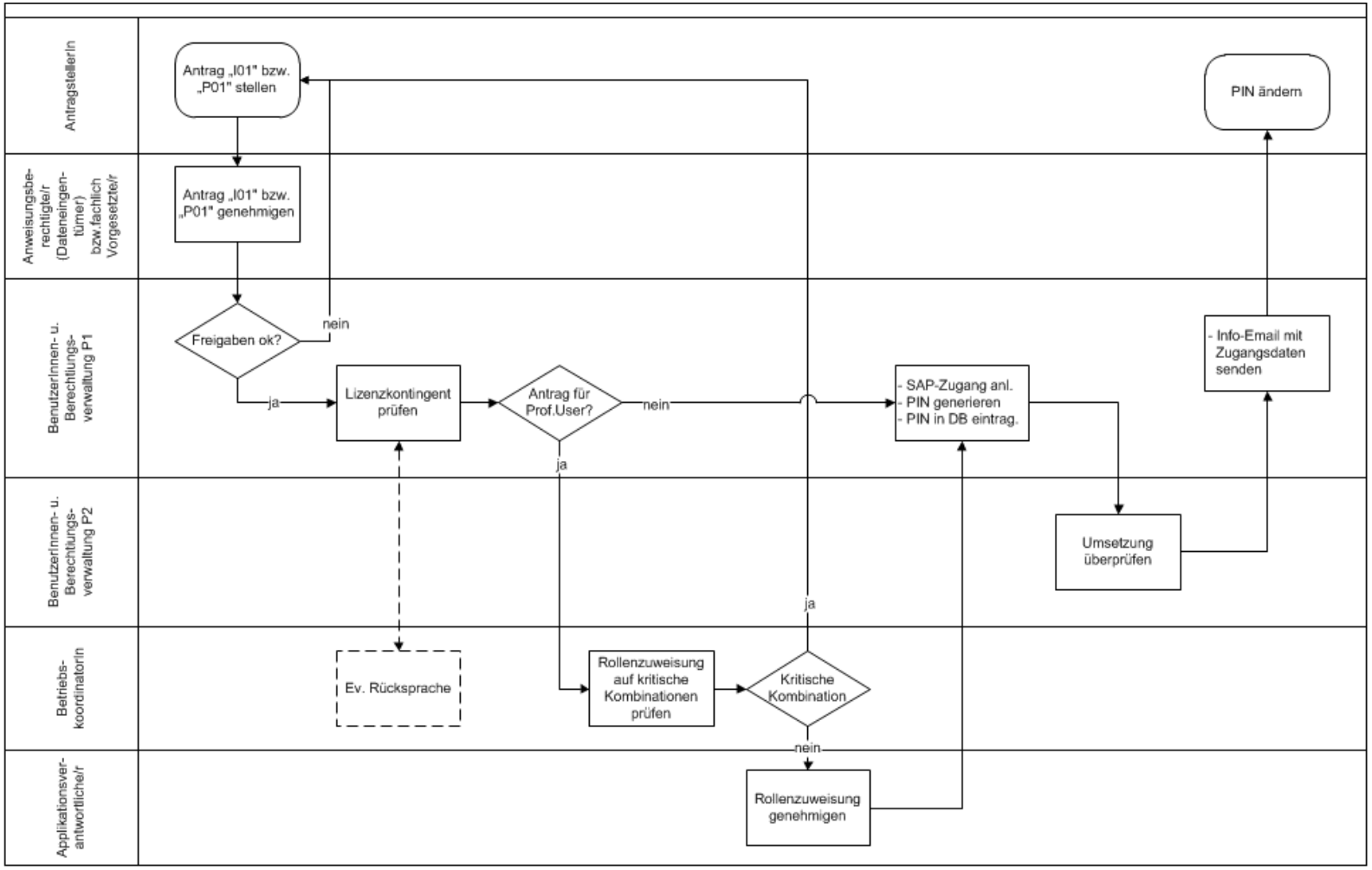
5.2.1 Rollenbeschreibung bzw. –definition

Rolle	Prozess	Beschreibung/Definition
AntragstellerIn	IKS1_Neuer SAP-Zugang IKS3_Passwort zurücksetzen IKS4_Übertragung eines SAP-Zuganges	Jede/r MitarbeiterIn der KFUG, die/der im Rahmen ihrer/seiner Arbeit einen SAP-Zugang benötigt bzw. auf die/den eine SAP-Lizenz übertragen werden soll
SAP-UserIn	IKS3_Passwort zurücksetzen IKS4_Löschen eines SAP-Zugangs IKS6_Berechtigungsänderung	Jede/r SAP-UserIn der KFUG
SAP Prof. o. Lim.Prof. UserIn	IKS7_Rollenänderung IKS8_Abwicklung ICR	Jede/r SAP Prof. oder Lim.Prof. UserIn der KFUG
Anweisungsberechtigte/r + (DateneigentümerIn)	IKS1_Neuer SAP-Zugang IKS4_Löschen eines SAP-Zugangs IKS5_Übertragung eines SAP-Zuganges IKS6_Berechtigungsänderung	Anweisungsberechtigte/r des Berechtigungsobjektes, von der die Lizenzkosten abgebucht werden; Dateneigentümer sind die Anweisungsberechtigten des Berechtigungsobjektes, auf die der neue SAP-Zugang berechtigt ist.
fachlich Vorgesetzte/r	IKS6_Berechtigungsänderung IKS7_Rollenänderung	Fachlich Vorgesetzte/r der/des SAP-Userin/s
BenutzerInnen- und Berechtigungsverwaltung	IKS1_Neuer SAP-Zugang IKS2_Neuer ESS-Zugang IKS3_Passwort zurücksetzen IKS4_Löschen eines SAP-Zuganges IKS5_Übertragung eines SAP-Zuganges IKS6_Berechtigungsänderung IKS7_Rollenänderung IKS8_Abwicklung ICR	MitarbeiterInnen des Competence Center SAP der Universität Graz
BetriebskoordinatorIn	IKS1_Neuer SAP-Zugang IKS6_Berechtigungsänderung IKS7_Rollenänderung IKS8_Abwicklung ICR	Fr. Hungerländer-Kropf (organisatorisch), Hr. Ortner (technisch)
Applikationsverantwortliche/r	IKS1_Neuer SAP-Zugang IKS6_Berechtigungsänderung IKS7_Rollenänderung IKS8_Abwicklung ICR	Applikation SAP HR (Hr. Lugger) Applikation SAP FI, FI-AA, CO, MM/SD, BW und VM (Hr. Zettl)
EntwicklerIn	IKS8_Abwicklung ICR	MitarbeiterInnen des Competence Center SAP der Universität Graz
Externer Lieferant	IKS8_Abwicklung ICR	Jede externe Firma, die in die Umsetzung eines ICR involviert ist
UNI-IT	IKS2_Neuer ESS-Zugang	Betreuer/in des automatischen Abgleichs der SAP-Zugangsdaten mit den LDAP-Daten

