GRC STANDARD CLOUD
SECURITY

T-Systems Austria GesmbH

Version 1.0
Stand 19.12.2016
Status Final

T · · Systems ·

IMPRESSUM

Herausgeber

T-Systems Austria GesmbH
Security Management
Rennweg 97-99
1030 Wien
AUSTRIA

Version	Stand	Status
1.0	19.12.2016	Final

Autor	Inhaltlich geprüft von	Freigegeben von
Krucher Martina	Thomas Lint	Thomas Masicek
Security Management TSA	Security Management TSA	Head of Cyber Security

Kurzinfo

Zusammenfassung der Security-Maßnahmen der GRC Standard Cloud Plattform von T-Systems Austria.

INHALTSVERZEICHNIS

1 MANAGEMENT SUMMARY

Cloud, Virtualisierung und Dynamic Services sind wichtige ICT-Trends des 21. Jahrhunderts. Generell bieten Cloud Technologien höhere Skalierbarkeit, variable Preisgestaltung nach Nutzung, hohe Standardisierung und allgemeine Kostensenkung im Vergleich zu herkömmlichen Outsourcing Dienstleistungen. Diskussionsbedarf besteht dabei hauptsächlich im Bereich IT-Sicherheit und Datenschutz, unteranderem aufgrund intransparenter Datenverarbeitung.

Die GRC (Governance Risk and Compliance) Standard Cloud ist ein von T-Systems Austria angebotenes Cloud-Service auf Basis von Avedos risk2value als Managed Service.

Beim Delivery-Modell GRC Standard Cloud ist die GRC-Umgebung in der vCloud von T-Systems Austria gehostet. Jeder Kunde des GRC Standard-Modells hat dabei seinen dedizierten Webserver; die darunterliegende Datenbank wird durch Mandantentrennung zwischen mehreren Kunden geteilt.

Die Cloud Services der T-Systems besitzen ein einheitliches Sicherheitsniveau, welches mittels T-Systems interner Standards definiert wurde und durch verschiedene Sicherheitsmaßnahmen erreicht wird. Die Sicherheitsmaßnahmen werden in diesem Dokument beschrieben, um Kunden über Sicherheitsprinzipien der GRC Standard Cloud, gehostet auf vCloud, zu informieren.

Generell sind die internen Standards der T-Systems Bestandteil des ISO/IEC 27001-zertifizierten Informations-Sicherheit-Management Systems. Dazu gehören unter anderem auch die Identifizierungen, Bewertungen und die Behandlung von Risiken. So wurde für Plattform vCloud eine Risikobewertung durchgeführt und entsprechende Sicherheitsmaßnahmen abgeleitet und umgesetzt. Die Wirksamkeit dieser Maßnahmen wurde im Rahmen von Konfigurations- und Penetrationtests verifiziert.

Dieses Dokument stellt die Sicherheitsmaßnahmen dar, welche von T-Systems Austria zur Absicherung der GRC Cloud Umgebung getroffen wurden.

2 CLOUD-BASIERTE ICT-LEISTUNGEN – GEFÄHRDUNGEN UND SCHUTZMASSNAHMEN

Im Vergleich zu traditionellen ICT-Dienstleistungen sind beim Risiko-Assessment für Cloud-basierte ICT-Services die Schwerpunkte anders verteilt. Die folgende Tabelle listet typische Gefährdungen Cloud-basierter Dienste wie der GRC Standard Cloud sowie spezielle Schutzmaßnahmen, welche von T-Systems zur Absicherung der GRC Cloud getroffen werden.

Gefährdungen	Schutzmaßnahmen

Ausspähen von Informationen / Spionage	▪ Netzwerktrennung in der vCloud sowie Sicherung mittels dedizierter virtualisierter Firewalls und gesicherten WAN-Verbindungen
	▪ Kunden-Trennung in der vCloud
	  ▪ auf Netzwerkebene mit logischer Trennung basierend auf virtuellen Netzwerken,
	  ▪ auf Systemebene mit Hypervisor-Sicherheit,
	  ▪ auf Speicherebene über Hypervisor-Verkapselung.

