


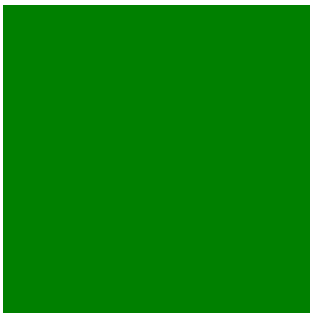

Prüfbericht 8/2013 zum Thema

Prüfung der Allgemeinen IT-Kontrollen

(Ordnungsmäßigkeitsprüfung)

STADT GRAZ STADTRECHNUNGSHOF

GZ.: StRH – 57525-2013

Graz, 18. Dezember 2013

Stadtrechnungshof der Landeshauptstadt Graz

A-8011 Graz

Kaiserfeldgasse 19

Fotos (v. links): Stadt Graz/Pichler (1, 2), Foto Fischer (3),
photo 5000 – www.fotolia.com (4)

Diesem Prüfbericht liegt der Stand der vorliegenden Unterlagen und Auskünfte bis zum 28. November 2013 zugrunde.

Inhaltsverzeichnis

Seite

1. Kurzfassung 7
2. Gegenstand und Umfang der Prüfung 9
   - **2.1. Auftrag und Überblick 9**
   - **2.2. Prüfungsziel und Auftragsdurchführung 10**
   - **2.3. Das IT-Umfeld des Hauses Graz 11**
3. Berichtsteil 14
   - **3.1. IT-Organisation 14**
   - 3.1.1. IT-Strategie und Governance 15
   - 3.1.2. Aufbauorganisation, Prozesse, Stellenbeschreibungen 16
   - 3.1.3. Zielvereinbarungen, Leistungsindikatoren 19
   - 3.1.4. Risikobewertung 20
   - 3.1.5. Schulungsplanung, MitarbeiterInnengespräche und Sachbudgetierung 22
   - 3.1.6. Reporting an das Management der ITG und an die oberste Führungsebene des Hauses Graz 24
   - 3.1.7. Systemlandschaft 26
   - 3.1.8. IT-Inventar 27
   - 3.1.9. Wartungsverträge 29
   - 3.1.10. Outsourced Services 30
   - 3.1.11. IT-Revisionen (intern/extern) 30
   - 3.1.12. IT-Richtlinien 32
   - **3.2. IT-Standardprozesse 35**
   - 3.2.1. Programmentwicklung und Programmänderungen 35
   - 3.2.2. Laufender IT-Betrieb 45
   - 3.2.3. Zugang zu Programmen und Daten 51
   - **3.3. Kontrollen im Bereich SAP-BASIS 59**
   - 3.3.1. Identifikation und Authentisierung 60
   - 3.3.2. Autorisierung 61

3.3.3. Systemintegrität 62

3.3.4. Änderungsmanagement in SAP 62

4. Beantwortung der Prüfungsfragen 63

5. Zusammenfassung der Empfehlungen 66

3.1. IT-Organisation 66

3.2. IT-Standardprozesse 67

3.3. Kontrollen im Bereich SAP-BASIS 70

6. Prüfungsmethodik 76

6.1. Prüfungsplanung und Durchführung 76

6.2. Zur Prüfung herangezogene Unterlagen 77

6.3. Besprechungen 78

Prüfen und Beraten für Graz 79

Abkürzungsverzeichnis

AD	Active Directory (Verzeichnisdienst von Microsoft Windows Server)
bzw.	beziehungsweise
BRP	Business Recovery Plan (der technische Teil eines betrieblichen Notfallwiederherstellungsplans)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Bundesrepublik Deutschland)
CIO	Chief Information Officer (Verantwortliche/r für Strategie, Planung und Betrieb von Informations- und Kommunikationstechnologie in einem Unternehmen)
COBIT	Control Objectives for Information and Related Technology (ein Rahmenwerk für IT-Governance)
COSO	Committee of Sponsoring Organizations of the Treadway Commission (Herausgeber des COSO-Modells, einem Standard für IKS)
FIPos	Finanzposition
GO	Geschäftsordnung
GZ	Geschäftszahl
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnik
INTOSAI	International Organization of Supreme Audit Institutions / Internationale Organisation der Obersten Rechnungskontrollbehörden
IS	Informationssicherheit
ISACA	Information Systems Audit and Control Association
ISKT	Informationssicherheitskompetenzteam
ISSAI	International Standards of Supreme Audit Institutions / Internationale Normen und Richtlinien für die staatliche Finanzkontrolle
IT	Informationstechnik
ITG	ITG Informationstechnik Graz GmbH
ITIL	IT Infrastructure Library
RFID	Radio-Frequency Identification

RPO	Recovery Point Objective (gibt den tolerierbaren Datenverlust an)
RTO	Recovery Time Objective (gibt den Zeitraum vom Zeitpunkt eines Schadens bis zur vollständigen Wiederherstellung an)
SAP	SAP-ERP, ein integriertes betriebswirtschaftliches Standard-softwarepaket der SAP Aktiengesellschaft
SAP-BASIS	Applikationsschicht in SAP (Umgebung, in der SAP-Programme laufen)
SLA	Service Level Agreement (Dienstgütevereinbarung / Dienst-leistungsvereinbarung)
StRH	Stadtrechnungshof
USV	unterbrechungsfreie Stromversorgung
QM	Qualitätsmanagement

FAZIT

Die bestehende Organisation des IT-Umfeldes des Hauses Graz wurde als guter Ausgangspunkt für die Umsetzung weiterer notwendiger Maßnahmen zur Stärkung des internen IT-Kontrollumfeldes angesehen.

1. Kurzfassung

Die vorliegende Prüfung beurteilte das Design und die Effektivität des internen Kontrollumfeldes des zentralen IT-Bereichs und die Kontrollen auf Applikationsebene im Bereich SAP-BASIS des Hauses Graz.

Die Prüfung wurde durchgeführt, um die Verlässlichkeit von Organisation und Systemen für die Verarbeitung rechnungslegungsrelevanter Informationen darzustellen und zu beurteilen.

Zur Beurteilung des Designs und der Effektivität des internen Kontrollumfeldes des zentralen IT-Bereichs des Hauses Graz wurden ausgewählte Schlüsselelemente eines internen Kontrollsystems aus IT-Organisation und IT-Prozessen evaluiert und geprüft. Die Ergebnisse hierzu wurden in den Kapiteln 3.1. und 3.2. dargestellt.

Zur Beantwortung der Prüfungsfrage nach der Angemessenheit der automatisierten Kontrollen im Bereich SAP-BASIS wurden ausgewählte Schlüsselelemente aus den Bereichen Identifikation und Authentisierung, Autorisierung Systemintegrität und Änderungsmanagement in SAP geprüft und die Ergebnisse und Empfehlungen in Kapitel 3.3. ausgeführt.

Der Stadtrechnungshof hob positiv hervor, dass die Strukturen der IT-Governance im Haus Graz geeignet waren, die notwendigen Abstimmung und Entscheidungen zu erzielen. Weiters waren die Qualität der vorliegenden Dokumentation der Aufbauorganisation, der Stellenbeschreibungen, der Systemlandschaft sowie die regelmäßige Beauftragung von externen Sicherheitsüberprüfungen, die der laufenden Optimierung der IT-Kontrollen dienten, als gut zu beurteilen.

Kritisch wies der Rechnungshof auf Verbesserungsbedarf in den Bereichen Programmentwicklung und Änderungsmanagement sowie bei der Verwaltung von BenutzerInnenberechtigungen hin. Hier wurde allgemein festgestellt, dass einerseits festgelegte Richtlinien nicht durchgängig eingehalten wurden und andererseits für wesentliche Bereiche noch Regelungsbedarf bestand. Weiters wies der Stadtrechnungshof kritisch auf die nicht durchgängig durchgeführte Durchführungsdokumentation von Schlüsselkontrollen sowie das Fehlen von, als wesentlich anzusehenden, Schlüsselkontrollen im Bereich SAP-BASIS hin.

Stellungname der ITG:

Zur zusammenfassenden Kritik stellt ITG fest, dass selbstverständlich auch aus Sicht der ITG im IT- Umfeld laufender Verbesserungs- bzw. Entwicklungsbedarf besteht. Zur Feststellung dieses Verbesserungsbedarfs leistet der vorliegende Prüfbericht einen wertvollen Beitrag in Bezug auf die IT-Kontrollen. Weitere Beiträge ergeben sich unter anderem aus der jährlichen Wirtschaftsprüfung der ITG, aus von ITG beauftragten Sicherheitsaudits, aus einer Prozessreifegradbestimmung anlässlich der beabsichtigten ISAE3402-Zertifizierung, aus Auftraggeberinnen-anforderungen, aus einer AnwenderInnenbefragung, aus dem ITG-Risikomanagement, aus dem Haus Graz weiten IT- Sicherheitsmanagement, aus aufgesetzten Qualitätsinitiativen sowie der laufenden strategischen und operativen IT-Steuerung. Das ermittelte Entwicklungspotenzial wird jeweils hinsichtlich seines Nutzens für das Haus Graz, seines Ressourcenbedarfs und seiner Wirkung auf die IT-Risiken bewertet. Daraus ergeben sich Prioritäten und die Einordnung in die Umsetzungsplanung. Die internen IT-Kontrollen, die den Gegenstand dieser Prüfung bilden, wirken zu Gunsten der IT- Risiken und in der Regel zu Lasten des Ressourceneinsatzes. Ein Übergewicht der Effizienzoptimierung führt zu Reduzierungen von Redundanzen und nicht direkt wertschöpfenden Prozessen und erhöht die IT-Risiken. Die Balance zu finden zwischen Risiko- und Ressourcenoptimierung ist über ein unternehmensweites Risikomanagement Bestandteil der IT- Governance.

Der vorliegende Prüfbericht betrachtet die Seite des Risikomanagements und verzichtet dabei auf Soll-Ist Betrachtungen nach Prozessreifegraden, wie sie in den IT-Referenzmodellen Standard sind.

Entgegnung des Stadtrechnungshofes:

Der Stadtrechnungshof anerkannte die ausführlichen Stellungnahmen der ITG zu diesem Bericht und bekräftigte sämtliche ausgesprochenen Empfehlungen.

Wie in Punkt 2.1 des Berichts ausdrücklich festgestellt, hatte die vorliegende Prüfung das IT-Kontrollumfeld des Hauses Graz aus der Perspektive der Verlässlichkeit von Organisation und Systemen für die Verarbeitung rechnungslegungsrelevanter Informationen zum Gegenstand. Die Beurteilung erfolgte somit danach, ob die rechnungslegungsrelevanten Informationsziele Vollständigkeit, Validität, Genauigkeit und Vertraulichkeit von Informationen sichergestellt wurden. Feststellungen und Empfehlungen wurden auf Basis von verfügbarer Evidenz für den Prüfzeitraum Jänner bis Oktober 2013 ausgesprochen. Eine entsprechende Soll-Ist Betrachtung nach

Prozessreifegraden (COBIT4.1) oder nach dem Prozessbefähigungsmodell (COBIT 5) war für die Beantwortung der Prüfungsfragen nicht vorgesehen.

Der Stadtrechnungshof begrüßte, dass zahlreiche ausgesprochene Empfehlungen entweder durch geplante Maßnahmen abgedeckt oder zumindest auf der Informationssicherheits-Themenliste des Informationssicherheitskompetenzteams aufgenommen worden waren.

Der Stadtrechnungshof befürwortete das in der Stellungnahme der ITG genannte und zuvor im Zuge der Prüfungs-Schlussbesprechung am 27. November 2013 von der Geschäftsführung der ITG angekündigte Vorgehen, die Empfehlungen in den IKT-Beirat einzubringen um dem aus Empfehlungen und Stellungnahmen dieses Berichtes ersichtlichen organisationsübergreifenden Steuerungs- und Koordinierungsbedarf zu begegnen und die Wirkung der Prüfung zu erhöhen.

2. Gegenstand und Umfang der Prüfung

2.1. Auftrag und Überblick

Die Prüfung wurde als § 3 GO-StRH Gebarungskontrolle angelegt, umfasste den Zeitraum von 1. Jänner 2013 bis 31. Oktober 2013 und sollte insbesondere folgende Prüfungsfragen beantworten:

- Sind das Design und die Effektivität des internen Kontrollumfeldes des zentralen IT-Bereiches der Komplexität und dem Risiko angemessen?
- Sind die automatisierten Kontrollen im Bereich SAP-BASIS angemessen?

Den Schwerpunkt der Prüfung bildete die Frage nach der Zweckmäßigkeit des internen Kontrollumfeldes des zentralen IT-Bereichs. Die Prüfung wurde durchgeführt, um die Verlässlichkeit von Organisation und Systemen für die Verarbeitung rechnungslegungsrelevanter Informationen darzustellen und zu beurteilen.

Bei der Prüfungsdurchführung wurde der Fokus auf den Magistrat Graz gelegt. Feststellungen und Empfehlungen konnten aber, auch wenn die Evidenz nur den Bereich des Magistrats betraf, der weiteren Verbesserung des internen Kontrollumfeldes und der SAP-BASIS Kontrollen des gesamten Hauses Graz dienen.

Im Speziellen sollte in der Prüfung und Berichterstattung auch insbesondere auf die Kriterien der Zweckmäßigkeit und Ordnungsmäßigkeit eingegangen werden.

2.2. Prüfungsziel und Auftragsdurchführung

Gemäß §2 GO-StRH oblag dem Stadtrechnungshof die Kontrolle der Gebarung der Stadt. Dies umfasste auch die Vorprüfung der Rechnungsabschlüsse, die Kontrolle von Institutionen, an denen sie beteiligt war oder die sie förderte, die Projektkontrolle und die Projektabwicklungskontrolle.

Der Stadtrechnungshof unterschied folgende Prüfungsarten (in Klammer die international definierten Prüfungsarten):

- Wirtschaftlichkeitsprüfung (performance audit)
- Ordnungs- und Rechtmäßigkeitsprüfung (financial ausdit)
- Ordnungsmäßigkeitsprüfung (compliance audit)
- Projektprüfungen
- Follow-Up-Prüfungen

Für die Durchführung dieser Prüfungen orientierte sich der Stadtrechnungshof an den INTOSAI-Richtlinien für die Finanzkontrolle. Diese international akzeptierten Standards sind Ergebnis bester Praktiken aus den Bereichen Prüftechnik, Prüfplanung und Prüforganisation. Deren Einhaltung unterstützte die Sicherung der Qualität von Empfehlungen, Stellungnahmen und Prüfurteilen des Stadtrechnungshofs.

Der für Ordnungs- und Rechtmäßigkeitsprüfungen des StRH anzuwendende INTOSAI Standard „ISSAI 1315 Erkennung und Beurteilung der Risiken wesentlicher Falschangaben durch die Gewinnung eines ausreichenden Verständnisses der Einheit und ihres Umfelds“ forderte von PrüferInnen, ein ausreichendes Verständnis über das interne Kontrollsystem und finanzinformationsrelevante IT-Systeme der zu prüfenden Entität zu erlangen. Beides war Voraussetzung für die risikobasierte Prüfungsplanung.

Weiters wurde für die Planung und Durchführung sämtlicher in der GO-StRH genannten Prüfungsarten des Stadtrechnungshofs eine Aussage über die Verlässlichkeit der IT-System generierten Informationen (Reports, Salden, Konten, Budgetaufstellungen, FIPos Details, Querschnitte, etc.) benötigt, da diese die Basis für die Beurteilung von Sachverhalten, für die Durchführung analytischer und substantieller Prüfungshandlungen und für die Berichterstellung waren.

Das interne Kontrollumfeld im IT-Bereich unterschied sich auf Grund des besonderen Geschäftsgegenstandes von dem internen Kontrollumfeld anderer Bereiche strukturell. Es war autonom organisiert und musste spezifische Bedrohungen und Risiken adressieren. Daher wurde das interne Kontrollumfeld im IT-Bereich dieser Prüfung unterzogen.

Die Zielsetzungen dieser Prüfung waren die Beurteilung

- des Designs und der Effektivität des internen Kontrollumfeldes des zentralen IT-Bereichs des Hauses Graz und
- der Kontrollen auf Applikationsebene im Bereich SAP-BASIS Haus Graz.

Nicht von der Prüfung umfasst werden sollten die folgenden Themen:

- Evaluierung und Prüfung von Funktionalitäten von SAP-Modulen außerhalb der SAP-BASIS (wie beispielsweise SAP-FI, SAP-CO, SAP-HR, etc.)
- Verarbeitung und Verbuchung von Transaktionen
- Evaluierung der Tätigkeiten der internen Revision
- rein technische Fragestellungen (z.B. Auslegung von Bandbreiten für Netzwerke)
- rechtliche Fragestellungen (z.B. im Bereich des Datenschutzes)
- inhaltliche Beurteilungen von Daten
- die inhaltliche Auswertung von Logfiles

Die Ergebnisse dieser Prüfung waren die Basis für

- die Optimierung des IT-Kontrollumfeldes,
- die risikoorientierte Prüfungsplanung der Vorprüfung des Rechnungsabschlusses,
- die Beurteilung der Verlässlichkeit IT-systemgenerierter Informationen sowie für
- vertiefende Prüfungen von IT-Systemen.

2.3. Das IT-Umfeld des Hauses Graz

Im Jahr 2010 wurden die IT-Abteilungen der Stadt Graz und der Holding Graz in der neu gegründeten ITG Informationstechnik Graz GmbH, Graz, zusammengeführt. Die ITG definierte zum Zeitpunkt der Prüfung ihren allgemeinen Aufgabenbereich auf ihrer Homepage wie folgt:

„Aufgabe der ITG ist die gebündelte Erbringung aller strategischen und operativen IKT-Aufgaben für die Stadt Graz, die Holding Graz und all deren Beteiligungen. Dies umfasst insbesondere das Design, die Entwicklung und Beschaffung, die Bereitstellung und den Betrieb von IKT-Services sowie der zugrunde liegenden IKT-Infrastruktur. Für die einzelnen Fachbereiche werden zudem Leistungen, wie AnwenderInnensupport (1st, 2nd, 3rd Level), Anforderungs- und Projektmanagement, Geschäftsprozessanalysen und -entwicklung, Print-Leistungen und vieles mehr erbracht."

Für die vorliegende Prüfung wurde der Prüfumfang des IT-Umfeldes des Hauses Graz, das ist die Stadt Graz, die Holding Graz und all deren Beteiligungen, auf folgende Bereiche, eingeschränkt:

- Aufbau- und Prozessorganisation der ITG als strategische Partnerin des Magistrats und der Holding Graz
- Organisation der Steuerung der IT-Strategie und der IT-Governance
- Richtlinien und Prozesse auf Seiten des Magistrats
- SAP-Produktivsystem des Magistrats

Stellungnahme der ITG:

Da unter „zentralem IT-Bereich“ des Hauses Graz vielfach die ITG verstanden wird, erlaubt sich die ITG die Klarstellung, dass in der Diktion des Stadtrechnungshofs der ´zentrale IT-Bereich`, wie in Kapitel 2.3. konkretisiert,

- die in gemeinsamer Verantwortung von Auftraggeberinnen und ITG liegende IT-Strategie und IT-Governance,
- Richtlinien und Prozesse der Auftraggeberinnen sowie
- die Organisation und Prozesse der ITG

umfasst.

So beziehen sich die vom Stadtrechnungshof ausgesprochenen Empfehlungen teils auf die IT- Governance, sind daher gemeinsam von Auftraggeberinnen und ITG zu bewerten, teils auf die Auftraggeberinnen alleine und sind daher an diese zu richten, teils auf die ITG. In der Stellungnahme zu Punkt 5. des Prüfberichts hat ITG eine Kategorisierung der Empfehlungen vorgenommen und die Empfehlungen, die sich auf die IT-Governance bzw. die Auftraggeberinnen beziehen, einer eigenen Kategorie zugeordnet. ITG schlägt vor, die Empfehlungen zur IT-Governance im IKT-Beirat zu behandeln, die Empfehlungen an die Auftraggeberinnen über den IKT-Beirat an die Auftraggeberinnen weiterzuleiten. Weiters wäre es aus Sicht der ITG zweckmäßig, den vorliegenden Rohbericht allen am „zentralen IT-Bereich“ Verantwortung tragenden Stellen zur Stellungnahme vorzulegen. […]

Ergänzend wird festgestellt, dass im Jahr 2010 die IT-Abteilungen der Stadt Graz und der Holding Graz rechtlich/organisatorisch zusammengeführt wurden und in der ITG am 1.1.2011 den Produktivbetrieb aufgenommen haben. Die Zusammenführung hatte das Ziel weitreichender Konsolidierung und daraus Synergiegewinnung. Die sogenannte ´Post Merger Integration`,

also

- das Konkretisieren, Weiterentwickeln und Einrichten der IT-Governance,
- das Implementieren der IT-Führungsverantwortung,
- das Weiterentwickeln und Einrichten der IT-Strukturen und -Gremien,
- die Team- und Kulturentwicklung,
- das Zusammenführen und Weiterentwickeln der Kompetenzen,
- das Entwickeln der IKT-Prozesse und der Supportprozesse,
- die Schaffung eines (Haus-Graz-weiten) IT-Risiko- und Sicherheitsmanagements,
- die Auswahl, Beschaffung und Implementierung geeigneter IT-Steuerungswerkzeuge,
- das Konsolidieren von IKT-Plattformen, wie IT-Domäne, Netzwerk, Sicherheitseinrichtungen, Server- und Storagesystemen, Backup- und Recoverysystemen, Mailsystem etc.,
- …

findet laufend und während des operativen IKT-Produktivbetriebs für das Haus Graz mit etwa 3.800 IT- und 6.000 TK-Anwenderinnen statt. Sie ist weit gediehen, aber nicht abgeschlossen. Jeder ´Post Merger Integrations`-Prozess bindet operative und insbesondere Managementkapazität, die ITG befindet sich in einer Transformationsphase und am Übergang zum Regelbetrieb.