5.2.2 Prozesse

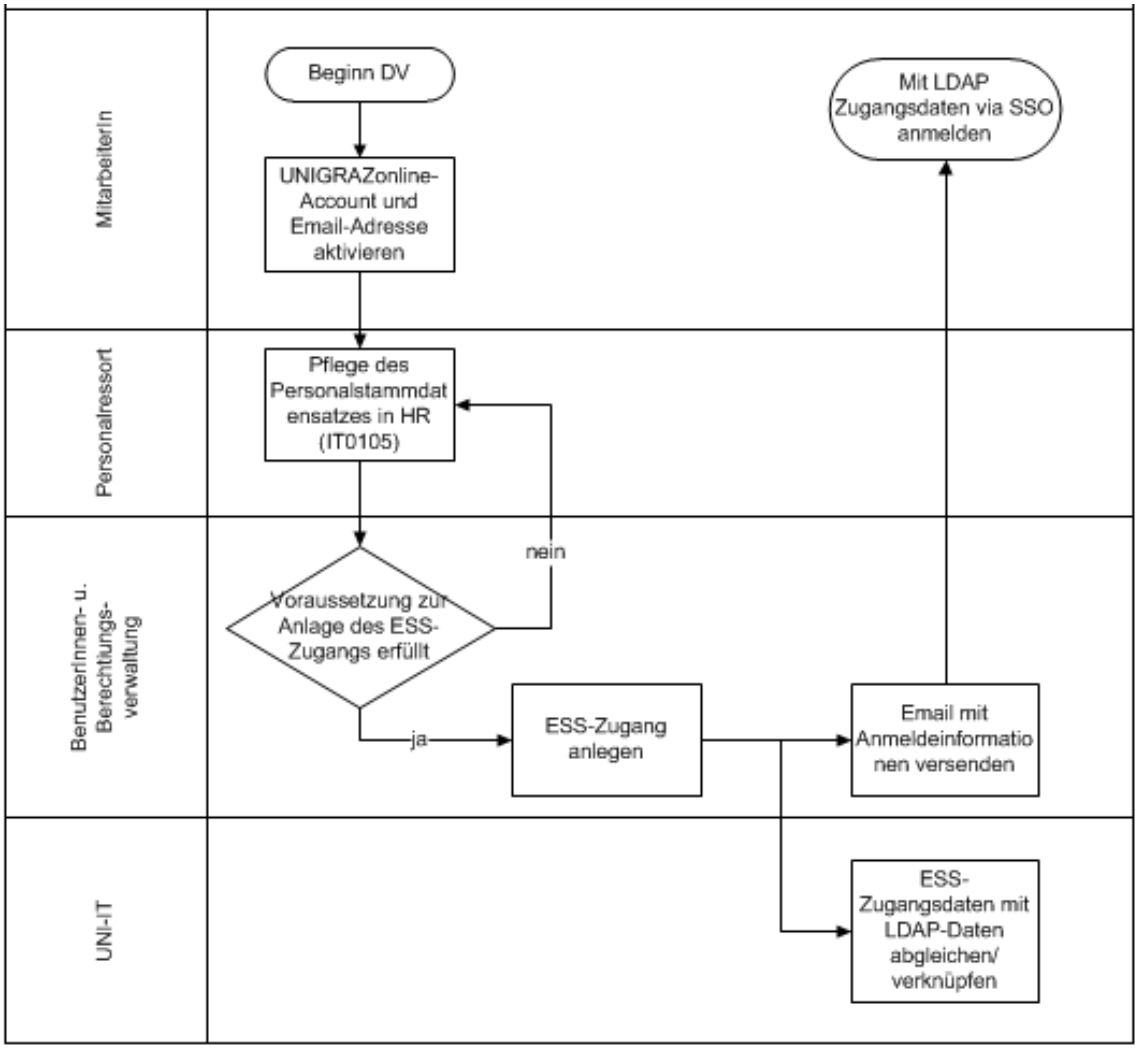
5.2.2.1 Prozess IKS1 – Neue/r SAP-UserIn

Dieser Prozess bezieht sich auf Punkt **2.1.2.1** in der Richtlinie.