Abhören	▪ Absicherung aller externen Kommunikationsverbindungen durch Überprüfung auf Paketebene (Reverse Proxy, Stateful-Firewall) ▪ Verschlüsselung (beispielsweise https beim vCloud Director)
Fehlplanung oder fehlende Anpassung	▪ Externe und interne Sicherheits- und Qualitätsprüfungen (auch durch Zertifizierungen belegt)
Offenlegung schützenswerter Informationen	▪ Funktionale und Penetration-Tests um den korrekten Prozessflow der Anwendung zu gewährleisten ▪ Zugriff auf vCloud Director aus dem Internet ist über die WAF und ein rollenbasiertes Berechtigungskonzept gesichert
Unbefugtes Eindringen in IT-Systeme	▪ Identity und Access Management für einen privilegierten Zugang zu Kunden- und Plattform-Systemen ▪ Security-Management-Prozesse einschließlich Risikomanagement, Sicherheitsvorfall-management, Schwachstellenmanagement ▪ Bestätigung des hohen Sicherheitsniveaus durch interne und externe Penetrationstest ▪ Segmentierung des Netzwerks ▪ Logging
Software-Schwachstellen oder Fehler	▪ Verifizierung des Sicherheitsniveaus durch interne und externe Penetrationstest

	▪ Funktionale Tests ▪ Patch Management basierend auf ITIL
Verstoß gegen Gesetze oder Regelungen	▪ Rechtliche Rahmenbedingungen für die Datenverarbeitung: österreichisches (und europäisches) Datenschutzrecht
Unberechtigte Nutzung oder Administration von Geräten und Systemen	▪ Administrative Arbeiten an der Cloud-Plattform erfolgen über interne Providerverbindungen ▪ Logging ▪ Zugriff auf alle Komponenten basierend auf einem rollenbasierten Berechtigungskonzept ▪ Segmentierung des Netzwerks
Fehlerhafte Nutzung oder Administration von Geräten und Systemen	▪ ITIL-basierte Prozesse für Patch Management, Change Management und Incident Management ▪ Zugriff auf alle Komponenten basierend auf einem rollenbasierten Berechtigungskonzept ▪ Logging
Missbrauch von Berechtigungen	▪ Security und Compliance Logging und Monitoring ▪ Identity und Access Management für einen privilegierten Zugang zu Kunden- und Plattform-Systemen

3 GRC CLOUD HOSTED @ T-SYSTEMS AUSTRIA DC

Die GRC Cloud wird vollständig auf der vCloud von T-Systems Austria betrieben. Diese ist in den Rechenzentren der T-Systems Austria in Wien gehostet.

T-Systems Austria betreibt in Wien zwei Rechenzentren an Standorten mit einer geografischen Distanz von rund 10 km. Beide Standorte übererfüllen die Tier3 Spezifikation des Uptime Institutes und sind nach ISO 9001: 2000, ISO 20000, ISO IEC 27001 und nach ISAE 3402 zertifiziert.

Die vCloud als Plattform für die GRC Cloud nutzt die folgenden Rechenzentren:

- Rechenzentrum T-Center, Rennweg 97-99, 1030 Wien, Österreich
- Rechenzentrum ODC (On-Demand-Center), Richard Neutra Gasse 10, 1210 Wien, Österreich

An beiden Standorten wurden Vorbereitungen getroffen, um den Betrieb der gesamten Systemlandschaft auch im Katastrophenfall sicherstellen zu können. Beide Standorte verfügen über ein komplett ausgerüstetes Lagezentrum.

Die Leitungslängen zwischen den primären Rechenzentren sind wie folgt:

- Weg Reichsbrücke: ca. 20 km
- Weg Floridsdorfer Brücke: ca. 30 km

Rechenzentrum T-Center

Im Hauptrechenzentrum T-Center verteilen sich 16 Rechenzentrumszellen symmetrisch auf zwei baulich getrennte Fundamentplatten. Diese statische Entkoppelung in zwei getrennte Gebäudeteile stellt selbst beim Einsturz einer Gebäudehälfte die weitere Nutzbarkeit des Standortes sicher.

Im Rechenzentrum stehen folgende **Flächen** zur Verfügung
- 2.913 m² Serverraumfläche.
- 6.000 m² Infrastrukturfläche (für NEA, Klima, Kaltwasser, USV und Batterien, etc.).

Die 16 Zellen erstrecken sich über 2 Etagen. Acht Zellen befinden sich im 2. Untergeschoss, 8 weitere Zellen im 4. Untergeschoss rund 15m unter Straßenniveau. Derzeit sind 14 Zellen nutzbar und 2 Zellen für künftige Erweiterung vorbereitet. Für die Erweiterungsflächen sind alle baulichen Voraussetzungen einschließlich Verkabelung und Verrohrung der Infrastruktur vorhanden, es fehlen lediglich die Gewerke (wie z.B. Doppelboden, Umluftkühler, etc.).