Entgegnung des Stadtrechnungshofes

Der Stadtrechnungshof anerkannte die Herausforderungen, die sich aus der Aufgabenstellung für die ITG ergaben und auch in der IT- Governance lagen. Er war sich auch dessen bewusst, dass sich die ITG noch in einer Transformationsphase befand. Die getroffenen Feststellungen und Empfehlungen leisten – wie bereits in den zuvor wiedergegebenen Ausführungen der ITG – einen Beitrag zur erfolgreichen Bewältigung dieser Transformationsphase. Gleichzeitig wies der Stadtrechnungshof darauf hin, dass der Geschäftsführer der ITG zugleich auch die Rolle des CIO des Hauses Graz innehatte. An dieser Doppelrolle orientierte sich die Prüfung und damit auch die Definition der „geprüften Stelle“ für die Einholung der Stellungnahme gemäß ISSAI 4100 Ziffer 152.

3. Berichtsteil

3.1. IT-Organisation

Die Organisation der IT bestimmte die grundlegende Organisationsstruktur und beinhaltete tangible Elemente wie beispielsweise die Aufbauorganisation, aber auch Intangibles wie Organisationskultur, Integrität und ethische Werte, Fehlerkultur sowie Risikobewussten der MitarbeiterInnen. Die Organisation der IT sollte einen geeigneten Rahmen für die Sicherstellung der rechnungslegungsrelevanten Informationsziele:

- Vollständigkeit
- Validität
- Genauigkeit
- Sicherstellung der Vertraulichkeit von Informationen

bieten. Die Qualität der IT-Organisation, als eine „weiche“ Größe, konnte nicht direkt gemessen werden. Vielmehr waren für die Beurteilung unterschiedlichste Prüfhandlungen, deren Ergebnisse nur in der Zusammenschau eine wertende Aussage zuließen, notwendig.

Es wurden Schlüsselelemente der IT-Organisation ausgewählt, die geeignet waren indikativ über das Design und die Effektivität des internen Kontrollumfeldes des zentralen IT-Bereichs des Hauses Graz Auskunft zu geben.

Im vorliegenden Fall wurden Schlüsselelemente der IT-Organisation, als anwendungsunabhängige Kontrollen, durch jeweils zwei Erhebungsschritte beurteilt:

1. Beurteilung der dokumentierten bzw. undokumentierten Praxis gegen Referenzmodelle. Dieser Schritt zielte auf die Prüfung der Effektivität von organisatorischen Maßnahmen ab.
2. Überprüfung der Einhaltung der dokumentierten bzw. undokumentierten Praxis. Dieser Schritt zielte auf die ordnungsgemäße Durchführung organisatorischer Maßnahmen ab.

Stellungnahme der ITG:

Wie vom Stadtrechnungshof in Kapitel 2.2 ausgeführt, unterscheidet sich das interne Kontrollumfeld im IT-Bereich strukturell von anderen Bereichen. Während das auf die Organisationseinheit bezogene interne Kontrollsystem (IKS) der ITG primär die Geschäftsrisiken der ITG adressiert und der jährlichen Wirtschaftsprüfung unterliegt, adressiert das vom Stadtrechnungshof geprüfte IT-Kontrollumfeld Risiken, die primär den Auftraggeberinnen durch

Anwendung der IT-Systeme entstehen. Die Anwendung der IT-Systeme setzt die Erfüllung der in Kapitel 2.3 angeführten ITG-Aufgaben sowie die Erfüllung von Auftraggeberinnen-Aufgaben voraus. Praktisch jeder Schritt der zur Aufgabenerfüllung erforderlichen Prozesse ist mit Risiken verbunden. Die Maßnahmen zur Risikosteuerung werden daher differenziert gesetzt. Die Basis und zugleich wirksamste wie effizienteste Form bilden intuitive Kontrollen kompetenter und verantwortungsbewusster MitarbeiterInnen in Verbindung mit verantwortungsbewusster Führungsarbeit. In unterschiedlichen Reifegraden implementierte Prozesse sowie prozesssteuernde und prozessbegleitende IT-Werkzeuge, wie das von ITG eingesetzte IT-Servicemanagement-Tool Omnitracker ermöglichen eine dokumentierte Praxis bei geringerer Risikobereitschaft. Die Beurteilung der Angemessenheit gesetzter bzw. zu setzender Maßnahmen muss aus Sicht von ITG zusätzlich zur Risikobewertung auch die Ressourcenverfügbarkeit sowie daraus abgeleitete Sollreifegrade berücksichtigen.

3.1.1. IT-Strategie und Governance

Die Anforderung an die IT-Strategie war, dass diese aus der Strategie des Hauses Graz abgeleitet war. Es war sicherzustellen, dass in geeigneter Form die IT-Strategie laufend zur Strategie des Hauses Graz abgestimmt wurde. Das IT-Budget sollte in diesem Sinn aus der IT-Strategie ableitbar sein. Hierfür war ein geeigneter Prozess einzurichten.

Die Risiken einer fehlenden oder mangelhaften Abstimmung der IT-Strategie mit der Strategie des Hauses Graz bestanden in einer mangelhaften IT-Unterstützung der Prozesse des Hauses Graz, einer mangelhaften IT-Unterstützung steuerungsrelevanter Informationen sowie in Fehlinvestitionen im Bereich IT.

Im Zuge der Prüfung wurde erhoben, dass innerhalb des Hauses Graz die ITG mit der Erbringung aller strategischen IKT-Aufgaben betraut war. Die Verbindung der IT-Strategie mit der Strategie des Hauses Graz erfolgte durch zwei Gremien:

- Der IKT-(Kunden-)Beirat, bestehend aus VertreterInnen des Magistrates und der Graz Holding, bildete das Gremium für die verbindlichen Vorgaben der AuftraggeberInnen gegenüber der ITG Informationstechnik Graz GmbH. Der Beirat beschloss die IT-Strategie, die Organisation der Aufgabenerbringung und legte die Preise der IT-Services fest.
- Das IKT-Board setzte sich aus allen AuftragsmanagerInnen, die in einem Vertragsverhältnis zur ITG standen, und Vertretern der ITG zusammen. Das IKT-Board hatte die Aufgabe, Problemstellungen, die nicht auf Ebene eines Auftragsmanagements gelöst werden konnten im Konsens zu lösen. War eine Lösung im Konsens nicht möglich, so musste der Punkt für eine Diskussion und Entscheidung im IKT-Kunden-Beirat vorbereitet werden.

Eine der initialen Aufgaben des IKT-Boards war es, sich selbst Statuten zu geben, die organisatorischen Rahmenbedingungen klar abzustecken und die Aufgaben schärfer zu definieren.

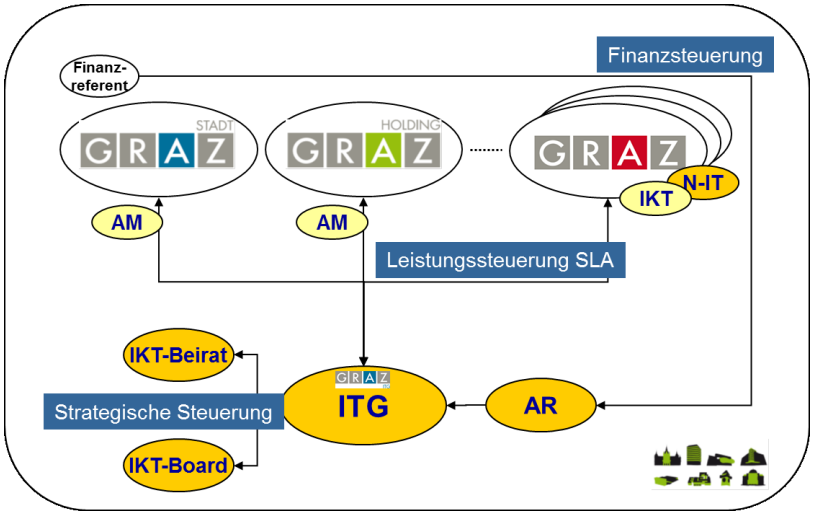

Abbildung 1 - Einbettung der ITG in die Organisation des Hauses Graz (Quelle: ITG)

Der Stadtrechnungshof zog den Schluss,

- dass die eingerichteten Strukturen der IT-Governance im Haus Graz geeignet sind, die notwendigen Abstimmung und Entscheidungen zu erzielen.

Stellungnahme der ITG:

Bezüglich der Strukturen der IT-Governance erwähnt ITG einschränkend, dass die Strukturen der IT- Governance im Haus Graz mit den drei Steuerungsebenen

- Finanzsteuerung (Finanzreferenten/Finanzdirektion),
- Leistungssteuerung (Auftraggeberinnen),
- Strategische Steuerung (IKT-Beirat)

noch keinen widerspruchsfreien Regelkreis bilden und ITG eine diesbezügliche Evaluierung mit den Beteiligten beabsichtigt.

3.1.2. Aufbauorganisation, Prozesse, Stellenbeschreibungen

Die Anforderung an die Aufbauorganisation war das Vorliegen einer vollständigen und aktuellen Dokumentation. Die Verantwortlichkeitsbereiche (fachlich,

budgetär, personell) mussten für sachkundige Dritte aus dieser nachvollziehbar sein. Wesentliche Prozesse hatten dokumentiert vorzuliegen, um Verantwortlichkeiten, Prozessbeginn und -ende sowie Schlüsselkontrollen darzustellen. Aktuelle Stellenbeschreibungen als Dokumentation von Aufgaben, Verantwortungsfeldern, notwendigen Qualifikationen und Vertretungsregelungen wurden ebenfalls als Prüfkriterium angesehen.

Zum Zeitpunkt der Prüfung lag ein Organigramm der ITG mit Stand 14. Mai 2013 vor, das Verantwortungsbereiche sowie die MitarbeiterInnenzuordnung dokumentierte. Weiters lag eine Prozesslandkarte der ITG auf Basis der ITIL-Prozesse vor. Kritische IT-Prozesse waren nicht detailliert dokumentiert. Aktuelle und umfassende Stellenbeschreibungen der ITG waren vorhanden.

Im Zuge der Prüfung wurde festgestellt, dass die kritische Rolle des zentralen IKT Auftragsmanagements im Magistrat ausschließlich von einem Mitarbeiter wahrgenommen wurde und für diesen trotz Notwendigkeit keine erkennbaren Maßnahmen zur Nachfolgeplanung vorlagen.

Der Stadtrechnungshof zog den Schluss,

- dass die vorliegende Dokumentation der Aufbauorganisation der ITG sowie die vorliegenden Stellenbeschreibungen der ITG die gestellten Anforderungen übertreffen.

Der Stadtrechnungshof empfahl,

- die Prozessdokumentation der ITG für kritische IT-Prozesse unter besonderer Berücksichtigung von Schlüsselkontrollen durch die Erstellung von Detailprozessen zu ergänzen;

Stellungnahme der ITG:

Die ITG hat ihre im Einsatz befindlichen Schlüsselprozesse detailliert dokumentiert. Die Prozessdokumentationen sind einerseits im Prozessmanagementwerkzeug Adonis abgebildet bzw. im Servicemanagementwerkzeug Omnitracker, wenn es sich um spezielle ITIL-Prozesse handelt. Folgende detaillierte Prozessbeschreibungen sind vorhanden:

- *Beschaffungsprozess* (in Vorbereitung ergänzend Lizenzmanagement) Durchgängiger Prozess von der Kundenanforderung, über den Einkauf in der ITG, die Auslieferung der IT-Güter und Leistungen an die KundInnen, bis hin zur Rechnungsabwicklung in der ITG und die Fakturierung an die KundInnen. Darstellung in Adonis.

- *Entsorgung von IKT-Geräten und Datenträgern*
  Behandelt die sachgerechte Entsorgung von IT-Geräten mit Fokus auf die Herstellung der Datensicherheit (dabei handelt es sich um die sachgerechte, nachvollziehbare Vernichtung der physischen Datenträger). Darstellung in Adonis.
- *Incidentmanagement* (Incidents und Serviceanfragen)
  Behandelt die Störungen und Anfragen der KundInnen der ITG von der Problemaufnahme über die ITG Serviceline, über die Bearbeitung der Fälle (über alle erforderlichen Bereiche hinweg) bis hin zur Lösung der Probleme und Anfragen. Darstellung und technische Umsetzung in Omnitracker.
- *Changemanagement* (Projekte, Kleinprojekte, Betriebschanges)
  Das Changemanagement behandelt die Dokumentation von Neueinführungen und Änderungen an IT-Systemen. Die entsprechenden Ziele, Planungen und Aktivitäten werden dabei in Form von Projekten, Kleinprojekten und Betriebschanges dargestellt. Darstellung und technische Umsetzung in Omnitracker.
- *Configurationmanagement* (Client-Geräte, Drucker, Tablets, Server, künftig: Netzwerkkomponenten, Smartphones)
  Das Configurationmanagement behandelt die Verwaltung der im Haus Graz eingesetzten IT- Güter. Für jedes IT-Gut wird damit der Life-Cycle von der Beschaffung des Gerätes, der Einsatzgebiete des Gerätes über den Life Cycle hinweg bis zur Ausmusterung nachvollzogen. Derzeit sind folgende IT-Güter im System: Client-Arbeitsplätze, Monitore, Drucker, Notebooks, Tablets, Server und Peripheriegeräte, wie Beamer, VPN-Token Cards. Als weiteres ist geplant auch die Netzwerkkomponenten, wie z.B. Switches, Router, sowie Smartphones in das System zu integrieren. Darstellung und technische Umsetzung in Omnitracker.
- *Problemmanagement*
  Das Problemmanagement behandelt die Analyse und Behebung von aufgetretenen Problemen beginnend von der Problemerkennung (oft über Fehlermeldungen im Incidentmanagement), die Analyse der Fehler bis hin zur endgültigen Behebung und Dokumentation. Darstellung und technische Umsetzung in Omnitracker.
- *Knowledgemanagement*
  Umfasst die Behandlung und Bereitstellung des Wissens in der ITG. Im Zuge der Aufgabenerfüllung sammelt sich Wissen bei den jeweils beteiligten Personen an. Um dieses Wissen auch allen anderen MitarbeiterInnen der ITG zur Verfügung zu stellen, schafft dieser Prozess die Möglichkeiten, das Wissen zu kategorisieren, zu prüfen und strukturiert darzustellen. Dies trägt zur Verminderung des in der IT

generell hohen Risikos der ´Single- Know-how`-Stellen bei. Darstellung und technische Umsetzung in Omnitracker.

Der Incidentmanagementprozess wird mit Fokus auf die ITG Serviceline periodisch intern geprüft, um auch die vertraglichen Verpflichtungen zum externen Partner überprüfen und kontrollieren zu können. Für 2014 ist vorgesehen, das Reviewing weiterer Prozesse zu beginnen. Die Weiterentwicklung der IKT-Prozesse zur Erreichung der jeweiligen Soll-Reifegrade ist ein kontinuierlicher Prozess jeder IT-Organisation. Die ITG hat mit Einrichtung der ITG die Kernprozesse neu definiert, die kontinuierliche Weiterentwicklung erfolgt plangemäß.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung. Die in der Stellungnahme erwähnten zusätzlichen Dokumente wurden weder im Rahmen der Prüfung noch bei der Schlussbesprechung vorgelegt. Sollten diese Dokumente in ausreichender Qualität vorhanden und wirksam sein, ging der StRH von der Umsetzung dieser Empfehlung aus.

Der Stadtrechnungshof empfahl,

- bei kritischen Rollen die Konzentration des gesamten Wissens auf einzelne MitarbeiterInnen zu vermeiden und eine abgestimmte Nachfolgeplanung zu betreiben.

Stellungnahme der ITG:

Aus dem Fließtext des vorliegenden Prüfberichts geht hervor, dass der Anlass für diese Empfehlung durch die Situation des Auftragsmanagements des Magistrats gegeben ist, sich daher auf die AuftraggeberInnen bezieht. Allerdings merkt ITG an, dass ´Single-Know-how`-Situationen im IT- Bereich aufgrund der Wissensspezialisierung unvermeidbar sind und auch in der ITG Risiken darstellen. Insbesondere wird ITG durch die restriktive Finanzsteuerung gezwungen, Redundanzen, die risikomindernd wirken, zu minimieren. Dem Risiko begegnet ITG teilweise dadurch, dass kritisches Systemwissen zusätzlich von externen Partnern getragen wird.

3.1.3. Zielvereinbarungen, Leistungsindikatoren

Das Prüfkriterium war die Existenz von Zielvereinbarungen und dazugehörenden Indikatoren, die sicherstellten, dass IT-Investitionen Wertbeiträge leisteten und die Erfüllung vereinbarter Ziele beurteilbar wurde.

Die Steuerung der IT-Governance erfolgte über den ITK-Beirat und das ITK-Board. Die ITG war in das Steuerungsmodell Graz eingebunden. Laut Steuerungsmodell Graz hatten Wirkungs- und Leistungsziele mit Messindikatoren hinterlegt zu werden. Im Zuge der Erhebung zeigte sich, dass neben den Zielvereinbarungen und Leistungsindikatoren des IT-Governance Rahmendokumentes und den abgeschlossenen SLAs innerhalb der ITG keine weiteren Zielvereinbarungen und Leistungsindikatoren zur Steuerung verwendet wurden. Diese Praxis erschien den Anforderungen angemessen.

3.1.4. Risikobewertung

Die Risikobewertung hatte die Ermittlung und Analyse interner und externer IT-naher Risiken im Hinblick auf die Erreichung der Ziele des Hauses Graz zu umfassen.

Es lag eine umfassende Risikolandkarte für die ITG vor. Die Risikolandkarte bildete Risiken der bzw. für die ITG ab. So wurde beispielsweise die Gefahr von Verlust der Vertraulichkeit auf Grund der falschen Vergabe von Benutzerrechten nur mit dem Risiko der falschen Umsetzung einer Berechtigungsänderungsanforderung verbunden, nicht aber mit dem Risiko einer falschen oder fehlenden Anforderung. Der Eintritt dieses Risiko konnte allerdings in der gezogenen Stichprobe (siehe Kapitel 3.2.3.) nachgewiesen werden, wurde aber im vorliegenden Dokument nicht adressiert, da es sich außerhalb des direkten Einflussgebiets der ITG befand. Aus der Risikobewertung wurden Maßnahmen abgeleitet. Bei Einsichtnahme zeigte sich, dass in der aktuellen Version sehr allgemeine Maßnahmen, wie beispielsweise "Konzept erstellen", genannt wurden. Für die Überwachung der Umsetzung der Maßnahmen wurde das QM der ITG als verantwortliche Rolle zugewiesen.

Der Stadtrechnungshof empfahl,

- in der Risikolandkarte IT-relevante Gefahren für das gesamte Haus Graz abzubilden.
- die Bewertung der Risiken und Ableitung von Maßnahmen aus einer Gesamtperspektive des Hauses Graz organisationsübergreifend festzulegen.
- identifizierte Maßnahmen klar und spezifisch zu formulieren, Verantwortlichkeiten und Termine festzulegen und zentral zu überwachen sowie in den Reportingprozess an das Management einfließen zu lassen.

Stellungnahme der ITG:

Das Informationssicherheitsmanagement/Risikomanagement (ISMS/RM) steuert und kontrolliert nachhaltig alle Maßnahmen, Verfahren und Regeln zur Sicherheit der IT. Es steuert die Vertraulichkeit, die Konsistenz und die Verfügbarkeit der Unternehmensdaten.

Wesentlich für die Bewertung von Maßnahmen ist dabei die Verknüpfung von IT-Risiken mit Unternehmensrisiken. Das ISMS/RM deckt folgende Aufgabenbereiche ab:

- Alle IT-Risiken systematisch erfassen und bewerten.
- Alle aktuellen Maßnahmen und Ziele, für die IT-Sicherheit relevant ist, in einer einfachen Darstellung festlegen. Die eigenen Sicherheits-Ziele und die Umsetzungsreihenfolge werden dabei vom Unternehmen selbst festgelegt. Die Messgrößen sind dabei die Reifegrade von Prozessen, welche IT- Sicherheit herstellen.
- Eine Organisation (Rollen und Prozesse) aufbauen, die sicherstellt, dass die Maßnahmen kontrolliert und gesichert überarbeitet werden.
- Die IT-Kontrollen stellen dabei sicher, dass Maßnahmen tatsächlich durchgeführt und gegebenenfalls verbessert werden.

Für die ITG besteht ein derartiges ISMS/RM und bewertet die Risiken nach dem BSI-Grundschutzkatalog. Das System umfasst jene Risiken, auf die die ITG durch Maßnahmen in ihrem Bereich selbst Einfluss auf Eintrittswahrscheinlichkeit und Schadenshöhe hat.

Da es in der Holding bereits ein Risikomanagement gibt und dort auch IT-Risiken eingetragen sind, wurden diese in das ISMS/RM der ITG übernommen und nachvollziehbar auf die vorhandenen Risikoklassen abgebildet.

Im Rahmen der Aktivitäten des ISKT (Informationssicherheits-kompetenzteam), das aus VertreterInnen des Magistrats, der Holding und der ITG besteht und, wie in der Informationssicherheitspolitik beschrieben, als auftragsgeberinnenseitiges Gremium für das Informationssicherheitsmanagement im Haus Graz zuständig ist, ist die Erarbeitung einer Richtlinie für ein Haus Graz weites Informationssicherheits-/Risikomanagement geplant, sodass die Unternehmens- und ITG-Anforderungen für ein solches System aufeinander abgestimmt werden. Folgende zwei Überlegungen werden dabei berücksichtigt:

- Nicht auf alle Bedrohungen der Umwelt muss im Unternehmen mit

allen Mitteln reagiert werden, da einzelne Bedrohungen kein (oder ein akzeptierbares) Risiko darstellen.