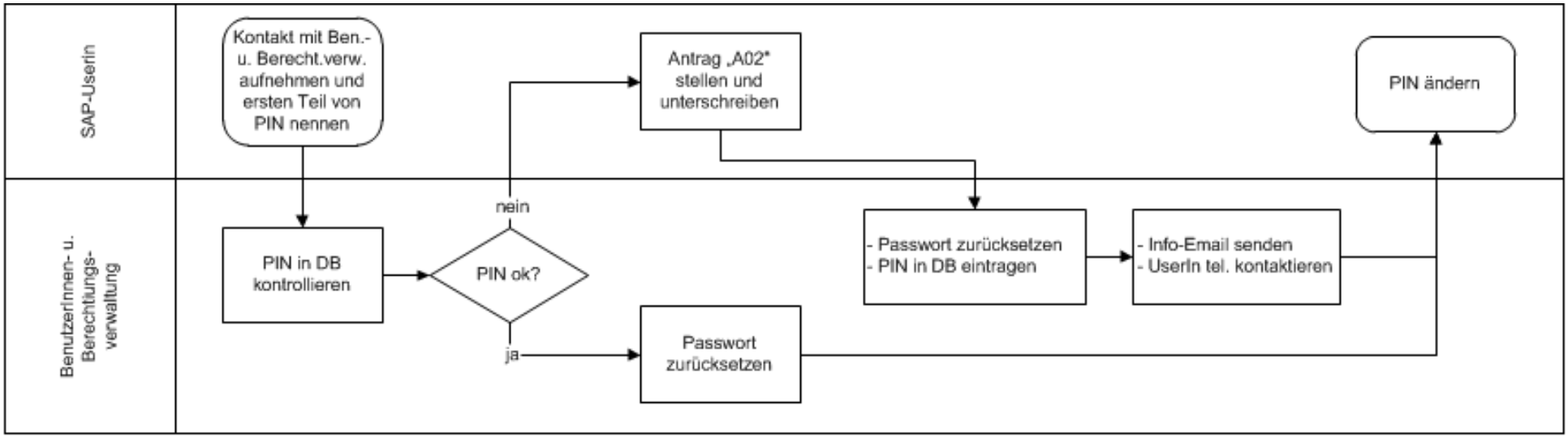
5.2.2.2 Prozess IKS2 – Neue/r ESS-UserIn

Dieser Prozess bezieht sich auf Punkt **2.1.2.2** in der Richtlinie.



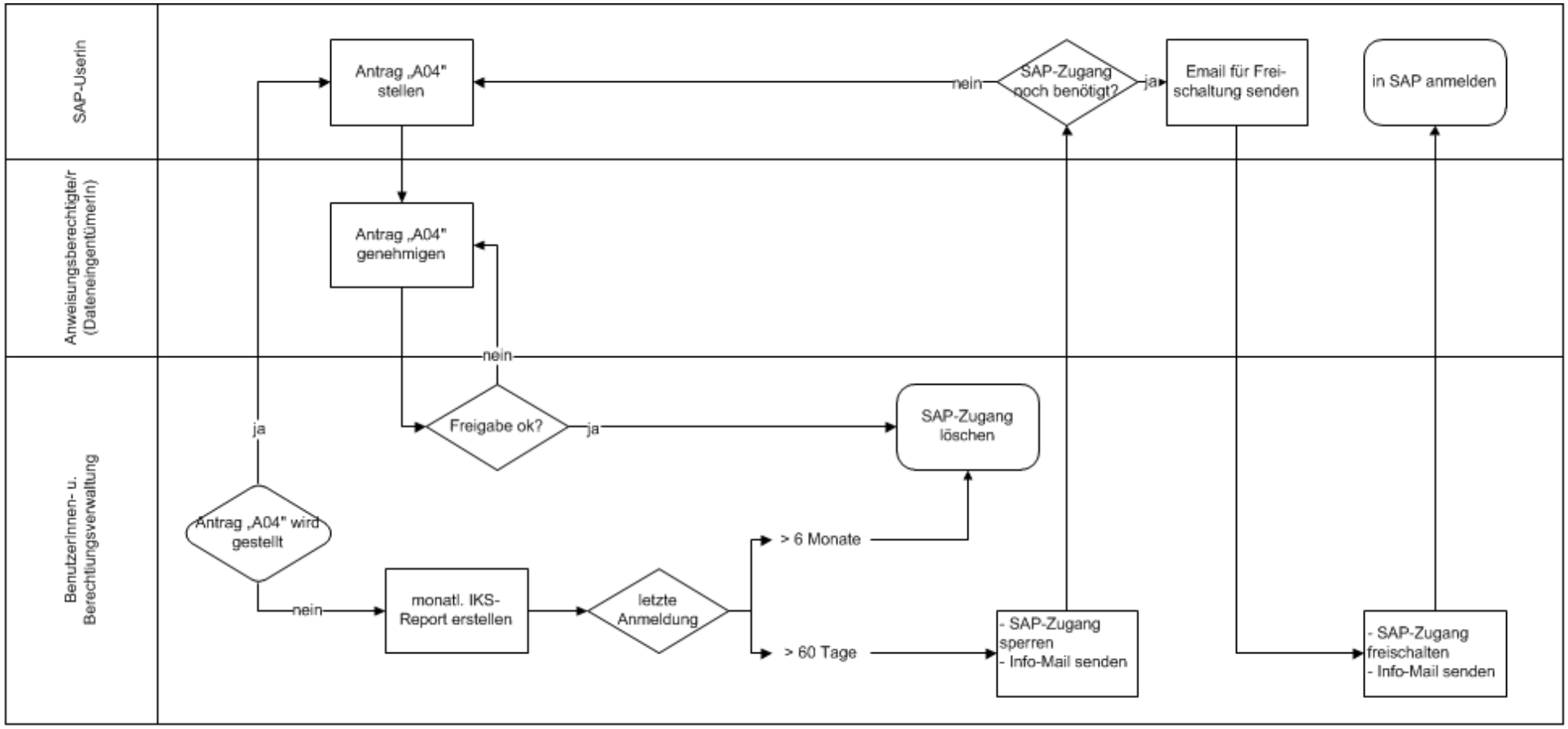
5.2.2.3 Prozess IKS3 - Passwort zurücksetzen