Das Rechenzentrum verfügt außerdem über wettergeschützte Anlieferungsmöglichkeit für LKWs im Untergeschoss. Über die Zufahrt auf der Seite des Rennwegs gibt es einen Lastenaufzug für Lieferungen in die Räumlichkeiten des 2. Untergeschoss.

Sicherheit

Im Bereich der Sicherheit wurden im Data-Center die folgenden **Maßnahmen** ergriffen:
- Elektromagnetisches Zutritts-System (Magnetkarte + PIN-Code, Vereinzelungsanlage),
- Kameraüberwachung mit digitaler Aufzeichnung mit ca. 400 Kameras,
- 7 x 24 Stunden Überwachung der Rechenzentrumsflächen, integriert in Gebäudeleittechnik,
- 7 x 24 Stunden Sicherheitsdienst durch 4 Personen vor Ort,
- Gesichertes Kommunikations-System über optisches und wireless Netzwerk.

Brandschutz

Zum Schutz gegen mögliche Brände verfügt das Rechenzentrum über eine hochmoderne Argon-Gaslöschanlage, welche brandfallgesteuert (automatisch) in Betrieb geht und dadurch die Sicherheit weiter erhöht.

Weitere Brandschutzeinrichtungen im Rechenzentrum des T-Centers sind:

- RAS Anlagen (zur Brandfrüherkennung),
- 2 separate Rauchmeldeleitungen für jede Alarm Zone,
- Direkte Alarm-Anbindung zur Feuerwehr.

Stromversorgung

Der reibungslose Betrieb eines Unternehmens ist heute von einer funktionierenden IT abhängig. Netzstörungen der verschiedensten Art verursachen Unterbrechungen, die zu erhebliche Kosten und Schäden von Unternehmen führen können.

Daher wurden im Bereich des Power-Managements folgende **Anlagen** integriert:

- USV-Anlagen mit Batterieanlagen für 70 bzw. 40 Minuten Überbrückungszeit bei Volllast,
- Redundante USV-Anlage für jeden Rechenzentrumsblock,
  - 8 Serverräume pro Block,
  - 2 Produktive / 1 Backup USV Anlage pro Block (6x 625 kVA).
- 4 Dieselaggregate, davon 3 ausschließlich für das Rechenzentrum.
  - 43.000 Liter Dieselkraftstoff in Tanks vor Ort.
  - Automatischer Start bei Stromausfall.
  - Nach 90 Sekunden 100% der Kapazität verfügbar.
- Getrennte EVU Einspeisungen (2 x 10 kV Leitungen / 4000 KW) mit Load-Sharing und Automatic-Failover.
- 14 redundant ausgelegte Transformatoren (10 kV) nach dem n+n+1 Prinzip (1 Transformator im „Cold-Standby“).
- 1,8 MW (redundant) im Rechenzentrum verfügbar.
- Stromschienen System, Rack-Zuführung redundant ausgelegt.

Klimaanlage

Die Kälteversorgung ist hocheffizient ausgelegt. Die Klimatisierung arbeitet mit einer Leistungszahl von ca. 6. Das bedeutet dass mit einem Leistungsinput von 1 Kilo Watt rund 6 Kilowatt Kühlleistung bereitgestellt werden können.

- 3 Kälteanlagen mit je 2.500kW redundant ausgelegt.
- 2 getrennte Kühlkreisläufe zu den Umluft-Kühlern plus 1 Backup-Kühlkreislauf

Rechenzentrum ODC

Die Fläche des zweiten Rechenzentrums beträgt ca. 3000m² reine Serverraumfläche. Derzeit werden vom AUFTRAGNEHMER knapp 300m² genutzt.

Sämtliche Infrastruktur Systeme für das Ausfall-Rechenzentrum befinden sich in einem eigenen Brandabschnitt und belegen eine Gesamtfläche von ca. 1500m².

Sicherheit

Im Bereich der Sicherheit wurden im Data-Center die folgenden Maßnahmen ergriffen:

- Elektromagnetisches Zutritts-System (Magnetkarte + PIN-Code, Vereinzelungsanlage)
- Automatisches Videoüberwachungssystem. Komplette Kameraüberwachung in den Außenbereichen und partielle Kameraüberwachung innerhalb des Gebäudes.
- 7 x 24 Stunden Überwachung der Rechenzentrumsflächen in Gebäudeleittechnik integriert
- 7 x 24 Stunden Sicherheitsdienst vor Ort.