- Nicht auf alle Bedrohungen, die im Unternehmen einen Schaden herbeiführen können, kann sofort geantwortet werden, da solche Reaktionen zu finanziellen oder organisatorischen Aufwänden führen, die im Kontext mit dem erwarteten/möglichen Schaden zu sehen sind.

Siehe dazu die Informationssicherheits-Themenliste des ISKT:

26	IS-Risikomanagement	IS-Richtlinie zum IS-Risikomanagement im Haus Graz schaffen (welcher Ansatz wird gewählt, welche Schutzbedarfskategorien, Vorgehensweise, Vorlagen etc.)

Die Empfehlung, identifizierte Maßnahmen spezifischer zu formulieren, mit Terminen zu versehen und zu überwachen, wird in die kommende Überarbeitung des ISMS/RM der ITG aufgenommen.

3.1.5. Schulungsplanung, MitarbeiterInnengespräche und Sachbudgetierung

MitarbeiterInnen spielten für die Qualität des IT-Umfelds eine zentrale Rolle. Daher waren insbesonders die Förderung von fachlicher Kompetenz und die Förderung der Integrität als Anforderungen zu stellen. Als Prüfkriterien wurden periodisch durchgeführte MitarbeiterInnengespräche, vereinbarte individuelle Zielvereinbarungen, die Erhebung des Fortbildungsbedarfs und die Erstellung individueller Bildungspläne innerhalb der ITG angesetzt. Die Schulung von IT-Nutzern, besonders unter dem Aspekt der Bewusstseinsbildung für IT-Risiken (Risk-Awareness) stellte ebenfalls eine Anforderung dar.

Zum Zeitpunkt der Prüfung wurden keine verpflichtenden, strukturierten MitarbeiterInnengespräche in der ITG durchgeführt. Hierzu war eine Einführung im ersten Quartal 2014 geplant. Die Planung von Schulungsmaßnahmen erfolgte jährlich durch die AbteilungsleiterInnen in Abstimmung mit den MitarbeiterInnen. Das Qualitätsmanagement sammelte diese Vorschläge und bereitete die Entscheidung der Geschäftsführung vor. Teilnahmebestätigungen wurden dokumentiert. Regelmäßige Risk-Awareness-Trainings für IT-BenutzerInnen fanden nicht statt.

Der Stadtrechnungshof empfahl,

- wie von der ITG geplant, strukturierte MitarbeiterInnengespräche einzuführen;

Stellungnahme der ITG:

Die Einführung von strukturierten MitarbeiterInnengesprächen wurde in der ITG im letzten Quartal 2013 gestartet und wird mit 1. Quartal 2014 auf alle Bereiche ausgeweitet. Die entsprechenden Vorlagen und Vorgehensweisen zur einheitlichen Behandlung dieses Themas in der ITG wurde von der Personalentwicklung der ITG zusammen mit den BereichsleiterInnen erarbeitet und abgestimmt.

Der Stadtrechnungshof empfahl,

- regelmäßige Risk-Awareness-Trainings für IT-BenutzerInnen im Haus Graz zu veranstalten.

Stellungnahme der ITG:

Da die Risk-Awareness weit über die Informationstechnik hinausreicht, liegt diese Entscheidung bei den Auftraggeberinnen und wurde die Thematik vom ISKT bereits aufgenommen. Um ein einheitliches Vorgehen im Haus Graz zu erreichen und mögliche Synergien zu nutzen, ist die Entwicklung eines Haus-Graz-weiten Vorgehens vorgesehen. Die ITG wird sich mit ihren MitarbeiterInnen einerseits den allgemein im ISKT entwickelten Trainings anschließen und andererseits für die speziellen Rollen im IKT-Bereich eigene, tiefer gehende Informationssicherheits- Trainings vorschreiben.

Siehe dazu die Informationssicherheits-Themenliste des ISKT:

30	Datenschutz	Einrichtung einer Datenschutz-Intranetseite (Wartung durch DS- Beauftragten)
17	Datenschutz	Datenschutzschulung gem § 14(2)3. DSG2000 Ist jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren.
18	Bewusstseinsbildung / Einschulung von MitarbeiterInnen	Sensibilisierungsprogramm zur IT-Sicherheit (S. 60) - Folder, News, Mail bzw. als Block in DPK, Einführungstag bzw. 3-Stufen-Modell zur MA-Sensibilisierung Holding (ISP, MA-Information in Form einer leicht verständlichen RL, IS-RL)
19	Bewusstseinsbildung / Einschulung von MitarbeiterInnen	Ähnlich dem Korruptionstest einen verbindlichen Test (e-learning) zur praktischen Datensicherheit (elektronisch und Papier)

Die IT-Budgetierung wurde durch die ITG-Geschäftsführung auf Basis einer bottom-up-Planung erstellt und war in das Grazer Steuerungsmodell eingebunden.

3.1.6. Reporting an das Management der ITG und an die oberste Führungsebene des Hauses Graz

Die Anforderung nach strukturierter Information und Kommunikation über den IT-Betrieb und IT-Projekte als Basis für die Festlegung von Zielen, die Überwachung der Zielerreichung sowie die zugehörige Berichterstattung hatte Grundlagen für Entscheidungen gewährleisten sollen. Operative IT-Messgrößen hatten aus zugesicherten Service Levels und strategischen IT-Messgrößen aus der Gesamtstrategie des Hauses Graz abgeleitet werden sollen.

Zum Zeitpunkt der Prüfung wurde die Geschäftsführung der ITG in regelmäßigen Besprechungen des ITG Führungsteams mit niedriger Strukturierung über laufende Agenden informiert. Ein regelmäßiger Statusreport über sämtliche laufende Projekte („Project-Dashboard“) befand sich in Planung.

Der Informationsfluss zwischen ITG, Magistrat und Holding sowie zum ITK-Beirat erfolgte ebenfalls durch regelmäßige Sitzungen. Zu den Sitzungen wurden im Zuge der Prüfung durch den Stadtrechnungshof stichprobenweise Protokolle eingesehen.

Der Stadtrechnungshof empfahl,

- die Umsetzung eines standardisierten periodischen Reportings über zu definierende operative und strategische Messgrößen.

Stellungnahme der ITG:

Ein standardisiertes periodisches Reporting über die finanziellen Messgrößen ist eingerichtet. Ein umfassendes Kennzahlensystem, insbesondere zur Beurteilung der Kostenstrukturen der IKT- Prozesse und IKT-Produkte im Haus Graz ist eingerichtet und dient als Basis für ein jährliches Benchmarking mit vergleichbaren deutschen und österreichischen Städten im Rahmen eines KGSt-Vergleichrings. Kennzahlen über die Leistung des ITG-Servicemanagement (Lösungsraten, Lösungsbereiche, Incidentschwerpunkte, …) werden standardisiert periodisch ausgewertet. Das von der ITG eingesetzte Servicesteuerungswerkzeug ermöglicht umfangreiche Auswertungen über alle an die ITG-gestellten Anforderungen, die bedarfs- und zielgruppengerecht abgerufen werden. Auswertungen über System-und Servicezustände werden im Anlassfall dem von der ITG eingesetzten

Monitoringwerkzeug entnommen. Laufendes periodisches Reporting in teils bewusst weniger strukturierter Form erfolgt in den eingerichteten Führungs- und Steuerungsgremien, wie ITG- Führungsteam, Change Advisory Board, Beirat, Aufsichtsrat. Eine Weiterentwicklung des Reportings, insbesondere in Richtung eines Dashboards, wird plangemäß erfolgen.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigt der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Der Stadtrechnungshof empfahl,

- die Umsetzung des geplanten „Project-Dashboards" in dem sämtliche laufenden Projekte monatsaktuell aufgelistet sind.

Stellungnahme der ITG:

Die ITG nutzt für das Management von Projekten die Werkzeuge Omnitracker (OT) und SAP. Alle Änderungen (Technische-Changes, Betriebs-Changes, Klein-Projekte und Projekte) werden im OT geführt. Die kaufmännische Abwicklung für Klein-Projekte und Projekte erfolgt im SAP. Das Managen dieser Änderungen erfolgt über ein eigens dafür eingerichtetes Change Advisory Board (CAB). Das ist besetzt durch Personen aus dem Business Management (BM), dem Projekt Management (PM) und IT-Services (ITS) und tagt monatlich.

Ein Request for Change (RfC) ist eine Anfrage an das Change Management, eine Änderung oder Erweiterung in der IT-Umgebung vorzunehmen. Hierbei kann es sich um eine beliebige Veränderung eines oder mehrerer Komponenten handeln. Ein interner RfC kann beispielsweise die Einrichtung einer neuen Serverlandschaft beinhalten, ein externer RfC für Kunden z.B. die Einrichtung oder Veränderung eines Intranets, die Entwicklung einer Applikation, etc.

Arten von Changes In Anlehnung an die aus ITIL bekannten Change-Typen wurden in der ITG vier eigene RfC-Typen definiert:

- Projekte
- Kleinprojekte,
- Betrieb-Changes
- Technische-Changes

Dokumentation im OT

Alle notwendigen Daten zur Steuerung von RfCs werden im OT geführt. Beispielhaft sind folgende Daten angeführt:

- ITG ProjektleiterIn
- Kunden ProjektleiterIn
- Zeitziele (Beginn Datum, Ende Datum)
- ITG Plan Stunden
- ITG Ist Stunden
- Status (Planung, Entwicklung, Implementierung, etc.)
- Dokumente für die Abwicklung (Angebote, Abnahmeprotokolle, etc.)

Dokumentation im SAP

Die kaufmännische Abwicklung erfolgt mittels SAP. Jedes Klein-Projekt bzw. Projekt wird im SAP- System als Kostenträger abgebildet (CO-Innenauftrag). Diesem Kostenträger werden alle externen Kosten (Dienstleistung, Material, etc.)zugeordnet. Nach Abnahme des Projekts durch die Kunden-ProjektleiterIn erfolgt die Fakturierung. Die Erlöse werden ebenso dem Kostenträger zugeordnet.

Projektcontrolling

Die dargestellte Abbildung der Klein-Projekte und Projekte im OT und SAP erlaubt der ITG somit ein tagaktuelles Reporting aller RfCs.

Project-Dashboard

Die Durchsprache aller RfCs erfolgt im monatlichen CAB-Meeting. Grundlage für diese Durchsprache sind die tagaktuellen Daten aus den Werkzeugen OT und SAP.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

3.1.7. Systemlandschaft

Als Anforderung wurde das Vorliegen einer übersichtlichen Darstellung der Systemlandschaft (Server, Programme, Schnittstellen, Netzwerk) festgelegt. Wesentliche Elemente, wie beispielsweise Firewalls oder Switches, hatten detailliert dokumentiert zu sein.

Dem Stadtrechnungshof wurde eine ausführliche und übersichtliche

Dokumentation der Systemlandschaft im Intranet der ITG zur Einsicht gegeben. Im Zuge der Einsichtnahme stellte sich heraus, dass die Dokumentation neben Übersichtsdarstellungen und Konzeptbeschreibungen auch aktuelle technische Daten und Konfigurationseinstellungen, die für die Aufrechterhaltung des laufenden Betriebs notwendig waren, beinhaltete. Der Zugriff auf die Dokumentation spezifischer sicherheitsrelevanter Informationen war laut Aussage der zuständigen MitarbeiterInnen durch logische Kontrollen restriktiv eingeschränkt.

Der Stadtrechnungshof zog den Schluss,

- dass die Dokumentation der Systemlandschaft, insbesonders die Dokumentation der kritischen Netzwerkinfrastruktur die Anforderungen vollkommen erfüllte und Vorbildwirkung besaß.

3.1.8. IT-Inventar

Die Anforderung war ein vollständiges und richtiges Inventar der IT-Hardware und IT-Software. Dies war für den geordneten laufenden Betrieb, als Basis von Risikobeurteilungen sowie für das Life-Circle-Management der IT-Investitionen notwendig.

Zum Zeitpunkt der Prüfung wurde das Hard- und Software Inventar im Anlageverzeichnis als Nebenbuch des Rechnungswesens geführt. Hierzu wurden vom Stadtrechnungshof keine Prüfhandlungen gesetzt, da dies nicht Teil des Prüfauftrages war. Weiters wurde die IT-Hardware, mit Ausnahme der Netzwerktechnik, zusätzlich in einem eigenen IT-Verwaltungswerkzeug verwaltet. Zwischen dem Nebenbuch und dem IT-Verwaltungswerkzeug gab es keine elektronische Schnittstelle, somit wurden beide Systeme parallel gepflegt. Für IT-Software lag kein vollständiges Verzeichnis vor.

Im Zuge der Prüfung wurde das IT-Hardwareinventar am 8. November 2013 mittels einer Stichprobe auf Vollständigkeit und Genauigkeit geprüft. Es wurden durch den Stadtrechnungshof zufällig zwanzig physische IT-Vermögensgegenstände (Computer, Monitore, Drucker, Scanner) ausgewählt und über die Inventarnummer bzw. Seriennummer zum IT-Hardwareinventar abgestimmt. Von zwanzig Stichprobenelementen mussten sechs als fehlerhaft zurückgewiesen werden. Die Fehler betrafen ausschließlich Altbestände.

Nach Durchführung der Prüfhandlungen wurde eine geplante Komplettinventur des IT-Anlagevermögens durch die ITG abgeschlossen. Die Inventurlisten wurden durch den Stadtrechnungshof eingesehen.

Im Zuge der Prüfung wurde festgestellt, dass die Verwertung von außer Dienst gestellter Hardware nicht entsprechend geregelt war. Hier stellte insbesonders

der Verlust der Vertraulichkeit durch die Weitergabe von ausgemusterten Speichermedien ein Risiko dar. Speichermedien, auf denen sich nicht für die Öffentlichkeit bestimmte Daten befanden, waren nach Ansicht des Stadtrechnungshofs physisch zu zerstören oder auf andere erprobte Weise irreversibel zu bereinigen. Hierzu hatte zu jedem Speichermedium eine Dokumentation vorzuliegen.

Der Stadtrechnungshof empfahl,

- das gesamte Inventar im bestehenden IT-Verwaltungswerkzeug zu verwalten;

Stellungnahme der ITG:

Im Zuge der Umsetzung des Configurationmanagement-Prozesses im System Omnitracker werden die unterschiedlichen Asset-Typen sukzessive in das System übernommen. Derzeit sind bereits folgende Asset-Typen im Omnitracker integriert: PCs, Monitore, Drucker, Notebooks, Tablets, Scanner, Server und Peripheriegeräte, wie Beamer, Dockingstations, Kameras, VPN-Tokencards. Für die weitere Migration in das System sind sowohl die Netzwerkkomponenten (Switches, Router,…) als auch mobile Devices (Smartphones,…) geplant. Ebenso werden in Zukunft auch Softwarekomponenten und Programme im Omnitracker-System in Form eines Lizenzmanagements im Prozess Configurationmanagement verwaltet.

Der Stadtrechnungshof empfahl,

- durch eine technische Verbindung, einen Prozess oder eine nachgelagerte Kontrolle eine laufende Abstimmung der verwalteten IT-Anlagen zwischen dem Anlagenbuch der Rechnungslegung und dem IT-Verwaltungswerkzeug sicherzustellen;

Stellungnahme der ITG:

Im Zuge der Optimierung der elektronischen Unterstützung des Beschaffungsprozesses der ITG werden in Zukunft nur mehr zwei IT-Systeme für die Anforderung, den Einkauf und die Auslieferung von IT-Gütern an die KundInnen in der ITG eingesetzt. Auf der einen Seite wird das System Omnitracker für die Anforderung, die Auslieferung und die Verwaltung von IKT-Systemen verwendet andererseits SAP für die finanzielle und buchhalterische Abwicklung. Die Einführung dieses Prozesses ist mit 1. Quartal 2014 vorgesehen.

Im Zuge dieses Ablaufes ist eine Verbindung zwischen den beiden Systemen Omnitracker und SAP vorgesehen, sodass für jedes IT-Gut in einem System

eine Referenz auf das andere System besteht um die entsprechenden Informationen in jedem System sofort ermitteln zu können.

Der Stadtrechnungshof empfahl,

- eine Richtlinie für die Verwertung ausgemusterter Hardware zu erstellen und deren Einhaltung durchzusetzen.

Stellungnahme der ITG:

Die Entsorgung ausgemusterter Hardware ist in der ITG mit dem Prozess „Entsorgung von IKT- Geräten und Datenträgern“ geregelt. Zu vernichtende Datenträgern von PCs und Servern werden dabei in der ITG in einer speziellen Box gesammelt und ab einer bestimmten Anzahl der Firma Saubermacher zur Vernichtung übergeben. Nach Vernichtung der Datenträger erhält die ITG ein Protokoll über die Vernichtung der Datenträger.

Außerdem ist in den Aktivitäten des ISKT auch die Aufbewahrung und Entsorgung von Informationen (physisch – z.B. Papierkorb als auch elektronischen Medien – z.B. Speichersticks, CDs,…) ein Thema. Die Ergebnisse dieses Themas sind dann in den oben genannten Prozess mit aufzunehmen.

Siehe dazu die Informationssicherheits-Themenliste des ISKT:

28	Aufbewahrung und Entsorgung von Daten/Informationen	Aufbewahrung und Wegwerfen von Informationen/Daten (Papierkorb) regeln

Entgegnung des Stadtrechnungshofes:

Im Zuge der Prüfung wurde an einem konkreten Beispiel nachgewiesen, dass die Entsorgung ausgemusterter Hardware nicht ordnungsgemäß erfolgte. Hierzu lag dem Stadtrechnungshof elektronischer Schriftverkehr mit der ITG vor. Somit bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

3.1.9. Wartungsverträge

Als Anforderung wurde festgelegt, dass die Entscheidung über den Abschluss von Wartungsverträgen für Hard- und Software strukturiert zu erfolgen hatten. Weiters musste eine zentrale Verwaltung sämtlicher abgeschlossener Wartungsverträge vorliegen.

Unstrukturierte Entscheidungen über den Abschluss und eine mangelhafte Verwaltung von Wartungsverträgen hatten die Verfügbarkeit und Sicherheit von

digitalen Informationen und Prozessen gefährden können. Wartungsverträge stellten außerdem wesentliche Fixausgaben dar, die regelmäßig auf Zweckmäßigkeit zu überprüfen waren.

Im Zuge der Prüfung wurde erhoben, dass die Entscheidung über den Abschluss von Wartungsverträgen auf fachlichen Vorschlag der AbteilungsleiterInnen durch die Geschäftsführung der ITG erfolgte. Die Beschaffung von Wartungsverträgen folgte dem festgelegten Beschaffungsprozess der ITG. Laufende Wartungsverträge wurden im Controlling in einer Tabelle verwaltet. Im Zuge der jährlichen Budgetierung wurde die Zweckmäßigkeit bestehender Wartungsverträge kritisch hinterfragt.

Der Stadtrechnungshof kam zum Schluss, dass die Organisation der Beschaffung und Verwaltung von Wartungsverträgen angemessen erfolgte.

3.1.10. Outsourced Services

Als organisatorische Anforderungen im Rahmen der Prüfung des allgemeinen internen Kontrollumfeldes der IT wurden für Outsourced Services das Vorliegen eines gültigen Vertrages, die vertragliche Regelung der Vertraulichkeit sowie angemessener SLA Kennzahlenziele als Anforderungen festgesetzt. Weiters wurde eine laufende Überwachung der Einhaltung des definierten Service Levels vorausgesetzt.

Der im Zuge der Prüfung vorgelegte Vertrag beinhaltete eine Leistungsbeschreibung, angemessene Messkriterien für die Beurteilung der Erfüllung des Service Levels sowie eine Geheimhaltungsklausel. Die dem Stadtrechnungshof vorgelegte Auswertung über die Lösungsrate von Störungen zwischen 1. Jänner und 31. Oktober 2013 waren geeignet, die definierte Leistung des vorliegenden Vertrages zu überwachen.

3.1.11. IT-Revisionen (intern/extern)

Ausgehend von der Ebene „Monitoring“ des COSO-Modells wurden interne und externe Überprüfungen der internen Kontrollen als Beurteilungskriterien festgelegt.

Im Zuge der Prüfung wurde erhoben, dass es keine dokumentierten internen Überprüfungen der internen Kontrollen gab. Externe Überprüfungen wurden jährlich beauftragt, zuletzt 2012/2013. Inhalte waren eine Social Hacking Attacke, Tests auf Verwundbarkeit, Penetration-Testing auf externe und interne Serversysteme sowie Konfigurationsüberprüfungen von Netzwerkkomponenten. Die externe Überprüfung kam zur Einschätzung, dass ein MITTLERES RISIKO, das heißt Nichtvorliegen einer akuten Gefahr, aber Vorliegen zumindest einer relevanten Sicherheitslücke, vorlag. Weiters nahm der Stadtrechnungshof in die Dokumentation der aus der Prüfung abgeleiteten Maßnahmen Einsicht.

Die abgeleiteten Maßnahmen wurden gemäß der vorliegenden Dokumente adressiert und großteils bereits umgesetzt.

Der Stadtrechnungshof zog den Schluss,

- dass regelmäßige externe IT-Sicherheits-Überprüfungen zu wechselnden Schwerpunkten einen sehr positiven Beitrag zur Weiterentwicklung des internen Kontrollumfeldes der IT leisteten.

Der Stadtrechnungshof empfahl

- die Einrichtung regelmäßiger und dokumentierter interner Überprüfungen der internen Kontrollen.

Stellungnahme der ITG:

Neben externen Überprüfungen, wie Penetrationstests, Social Engineering, Konfigurations- und Updateprüfungen, welche jährlich durchgeführt werden, werden zur Erhöhung der Sicherheit auf technischer und organisatorischer Ebene auch interne Überprüfungen herangezogen. Diese internen Überprüfungen umfassen neben den obligatorischen Sicherheits- wie Verwundbarkeitsprüfungen auch den Test von Verfügbarkeit, bedarfsgerechte Nutzung von Ressourcen, Plausibilität der Konfigurationen von Infrastruktursystemen wie auch Services (Fileservice, Sharepoint, etc).