Dieser Prozess bezieht sich auf Punkt **2.1.2.3** in der Richtlinie.



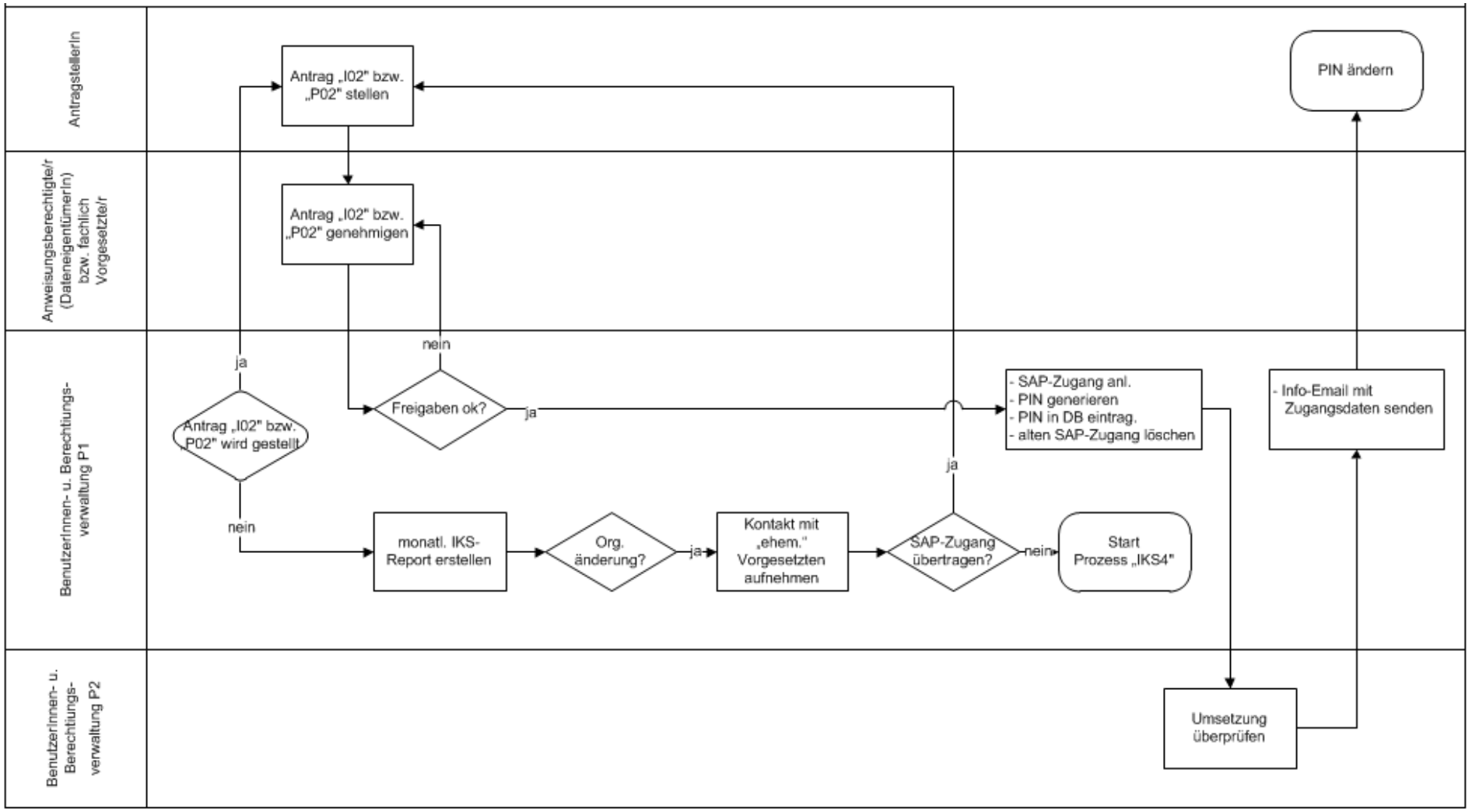
5.2.2.4 Prozess IKS4 - Sperren, Freischalten und Löschen eines SAP-Zugangs