Brandschutz

Als Brandschutzmaßnahmen im Ausfall-Rechenzentrum können folgende Anlagen genannt werden:

- Zwei separate Rauchmeldeleitungen für jede Alarm Zone.
- RAS Anlagen (Brandfrüherkennung).
- Automatische Gaslöschanlage (INERGEN).
- Direkte Alarm-Anbindung zur Feuerwehr.

Stromversorgung

Die Energieversorgung ist auch im ODC-Data Center gegen jegliche Unterbrechung gesichert. Hier können folgende Anlagen aufgezählt werden:

- Redundante Dieselaggregate.
  - 100.000 Liter Dieselkraftstoff in Tanks vor Ort.
  - 2 x 2000 kVA
  - Automatischer Start bei Stromausfall.
  - Nach 90 Sekunden 100% der Kapazität verfügbar.
- USV-Anlagen mit Batterieanlagen für 20 Minuten Überbrückungszeit bei Volllast.
- Redundante USV-Anlage.
  - 2 Produktive / 1 Backup USV Anlage pro Block.
- Redundante EVU Einspeisungen (10 kV Leitungen / 4000 KW).
- Zwei redundant ausgelegte Transformatoren nach dem n+1 Prinzip mit je 4MW.

Klimaanlage

Die Kälteversorgung kann durch folgende Daten charakterisiert werden:

- 2 x 3 Kälteanlagen mit je 640kW.
- Zwei getrennte Kühlkreisläufe zu den Umluft-Kühlern (Ringleitung).

Verbindung zwischen den Rechenzentren

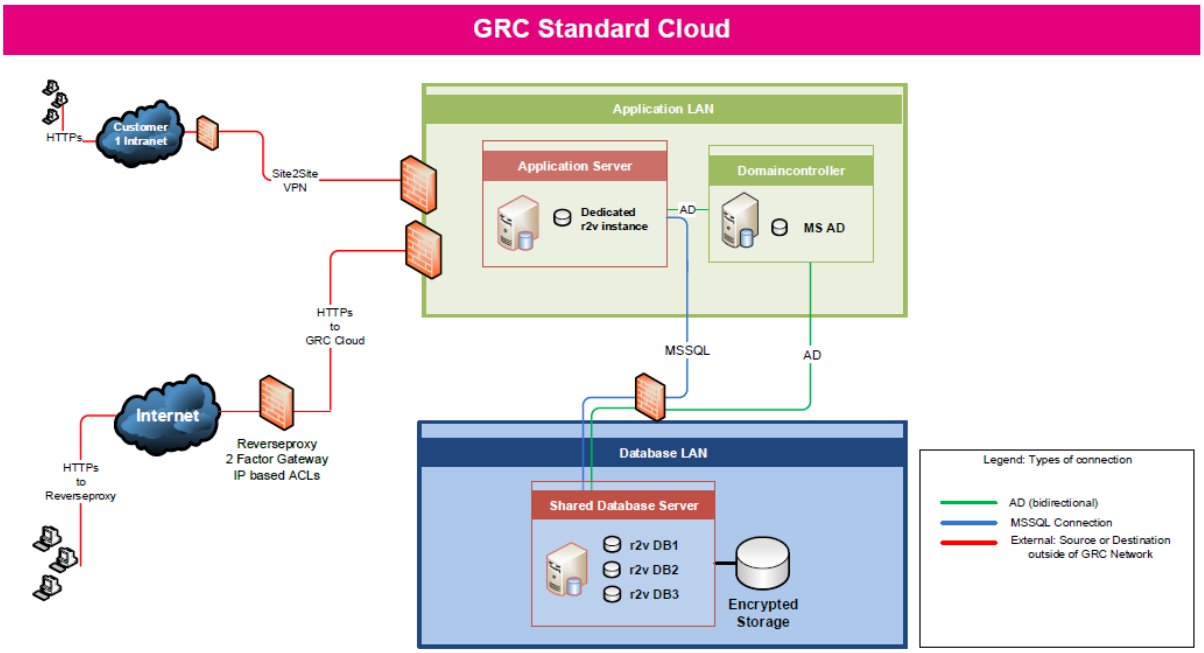
Die Verbindung der beiden Standorte T-Center sowie ODC erfolgt mittels Single Mode Fasern (Dark Fibre) und ist wegredundant ausgeführt. Die gebäudeseitige Einspeisung erfolgt von 2 unterschiedlichen Punkten. Die Donauquerung erfolgt sowohl über die Reichsbrücke als auch über die Floridsdorfer Brücke.