Die internen Tests teilen sich in technisch automatisierte und manuelle Prüfungen.

- Die technisch automatisierte Überprüfung orientiert sich am Gefahrenpotential eines gefährdeten Systems, Netzwerks oder der entsprechenden Anwendung und dient zur zusätzlichen Identifikation von Schwachstellen bzw. dem Aufdecken potenzieller Fehler. Hierbei werden mittels Prüfsoftware in regelmäßigen Abständen Scans der betreffenden Systeme auf Verwundbarkeit durchgeführt, Konfigurationen grundsätzlich auf Plausibilität geprüft und deren Ergebnisse vom technischen Sicherheitsverantwortlichen ausgewertet.
- Die manuelle Prüfung umfasst neben Basiskonfigurationstests von Komponenten und Lösungen vor allem plattformspezifisch administrative Bereiche, wie auch grundsätzliche Design- und Buildtests, die sicherstellen, dass die technologische Richtung in Übereinstimmung mit der Unternehmensstrategie ist (wirtschaftliche und investitionssichere, agile und standardisierte Infrastruktursysteme).

- Ein Spezialfall einer internen Prüfung ist der jährlich stattfindende Verfügbarkeitstest, in dessen Verlauf gemeinsam mit einem externen Partner die Redundanz bzw. Verfügbarkeit von Netzwerk- und Serversystemen geprüft werden. Hierbei werden neben grundsätzlichen Backbonetests wesentliche Core-Komponenten nach einem definierten Plan abgeschaltet bzw. in einen definierten Fehler-Zustand gebracht. Dabei wird das erzwungene Fehlerverhalten wie die Wirksamkeit der Backupinstanzen – inkl. Konvergenz- bzw. Übernahmezeiten - dokumentiert und mit dem erwarteten Ergebnis verglichen. Auf diesem Weg wird sichergestellt, dass Infrastruktur bzw. Services Ausfällen standhalten können bzw. deren Wiederanlauf innerhalb definierter Zeiträume gewährleistet ist.

Als Basis aller Überprüfungen dient ein Masterplan, in dem Inhalt, Reihenfolge, Frequenz der Kontrollen bzw. der zu kontrollierenden Systeme bestimmt sind.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

3.1.12. IT-Richtlinien

Es waren IT-Richtlinien vorzulegen, die den sachgerechten und sicheren Umgang mit Hardware, Software, Daten und Internet regelten. Diese Richtlinien waren jeder/m MitarbeiterIn zugänglich zu machen.

Im Zuge der Prüfung wurden die im Intranet des Magistrats verfügbaren Organisationsvorschriften der Kategorie Informationssicherheit eingesehen und deren Zweckmäßigkeit evaluiert. Es lagen folgende Organisationsrichtlinien vor:

Dokument	**Geplante nächste Revision**	**Letzte Revision**
Informationssicherheitspolitik Haus Graz	keine geplante Revision	Version 3.0
BenutzerInnenverwaltung in IT-Strukturen (IS-Richtlinie 1/2005)	September 2007	Revision 2006
Benutzung des Internets (IS-Richtlinie 1/2006)	Mai 2007	Mai 2006
Benutzung und Behandlung von elektronischer Post (IS-Richtlinie 2/2005)	Dezember 2009	Revision 2008-2

Kennwortrichtlinie	keine geplante Revision	Version 2.0
Sicherheitsklassifikation (IS-Richtlinie 2/2009)	2010	Mai 2009

Von den sechs gesichteten Dokumenten wiesen vier geplante Revisionszeitpunkte aus. Keine der vier geplanten Revisionen wurde durchgeführt. Die Revisionsbezeichnungen der gesichteten Organisationsvorschriften folgen keiner nachvollziehbaren Systematik.

Der Stadtrechnungshof empfahl,

- zur Richtlinie BenützerInnenverwaltung in IT-Strukturen (IS-Richtlinie 1/2005 – Revision 2006): Neuregelung zur zentralen Veranlassung von berechtigungsrelevanten Änderungen der Stammdaten (Eintritt, Versetzung, Abteilungswechsel, Austritt, Pensionierung) durch das Personalamt bzw. die Personalabteilungen. Bestehende Berechtigungen wären mit dem Stichtag der Veränderung und vor Vergabe der neuen Berechtigungen zu entziehen. Berechtigungsanforderungen sollten durch die befugten Personen innerhalb der Dienststellen bzw. Abteilungen erfolgen. Weiters wäre die Zweckmäßigkeit und Ordnungsmäßigkeit des Richtlinieninhalts bezüglich der Formulierung *„Sicherung des Postfachinhaltes über Outlook in eine PSD-Datei auf Datenträger (z.B. CD) für den/die InhaberIn des Postfaches“* zu prüfen – diese Regelung widersprach Erfordernissen des Amtsgeheimnisses.

Stellungnahme der ITG:

In der ITG werden Personalveränderungen über das Ticketsystem von den KundInnen eingebracht und auch in diesem abgearbeitet, d.h. gemeldete Personalveränderungen (Eintritt, Versetzung, Abteilungswechsel, Austritt) und die entsprechende Bearbeitung bzw. die damit durchgeführten Aktivitäten an den Systemen sind dokumentiert.

Im Zuge der zu bearbeitenden Themen des ISKT soll eine Haus-Graz weite Regelung für die Prozesse zu MitarbeiterInnen-Veränderungen geschaffen werden (Eintritt, Veränderung, Abteilungswechsel, Ausscheiden aus dem Unternehmen). Wichtig dabei ist, dass alle Meldungen von Personalveränderungen zeitgerecht an die ITG gemeldet werden, um die entsprechenden Änderungen bzgl. Berechtigungen rechtzeitig durchführen zu können. Die Empfehlung des StRH wird im Zuge der Bearbeitung dieses Themas im ISKT eingebracht.

Siehe dazu die Informationsicherheits-Themenliste des ISKT:

2	Eintritt, Austritt und Wechsel von MitarbeiterInnen	klare und prüfbare Regelung was zu tun ist, bei Ausscheiden von MA oder Änderungen des Aufgabengebietes

Der Stadtrechnungshof empfahl,

- zur Richtlinie Benutzung und Behandlung von elektronischer Post (IS-Richtlinie 2/2005 – Revision 2008-2): Klärung der Klausel zur privaten Verwendung der dienstlichen eMail-Infrastruktur in Hinblick auf Data-Ownerschaft der eMail Korrespondenz sowie Ergänzung der Richtlinie um einen Passus, der das Beantworten von SPAM-eMails untersagt.

Stellungnahme der ITG:

Im Zuge der zu bearbeitenden Themen des ISKT soll eine Haus-Graz weite Regelung für die Behandlung von elektronischer Post und Zugriff auf die Postfächer geschaffen werden. Die Empfehlung des StRH wird im Zuge der Bearbeitung dieses Themas im ISKT eingebracht.

Siehe dazu die Informationsicherheits-Themenliste des ISKT:

9	Email-Nutzung und Zugriff auf email-Postfächer	IS-Richtlinie zur Email-Nutzung überarbeiten und Richtlinien über den Zugriff auf email-Postfächer einbauen

Der Stadtrechnungshof empfahl,

- zur Richtlinie Kennwortrichtlinie: Umwandlung der Empfehlungen zu der Komplexität von Passwörtern in Vorschriften und ihre systemische Durchsetzung.

Stellungnahme der ITG:

Im ersten Quartal 2013 wurde vom ISKT eine Haus-Graz weite Kennwortrichtlinie erarbeitet. In der Holding wurde diese Richtlinie per Vorstandsbeschluss und in der Stadt per Präsidialerlass (02/2013) in Kraft gesetzt. Die technische Umsetzung dieser Richtlinie erfolgt schrittweise und ist mit Ende dieses Jahres abgeschlossen. Die Empfehlung des StRH bzgl. der Empfehlung der Zusammensetzung des Kennwortes wird in die nächste gemeinsame Überarbeitung dieser Richtlinie in das ISKT eingebracht.

Der Stadtrechnungshof empfahl,

- Zu Revisionierungen: Durchführung der geplanten Revisionen und/oder Evaluierung der Revisionszyklen sowie Festlegung einer einheitlichen Revisionsnummerierung.

Stellungnahme der ITG:

Die Revisionierung (Revisionszyklen, Nummerierung) obliegt den Richtlinien-Verantwortlichen, dies sind die Holding und der Magistrat für Haus Graz weite Regelungen. Für ältere Richtlinien ist nur jeweils eine der beiden Organisationen für die jeweilige Richtlinie verantwortlich. Die ITG hat diesbezüglich keine Ermächtigung eine Revisionierung von Richtlinien vorzuschreiben, anzuordnen bzw. durchzuführen. Die ITG wird die Empfehlung des StRH an die entsprechenden Stellen weiterleiten.

3.2. IT-Standardprozesse

Neben Aspekten der IT-Organisation wurden zur Beurteilung des Designs und der Effektivität des internen Kontrollumfeldes des zentralen IT-Bereichs des Hauses Graz ausgewählte Kontrollen in IT-Standardprozessen evaluiert und geprüft. Als zu adressierende IT-Standardprozesse wurden Programmentwicklung und Programmänderungen, Prozesse des laufenden Betriebs sowie Prozesse rund um den Zugang und die Beschränkung des Zugangs zu Programmen und Daten festgelegt. Innerhalb dieser IT-Standardprozesse wurden Schlüsselkontrollen als Anforderung formuliert, die als Prüfkriterien dienten.

Im vorliegenden Fall wurden Schlüsselkontrollen der IT-Standardprozesse als anwendungsunabhängige Kontrollen durch jeweils drei Erhebungsschritte beurteilt:

1. Risikoorientierte Definition von Schlüsselkontrollen als Prüfkriterien.
2. Prüfung der Existenz der Schlüsselkontrollen bzw. kompensierender Kontrollen.
3. Prüfung der Effizienz der Kontrolle.

3.2.1. Programmentwicklung und Programmänderungen

Programmentwicklungen und Programmänderungen wurden im Haus Graz aus Sicht der Prüfung der IT-Standardprozesse organisatorisch nicht unterschieden. Somit wurden beide Prozesse zusammengefasst.

Als Anforderungen wurden folgende Schlüsselkontrollen gestellt:

- Vorliegen von aktuellen und relevanten Richtlinien, die Entwicklung und Änderungsmanagement regelten. Beide Bereiche enthielten

grundsätzliche technische und kaufmännische Risiken. So hatte eine Entwicklungsrichtlinie beispielsweise Coding-Standards zu enthalten, da nicht standardisierter Programmcode spätere Wartungen und Erweiterungen erschwert und auch ein Angriffspunkt für Hacker-/ CrackerInnenattacken sein konnten (z. B. Buffer Overflow Attacks).

- Die Anforderung einer Programmentwicklung oder einer Änderung hatte strukturiert zu erfolgen. Hier war besonders auf die Organisation des Prozesses, auf dokumentierte Freigaben (wirtschaftliche, technische, strategische) sowie auf verständliche und ausreichend detaillierte Beschreibung der funktionalen und nichtfunktionellen Anforderungen zu achten. Die Verantwortung für die funktionelle Beschreibung war, unbeschadet von der Inanspruchnahme von Beratungsleitungen durch die ITG oder Dritte bei der anfordernden Abteilung einzufordern. Im Falle von Anforderungen, die eine IT-Unterstützung von Prozessen beinhaltete, hatte vor Beschreibung der funktionalen und nichtfunktionalen Anforderungen eine Festlegung der Zielprozessorganisation unter Berücksichtigung von Erfordernissen der Effektivität, der Effizienz und des internen Kontrollsystems in Abstimmung mit der jeweilig verantwortlichen Organisationsentwicklungsabteilung und den IKS-Verantwortlichen zu erfolgen.
  Hier bestanden grundsätzlich Risiken, dass Entwicklungen oder Änderungen unkoordiniert, nicht in eine Geschäftsstrategie, Prozesslandschaft und Plattformpolitk eingebettet erfolgten. Drohende Folgen wären in diesen Fällen wirtschaftlicher Schaden, aber auch die Gefährdung der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen gewesen.
- Jede Entwicklung und Änderung war in dokumentierter Weise zu testen. Testpläne (Testszenarien, Testdaten) hatten bereits in der Definition der Anforderungen geplant und festgelegt zu werden. Hier war sicherzustellen, dass Tests nicht in der Produktivumgebung erfolgten und, wenn Produktivdaten für Testzwecke verwendet wurden, diese unterscheidbar gemacht wurden. Die Dokumentation der Tests sollte für sachkundig Dritte nachvollziehbar die getestete Version, die verwendeten Testdaten, die durchgeführten Testschritte und deren Ergebnisse sowie die herangezogenen Kriterien beinhalten. Die Vertraulichkeit von Daten war auch in Entwicklungs- und Testumgebungen sicherzustellen. Für die Verwendung von Produktionsdaten zu Testzwecken war bei der/dem DatenbesitzerIn eine Genehmigung einzuholen. Diese(r) hatte eventuell notwendige Anonymisierungen und sonstige Veränderungen der Daten zur Wahrung der Datenvertraulichkeit als Voraussetzungen für Genehmigungen vorzuschreiben und zu kontrollieren.

- Bedingung für die Produktivstellung einer Entwicklung oder Änderung musste eine dokumentierte Freigabe durch die TesterInnen sowie der Programmbesitzerin bzw. des Programmbesitzers sein.
- Die Produktivsetzung hatte nicht durch EntwicklerInnen zu erfolgen.

Im Zuge der Prüfung wurde festgestellt, dass der Ablauf von Entwicklungen und Änderungen in einer Prozessbeschreibung festgelegt war. Weiters lag eine umfassende und verständliche Projektmanagementrichtlinie vor. Die vorliegende Entwicklungsrichtlinie für SAP Entwicklungen regelte ausschließlich die Namenskonvention für Objekte, gab aber keine Coding-Standards vor. Für Entwicklungen außerhalb von SAP war keine Entwicklungsrichtlinie verfügbar.

Der Stadtrechnungshof empfahl,

- die Erstellung einer Entwicklungsrichtlinie, die Coding-Standards vorgibt.

Stellungnahme der ITG:

Im Bereich der IT-Services findet die Entwicklung von Anwendungen hauptsächlich bei Software Partnern statt. Deren Entwicklungsrichtlinien, insbesondere die Coding- Standards, orientieren sich abhängig von der Entwicklungssprache an bekannten Standards:

Java: http://www.oracle.com/technetwork/java/codeconv-138413.html

C#: http://msdn.microsoft.com/en-us/library/ff926074.aspx

Finden im Zuge einer Softwareerstellung/-erweiterung gemeinsame Entwicklungstätigkeiten von ITG und externen Partnern statt, dann werden die Vorgaben der Software Partner übernommen. Reine Eigenentwicklungen orientieren sich auch an den oben genannten Standards. Für die Entwicklung von Java Anwendungen wird die Entwicklungsumgebung Eclipse verwendet. Die Sun Java Coding Conventions werden durch erweiterte Einstellungen in Eclipse definiert. Diese Einstellungen sind über ein Preferences- Datei (https://rzmsv166.intra.graz.at/svn/itg/itservices/coding/java/eclipse_coding.epf) zu importieren.

Für die Entwicklungen im .NET Bereich (C#, VB#, ASP.net, etc…) wird von ITG die aktuelle Version des Microsoft Visual Studio verwendet. Hier wird der eingebaute Code Formatter verwendet. Die Namenskonvention ist abhängig von der jeweiligen Entwicklungssprache und richtet sich nach den jeweiligen Guidelines. Die Nomenklatur wird grundsätzlich immer in Englisch durchgeführt mit Ausnahmen für deutsche Fachbegriffe und Konzepte bei einzelnen Klassen- Objekte. Die verwendeten Namen sollen sinnerklärend

sein.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Sämtliche Entwicklungen und Änderungen wurden in einem geeigneten IT-Service-Desk Werkzeug und im Falle von externen Leistungen/Beschaffungen auch in SAP verwaltet. Es gab im Ablauf keine Unterscheidung zwischen internen (ITG intern) und externen (Kunden Haus Graz) Projekten.

Es wurde zwischen Kleinprojekten und Nicht-Kleinprojekten unterschieden. Diese Unterscheidung hatte Auswirkung auf die Anwendung von Projektwerkzeugen. Es lagen dokumentierte Unterscheidungskriterien vor. Die Klassifizierungs-entscheidung erfolgte durch die jeweilige Projektleitung der ITG.

Der Stadtrechnungshof empfahl,

- die Einführung einer nachgelagerten Kontrolle, die eine sachlich angemessene Projektkategorisierung in Kleinprojekte und Nicht-Kleinprojekten sicherstellt.

Stellungnahme der ITG:

Projektdefinition

Projekte in der ITG sind Aufgabenstellungen, bei denen ein klar abgegrenztes Ergebnis in einer bestimmten Zeit, mit bestimmten Ressourcen in einer temporär eingerichteten Projektorganisation erreicht werden soll. In vielen Fällen werden Projekte von der ITG für Kunden, wie beispielsweise die Holding Graz oder den Magistrat Graz, erbracht. Dazu tritt die ITG als Generalunternehmer auf und bedient sich auch externer Lieferanten für die erfolgreiche Umsetzung dieser Projekte.

Projektklassifikation

Die Klassifikation von Projekten beeinflusst die Wahl der Projektmanagement-Methode sowie die Ressourcenplanung (Kosten/Personen/Mittel). Je nach Projektdauer, nach Erfahrung der ProjektleiterInnen und des Projektteams und den verfügbaren Ressourcen, werden Projekte innerhalb der ITG unterschiedlich klassifiziert. Mögliche Einstufungskriterien sind Komplexität, Kosten, Intensität der Projektabwicklung, Risiko oder Wirtschaftlichkeit, welche mit konkreten

Zahlenwerten oder durch eine verbale Gewichtung skaliert werden.

Die Projektklassifikation in Kleinprojekte (KP) und Projekte (P) wird durch die ITG-ProjektleiterIn durchgeführt. Kleinprojekte (KP) werden nur mit dem Werkzeug OT unterstützt, Projekte (P) zusätzlich mit Microsoft SharePoint. Die Einführung einer weiteren nachgelagerten Kontrolle ist nicht vorgesehen.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Im Zuge der stichprobenartigen Einsichtnahme in laufende und abgeschlossene Projekte wurde festgestellt, dass Qualität und Umfang der Beschreibung der Anforderungen kein einheitliches Mindestniveau erfüllte und teilweise nur aus einem erweiterten Projekttitel bestand. Weiters wurde erhoben, dass MitarbeiterInnen der ITG im Zuge des Services „Business-Engineering“ unter anderem Beratungstätigkeiten im Zusammenhang mit der Identifikation von Erweiterungspotentialen von Programmen als auch die Erarbeitung von Pflichtenheften und ROI-Berechnungen durchführten. Im Zuge der Einsichtnahme wurde außerdem festgestellt, dass bei einer großen Anzahl an Projekten keine kundenseitige Projektleitung dokumentiert war.

Der Stadtrechnungshof empfahl,

- zu jedem Entwicklungs- und Änderungsprojekt ausnahmslos vor Projektbeginn eine Beschreibung der Anforderungen in einem Detaillierungsgrad, der die Prüfung der Umsetzung gegen diese ermöglicht, einzufordern.

Stellungnahme der ITG:

Gemäß der von der ITG entwickelten und gelebten ITG-Projektmanagement-Richtlinie sind die detaillierten Anforderungen im Zuge eines Projektes von den anfordernden Auftraggeberinnen zu übermitteln. Sollte die Auftraggeberin selbst nicht in der Lage sein, die Anforderung im geforderten Detaillierungsgrad zu liefern, werden im Zuge der Angebotslegung die Anforderungen durch das ITG- Businessmanagement gemeinsam mit der Auftraggeberin erarbeitet. Die Anforderungsdefinition in dieser Projektphase muss der Qualität eines Lastenheftes genügen, das auch an externe Lieferanten zur Angebotslegung übergeben werden kann. Ausnahmen dazu sind nur dann vorgesehen, wenn

1. die Anforderungen noch zu unspezifisch sind und erst im Zuge eines

Projektes erarbeitet werden und die Projektabwicklung ohne großes Risiko erfolgen kann (Abwicklung über ITG und ein zuvor definiertes Stundenkontingent) oder

2. die Erhebung der Anforderungen so komplex und aufwendig ist, dass ein eigenes Vorprojekt für die Anforderungsdefinition über die ITG abgewickelt wird oder

3. die Anforderungen mit einfachen Standardlösungen umsetzbar sind, welche von der ITG intern oder mit externen Dienstleistern angeboten werden und bereits für ähnliche Anforderungen zum Einsatz gekommen sind.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Der Stadtrechnungshof empfahl,

- zu jedem Projekt eine verantwortliche, entscheidungsbefugte sowie prozessual und inhaltlich sachkundige Projektleitung auf Seite von Magistrat und Holding einzufordern

Stellungnahme der ITG:

In den Projektmanagement Richtlinien der ITG sind die Rollen für die Abwicklung von IT Projekten definiert. Die Verantwortung, die Aufgaben und die Befugnisse der jeweiligen Projektrollen (Kunde, ITG, Lieferant) sind für die jeweiligen Rollen definiert.

Kundenseitig sind, in Abhängigkeit von der Komplexität des Projekts, folgende Rollen notwendig:

- Kunden-Projektauftraggeberin
- Kunden-ProjektleiterIn
- Kunden-AuftragsmanagerIn

Alle IT Projekte verlangen mindestens die Benennung einer Kunden-ProjektleiterIn. Ohne die Benennung einer Kunden-ProjektleiterIn kann im OT kein Projekt angelegt werden.