Dieser Prozess bezieht sich auf Punkt **2.1.2.5** der Richtlinie



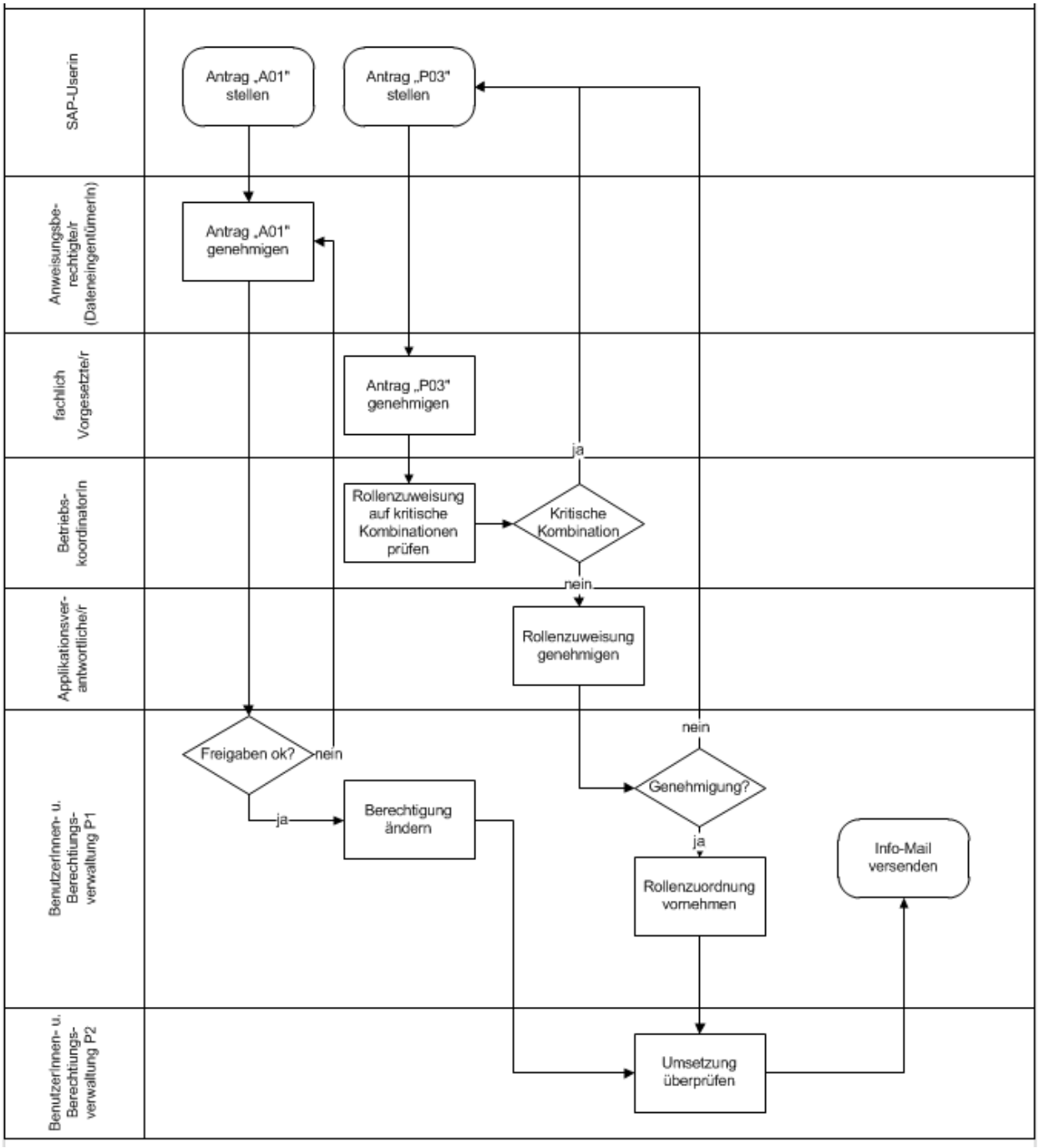
5.2.2.5 Prozess IKS5 - Übertragung eines SAP-Zugangs

Dieser Prozess bezieht sich auf Punkt **2.1.3.1.3** in der Richtlinie.



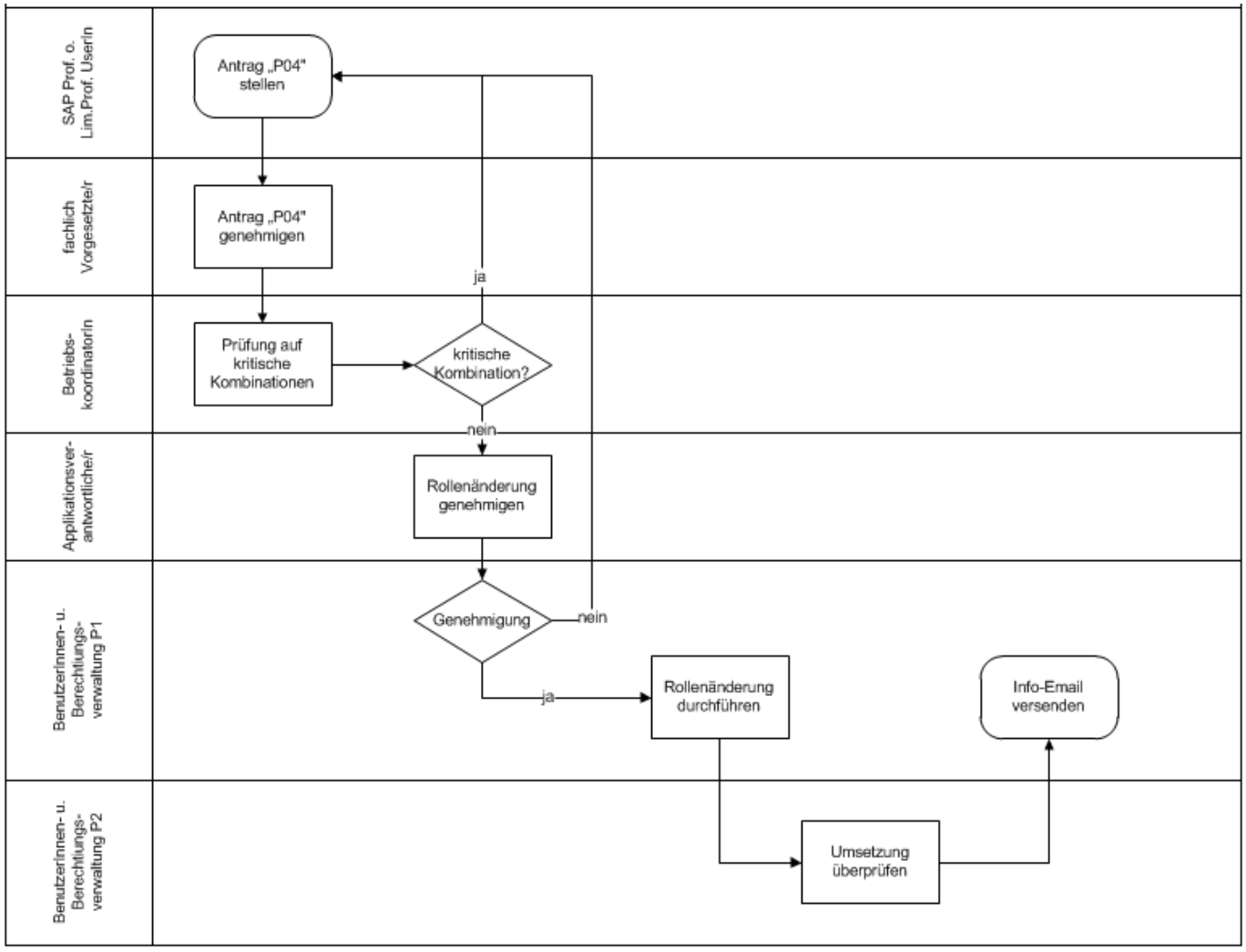
5.2.2.6 Prozess IKS6 - Berechtigungsänderung