Durch die Kopplung dieser beiden Rechenzentren entsteht der sogenannte „Twin Core“-Rechenzentrumsverbund.

Die Leitungslängen zwischen den Rechenzentren sind ca. 20 km über den Weg Reichsbrücke und 30 km über den Weg Floridsdorfer Brücke.

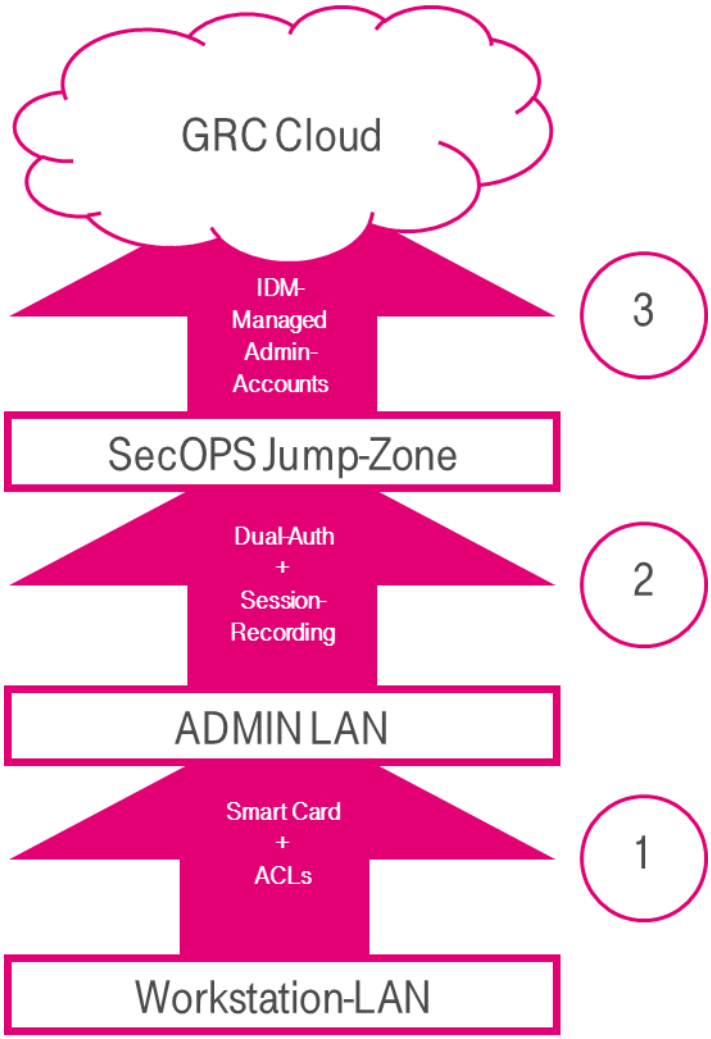
4 DELIVERY-MODELL GRC STANDARD CLOUD

Die GRC Standard Cloud nutzt die vCloud von T-Systems Austria als darunter liegende Plattform. Innerhalb der GRC Cloud besitzt jeder Kunde beim Delivery-Modell GRC Standard Cloud einen dedizierten Application Server. Die Datenbank ist eine Shared-Instanz zwischen mehreren Kunden, wobei die Mandantentrennung innerhalb der MSSQL Datenbank umgesetzt ist. Die Datenbank ist auf verschlüsseltem Storage abgelegt.
Die nachfolgende Grafik stellt die Architektur des Modells GRC Standard Cloud dar.



5 ADMINISTRATIVER ZUGRIFF AUF GRC STANDARD CLOUD

Der Betrieb und somit der administrative Zugriff auf die Komponenten der GRC Standard Cloud geschieht allein durch das Security Operations Team von T-Systems Austria. Wie die nachfolgende Grafik zeigt, ist der Zugriff auf die GRC Cloud nur möglich, wenn die drei in der Grafik abgebildeten Stufen durchlaufen werden. Diese werden nachfolgend erläutert.



Stufe 1

Damit die Administratoren des Security Operations Teams vom Workstation-LAN auf das Admin LAN zugreifen können, benötigen sie eine personalisierte Smart Card mit Zertifikat. Der Zugriff auf das Admin LAN ist über ein Smart-Card basiertes VPN möglich, wobei der Administrator zum Zugriff in der richtigen Admin LAN Gruppe sein muss. Die Mitgliedschaften in den gruppenbasierten ACLs (Access Control Lists) müssen alle sechs Monate durch den Vorgesetzten des Mitarbeiters reviewt werden.