Entgegnung des Stadtrechnungshofes:

Auf Grund der Ergebnisse der im Zuge der Prüfung erhobenen Stichprobe bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Der Stadtrechnungshof empfahl,

- in Fällen in denen in einer Abteilung kein(e) MitarbeiterIn ausreichend für die Rolle als kundenseitig Projektleitung geeignet scheint, Unterstützung durch das jeweilige zentrale IKT-Auftragsmanagement beizustellen.

Stellungnahme der ITG:

Die Auswahl der Kunden-ProjektleiterIn liegt in der Verantwortung unserer Auftraggeberinnen. ITG begrüßt den Vorschlag, möchten aber darauf hinweisen, dass das IKT-Auftragsmanagement gemäß seiner in der IT-Governance zugeordneten Aufgaben zwar für Projektcontrolling, nicht aber für fachliche Projektleitung zuständig ist und dies auch die definierte Zielkapazität überschreiten würde.

Entgegnung des Stadtrechnungshofes

Der Stadtrechnungshof wies darauf hin, dass das „Beistellen von Unterstützung durch das IKT-Auftragsmanagement“ nicht mit der „Unterstützung durch das IKT-Auftragsmanagement“ vermengt werden dürfe und somit die Gefahr einer Kapazitätsüberschreitung nicht bestand.

Eine Prüfung, ob eine Änderung oder Entwicklung der Haus Graz Strategie und der IT-Strategie entsprach, erfolgte durch die ITG undokumentiert.

Der Stadtrechnungshof empfahl,

- die Prüfung der Konformität einer Entwicklung oder Änderung zur IT Strategie vor Annahme von Aufträgen dokumentierter Weise durchzuführen.

Stellungnahme der ITG:

Dieser Punkt muss differenziert betrachtet werden.

1. Alle bekannten Anforderungen mit Projektcharakter wurden im Zuge der Strategie- und Projektportfolioentwicklung vom IKT-Board gegen die IT Strategie geprüft, bewertet und priorisiert. Dabei kam man zum Schluss, dass fachbereichsspezifische Projektanforderungen (bekannte, bzw. auch unterjährig eingebrachte) in diesem Gremium

nicht bewertet und priorisiert werden können. Dies kann nur innerhalb der jeweiligen Organisationseinheit durchgeführt werden. Die ITG kann dabei nur die Prüfung gegen Vorgaben aus der IT-Architektur durchführen und entsprechende Umsetzungsvorschläge unterbreiten. Umsetzungsvorschläge, welche aus wirtschaftlichen oder anderen Gründen gegen die Vorgaben der IT-Architektur verstoßen, werden im Rahmen des ITG-Führungsteam-Meetings, bzw. im kürzlich eingeführten Change Advisory Board (CAB) diskutiert und einer dokumentierten Entscheidung zugeführt.

2. Anforderungen, die nur einen Änderungs- (technischer Change) oder Service Request- Charakter haben, können aufgrund der Vielzahl ebenso nur gegen die Vorgaben aus der IT-Architektur geprüft werden. Dabei werden nur unvermeidbare Verstöße gegen diese Vorgaben dokumentiert.

Im Zuge der Weiterentwicklung des Prozesses zur Service Request Abwicklung werden weiter gehende Empfehlungen des Stadtrechnungshofs geprüft werden. Eine detaillierte Prüfung in diesen Fällen gegen die gesamte IT-Strategie wäre zwar wünschenswert, würde aber sowohl auf Seite ITG wie auch auf Kundenseite (IKT-Auftragsmanagement, Organisationsentwicklung und Fachabteilungen) zusätzliche Personalressourcen erfordern.

Der Stadtrechnungshof empfahl,

- die Erstellung eines verbindlichen Prozesses, der sicherstellt, dass mit der IT-Anforderung verbundene organisatorische Themen abgeklärt wurden.

Stellungnahme der ITG:

ITG teilt die Meinung des Stadtrechnungshofs, die notwendigen Maßnahmen können aber nur von unseren Auftraggeberinnen umgesetzt werden.

Entgegnung des Stadtrechnungshofes

Wie bereits oben angeführt, verwies der Stadtrechnungshof auf die Doppelrolle des Geschäftsführers der ITG und des CIO des Hauses Graz. Die Empfehlung an die ITG zielte darauf ab, diese Rollen sowie die Mitgliedschaft im IKT-Board und das Bekenntnis der ITG als „strategischer Partner“ der AuftraggeberInnen für die Umsetzung der Empfehlung zu nutzen. Aufgrund der Stellungnahme der ITG geht der Stadtrechnungshof davon aus, dass die ITG die Rollen im Sinne der Empfehlung nutzen wird.

Tests erfolgten mit Produktivdaten in Testumgebungen. Einwilligungen von den DateneignerInnen wurden hierzu nicht eingeholt. Die Dokumentation von Tests

und Testergebnissen erfolgte in den Projekten der gezogenen Stichprobe nicht systematisch in einer dem Zweck genügenden Form. Abnahmeprotokolle konnten für die gezogene Stichprobe nur vereinzelt vorgelegt werden. Dokumentierte Freigaben durch ProgrammbesitzerInnen waren keine Voraussetzung für Produktivsetzungen. Produktivsetzungen erfolgten auch durch EntwicklerInnen.

Der Stadtrechnungshof empfahl,

- jeden Test nachvollziehbar zu dokumentieren;

Stellungnahme der ITG:

Entsprechend einer verteilten Systemlandschaft kommen bei der ITG für Schlüsselprodukte wie SAP oder ELAK getrennte Systeme für die Entwicklung, Qualitätssicherung und Produktivbetrieb zum Einsatz. Eine verteilte SAP-Systemlandschaft ist von besonderer Bedeutung. Nur durch den Aufbau eines 3-stufigen Systemverbundes kann die Sicherheit und Stabilität der Produktivsysteme gewährleistet werden.

Die Entwicklung und Parametrisierung erfolgt ausschließlich auf den Entwicklungssystemen. Nach Abschluss der Entwicklung werden Änderungen über das standardisierte Transportwesen der SAP in die jeweiligen Qualitätssicherungssysteme transportiert. Das Testen von Änderungen erfolgt 2-stufig. Die MitarbeiterInnen der ITG testen jegliche Änderungen auf den jeweiligen Test- und Qualitätssicherungssystemen. Nach Freigabe durch die ITG können Kunden am Qualitätssicherungssystem mit Produktivdaten geänderte bzw. neue Funktionalität testen.

Die Dokumentation der Tests und Testergebnisse liegt in der Verantwortung der TesterInnen (ITG und Kunde). Nach Kundenfreigabe (Abnahme) erfolgt der Transport in das Produktivsystem. Das SAP systemimmanente Transportwesen erlaubt eine lückenlose Nachvollziehbarkeit von Änderungen. Eine vollständige Dokumentation der Tests erhöht den administrativen Aufwand und würde die Produktivität maßgeblich beeinträchtigen.

Entgegnung des Stadtrechnungshofes:

Auf Grund der durchgeführten Befragungen sowie auf Basis der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Der Stadtrechnungshof empfahl,

- Änderungen oder Entwicklungen ausnahmslos nur nach einer

dokumentierten Freigabe durch die anfordernde Abteilung sowie etwaige andere betroffene Abteilungen und System-OwnerInnen produktiv zu stellen;

Stellungnahme der ITG:

Die aktuelle Projektkultur im Haus Graz sieht weitgehend so aus, dass dokumentierte Freigaben sehr zögerlich bis gar nicht durchgeführt werden. Die vom Stadtrechnungshof empfohlene Vorgabe muss durch organisatorische Maßnahmen bei unseren Kunden unterstrichen werden, da sonst eine wirtschaftliche und effiziente Umsetzung von Änderungen und Entwicklungen nicht gewährleistet werden kann.

Der Stadtrechnungshof empfahl,

- eine Genehmigung durch die/den DatenbesitzerIn für die Verwendung von Produktionsdaten verpflichtend einholen zu lassen;

Stellungnahme der ITG:

Die ITG wird der Empfehlung Folge leisten.

Anmerkung

Das Testen auf Entwicklungs- und Qualitätssicherungssystemen ist oft nur mit Produktionsdaten sinnvoll möglich. Die Aktualisierung dieser Systeme erfolgt daher meist auf Anforderung der zuständigen Fachabteilungen.

Der Stadtrechnungshof empfahl,

- eine organisatorische Trennung zwischen Entwicklung und Transport in Produktivsysteme durchzusetzten. Sollte dies nicht möglich sein, wären angemessene nachgelagerte Kontrollen zu implementieren (z. B. Logging mit regelmäßiger, dokumentierter Durchsicht auf nicht freigegebene Transporte);

Stellungnahme der ITG:

Eine organisatorische Trennung zwischen Entwicklung und der Freigabe von Entwicklungen ist laut obigen Ausführungen gegeben. Eine Trennung zwischen Entwicklung und Transport wäre wünschenswert, ist aus kapazitiven Gründen aber nicht vorgesehen. Das Monitoring offener Transportaufträge erfolgt durch die jeweiligen EntwicklerInnen.

Entgegnung des Stadtrechnungshofes:

Der Stadtrechnungshof bekräftigte seine Empfehlung zur Einrichtung einer angemessen nachgelagerten Kontrolle. Das in der Stellungnahme beschriebene Monitoring offener Transportaufträge durch die jeweiligen EntwicklerInnen stellte nicht sicher, dass ausschließlich getestete und freigegebene Entwicklungen und Änderungen produktiv gestellt wurden.

Der Stadtrechnungshof empfahl,

- die bestehende ITG-Projektmanagementrichtlinie unter Hinzuziehung der Organisationsentwicklungsverantwortlichen zu einer allgemeinen Haus Graz Projektmanagementrichtlinie weiterzuentwickeln, diese zu schulen und die ausnahmslose Einhaltung der Richtlinie von den höchsten Führungsebenen durchzusetzten.

Stellungnahme der ITG:

Die ITG freut sich über die Anerkennung ihrer Projektmanagementrichtlinie durch den Stadtrechnungshof. Gerne steht ITG mit ihrer Kompetenz für die Weiterentwicklung der PM- Richtlinie im Haus Graz zur Verfügung.

3.2.2. Laufender IT-Betrieb

Unter dem IT-Standardprozess laufender IT-Betrieb wurden Backup- und Recoveryprozesse und die laufende Überwachung der IT-Infrastruktur zusammengefasst.

Als Anforderungen wurden folgende Schlüsselkontrollen gestellt:

- Das Vorliegen geeigneter Maßnahmen zur Sicherstellung der Datenverfügbarkeit. Als wesentliche Kriterien für die Eignung der Maßnahmen wurden die physische Sicherheit von Backups sowie der maximale Datenverlust (RPO) und die Wiederherstellungszeit (RTO) herangezogen.
- Die laufende Überwachung der Durchführung der Maßnahmen zur Sicherstellung der Datenverfügbarkeit.
- Das Vorliegen geeigneter und dokumentierter Recovery Prozesse sowie der Nachweis, dass die Wiederherstellung von Daten von Sicherungsmedien funktionierte.
- Die laufende Überwachung der IT-Infrastruktur. Unter dem Aspekt der Datenverfügbarkeit war hier besonderes Augenmerk auf das Kapazitätsmanagement, auf die Status von Servern sowie auf die Netzinfrastruktur zu legen. Ebenfalls hatten Schnittstellen dokumentiert und überwacht zu werden. Die Dokumentation von Schnittstellen hatte

zumindest die beteiligten Systeme, den Zweck, den Inhalt, den technischen Aufbau, vorhandene Kontrollen, inhaltlich Verantwortliche sowie Verantwortliche für die Überwachung zu beinhalten.

Im Zuge der Prüfung wurde festgestellt, dass die Sicherstellung der Datenverfügbarkeit einerseits durch zwei redundante Rechenzentren und andererseits durch periodische Sicherungen erfolgte. Da keine aktuelle Backuprichtlinie vorlag, wurde alternativ die bestehende Praxis erhoben. Eine Beurteilung der Angemessenheit der Backupintervalle auf Basis harter Evidenz konnte nicht vorgenommen werden, da diese auf Basis von durch die höchste Führungsebene genehmigte RTO und RPO Werten, abgeleitet aus den jeweiligen Verpflichtungen und Notwendigkeiten erfolgen müsste. Die Verantwortung für die Sicherstellung von Datenverfügbarkeit oblag, auch bei Beauftragung der ITG als Servicepartner, den obersten Führungseben in Magistrat und Holding. Das produktive SAP-System des Magistrats wurde täglich auf externe Backupdatenträger gesichert – dies erschien angemessen. Die ITG gab an, dass noch im ersten Quartal 2014 eine vollständige Backuprichtlinie erstellt werden sollte.

Der Stadtrechnungshof empfahl,

- auf Basis von der höchsten Führungsebene genehmigten, tolerablen Ausfallszeiten (RTO) und Datenverlustmengen (RPO) eine Backuprichtlinie zu erstellen.

Stellungnahme der ITG:

Aus technischer Sicht hat sich die ITG bereits eingehend mit dem Themen RTO und RPO beschäftigt, im Rahmen der Vorhaben des ISKT ist die Erstellung einer Backup-Richtlinie auf Basis von RTO- und RPO-Bewertungen vorgesehen, da die Auslegung des Backups von der Wichtigkeit und Kritikalität der Applikationen und Informationen aus Sicht der AuftraggeberInnen abhängig ist. Die Produktivsetzung dieser Richtlinie erfolgt dann durch den IKT-Beirat, d.h. die Genehmigung dafür erfolgt auf höchster Führungsebene.

Siehe dazu die Informationssicherheits-Themenliste des ISKT:

25	Backup	Sicherungszyklen, Aufbewahrungszeit-räume, Generationen, RTO, RPO,…

Im Zuge der Prüfung wurden Backupprotokolle eingesehen und festgestellt, dass eine angemessene laufende Überwachung der Durchführung der Backups vorlag.

Laut Aussage der ITG wurden Backupmedien in einem Safe in einem Gebäude, in dem sich kein Rechenzentrum befand, gelagert. Dies entsprach den Anforderungen.

Es lag kein aktueller ITK-Notfallwiederherstellungsplan (BRP) vor. Die Entwicklung eines aktuellen BRP war bis April 2014 geplant. Rücksicherungen wurden nicht regelmäßig und dokumentiert getestet. Laufende Rücksicherungen, die im Rahmen des Incident-Handlings erfolgten, verliefen gemäß Aussage eines verantwortlichen Mitarbeiters erfolgreich. Hierzu lag keine Dokumentation vor.

Der Stadtrechnungshof empfahl,

- die Erstellung und das Testen eines Haus-Graz-weiten ITK-Notfallwiederherstellungsplans (BRP) bzw. die Erstellung und das Testen von abgestimmten Teilplänen;

Stellungnahme der ITG:

Ein Desaster Recovery Plan (DRP) wurde in der ITG bereits 2012 erstellt. Dieser beruht auf den im Einsatz befindlichen IT-Services mit deren Abhängigkeiten voneinander und den zugeordneten Wiederanlaufklassen (diese wurden vorerst von der ITG intern festgelegt). Der DRP umfasst die Hauptverfahrensanweisungen zur Abhandlung im Katastrophenfall und Detailanweisungen auf Serviceebene als Abarbeitungsunterlage bei einem Desaster.

Auf Basis dieses DRP wurde im heurigen Jahr ein Papiertest durchgeführt, um das Arbeiten damit zu üben und die Vorteile der Verwendung eines DRP zu erkennen. Außerdem wurde der DRP im Jahr 2013 überarbeitet und Anpassungen vorgenommen.

Entgegnung des Stadtrechnungshofes:

Die in der Stellungnahme erwähnten zusätzlichen Dokumente wurden weder im Rahmen der Prüfung noch bei der Schlussbesprechung vorgelegt. Sollten diese Dokumente in ausreichender Qualität vorhanden und wirksam sein, ging der StRH von der Umsetzung dieser Empfehlung aus.

Der Stadtrechnungshof empfahl,

- die Durchführung regelmäßiger und dokumentierter Rück-sicherungstests;

Stellungnahme der ITG:

Jüngste Erfahrungen haben gezeigt, dass nicht große Naturkatastrophen oder Fahrlässigkeit bzw. gezielte Sabotage von MitarbeiterInnen die häufigste Ursache für Datenverlust sind. Vielmehr verursachen Hardwarefehler, unleserliche Tapes beim Restore oder menschliches Versagen in Form von BedienerInnenfehlern oder aber fehlerhafte Software die meisten Datenverluste. Um die dargestellten Risiken zu minimieren, werden abhängig von der Wiederanlaufklasse aus dem DRP (Desaster Recovery Plan) Desasterfälle simuliert, bzw. für unternehmenskritische Daten sogar außerhalb der Rechenzentren der ITG im Zuge des Restore-Tests wiederhergestellt. Da das laufende Backup/Restore-Konsolidierungsprojekt, d.h. die Migration zweier Backup/Restore- Systeme auf eine Haus Graz weite, zentrale wie hoch verfügbare Plattform bzw. auch die notwendigen Konsolidierungsarbeiten mit Ende des Jahres 2013 abgeschlossen sind, werden im Sinne der Effizienz die zum Projekt gehörenden Desaster Recovery Tests plangemäß im ersten Quartal 2014 durchgeführt. Aufgrund begrenzter finanzieller bzw. personeller Ressourcen können nicht alle Systeme testweise restored werden. Es wird dennoch eine Katastrophe hohen Ausmaßes simuliert – „einer der beiden RZ-Standorte und die komplette Backup/Restore-Infrastruktur sind zerstört“. D.h. mit der Zweitkopie der Daten auf Band werden auf einer Standardhardware die entsprechenden Daten und Services wiederhergestellt. Der Vorgang wird protokolliert bzw. dokumentiert. Die Dauer der Tests wird auf 10 Tage geschätzt, in dem maximal 50 Systeme bzw. 20 TByte wiederhergestellt werden und deren Wiederanlauf dokumentiert wird. Im Zuge der jeweiligen Restoreprozedur werden Betriebssysteme, Applikationen und Datenbanken auf Funktionsfähigkeit überprüft und ein Wissenstransfer innerhalb der ITG angestoßen bzw. eine Liste mit Verbessungsvorschlägen wie –maßnahmen erstellt. Die Ergebnisse der Tests fließen auch in das neue Desaster Recovery Handbuch ein, in dem neben der Darstellung der Restoreprozeduren, auch der Iststand der Systeme aus Backupsicht detailliert beschrieben wird. Gleichzeitig wird damit begonnen, ein neues Backup/Restore-Handbuch für die konsolidierte Backup/Restore-Plattform des Hauses Graz zu erstellen. Dieses beinhaltet neben detaillierten Plattformbeschreibungen auch die entsprechenden Restoreanleitungen für die jeweiligen Systeme.

Der Stadtrechnungshof empfahl,

- die Dokumentation und regelmäßige Auswertung der Erfolgsraten im Rahmen des Incident-Handlings durchgeführter Rücksicherungen.

Stellungnahme der ITG:

Anforderungen von AnwenderInnen für Datenrücksicherungen werden über die ITG Serviceline im Omnitracker aufgenommen, mit der entsprechenden Kategorie (Rücksicherung) versehen und an den entsprechenden Bereich zur Durchführung von Restores weitergeleitet. Dabei wird im Ticket von den BenutzerInnen angegeben, was rückzusichern ist und von der Technik die entsprechende

Rückmeldung (Erfolgsmeldung über die Rücksicherung) angegeben, die auch der AnforderIn bei Abschluss des Tickets automatisch übermittelt wird.

Von den im Jahr 2013 bisher durchgeführten und ausgewerteten Rücksicherungen (53 Tickets) wurden alle Operationen, selbst komplexe, sich über mehrere Serverinstanzen erstreckende Restores fehlerfrei durchgeführt.

Entgegnung des Stadtrechnungshofes:

Im Zuge der Prüfung wurden die in der Stellungnahme genannten Informationen trotz gezielter Nachfrage am 8. November 2013 nicht vorgelegt. Der Stadtrechnungshof nimmt diese Feststellung somit gerne zur Kenntnis, konnte deren Richtigkeit jedoch nicht anhand von Dokumenten überprüfen.

Die IT-Infrastruktur wurde in geeigneter Weise durch ein Werkzeug überwacht.

Schnittstellen zwischen Systemen lagen nicht vollständig dokumentiert vor. Somit gab es auch keine dokumentierten Verantwortlichkeiten für die inhaltliche und technische Überwachung der Schnittstellen sowie für Kontrollen, die die Vollständigkeit, Genauigkeit, Validität und die Datenvertraulichkeit sicherzustellen hatten.

So fand der Stadtrechnungshof im Filesystem einen Ordner ohne jede Zugriffseinschränkung, der unter anderem einer Schnittstelle zwischen Systemen des Magistrats diente. Die ITG schränkte die Berechtigungen nach Benachrichtigung durch den Stadtrechnungshof umgehend ein.

Der Stadtrechnungshof empfahl,

- die Dokumentation sämtlicher Schnittstellen;

Stellungnahme der ITG:

Schnittstellen dienen dazu den Datenaustausch zwischen Systemen zu automatisieren. Die ITG forciert eine Serviceorientierte Anwendungsarchitektur (SOA) und stellt Funktionalitäten, die von mehreren

Systemen und Anwendungen benötigt werden in gekapselten Services zur Verfügung. Diese Services verfügen über genau definierte Webservice-Schnittstellen, die über ein WSDL-File spezifiziert werden.

Es gibt auch die File-Schnittstellen, bei denen der Datenaustauch über Dateien im Filesystem erfolgt. Hier muss die Berechtigungsstruktur im Filesystem entsprechend konfiguriert und dokumentiert sein, dass nur berechtigte Personen und Systeme auf die Dateien zugreifen können.

SAP stellt ebenfalls eine Reihe von Programmierschnittstellen zur Verfügung, mit denen externe Anwendungen in ein SAP-System integrieren können. Mit Hilfe dieser Schnittstellen können Client/Server-Anwendungen geschrieben werden, die mit einem SAP-System kommunizieren. Folgende Typen von Schnittstellen sind möglich:

Batch Input

Die Batch-Input-Schnittstelle ermöglicht die automatisierte Eingabe von Daten in R/3 mit Hilfe von R/3-Transaktionen.