Dieser Prozess bezieht sich auf Punkt **2.1.3.1.3** in der Richtlinie.



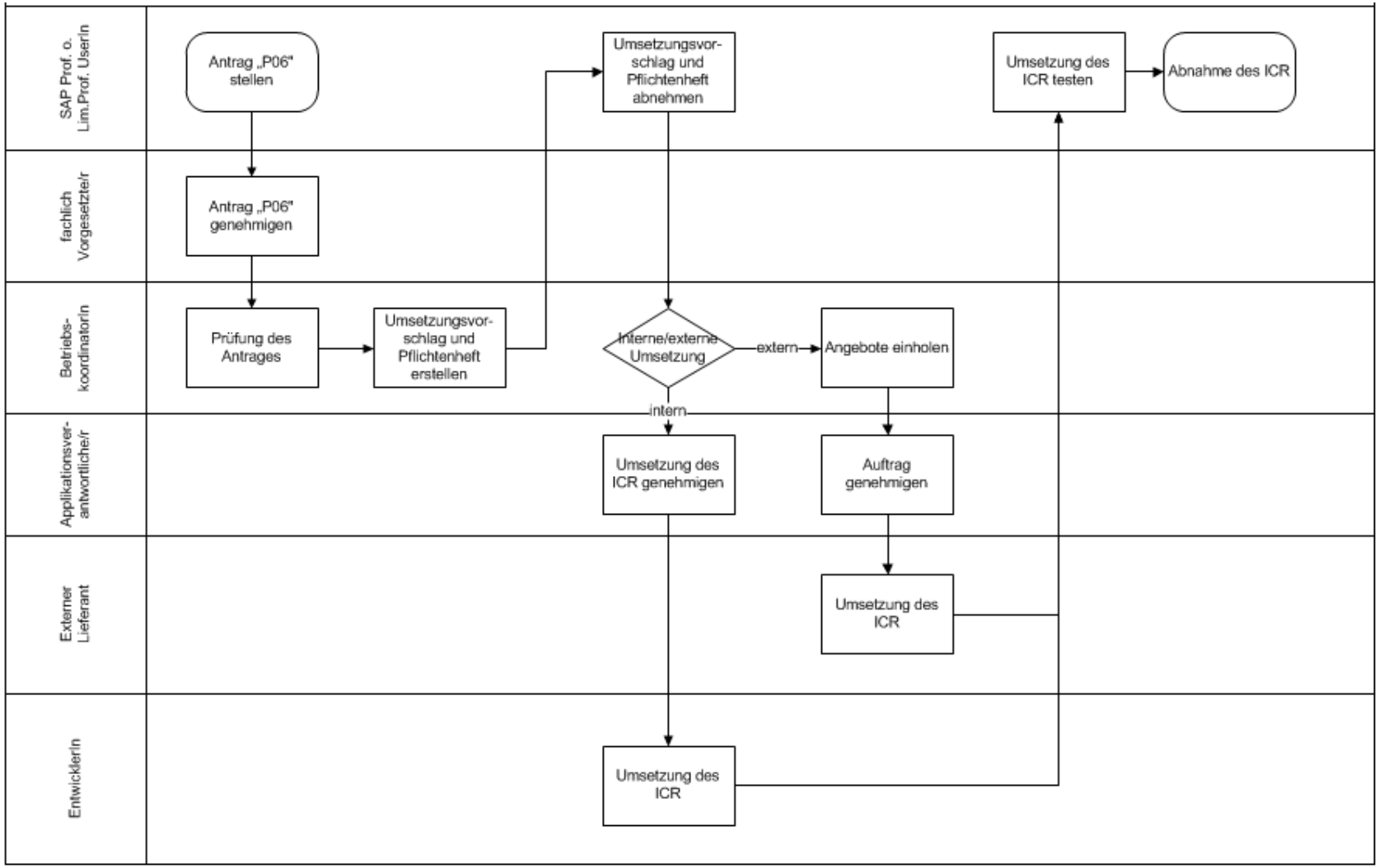
5.2.2.7 Prozess IKS7 – Rollenänderung

Dieser Prozess bezieht sich auf Punkt **2.1.3.1.4** in der Richtlinie.



5.2.2.8 Prozess IKS8 - Abwicklung Interner Change Request (ICR)

Dieser Prozess bezieht sich auf Punkt **2.2.2.1** in der Richtlinie.



5.3 Auszug aus Angebot „VPN-Anbindung“; Seite 9

2.2 Leistungsumfang

Die BRZ GmbH erbringt folgende Leistungen:

- Herstellung der VPN-Anbindung
- Betreuung und Entstörung der Infrastruktur, vom Router (inklusive) an der Universität bis zum UNISAP-Server
- Es gelten die Verfügbarkeitszeiten des definierten SLA mit der Karl-Franzens-Universität Graz; für Pönalisierungen ist allerdings nur die zentrale Messklammer maßgeblich

2.3 Leistungsabgrenzung

Es sind nur jene Leistungen Bestandteil des Angebotes, die unter Punkt 2.2 (Leistungsumfang) abschließend aufgezählt sind.

5.4 Auszug aus dem SAP Hinweis 112388 – Protokollierungspflichtige Tabellen

Gemäß dem Prüfleitfaden FI des Arbeitskreises Wirtschaftsprüfung und Revision, Deutschland, in der aktuellen Fassung sind eine Reihe von Tabellen protokollierungspflichtig.

Der Prüfleitfaden ist im Portal der DSAG unter: http://www.dsag.de/go/leitfaeden abrufbar.

Mit dem Report RDDPRCHK des Audit Informationssystems können die Einstellungen zur Tabellenprotokollierung für die folgenden Tabellen geprüft werden.

Steht das AIS bzw. der Report nicht zur Verfügung, kann man mit Transaktion SE16 für Tabelle DD09L ermitteln, bei welchen dieser Tabellen das Protokollierungskennzeichen fehlt. Dazu kann nach den folgenden Tabellen selektiert werden, wobei für das Feld PROTOKOLL auf den Wert ' ' abgegrenzt wird:

T000
T001*
T003*
T004*
T007*
T008*
T012*
T030
T033*
T042* (außer T042FSL, T042U, T042X)
T044A
T044Z
T074
T077*
T078*
T079*
T169* (außer T169O)
TACTZ
TADIR
TASYS
TBAER
TBRG
TCUR*
TDDAT
TDEVC
TSTC
TSYST

(SAP-Tabellen mit Namen T9* sind nicht protokollierungspflichtig. Mit der Transaktion SCU3 bzw. mit dem Report RSTBHIST kann man die Liste der Tabellen mit Protokollierung erstellen. Allerdings ist es damit nicht möglich, nach fehlenden Tabellen zu suchen.)

5.5 Auszug aus der Preis- und Konditionenliste für die Überlassung und Pflege von mySAP.com, Version 4.0a; Stand 2002

Auszug aus der Preis- und Konditionenliste für die Überlassung und Pflege von mySAP.com
Version 4.0a/Stand 2002
SAP Österreich GmbH

A.2.1. DEFINIERTE NUTZER

Ein Definierter Nutzer ist ein Mitarbeiter des Auftraggebers, seiner verbundenen Unternehmen oder ein Mitarbeiter von Drittunternehmen, der berechtigt ist, direkt oder indirekt auf die überlassene Software zuzugreifen.[1] (...)

C. 6. SYSTEMVERMESSUNG

(..) SAP weist darauf hin, dass der Systemzugriff mehrerer Personen als ein Definierter Nutzer unzulässig ist. Dies gilt auch für Nutzer, die indirekt auf die Software zugreifen. Soweit SAP einen solchen Verstoß gegen die vertraglichen Vereinbarungen im Rahmen der Systemvermessung bemerkt, stellt SAP als Schadensersatz den für die weitergehende Nutzung anfallenden Betrag gemäß der geltenden Preis- und Konditionenliste in Rechnung. Höherer Schadensersatz bleibt vorbehalten.[2] (...)

[1] Siehe SAP Österreich GmbH: Preis- und Konditionenliste für die Überlassung und Pflege von mySAP.com; Version 4.0a; Stand 2002; S 5
[2] Siehe SAP Österreich GmbH: Preis- und Konditionenliste für die Überlassung und Pflege von mySAP.com; Version 4.0a; Stand 2002; S 47