RFC

Das Protokoll des SAP Remote Function Call (RFC) ermöglicht es, aus externen Anwendungen heraus ABAP-Funktionsbausteine aufzurufen. Eine externe Anwendung, die die RFC-Schnittstelle verwendet, kann sowohl als Client als auch als Server zu einem SAP-System fungieren.

BAPI

SAP-Business-Objekte liefern eine objektorientierte Sicht der SAP-Datenstrukturen und -Funktionen. Das Business-API (BAPI) ist eine Schnittstelle, über die die Methoden dieser SAP-Business-Objekte aufgerufen werden kann.

IDoc

Die Schnittstelle Intermediate Document (IDoc) ist ein SAP-Standardformat für den Datenaustausch zwischen SAP-Systemen und zwischen einem SAP-System und einer externen Anwendung. Ein IDoc-Dokument definiert einen SAP- Standarddatencontainer (Schablone) zum Senden oder Empfangen von Daten aus einem SAP-System.

Im SAP System des Magistrats kommen überwiegend Batch-Input Schnittstellen zum Einsatz. Die ITG dokumentiert den technischen Teil der Schnittstellen. Diese Dokumentation erfolgt im Programm der Schnittstelle

selbst. Unsere Kunden verantworten die Dokumentation für die Bewirtschaftung der Schnittstelle (Periodizität der Ausführung, Fehlerbehandlung, etc). Gerne folgt ITG der Empfehlung des Stadtrechnungshofs, gemeinsam mit unseren Kunden die Dokumentation weiter zu entwickeln.

Der Stadtrechnungshof empfahl,

- die dokumentierte Überwachung kritischer Schnittstellen.

Stellungnahme der ITG:

Das SAP System verfügt über standardisierte Mittel zur Überwachung von Schnittstellen. Im Zuge der Implementierung von Schnittstellen werden unseren Auftraggeberinnen diese Werkzeuge vorgestellt. Die Nutzung dieser Hilfsmittel liegt in der Verantwortung unserer AnwenderInnen.

Die Batch-Input-UserIn (Kunde) führt den Datentransfer in das SAP-System basierend auf der Übernahmetechnik 'Batch-Input' durch. Dieser Datentransfer erfolgt in zwei Schritten: Mittels eines Datentransferprogrammes werden die Fremddaten eingelesen und in Form einer Batch-Input-Mappe im SAP-System abgelegt. Durch das Abspielen der Batch-Input-Mappe gelangen die Daten in die jeweiligen Datenbanktabellen der Applikation. Die Überwachung der Transaktionen erfolgt durch die UserIn (Kunde). Mittels der Standardtransaktionen (SM35 Batch-Input-Monitoring, SM35P Batch-Input Protokoll-Monitoring) können unsere AnwenderInnen die Schnittstellen überwachen. Die ITG wird im Zuge der Überarbeitung der Schnittstellendokumentation auf diese Standardwerkzeuge hinweisen.

3.2.3. Zugang zu Programmen und Daten

Der Themenkreis Zugang zu Programmen und Daten wurde gegen folgende Anforderungen an Schlüsselkontrollen geprüft:

- Vorliegen eines aktuellen und angemessenen Berechtigungskonzeptes.
- Restriktive Vergabe von Berechtigungen.
- Vorliegen eines geordneten und zweckmäßigen Prozesses für die Berechtigungsverwaltung im Zusammenhang mit Ein- und Austritten sowie Abteilungswechseln von MitarbeiterInnen, der Verwaltung der Berechtigungen von AdministratorInnen und der Organisation der Berechtigungsvergabe sowie des Berechtigungsentzuges für externe IT-Benutzer, wie beispielsweise IT-BeraterInnen.
- Vorliegen geeigneter physischer Sicherheitskontrollen für die Räumlichkeiten der IT und sowie für die Rechenzentren. Zutrittsberechtigungen waren restriktiv zu vergeben und im Falle von

kritischer Infrastruktur musste die Nachvollziehbarkeit des Zutritts gegeben sein.
- Geeignete Maßnahmen zum Schutz vor Schadsoftware.

Es lag kein Berechtigungskonzept vor. Eine Namenskonvention wurde eingesetzt und diesem Konzept nicht entsprechende Altbestände sollten bis Juni 2014 bereinigt werden. Eine Einsichtnahme in AD und SAP bestätigte sowohl die Umsetzung der Namenskonvention als auch bestehende Altbestände, die dieser noch widersprachen. Die im Zuge der Prüfung erhobene Praxis der Verwaltung von IT-Berechtigungen zeigte, dass die jeweiligen Abteilungen den Anstoß für alle berechtigungsrelevanten Änderungen gaben. Namentlich nominierte MitarbeiterInnen aus den Abteilungen meldeten Ein- und Austritte in der jeweils eigenen Abteilung und forderten Änderungen des Berechtigungsumfangs an. Die Anforderungen erfolgten über ein geeignetes Werkzeug.

Diese Praxis beinhaltete große Risiken, da nicht sichergestellt war, dass die Benutzerberechtigungen austretende MitarbeiterInnen deaktiviert und im Falle von Versetzungen und Abteilungswechsel die Berechtigungen der ursprünglichen Abteilung entzogen wurden. Weiters wurde festgestellt, dass die bestehende Praxis der dezentralen Anforderung von Benutzerrechteänderungen im Falle von Beendigungen von Dienstverhältnissen der gültigen Richtlinie „BenutzerInnenverwaltung in IT-Strukturen“ des Magistrats widersprach. Diese Richtlinie sah für diese Fälle einen zentralen Änderungsanstoß durch das Personalamt vor.

An Hand einer im Zuge der Prüfung durchgeführten Stichprobe konnte gezeigt werden, dass diese Risiken eingetreten waren und die bestehende Praxis fehleranfällig war.

Der Stadtrechnungshof empfahl,

- jede Veranlassung zur Änderung von berechtigungsrelevanten Stammdaten (Eintritt, Versetzung, Abteilungswechsel, Austritt, Pensionierung) durch das Personalamt bzw. die Personalabteilungen der Holding zu veranlassen und bestehende Berechtigungen bis zum Stichtag der Veränderung und vor Vergabe der neuen Berechtigungen zu entziehen. Berechtigungsanforderungen sollten durch Vorgesetzte erfolgen;

Stellungnahme der ITG:

In der ITG werden Personalveränderungen über das Ticketsystem von den KundInnen eingebracht und auch in diesem abgearbeitet, d.h. gemeldete Personalveränderungen (Eintritt, Versetzung, Abteilungswechsel, Austritt)

und die entsprechende Bearbeitung bzw. die damit durchgeführten Aktivitäten an den Systemen sind dokumentiert.

Im Zuge der zu bearbeitenden Themen des ISKT soll eine Haus-Graz weite Regelung für die Prozesse zu MitarbeiterInnen-Veränderungen geschaffen werden (Eintritt, Veränderung, Abteilungswechsel, Ausscheiden aus dem Unternehmen). Wichtig dabei ist, dass alle Meldungen von Personalveränderungen zeitgerecht an die ITG gemeldet werden, um die entsprechenden Änderungen bzgl. Berechtigungen rechtzeitig durchführen zu können.

Die Empfehlung des StRH wird im Zuge der Bearbeitung dieses Themas im ISKT eingebracht.

Siehe dazu die Informationsicherheits-Themenliste des ISKT:

2	Eintritt, Austritt und Wechsel von MitarbeiterInnen	klare und prüfbare Regelung was zu tun ist, bei Ausscheiden von MA oder Änderungen des Aufgabengebietes

Der Stadtrechnungshof empfahl,

- ein Berechtigungskonzept für kritische Berechtigungen sowie deren Kombination zu entwickeln;

Stellungnahme der ITG:

Die ITG setzt für die Realisierung des zentralen Verzeichnisdienstes des Hauses Graz das Active Directory von Microsoft ein. Die Schaffung eines Haus Graz weit einheitlichen Directories dient als Basis zur zentralen Verwaltung aller Microsoft Backoffice Dienste und Berechtigungen und schafft für alle MitarbeiterInnen des Hauses Graz einen einheitlichen Zugang zu Ressourcen wie Mail, Filesystem, SQL Datenbanken, Share Point etc.

Da die UserInnenmigration der beiden Domains Magistrat und Holding nunmehr ordnungsgemäß abgeschlossen ist, wird das Admin-Berechtigungskonzept, wie im Domain Gesamtkonzept geplant, in definierten Schritten im Jahr 2014 umgesetzt. Zu diesem Zweck werden sämtliche administrativen Berechtigungen in der Domain überprüft und gegebenenfalls überarbeitet. Administratoren werden ausnahmslos mit personalisierten Admin-Accounts ausgestattet und dem produktiven Account, der bis jetzt die Adminrechte innehatte, werden sämtliche Adminberechtigungen entzogen.

Es wird eine verschärfte Passwort-Richtlinie für Admin-Accounts eingeführt, außerdem wird evaluiert, wie AdministratorInnenberechtigungen nach genauer Prüfung ohne Domain-Adminrechte abgedeckt werden können. Spezielle Domain-Adminrechte wie Schema-Admin und Organisations- Admin wurden bereits durch das Modell einer „Empty Root Domain“ von den Domainadmins getrennt.

Lokale Adminrechte auf Memberservern werden nur mehr über Gruppen auf den Servern vergeben, in welcher die dafür notwendigen AdministratorInnen Mitglied sind. Dadurch sind für ServeradministratorInnen keinerlei Domain-Adminrechte mehr notwenig. Die Gruppenerstellung auf den jeweiligen Servern erfolgt Script gesteuert.

Nach Abschluss dieser Maßnahmen erfolgt ein erstes Review sämtlicher Serviceaccounts, speziell derjenigen welche Domainadminrechte innehaben. Jenen Konten, welche nicht durch technische Gegebenheiten eine absolute Domainadmin-Notwendigkeit rechtfertigen, werden diese Rechte entzogen. Das Review wird in Folge institutionalisiert, und laut Masterplan in zyklischen Abständen wiederholt.

Der Stadtrechnungshof empfahl,

- die Verwendung von Superusern im Produktivsystem durch Trennung der Funktionen zu vermeiden oder alternativ dokumentierte nachgelagerte Kontrollen zu implementieren;

Stellungnahme der ITG:

ITG nimmt die Empfehlung des Stadtrechnungshofs an.

Der Stadtrechnungshof empfahl,

- Periodische Reviews der Berechtigungen durch die Data-Owner einzuführen;

Stellungnahme der ITG:

Data-Owner für fachspezifische Informationen sind die entsprechenden Fachabteilungen, daher liegt ein Review der entsprechenden Berechtigungen in der Verantwortung der Fachabteilungen und ist von diesen anzustoßen.

Die ITG kann für solche Reviews auf Anforderung die entsprechenden Informationen (wer aus einer Abteilung besitzt welche Berechtigungen) zur Verfügung stellen. Die Entscheidung, ob die Zuordnung von Berechtigungen zu Personen des Fachbereiches korrekt ist, liegt aber im Fachbereich selbst

(Stellenbeschreibung bzw. Tätigkeit der MitarbeiterIn).

Der Stadtrechnungshof empfahl,

- Dezentrale Berechtigungsvergaben auf Ebene des Filesystems in der Komplexität zu beschränken, um die Überprüfbarkeit durch Data-Owner zu ermöglichen.

Stellungnahme der ITG:

Im Rahmen des File Server Projektes, welches eine zentrale, hochverfügbare Plattform für das Haus Graz vorsieht, ist auch ein neues Berechtigungsmodell vorgesehen. Dies wurde als Projekt im Rahmen des ISKT (Informations Sicherheits Kompetenz Team) eingebracht, vom Gremium als hochprior eingestuft und wird im Lauf des Jahres 2014 vom ISKT aufbereitet und dem Management des Hauses Graz zur Freigabe vorgelegt.

Das neue, Haus Graz weit gültige Berechtigungsmodell sieht vor, dass nur noch bis zur 3. Berechtigungsebene Berechtigungen zentral, d.h. von der ITG vergeben werden. Sollten in Unterverzeichnissen ab der 3. Ebene Berechtigungen gewünscht werden, so sollen diese mit einer neuen Freigabe realisiert werden, welche dem gleichen Regelwerk unterliegt. Dadurch wird die Komplexität stark verringert und eine Überprüfbarkeit geschaffen. Solch ein Modell ist bei den bestehenden File Server Systemen der Holding bereits im Einsatz. Der vorgesehene Beginn zur Umsetzung des Projektes zur Schaffung der neuen File Server Plattform bzw. der Umstellung/Auflösung bestehender komplexer Ordner- bzw. Freigabestrukturen ist das 1. Quartal 2014.

Problematisch bei der Umsetzung des Projektes gestaltet sich die Tatsache, dass es derzeit insbesondere in den Abteilungen des Magistrats in der Regel kaum AnsprechpartnerInnen gibt, welche sich mit dem Thema Abteilungsberechtigungen befassen. Daher wird das angestrebte und mit einigen Bereichen der Stadt Graz bereits erfolgreich durchgeführte Berechtigungs/Gruppen- Review mit den jeweiligen Dataownern nur eingeschränkt möglich sein. Auch dieser Punkt wird im Zuge des Gesamtprojektes vom ISKT aufbereitet und ein Lösungsvorschlag dem Management des Hauses Graz vorgelegt.

6	Berechtigungskonzept Fileserver / Sharepoint	Regelungen zu Berechtigungskonzepten auf dem Fileserver
7	Fileserver - Struktur	Verzeichnisstrukturen am Fileserver mit den entsprechenden Berechtigungsvergaben

Die IT-Räumlichkeiten wurden durch RFID-Schlösser gesichert. Die Türschlösser der Serverräume wurden geloggt. Im Zuge der Prüfung wurde in Logs von Türen der Rechenzentren Einsicht genommen. Es zeigte sich, dass Zutrittsberechtigungen grundsätzlich restriktiv vergeben werden, allerdings fand sich in der Stichprobe eine geringe Anzahl von Zutritten durch anonyme Zutrittskarten, wie beispielsweise für Servicefirmen.

Der Stadtrechnungshof empfahl,

- keine anonymen Zutrittskarten auszugeben, oder alternativ sicher zu stellen, dass für jede anonyme Karte zu jedem Zeitpunkt die/der InhaberIn archivecht dokumentiert ist.

Stellungnahme der ITG:

Für den Bereich [redacted] wurden im Zuge der Zusammenführung der beiden IT-Abteilungen alle berechtigten Zutrittskarten aus dem System gelöscht, danach die Zutrittsregeln bzw. –Rollen gezielt für jede betroffene Person neu mittels Dienstausweis berechtigt. Externe Partner bekamen/bekommen bei Bedarf auf den Namen des jeweiligen Unternehmens und den Namen der berechtigten Person frei geschaltene Zutrittskarten. Somit ist der Zutritt zu den IT-Räumlichkeiten des [redacted] nachvollziehbar, da jeder einzelne Zutritt mittels Logdatei Zutritt protokolliert ist. Generell ist der Zutritt zu den IT-Räumlichkeiten des Standortes [redacted] wie im Bereich [redacted] geregelt, wobei auch hier jeder Zutritt protokolliert wird. Die Zutritte zu den IT- Räumlichkeiten zum IT- Standort [redacted] sind derzeit aus historischen, holdinginternen Gründen zu zahlreich, werden jedoch von einer internen Dienststelle aus dem Bereich der Holding geregelt. Von Seiten der ITG wurde eine Liste mit allen zurzeit berechtigten Karten übermittelt bzw. auch eine Liste mit den aus ITG-Sicht in Zukunft zu autorisierenden Zutrittspersonen erstellt. Derzeit wird eine Bereinigung der Berechtigungsstruktur auf Seiten der Holding durchgeführt.

An dieser Stelle ist darauf hinzuweisen, dass die ITG beabsichtigt, ihre Infrastruktur aus dem Rechenzentrum [redacted] Ende des Jahres 2014 an einen neuen Standort zu übersiedeln.

Im Zuge der Prüfung wurden beide redundante Rechenzentren begangen. Der Abstand beider Rechenzentren zueinander erfüllte die Anforderung eines Mindestabstandes von 1.500 Metern nicht. Die Rechenzentren waren zum Zeitpunkt der Prüfung versperrt und, bis auf das Fehlen eines automatischen Löschsystems, dem Zweck entsprechend ausgestattet. Sämtliche Räumlichkeiten waren in vorbildlicher Weise aufgeräumt und sauber. Anzumerken war, dass die unter Punkt 2.6.2 Server-Housing des „Rahmen IT-Governance“ Dokumentes

zwischen ITG, Holding Graz und dem Magistrat genannte Verfügbarkeit von „USV/Dieselstromversorgung“ nicht im festgelegtem Umfang gegeben war. Weiters legte dieses Dokument nicht näher definierte Brandschutzmaßnahmen fest.

Der Stadtrechnungshof empfahl,

- die Erbringung der in dem Dokument „Rahmen IT-Governance“ definierten Leistungen regelmäßig zu überprüfen;

Stellungnahme der ITG:

Das Dokument „Rahmen IT-Governance“ regelt im Kapitel 1.2.2 die Darstellung der jeweils aktuellen IT-Services im getrennt von diesem Dokument zu führenden und geführten IT-Servicekatalog. Die geübte Vorgehensweise bei Änderungen der Leistungen ist ausführlich im Kapitel 4. festgelegt. Die Überwachungs- und Kontrollrechte hinsichtlich der Leistungen und Bedingungen sind im Kapitel 6.4.1. ausgeführt und betreffen in der Regel Gremien, die aus VertreterInnen der Auftraggeberinnen und teils der ITG bestehen.

Entgegnung des Stadtrechnungshofes:

Auf Grund der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Der Stadtrechnungshof empfahl,

- die Prüfung von Punkt 2.6.2. Server-Housing des „Rahmen IT-Governance“ Dokumentes auf Klarheit der Anforderung sowie auf Zweckmäßigkeit;

Stellungnahme der ITG:

Bei den im Kapitel 2.6 dargestellten Housing/Hosting Services handelt es sich um zusätzliche, also optionale Services der ITG, die im Einzelfall der Anforderung, wie in den Kapiteln 2.6.1 und 2.6.2 ausformuliert, hinsichtlich Verfügbarkeitsparametern und anderer Kriterien über Einzel-SLAs zu regeln sind. Daher ergibt sich die Klarheit der Anforderung erst aus dem SLA und nicht aus diesem Rahmendokument.

Entgegnung des Stadtrechnungshofes:

Auf Grund der im Zuge der Prüfung von der ITG vorgelegten Unterlagen bekräftigte der Stadtrechnungshof seine Feststellung und seine Empfehlung.

Der Stadtrechnungshof empfahl,

- im Falle einer räumlichen Veränderung eines der Rechenzentren bei der Wahl eines neuen Standortes möglichst einen Mindestabstand der redundanten Rechenzentren zueinander von 1.500 Metern zu berücksichtigen.

Stellungnahme der ITG:

Aufgrund der Zusammenführung der IT Holding und Magistrat zu einer konzernweiten IT wurden Strategien, Ziele sowie daraus abgeleitete Maßnahmen ermittelt, welche die Ressourcen der vorhandenen Rechenzentren bedarfsgerecht optimieren, sodass derzeit zwei Rechenzentren betrieben werden, in denen geschäftskritische Systeme/Anwendungen hochredundant, d.h. standortredundant dem Haus Graz zur Verfügung stehen.

Um mit minimal geplanten Ausfallzeiten arbeiten zu können, ist sichergestellt, dass an jedem Standort eine multiredundante Infrastruktur (Stromversorgung, Netzwerk, Klimatisierung, etc.) zur Verfügung steht bzw. die Standorte miteinander multiredundant verbunden sind (Datacenter-Network).

Damit IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können bzw. ihre Wiederherstellung gewährleistet ist, plant die ITG den Betrieb zweier georedundanter Parallel-Rechenzentren.

Im Zuge der Umsetzung wurden bereits zahlreiche Maßnahmen, wie die Modernisierung des bestehenden Rechenzentrums [redacted], getroffen. Die Räumlichkeiten des Rechenzentrums [redacted] werden voraussichtlich mit Ende des Jahres 2014, spätestens Ende 2015, geräumt. Die vorhandene, bereits konsolidierte und logisch in das hochredundante Datacenter integrierte Infrastruktur wird an einem Standort untergebracht, der den Anforderungen eines georedundanten Parallel-Rechenzentrum-Betriebes entspricht.

Wobei sich Geo-Redundanz grundsätzlich nach mehreren Parametern richtet. In Österreich wird in der kleinsten Implementation von Geo-Redundanz gesprochen, wenn die Systemräume in voneinander getrennten Räumen vorliegen. Im Gegensatz dazu ist Desaster Redundanz bereits erfüllt, wenn sich die Systemräume in getrennten Brandabschnitten befinden. Die Parameter, nach denen sich Geo-Redundanzen richten, wären zum Beispiel Erdbebenrisiko, Überschwemmungsrisiko, Bedrohung durch Flugbetrieb und

andere Risikofaktoren. Aufgrund dessen ist dieses Thema kaum geregelt bzw. ist es schwer, eine generelle Definition für Geo-Redundanz zu finden, weil natürlich diese Parameter beispielsweise in Graz anders wiegen als in Los Angeles. Weitere Parameter werden von diversen Hardware-Herstellern definiert, in dem es für diverse Funktionen nur bis zu einer gewissen Entfernung Support seitens des Herstellers gibt.

Daher greift die Empfehlung eines Mindestabstandes zwischen Rechenzentren zu kurz, da erst aus der Abwägung aller Risikofaktoren auf Georedundanz geschlossen werden kann.