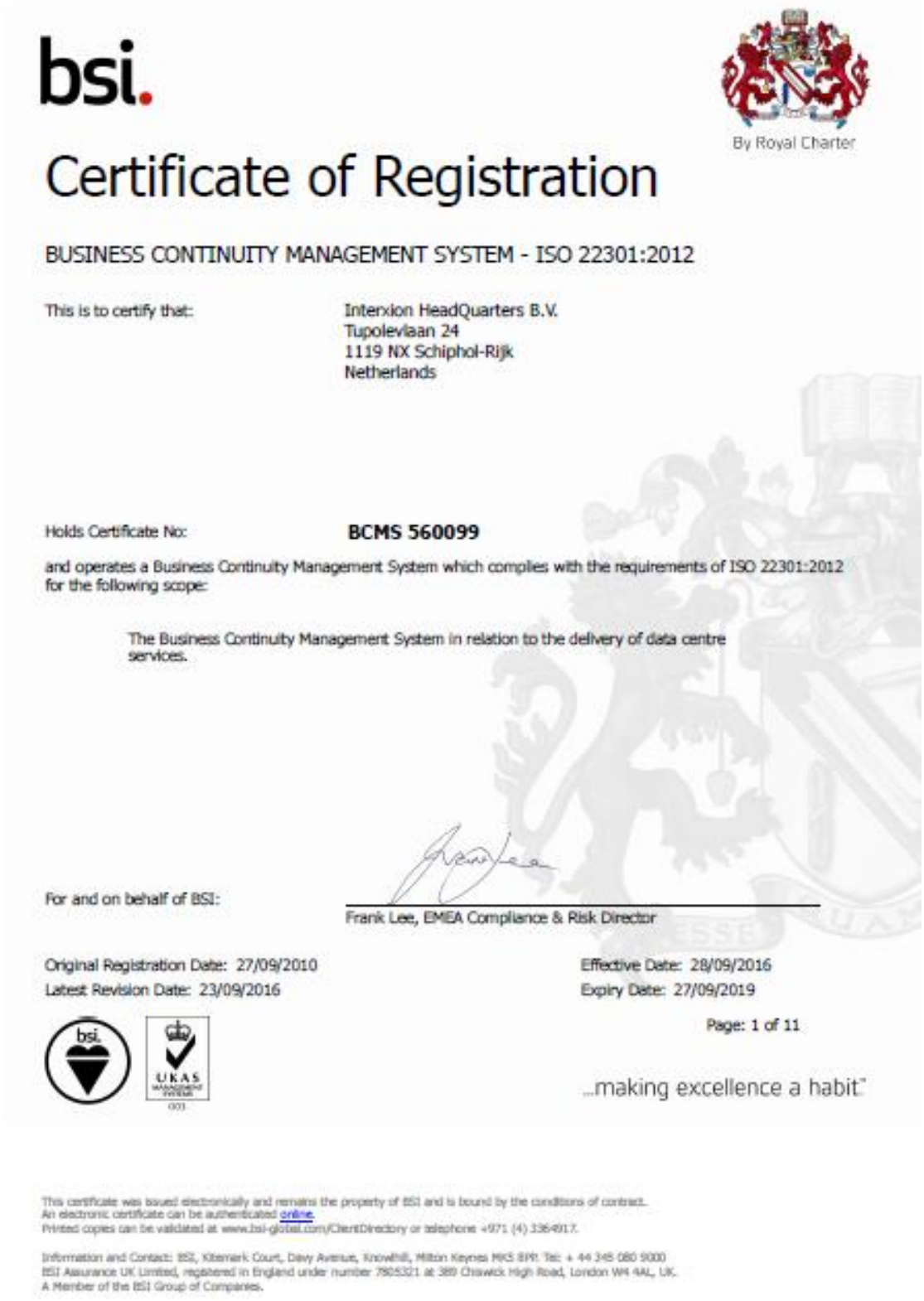
5.6 Auszug aus der Beilage ./1 zum Betriebsvertrag uni.verse, S. 50

SAP besitzt die vertraglich festgelegte Befugnis, jederzeit die Einhaltung des Nutzungsvolumens nach den Vorgaben der Preis- und Konditionenliste zur Feststellung der Vergütung für einen Zukauf zu vermessen.

Wird im Zuge einer Vermessung eine Überschreitung des Vertragswertes festgestellt, wird die entsprechende Überschreitung als Abruf zu diesem Rahmenvertrag verrechnet. Die SAP Software enthält ein Vermessungsprogramm, mit dessen Hilfe jedes System die Informationen produziert, die für die Vergütung der Installationen maßgeblich sind. Das Vermessungsprogramm dient ausschließlich zur Ermittlung der Anzahl von Nutzern und den genutzten Einheiten der SAP-Produkte. Die Ergebnisse werden entsprechend den vertraglich vereinbarten Konditionen bewertet.

5.7 Sicherheitszertifikat gem. ISO 27001 (BRZ)

5.8 Sicherheitszertifikat gem. ISO 22301 und ISO 27001 bzw. ISAE3402 (Axians ICT Austria)



bsi.

By Royal Charter

Certificate of Registration

BUSINESS CONTINUITY MANAGEMENT SYSTEM - ISO 22301:2012

This is to certify that: Interxion HeadQuarters B.V.
Tupolevlaan 24
1119 NX Schiphol-Rijk
Netherlands

Holds Certificate No: **BCMS 560099**

and operates a Business Continuity Management System which complies with the requirements of ISO 22301:2012 for the following scope:

The Business Continuity Management System in relation to the delivery of data centre services.

For and on behalf of BSI:

Frank Lee, EMEA Compliance & Risk Director

Original Registration Date: 27/09/2010
Latest Revision Date: 23/09/2016

Effective Date: 28/09/2016
Expiry Date: 27/09/2019

Page: 1 of 11

...making excellence a habit.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +971 (4) 3364917.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Der Report gem. ISO 27001 bzw. ISAE3402 liegt bei den SAP-BetriebskoordinatorInnen auf.

5.9 Formulare

Alle Formulare, deren Notwendigkeit sich aus den vorhergehenden Kapiteln ergibt, sind unter http://intranet.uni-graz.at/einheiten/SAP/Pages/formulare.aspx abrufbar.

Die Antragsformulare sind an die BenutzerInnen- und Berechtigungsverwaltung zu übermitteln und dort aufzubewahren.

Änderungen an den Formularen können nach Absprache mit der/dem Applikationsverantwortlichen durch die Betriebskoordination vorgenommen werden.