Entgegnung des Stadtrechnungshofes:

Der Stadtrechnungshof bekräftigte seine Empfehlung und merkte an, dass der empfohlene Mindestabstand dem BSI-Hinweis zur räumlichen Entfernung zwischen redundanten Rechenzentren folgte. Somit fußte die Empfehlung auf der selben Quelle wie der in Kapitel 3.1.4. von der ITG als Referenz für das Informationssicherheitsmanagement/Risikomanagement gewählte Grundschutzkatalog.

Geeignete Maßnahmen zum Schutz vor Schadsoftware waren eingerichtet.

3.3. Kontrollen im Bereich SAP-BASIS

Anforderungen im Bereich SAP-BASIS wurden für die Felder

- Identifikation und Authentisierung,
- Autorisierung,
- Systemintegrität und
- Änderungsmanagement

festgesetzt. Für jeden Bereich wurden Schlüsselkontrollen sowie dazugehörige Anforderungen an diese anwendungsabhängigen Kontrollen definiert.

Um die Beurteilung und Umsetzung der Empfehlungen zu erleichtern, wurden der ITG Teile der Prüfdokumentation des Stadtrechnungshofes zur Verfügung gestellt, die technische Details zu den angesetzten Kriterien, Feststellungen und Empfehlungen enthielten.

Stellungnahme der ITG:

Aufgaben und Ressourcen SAP CCC Das SAP CCC zeichnet innerhalb der ITG für den Betrieb der SAP Applikationen verantwortlich. Die Aufgaben des SAP CCC umfassen Steuerungsprozesse, Kernprozesse und Supportprozesse. Beispielhaft seien einige Aufgaben aufgelistet:

Steuerungsprozesse

- Anforderungsmanagement
- Entwicklung der SAP-CCC Angebote
- etc.

Kernprozesse

- Applikationsmanagement
- Infrastrukturmanagement
- Evaluation der Services
- Releasemanagement
- etc.

Supportprozesse

- Lizenzmanagement
- Beschaffungsmanagement
- etc.

Um diese Aufgaben professionell zu erfüllen, empfiehlt die SAP ein Mindestmaß an Personalkapazitäten. Natürlich gibt es keine allgemein gültige Formel zur Berechnung der Personalausstattung von SAP CCCs. Die Anzahl der notwendigen Personalkapazität ist abhängig vom jeweiligen Nutzungsgrad der SAP Applikationen, vom Reifegrad der Organisation und von der Anzahl der SAP-AnwenderInnen. Die von SAP empfohlene Bandbreite liegt zwischen ein bis zwei MitarbeiterInnen pro 100 AnwenderInnen.

Die AnwenderInnenanzahl beträgt im Haus Graz ca. 1500, daraus ergäbe sich eine notwendige Personalkapazität von 15-30 MitarbeiterInnen. Zur Durchführung dieser mannigfaltigen Aufgaben eines SAP CCCs stehen der ITG derzeit 8 MitarbeiterInnen zur Verfügung. Wobei derzeit ca. 3 MitarbeiterInnen mit der Durchführung von Projekten betraut sind. Die geplante verstärkte Nutzung von SAP und der damit verbundene Anstieg von AnwenderInnen verlangt kurz- bzw. mittelfristig eine signifikante Verstärkung der Personalkapazität.

3.3.1. Identifikation und Authentisierung

Ein angemessener Zugriffsschutz war durch das Setzen von Systemparametern für die Anmeldekontrollen sicherzustellen. Hierzu gehörten beispielsweise Einstellungen, die die gewünschte Kennwortqualität systemisch erzwangen, Benutzerpasswörter in ihrer Gültigkeit beschränkten, Sonderbenutzer sicher konfigurierten und die Anforderung, dass die Effektivität der Anmeldekontrollen überwacht wurde.

Die zuvor erhobenen Mängel der Benutzerverwaltung (siehe Kapitel 3.2.3.), der Passwortrichtlinie (siehe Kapitel 3.1.12.) sowie die im Zuge der Prüfung des Produktivmandanten des Magistrats durch den Stadtrechnungshof eingesehenen Einstellungen führten zum Schluss, dass die automatischen Kontrollen in SAP-BASIS für Identifizierung und Authentisierung das IT-Kontrollziel des eingeschränkten Zugriffschutzes und somit indirekt die Erreichung sämtliche IT-Kontrollziele nicht sicherstellten.

Der Stadtrechnungshof empfahl,

- die automatisierten Kontrollen des Bereiches Identifikation und Authentisierung in SAP zu überarbeiten.

Stellungnahme der ITG:

Das SAP System erlaubt die Abbildung der im Haus Graz gültigen Kennwortrichtlinie. Nach Freigabe der Umsetzung der Kennwortrichtlinie durch unsere Auftraggeberinnen kommt ITG gerne der Empfehlung des Stadtrechnungshofs nach.

3.3.2. Autorisierung

Die Vergabe von Berechtigungen, die Benutzern Zugriff auf Funktionen und Daten in SAP ermöglichten, hatte auf einer „need-to-know“-Basis unter Berücksichtigung des Prinzips der Funktionstrennung zu erfolgen. Dies besagt, dass der geringstmögliche Berechtigungsumfang zu vergeben war, wobei die Berechtigung für kritische Prozessschritte so zu vergeben waren, dass zumindest Vier-Augen-Prinzipien systemisch erzwungen würden.

Im Zuge der Prüfung wurde festgestellt, dass im Produktivsystem des Magistrats die Prinzipien des geringstmöglichen Berechtigungsumfangs und der Funktionstrennung innerhalb der SAP-AdministratorInnen und EntwicklerInnen, im Bereich externer BeraterInnen und im Bereich von (Fach-)Abteilungen des Magistrats nicht eingehalten wurden. Dies führte zum Schluss dass die vorliegende Praxis der Autorisierung in SAP die Vollständigkeit, Genauigkeit und Validität von rechnungslegungsrelevanten Daten gefährdeten und die Vertraulichkeit von Daten sowie die Nachvollziehbarkeit von Änderungen nicht sicherstellte.

Der Stadtrechnungshof empfahl,

- den Bereich der Autorisierung in SAP zu überarbeiten.

Stellungnahme der ITG:

Die Anlage bzw. Änderung von UserInnen und Berechtigungen erfolgt über

einen standardisierten Prozess. Eine definierte Gruppe von KundenmitarbeiterInnen hat das Recht, UserInnen und Berechtigungen zu beantragen. Diese Gruppe entspricht jenem Personenkreis, welcher im SAP-System die Berechtigung zur Freigabe von Bestellungen hat.

Die Meldung erfolgt über ein Ticket im Omnitracker (OT) mittels Standard Antragsformular. Die Überprüfung, ob die meldende Person das Recht besitzt, das Anlegen bzw. Ändern von UserInnen und Berechtigungen zu beantragen, erfolgt durch die Prüfung gegen die Liste der dazu Berechtigten. Das Standard Antragsformular bietet die Möglichkeit auf Referenz UserInnen zu verweisen. Die ITG nimmt die Empfehlung des Stadtrechnungshofs an, die Granularität zu verfeinern.

3.3.3. Systemintegrität

Die von SAP vorgesehenen Kontrollen mussten zum Schutz von System- und Datenintegrität aktiviert werden. Wesentlich waren besonders Anforderungen an die Nachvollziehbarkeit von Transaktionen. Die Datenbank, in der die Daten des SAP-Systems gehalten wurden, und das Betriebssystem waren unter Berücksichtigung der Sicherheitserfordernisse zu implementieren, zu konfigurieren, zu betreiben und zu überwachen.

Im Zuge der Prüfung wurde festgestellt, dass die automatischen Kontrollen in SAP-BASIS im Produktivsystem des Magistrats die Wahrung der Systemintegrität nicht sicherstellten.

Der Stadtrechnungshof empfahl,

- die automatisierten Kontrollen des Bereiches Systemintegrität in SAP zu überarbeiten.

Stellungnahme der ITG:

ITG nimmt die Empfehlung des Stadtrechnungshofs an und wird die diesbezüglich vorgesehene Verbesserungsinitiative forcieren.

3.3.4. Änderungsmanagement in SAP

Softwareänderungen hatten einem dokumentierten Prozess zu folgen. Es war sicherzustellen, dass ausschließlich getestete und freigegebene Programmänderungen produktiv gestellt wurden. SAP war so zu konfigurieren, dass die Nachvollziehbarkeit von Änderungen gegeben war.

Die zuvor erhobenen Mängel im Bereich Programmentwicklung und Programmänderungen (siehe Kapitel 3.2.1.) sowie eingesehene Konfigurationen in SAP führten zum Schluss, dass die automatischen Kontrollen in SAP-BASIS sowie die Organisation des Änderungsmanagements die Vollständigkeit, Genauigkeit,

Validität und Vertraulichkeit von rechnungslegungsrelevanten Daten nicht sicherstellte.

Der Stadtrechnungshof empfahl,

- die automatisierten Kontrollen und die Gestaltung des Prozesses des Bereiches Änderungsmanagement in SAP zu überarbeiten.

Stellungnahme der ITG:

Entsprechend einer verteilten Systemlandschaft kommen bei der ITG getrennte SAP Systeme für die Entwicklung, Qualitätssicherung und Produktivbetrieb zum Einsatz. Eine verteilte SAP- Systemlandschaft ist von besonderer Bedeutung. Nur durch den Aufbau eines 3-stufigen Systemverbundes kann die Sicherheit und Stabilität der Produktivsysteme gewährleistet werden.

Die Entwicklung und Parametrisierung erfolgt ausschließlich auf den Entwicklungssystemen. Nach Abschluss der Entwicklung werden Änderungen über das standardisierte Transportwesen der SAP in die jeweiligen Qualitätssicherungssysteme transportiert. Das Testen von Änderungen erfolgt 2-stufig. Die MitarbeiterInnen der ITG testen jegliche Änderungen auf den jeweiligen Test- und Qualitätssicherungssystemen. Nach Freigabe durch die ITG können Kunden am Qualitätssicherungssystem mit Produktivdaten geänderte bzw. neue Funktionalität testen.

Die Dokumentation der Tests und Testergebnisse liegt in der Verantwortung der TesterInnen (ITG und Kunde). Nach Kundenfreigabe (Abnahme) erfolgt der Transport in das Produktivsystem. Das SAP systemimmanente Transportwesen erlaubt eine lückenlose Nachvollziehbarkeit von Änderungen. Eine vollständige Dokumentation der Tests erhöht den administrativen Aufwand und würde die Produktivität maßgeblich beeinträchtigen. Gemeinsam mit unseren Auftraggeberinnen wird ITG den Prozess des Änderungsmanagements überarbeiten.

4. Beantwortung der Prüfungsfragen

Sind das Design und die Effektivität des internen Kontrollumfeldes des zentralen IT-Bereiches der Komplexität und dem Risiko angemessen?

Die IT-Organisation, als ein Teil des internen Kontrollumfeldes des zentralen IT-Bereichs, war in Design und Effektivität der Komplexität und dem Risiko des Hauses Graz grundsätzlich angemessen.

Der IT-Standardprozess „laufender Betrieb“ wies Schwächen in Teilbereichen aus und war somit nur bedingt den Anforderungen angemessen.

Schlüsselkontrollen der IT-Standardprozesse „Programmentwicklung“, „Änderungsmanagement“ sowie „Zugang zu Programmen und Daten“ waren in Design und Effektivität der Komplexität und dem Risiko nicht angemessen.

Sind die automatisierten Kontrollen im Bereich SAP-BASIS angemessen?

Die automatisierten Kontrollen im Bereich SAP-BASIS für den Magistrat Graz waren nicht angemessen.

Welche Konsequenzen resultieren aus diesen Feststellungen?

Den Gremien der IT-Governance und der Informationssicherheit des Hauses Graz sowie der ITG wurden Verbesserungsfelder des internen Kontrollumfeldes aufgezeigt. Empfehlungen betrafen organisatorische Optimierungen, Bedarf für Richtlinien sowie empfohlene Parametereinstellungen in SAP, die aus Sicht des Stadtrechnungshofes kurz und mittelfristig umsetzbar waren.

Der Stadtrechnungshof stellte fest dass keine Prüfsicherheit aus IT-basierten bzw. IT-abhängigen Kontrollen gewinnbar war und berücksichtigte dies im Zuge seiner risikobasierten Prüfungsplanung. Die Verlässlichkeit von IT-generierten Finanzinformationen wurde als niedrig eingestuft. Daher wurde es weiterhin als notwendig erachtet, jede IT-generierte Finanzinformation, die im Zuge von Prüfungen des Stadtrechnungshofes Verwendung fand, individuell zur Einschätzung der Verlässlichkeit zu prüfen.

Stellungnahme der ITG:

IT-Referenzmodelle wie Cobit 5, an dem die ITG ihre Ausrichtung orientiert, unterstützen Unternehmen, in unserem Fall das Haus Graz, den optimalen Wert aus dem IT-Einsatz zu schöpfen. Dies wird erreicht durch Schaffen und Halten der Balance zwischen dem Erzielen von Kundennutzen und dem Optimieren der Risiken und des Ressourceneinsatzes. Die Angemessenheit der IT-Kontrollen leitet sich daher wesentlich aus der Risikobereitschaft und der Bereitschaft für Ressourceneinsatz im Haus Graz ab. Da dies unternehmens- bzw. branchenspezifisch sehr unterschiedlich beurteilt wird, haben die IT-Referenzmodelle Reifegradmodelle entwickelt. Dies ermöglicht die Festlegung von prozessspezifischen Soll-Werten, die dem jeweiligen Unternehmen die Differenz des aktuellen Status zum zu erzielenden Sollwert aufzeigen und entsprechende Maßnahmen auslösen. Die ITG hat im Zuge ihrer beabsichtigten ISAE 3402 Zertifizierung eine Reifegradbestimmung nach diesem Modell vornehmen lassen und auch das Informationssicherheits- und

das Risikomanagementsystem der ITG bauen auf Reifegradmodellen auf. Das Cobit 5 Reifegradmodell kennt angelehnt an die ISO 15504 die folgenden IT-Prozessreifegrade:

0… es wird der Zweck des Prozesses nicht erreicht,
1… Prozesse werden intuitiv exekutiert und erreichen den Zweck,
2… Prozesse werden geplant/beobachtet/angepasst und die Prozessergebnisse (Produkte) angemessen geprüft,
3… Prozesse werden beschrieben und geordnet implementiert,
4… für den Prozess werden Ziele definiert und die Zielerreichung überwacht,
5… Prozesse werden kontinuierlich verbessert in Hinblick auf die Geschäftsziele.
Aus Sicht der ITG haben die IT-Standardprozesse "Programmentwicklung, Änderungsmanagement" sowie "Zugang zu Programmen und Daten", deren Schlüsselkontrollen vom Stadtrechnungshof als nicht angemessen beurteilt wurden, selbstverständlich Verbesserungspotenzial, aber im direkt der ITG obliegenden Verantwortungsbereich im Wesentlichen einen Prozessreifegrad, der den Anforderungen und dem zugebilligten Ressourceneinsatz entspricht. Dies gilt ebenso für den IT- Standardprozess "laufender Betrieb", deren Schlüsselkontrollen vom Stadtrechnungshof als bedingt angemessen beurteilt wurden. Bezüglich der automatisierten Kontrollen im Bereich SAP-BASIS teilt die ITG die Einschätzung des Stadtrechnungshofs und wird Verbesserungen unmittelbar vornehmen. Dieser Bereich wurde in der neuen IT-Organisation des Hauses Graz noch keiner umgesetzten Verbesserungsinitiative unterzogen. Ein diesbezügliches internes Initialassessment hat stattgefunden und hat vergleichbares Verbesserungspotenzial aufgezeigt. Die Umsetzung der daraus abgeleiteten Maßnahmen wird die ITG unter Berücksichtigung der Empfehlungen des Stadtrechnungshofs forcieren.

Entgegnung des Stadtrechnungshofes:

Der Stadtrechnungshof betonte, dass die vorliegende Prüfung das IT-Kontrollumfeld des Hauses Graz aus der Perspektive der Verlässlichkeit von Organisation und Systemen für die Verarbeitung rechnungslegungsrelevanter Informationen zum Gegenstand hatte. Die Beurteilung erfolgte somit danach, ob die rechnungslegungsrelevanten Informationsziele Vollständigkeit, Validität, Genauigkeit und Vertraulichkeit von Informationen sichergestellt wurden. Im Übrigen gab der Stadtrechnungshof zu bedenken, dass es wesentliche konzeptionelle Unterschiede zwischen dem Prozessreifegradmodell (COBIT4.1) und dem Prozessbefähigungsmodell (COBIT 5) gibt.

5. Zusammenfassung der Empfehlungen

3.1. IT-Organisation

Der Stadtrechnungshof empfahl,

- die Prozessdokumentation der ITG für kritische IT-Prozesse unter besonderer Berücksichtigung von Schlüsselkontrollen durch die Erstellung von Detailprozessen zu ergänzen;
- bei kritischen Rollen die Konzentration des gesamten Wissens auf einzelne MitarbeiterInnen zu vermeiden und eine abgestimmte Nachfolgeplanung zu betreiben;
- in der Risikolandkarte IT-relevante Gefahren für das gesamte Haus Graz abzubilden;
- die Bewertung der Risiken und Ableitung von Maßnahmen aus einer Gesamtperspektive des Hauses Graz organisationsübergreifend festzulegen;
- identifizierte Maßnahmen klar und spezifisch zu formulieren, Verantwortlichkeiten und Termine festzulegen und zentral zu überwachen sowie in den Reportingprozess an das Management einfließen zu lassen;
- wie davon der ITG geplant, strukturierte MitarbeiterInnengespräche einzuführen;
- regelmäßige Risk-Awareness-Trainings für IT-BenutzerInnen im Haus Graz zu veranstalten;
- die Umsetzung eines standardisierten periodischen Reportings über zu definierende operative und strategische Messgrößen;
- die Umsetzung des geplanten „Project-Dashboards" in dem sämtliche laufenden Projekte monatsaktuell aufgelistet sind;
- das gesamte Inventar im bestehenden IT-Verwaltungswerkzeug zu verwalten;
- durch eine technische Verbindung, einen Prozess oder eine nachgelagerte Kontrolle eine laufende Abstimmung der verwalteten IT-Anlagen zwischen dem Anlagenbuch der Rechnungslegung und dem IT-Verwaltungswerkzeug sicherzustellen;

- eine Richtlinie für die Verwertung ausgemusterter Hardware zu erstellen und deren Einhaltung durchzusetzen;
- die Einrichtung regelmäßiger und dokumentierter interner Überprüfungen der internen Kontrollen;
- zur Richtlinie BenützerInnenverwaltung in IT-Strukturen (IS-Richtlinie 1/2005 – Revision 2006): Neuregelung zur zentralen Veranlassung von berechtigungsrelevanten Änderungen der Stammdaten (Eintritt, Versetzung, Abteilungswechsel, Austritt, Pensionierung) durch das Personalamt bzw. die Personalabteilungen. Bestehende Berechtigungen wären mit dem Stichtag der Veränderung und vor Vergabe der neuen Berechtigungen zu entziehen. Berechtigungsanforderungen sollten durch die befugten Personen innerhalb der Dienststellen bzw. Abteilungen erfolgen. Weiters wäre die Zweckmäßigkeit und Ordnungsmäßigkeit des Richtlinieninhalts bezüglich der Formulierung *„Sicherung des Postfachinhaltes über Outlook in eine PSD-Datei auf Datenträger (z.B. CD) für den/die InhaberIn des Postfaches“* zu prüfen – diese Regelung widersprach Erfordernissen des Amtsgeheimnisses;
- zur Richtlinie Benutzung und Behandlung von elektronischer Post (IS-Richtlinie 2/2005 – Revision 2008-2): Klärung der Klausel zur privaten Verwendung der dienstlichen eMail-Infrastruktur in Hinblick auf Data-Ownerschaft der eMail Korrespondenz sowie Ergänzung der Richtlinie um einen Passus, der das Beantworten von SPAM-eMails untersagt;
- zur Richtlinie Kennwortrichtlinie: Umwandlung der Empfehlungen zu der Komplexität von Passwörtern in Vorschriften und ihre systemische Durchsetzung;
- zur Richtlinie Revisionierungen: Durchführung der geplanten Revisionen und/oder Evaluierung der Revisionszyklen sowie Festlegung einer einheitlichen Revisionsnummerierung.

3.2. IT-Standardprozesse

Der Stadtrechnungshof empfahl,

- die Erstellung einer Entwicklungsrichtlinie, die Coding-Standards vorgibt;
- die Einführung einer nachgelagerten Kontrolle, die eine sachlich angemessene Projektkategorisierung in Kleinprojekte und Nicht-Kleinprojekten sicherstellt;
- zu jedem Entwicklungs- und Änderungsprojekt ausnahmslos vor

Projektbeginn eine Beschreibung der Anforderungen in einem Detaillierungsgrad, der die Prüfung der Umsetzung gegen diese ermöglicht, einzufordern;

- zu Jedem Projekt eine verantwortliche, entscheidungsbefugte sowie prozessual und inhaltlich sachkundige Projektleitung auf Seite von Magistrat und Holding einzufordern;
- in Fällen in denen in einer Abteilung kein(e) MitarbeiterIn ausreichend für die Rolle als kundenseitig Projektleitung geeignet scheint, Unterstützung durch das jeweilige zentrale IKT-Auftragsmanagement beizustellen;
- die Prüfung der Konformität einer Entwicklung oder Änderung zur IT Strategie vor Annahme von Aufträgen dokumentierter Weise durchzuführen;
- die Erstellung eines verbindlichen Prozesses, der sicherstellt, dass mit der IT-Anforderung verbundene organisatorische Themen abgeklärt wurden;
- jeden Test nachvollziehbar zu dokumentieren;
- Änderungen oder Entwicklungen ausnahmslos nur nach einer dokumentierten Freigabe durch die anfordernde Abteilung sowie etwaige andere betroffene Abteilungen und System-OwnerInnen produktiv zu stellen;
- eine Genehmigung durch die/den DatenbesitzerIn für die Verwendung von Produktionsdaten verpflichtend einholen zu lassen;
- eine organisatorische Trennung zwischen Entwicklung und Transport in Produktivsysteme durchzusetzten. Sollte dies nicht möglich sein, wären angemessene nachgelagerte Kontrollen zu implementieren (z. B. Logging mit regelmäßiger, dokumentierter Durchsicht auf nicht freigegebene Transporte);
- die bestehende ITG-Projektmanagementrichtlinie unter Hinzuziehung der Organisationsentwicklungsverantwortlichen zu einer allgemeinen Haus Graz Projektmanagementrichtlinie weiterzuentwickeln, diese zu schulen und die ausnahmslose Einhaltung der Richtlinie von den höchsten Führungsebenen durchzusetzten;
- auf Basis von der höchsten Führungsebene genehmigten, tolerablen Ausfallszeiten (RTO) und Datenverlustmengen (RPO) eine Backuprichtlinie zu erstellen;

- die Erstellung und das Testen eines Haus-Graz-weiten ITK-Notfallwiederherstellungsplans (BRP) bzw. die Erstellung und das Testen von abgestimmten Teilplänen;
- die Durchführung regelmäßiger und dokumentierter Rücksicherungstests;
- die Dokumentation und regelmäßige Auswertung der Erfolgsraten im Rahmen des Incident-Handlings durchgeführter Rücksicherungen;
- die Dokumentation sämtlicher Schnittstellen;
- die dokumentierte Überwachung kritischer Schnittstellen;
- jede Veranlassung zur Änderung von berechtigungsrelevanten Stammdaten (Eintritt, Versetzung, Abteilungswechsel, Austritt, Pensionierung) durch das Personalamt bzw. die Personalabteilungen der Holding zu veranlassen und bestehende Berechtigungen bis zum Stichtag der Veränderung und vor Vergabe der neuen Berechtigungen zu entziehen. Berechtigungsanforderungen sollten durch Vorgesetzte erfolgen;
- ein Berechtigungskonzept für kritische Berechtigungen sowie deren Kombination zu entwickeln;
- die Verwendung von Superusern im Produktivsystem durch Trennung der Funktionen zu vermeiden oder alternativ dokumentierte nachgelagerte Kontrollen zu implementieren;
- Periodische Reviews der Berechtigungen durch die Data-Owner einzuführen;
- Dezentrale Berechtigungsvergaben auf Ebene des Filesystems in der Komplexität zu beschränken, um die Überprüfbarkeit durch Data-Owner zu ermöglichen;
- keine anonymen Zutrittskarten auszugeben, oder alternativ sicher zu stellen, dass für jede anonyme Karte zu jedem Zeitpunkt die/der InhaberIn archivecht dokumentiert ist;
- die Erbringung der in dem Dokument „Rahmen IT-Governance“ definierten Leistungen regelmäßig zu überprüfen;
- die Prüfung von Punkt 2.6.2. Server-Housing des „Rahmen IT-Governance“ Dokumentes auf Klarheit der Anforderung sowie auf Zweckmäßigkeit;

- im Falle einer räumlichen Veränderung eines der Rechenzentren bei der Wahl eines neuen Standortes möglichst einen Mindestabstand der redundanten Rechenzentren zueinander von 1.500 Metern zu berücksichtigen.

3.3. Kontrollen im Bereich SAP-BASIS

Der Stadtrechnungshof empfahl,

- die automatisierten Kontrollen des Bereiches Identifikation und Authentisierung in SAP zu überarbeiten;
- den Bereich der Autorisierung in SAP zu überarbeiten;
- die automatisierten Kontrollen des Bereiches Systemintegrität in SAP zu überarbeiten;
- die automatisierten Kontrollen und die Gestaltung des Prozesses des Bereiches Änderungsmanagement in SAP zu überarbeiten.

Der Stadtrechnungshof zog die Schlüsse,

- dass die eingerichteten Strukturen der IT-Governance im Haus Graz geeignet sind, die notwendigen Abstimmung und Entscheidungen zu erzielen;
- dass die Dokumentation der Systemlandschaft, insbesonders die Dokumentation der kritischen Netzwerkinfrastruktur die Anforderungen vollkommen erfüllte und Vorbildwirkung besaß;
- dass regelmäßige externe IT-Sicherheits-Überprüfungen zu wechselnden Schwerpunkten einen sehr positiven Beitrag zur Weiterentwicklung des internen Kontrollumfeldes der IT leisteten.

Stellungnahme der ITG:

Die folgenden Empfehlungen des Stadtrechnungshofs bestätigen aus Sicht der ITG die heute im IT- Bereich des Hauses Graz geübte Praxis bzw. die getroffenen Entscheidungen und bereits definierten Maßnahmen und es ergibt sich daraus aus Sicht der ITG kein zusätzlicher Handlungsbedarf:

Der Stadtrechnungshof empfahl,

- die Prozessdokumentation der ITG für kritische IT-Prozesse unter besonderer Berücksichtigung von Schlüsselkontrollen durch die Erstellung von Detailprozessen zu ergänzen;
- wie von der ITG geplant, strukturierte MitarbeiterInnengespräche einzuführen;
- die Umsetzung eines standardisierten periodischen Reportings über zu definierende operative und strategische Messgrößen
- die Umsetzung des geplanten „Project-Dashboards" in dem sämtliche laufenden Projekte monatsaktuell aufgelistet sind. • das gesamte Inventar im bestehenden IT-Verwaltungswerkzeug zu verwalten;
- durch eine technische Verbindung, einen Prozess oder eine nachgelagerte Kontrolle eine laufende Abstimmung der verwalteten IT- Anlagen zwischen dem Anlagenbuch der Rechnungslegung und dem IT- Verwaltungswerkzeug sicherzustellen;
- eine Richtlinie für die Verwertung ausgemusterter Hardware zu erstellen und deren Einhaltung durchzusetzen.
- die Einrichtung regelmäßiger und dokumentierter interner Überprüfungen der internen Kontrollen
- zu jedem Entwicklungs- und Änderungsprojekt ausnahmslos vor Projektbeginn eine Beschreibung der Anforderungen in einem Detaillierungsgrad, der die Prüfung der Umsetzung gegen diese ermöglicht, einzufordern.
- zu jedem Projekt eine verantwortliche, entscheidungsbefugte sowie prozessual und inhaltlich sachkundige Projektleitung auf Seite von Magistrat und Holding einzufordern
- die Prüfung der Konformität einer Entwicklung oder Änderung zur IT Strategie vor Annahme von Aufträgen dokumentierter Weise durchzuführen
- die Erstellung und das Testen eines Haus-Graz-weiten ITK-Notfallwiederherstellungsplans (BRP) bzw. die Erstellung und das Testen von abgestimmten Teilplänen;
- die Durchführung regelmäßiger und dokumentierter Rücksicherungstests;
- die Dokumentation und regelmäßige Auswertung der Erfolgsraten im Rahmen des Incident- Handlings durchgeführter Rücksicherungen.
- ein Berechtigungskonzept für kritische Berechtigungen sowie deren Kombination zu entwickeln;
- Dezentrale Berechtigungsvergaben auf Ebene des Filesystems in der Komplexität zu beschränken, um die Überprüfbarkeit durch Data-

Owner zu ermöglichen.

- keine anonymen Zutrittskarten auszugeben, oder alternativ sicher zu stellen, dass für jede anonyme Karte zu jedem Zeitpunkt die/der InhaberIn archivecht dokumentiert ist.

Die folgenden Empfehlungen des Stadtrechnungshofs adressieren primär die IT-Governance oder die Auftraggeberinnen und ITG schlägt vor, diese im IKT-Beirat zu behandeln:
Der Stadtrechnungshof empfahl,

- bei kritischen Rollen die Konzentration des gesamten Wissens auf einzelne MitarbeiterInnen zu vermeiden und eine abgestimmte Nachfolgeplanung zu betreiben.
- in der Risikolandkarte IT-relevante Gefahren für das gesamte Haus Graz abzubilden.
- die Bewertung der Risiken und Ableitung von Maßnahmen aus einer Gesamtperspektive des Hauses Graz organisationsübergreifend festzulegen.
- regelmäßige Risk-Awareness-Trainings für IT-BenutzerInnen im Haus Graz zu veranstalten.
- zur Richtlinie BenützerInnenverwaltung in IT-Strukturen (IS-Richtlinie 1/2005 – Revision 2006): Neuregelung zur zentralen Veranlassung von berechtigungsrelevanten Änderungen der Stammdaten (Eintritt, Versetzung, Abteilungswechsel, Austritt, Pensionierung) durch das Personalamt bzw. die Personalabteilungen. Bestehende Berechtigungen wären mit dem Stichtag der Veränderung und vor Vergabe der neuen Berechtigungen zu entziehen. Berechtigungsanforderungen sollten durch die befugten Personen innerhalb der Dienststellen bzw. Abteilungen erfolgen. Weiters wäre die Zweckmäßigkeit und Ordnungsmäßigkeit des Richtlinieninhalts bezüglich der Formulierung „Sicherung des Postfachinhaltes über Outlook in eine PSD-Datei auf Datenträger (z.B. CD) für den/die InhaberIn des Postfaches“ zu prüfen – diese Regelung widersprach Erfordernissen des Amtsgeheimnisses.
- zur Richtlinie Benutzung und Behandlung von elektronischer Post (IS-Richtlinie 2/2005 – Revision 2008-2): Klärung der Klausel zur privaten Verwendung der dienstlichen eMail-Infrastruktur in Hinblick auf Data- Ownerschaft der eMail Korrespondenz sowie Ergänzung der Richtlinie um einen Passus, der das Beantworten von SPAM-eMails untersagt.
- zur Richtlinie Kennwortrichtlinie: Umwandlung der Empfehlungen zu der Komplexität von Passwörtern in Vorschriften und ihre

systemische Durchsetzung

- Zu Revisionierungen: Durchführung der geplanten Revisionen und/oder Evaluierung der Revisionszyklen sowie Festlegung einer einheitlichen Revisionsnummerierung.
- in Fällen in denen in einer Abteilung kein(e) MitarbeiterIn ausreichend für die Rolle als kundenseitig Projektleitung geeignet scheint, Unterstützung durch das jeweilige zentrale IKT-Auftragsmanagement beizustellen.
- die Erstellung eines verbindlichen Prozesses, der sicherstellt, dass mit der IT-Anforderung verbundene organisatorische Themen abgeklärt wurden.
- Änderungen oder Entwicklungen ausnahmslos nur nach einer dokumentierten Freigabe durch die anfordernde Abteilung sowie etwaige andere betroffene Abteilungen und System-OwnerInnen produktiv zu stellen;
- die bestehende ITG-Projektmanagementrichtlinie unter Hinzuziehung der Organisationsentwicklungsverantwortlichen zu einer allgemeinen Haus Graz Projektmanagementrichtlinie weiterzuentwickeln, diese zu schulen und die ausnahmslose Einhaltung der Richtlinie von den höchsten Führungsebenen durchzusetzten.
- auf Basis von der höchsten Führungsebene genehmigten, tolerablen Ausfallszeiten (RTO) und Datenverlustmengen (RPO) eine Backuprichtlinie zu erstellen.
- jede Veranlassung zur Änderung von berechtigungsrelevanten Stammdaten (Eintritt, Versetzung, Abteilungswechsel, Austritt, Pensionierung) durch das Personalamt bzw. die Personalabteilungen der Holding zu veranlassen und bestehende Berechtigungen bis zum Stichtag der Veränderung und vor Vergabe der neuen Berechtigungen zu entziehen. Berechtigungsanforderungen sollten durch Vorgesetzte erfolgen;
- Periodische Reviews der Berechtigungen durch die Data-Owner einzuführen;
- die automatisierten Kontrollen des Bereiches Identifikation und Authentisierung in SAP zu überarbeiten.
- die Erbringung der in dem Dokument „Rahmen IT-Governance“ definierten Leistungen regelmäßig zu überprüfen;

Die folgenden Empfehlungen des Stadtrechnungshofs beurteilt ITG nach einer Grobbewertung des dadurch erzielten Nutzens, des damit adressierten Risikos und des damit verbundenen Ressourceneinsatzes als nicht prioritär und ist daher keine unmittelbare Maßnahmenfestlegung

damit verbunden:
Der Stadtrechnungshof empfahl,

- die Erstellung einer Entwicklungsrichtlinie, die Coding-Standards vorgibt.
- die Einführung einer nachgelagerten Kontrolle, die eine sachlich angemessene Projektkategorisierung in Kleinprojekte und Nicht-Kleinprojekten sicherstellt.
- eine organisatorische Trennung zwischen Entwicklung und Transport in Produktivsysteme durchzusetzten. Sollte dies nicht möglich sein, wären angemessene nachgelagerte Kontrollen zu implementieren (z. B. Logging mit regelmäßiger, dokumentierter Durchsicht auf nicht freigegebene Transporte)
- die Prüfung von Punkt 2.6.2. Server-Housing des „Rahmen IT-Governance“ Dokumentes auf Klarheit der Anforderung sowie auf Zweckmäßigkeit;
- im Falle einer räumlichen Veränderung eines der Rechenzentren bei der Wahl eines neuen Standortes möglichst einen Mindestabstand der redundanten Rechenzentren zueinander von 1.500 Metern zu berücksichtigen.

Die folgenden Empfehlungen des Stadtrechnungshofs lösen für die ITG eine unmittelbare Maßnahmenfestlegung mit Umsetzungsplanung unter Berücksichtigung einsetzbarer Ressourcen aus:

Der Stadtrechnungshof empfahl,

- identifizierte Maßnahmen klar und spezifisch zu formulieren, Verantwortlichkeiten und Termine festzulegen und zentral zu überwachen sowie in den Reportingprozess an das Management einfließen zu lassen.
- eine Genehmigung durch die/den DatenbesitzerIn für die Verwendung von Produktionsdaten verpflichtend einholen zu lassen;
- die dokumentierte Überwachung kritischer Schnittstellen.
- die Verwendung von Superusern im Produktivsystem durch Trennung der Funktionen zu vermeiden oder alternativ dokumentierte nachgelagerte Kontrollen zu implementieren;
- den Bereich der Autorisierung in SAP zu überarbeiten.
- die automatisierten Kontrollen des Bereiches Systemintegrität in SAP zu überarbeiten.

Die folgenden Empfehlungen bedürfen aus Sicht der ITG einer weitergehenden Risiko-/Ressourcen- Analyse und abhängig vom Ergebnis

wird ITG eine Beurteilung vornehmen und diese mit dem Stadtrechnungshof abstimmen:

Der Stadtrechnungshof empfahl,

- jeden Test nachvollziehbar zu dokumentieren;
- die Dokumentation sämtlicher Schnittstellen;
- die automatisierten Kontrollen und die Gestaltung des Prozesses des Bereiches Änderungsmanagement in SAP zu überarbeiten.

Entgegnung des Stadtrechnungshofes:

Der Stadtrechnungshof betonte, dass er nur in den Fällen Empfehlungen aussprach, wo basierend auf den erhobenen Prüfnachweisen Handlungsbedarf gegeben war. Sollten die bestehenden Pläne so umgesetzt werden, dass sie die Umsetzung der Empfehlungen herbeiführen, so bekräftigt diese Übereinstimmung die Notwendigkeit der Umsetzung dieser Pläne.

6. Prüfungsmethodik

6.1. Prüfungsplanung und Durchführung

Die Prüfungsplanung und Durchführung der Prüfung orientierte sich am anzuwendenden INTOSAI Standard „ISSAI 5310 Information System Security Review Methodology“ sowie an den „IS Audit and Assurance Standards und Guidelines“ des ISACA Standards Board. Weitere Quellen waren die beiden Fachgutachten KFS DV1 und KFS DV 2 des Fachsenats für Datenverarbeitung der Kammer der Wirtschaftstreuhänder, COBIT® 5 for Assurance (ISACA), sowie der Prüfleitfaden SAP ERP 6.0 der deutschsprachigen SAP Anwendergruppe (DSAG).

Zur Beurteilung des Designs und der Effektivität des internen Kontrollumfeldes des zentralen IT-Bereichs des Hauses Graz wurden ausgewählte Schlüsselelemente eines internen Kontrollsystems aus IT-Organisation und IT-Prozessen evaluiert und geprüft. So wurde in Richtlinien eingesehen, Befragungen durchgeführt, Attribut-Stichproben gezogen sowie Begehungen durchgeführt. Die Ergebnisse hierzu wurden in den Kapiteln 3.1. IT-Organisation sowie 3.2. IT-Standardprozesse dargestellt.

Zur Beantwortung der Prüfungsfrage nach der Angemessenheit der automatisierten Kontrollen im Bereich SAP-BASIS wurden unter anderem etwa 50 kritische Systemparameter, sämtliche Standardbenutzer mit besonderen Berechtigungen, die Vergabe sämtlicher kritische Berechtigungsprofile sowie sicherheitsrelevante Einstellungen zu Datenbankzugriffen, Systemänderbarkeit, Mandantenänderbarkeit, Batch-Input-Mappen und der Sicherstellung der Nachvollziehbarkeit von Transaktionen im Produktivmandanten des Magistrats eingesehen und die Ergebnisse und Empfehlungen unter dem Kapitel 3.3. Kontrollen im Bereich SAP-BASIS ausgeführt.

6.2. Zur Prüfung herangezogene Unterlagen

Berichte über externe Prüfungen:

Management Summary und Maßnahmenplan der Security Prüfung 2012, undatiert

Dokumentationen:

Kurzfassung Netzwerk/Security-Plattform, erstellt aus der Online Dokumentation am 6. November 2013

Schnittstellenübersicht Magistrat, erstellt am 11. November 2013

Organigramme und Prozessdokumentation:

ITG ITIL-Prozesse im Lifecycle, Stand 16. Mai 2011

Organigramm der ITG, Stand 14. Mai 2013

Richtlinien:

BenutzerInnenverwaltung in IT-Strukturen IS-Richtlinie 1/2005, Revision 2006

Benutzung des Internets IS-Richtlinie 1/2006, Mai 2006

Benutzung und Behandlung von elektronischer Post IS-Richtlinie 2/2005, Revision 2008-2

Informationssicherheitspolitik Haus Graz, Version 3.0

Kennwortrichtlinie, Version 2.0

Projektmanagement Richtlinie ITG, Stand November 2012

Rahmen zur Ausrichtung der Informationstechnik Graz – IT-Governance, 12. März 2012

Sicherheitsklassifikation IS-Richtlinie 2/2009, Mai 2009

Systemzugang zur prüferischen Einsicht:

Filesystem Magistrat Graz

SAP-ERP, Magistrat, Nutzung des Profils „System Audit“

Strategie / Steuerung:

Rahmen zur Ausrichtung der Informationstechnik Graz – IT-Governance, 12. März 2012

SLAs Nr.: 01, 09, 11, 20, 22, 50, 54, 60, 102, 128, 275, 319, 358 sowie die SLAs zu Eulvis, GIS und Opentext

Protokoll zur konstituierenden Sitzung des IKT-Board vom 31.Mai 2012

Protokolle des IKT-Beirates vom 16. Oktober 2013, 27. Juni 2013 und 20. März 2013

Protokolle von ITG-Führungsteamsitzungen vom 27.11.2013, 20.11.2013, 13.11.2013, 28.10.2013, 23.10.2013, 9.10.2013, 02.10.2013, 18.09.2013, 28.08.2013 und vom 14.08.2013

Verträge / Vereinbarungen:

Vereinbarung zur Zusammenarbeit – 1st Level Support, 18. Mai 2000

6.3. Besprechungen

- Erhebungen fanden am 5., 8., 11., 15 und 28. November 2013 in den Räumlichkeiten der ITG statt.
- Am 25. November 2013 fand eine Besprechung mit dem IKT-Auftragsmanagement des Magistrats Graz in den Räumlichkeiten des IKT-Auftragsmanagement statt.
- Die Schlussbesprechung wurde am 27. November 2013 in den Räumlichkeiten des StRH durchgeführt.

Prüfen und Beraten für Graz

Seit 1993 prüft und berät der Stadtrechnungshof der Landeshauptstadt Graz unabhängig die finanziellen und wirtschaftlichen Aktivitäten der Stadtverwaltung. Seit 2011 ist er darüber hinaus die einzige Stelle, die in das gesamte Haus Graz, also die Stadtverwaltung und die Beteiligungen der Stadt Einblick nehmen darf.

Der vorliegende Bericht ist ein Prüfungsbericht im Sinne des § 16 der Geschäftsordnung für den Stadtrechnungshof. Er kann personenbezogene Daten im Sinne des § 4 Datenschutzgesetz 2000 enthalten und dient zur Vorlage an den Kontrollausschuss.

Die Beratungen und die Beschlussfassung über diesen Bericht erfolgen gemäß dem Statut der Landeshauptstadt Graz 1967 in nichtöffentlicher und vertraulicher Sitzung.

Die Mitglieder des Kontrollausschusses werden daran erinnert, dass sie die Verschwiegenheitspflicht wahren und die ihnen in den Sitzungen des Kontrollausschusses zur Kenntnis gelangten Inhalte vertraulich zu behandeln haben.

Eine hinsichtlich der datenschutzrechtlichen Einschränkungen anonymisierte Fassung dieses Berichtes ist ab dem Tag der Vorlage an den Kontrollausschuss im Internet unter http://stadtrechnungshof.graz.at abrufbar.

Der Stadtrechnungshofdirektor

Mag. Hans-Georg Windhaber, MBA

GRAZ DIGITALE SIGNATUR	**Signiert von**	Windhaber Hans-Georg
	Zertifikat	CN=Windhaber Hans-Georg,O=Magistrat Graz,L=Graz, ST=Styria,C=AT
	Datum/Zeit	2013-12-18T13:55:41+01:00
	Hinweis	Dieses Dokument wurde digital signiert und kann unter: http://egov2.graz.gv.at/pdf-as verifiziert werden.