Stufe 2

Nach der Authentifzierung im Admin LAN durch die Smart Card ist es dem Administrator des Security Operations Teams möglich, sich auf einen Sprungserver (SecOPS Jump Server) zu verbinden. Für die Verbindung auf den SecOPS Sprungserver ist eine zweifache Authentifizierung im Admin LAN notwendig: der Administrator benötigt einerseits einen

Internationalen T-Systems Account, andererseits einen Account in der eigenen administrativen Domäne von T-Systems Security Operations in der vCloud – T-SEC. Alle Domänen besitzen für administrative Zwecke gehärtete Domain-Settings (Session Timeout, Password Ageing, Lockout) und werden regelmäßig in Audits überprüft.

Die Sprungserver im Admin LAN sind darüber hinaus mit einer Software zum Session Recording (ObserveIT) ausgestattet. Mit dieser Software ist es möglich, administrative Tätigkeiten auf den Kunden-Systemen der GRC Cloud aufzuzeichnen und im Anlassfall detailliert zu untersuchen. Darüber hinaus werden Authentifizierungs-Logs der Sprungserver für 90 Tage aufbewahrt.

Stufe 3

Innerhalb der GRC Cloud geschieht die Account-Verwaltung der administrativen Accounts der einzelnen Hosts (root, Administrator) durch die RMDB (Rights Management Database) von T-Systems Austria. Die RMDB gewährleistet die zentrale technische Umsetzung des Benutzerverwaltungsprozesses in der GRC Cloud. Sämtliche vergebene Rechte werden durch entsprechende Tasks in der RMDB periodisch auf ihren fortwährenden Bedarf überprüft und die Ergebnisse werden revisionssicher dokumentiert. Die Rechtevergabe in der RMDB ist so implementiert, dass nur das Security Operations Teams von T-Systems Austria Zugriff auf die Passwörter der GRC Cloud Komponenten hat. Innerhalb der RMDB wird außerdem ein periodischer Review über die Zugriffsrechte durchgeführt.

Die RMDB ermöglicht darüber hinaus einen automatisierten Passwort-Wechsel der administrativen Accounts der GRC Cloud (root, Administrator), wodurch ein Audit-konformer Passwort-Lebenszyklus von maximal 90 Tagen effektiv und nachweisbar sichergestellt wird.

6 QUALITÄTSMANAGEMENT

Grundsätzlich verfolgt das Qualitätsmanagement bei T-Systems fünf Hauptziele:

- Die Kundenperspektive muss in Qualitätsziele für T-Systems und die Leistungseinheiten von T-Systems übersetzt werden (**Kundenzentrierung**).
- Qualität muss **proaktiv** gewährleistet werden, indem durchgängig Qualitätsziele in die Planungs- und Implementierungsphasen (Plan und Build) eingebaut werden.
- Qualität muss **reaktiv** gewährleistet werden, indem die Kundenlösung ständig auf übergreifende oder spezifische Qualitätsdefizite überwacht wird und auf Abweichungen reagiert wird (Qualität in der Run Phase).
- Es muss ein **Überblick** über die aktuelle Qualitätssituation und die Leistungsqualität der leistungserbringenden Einheiten aus Sicht des Kunden geschaffen werden.
- Die **Qualitätsstandards** müssen über alle leistungserbringenden Einheiten **harmonisiert** werden.

Um diese Ziele zu erreichen, hat T-Systems die ständige Verbesserung der Servicequalität auf mehrere Pfeiler gestellt:

- Ein integriertes Managementsystem fördert und entwickelt kunden- und qualitätsorientiertes Handeln.
- Kundenorientierung: Der Kunde entscheidet, was Qualität ist. Best Practices und Excellence-Modelle dienen als Richtschnur für Kundenorientierung.
- Corporate Process Management: Exzellentes Prozessmanagement ist ein entscheidender Hebel zur Steigerung der Kundenzufriedenheit.
- Projektmanagement als Kernkompetenzen: Nur mit einem effektiven Projektmanagement lassen sich Kundenanforderungen erwartungsgemäß erfüllen.
- Erfolgreiches Service Management heißt, schnell auf Probleme zu reagieren und die Qualität und Wirtschaftlichkeit des Service laufend zu verbessern.

1.1 Integriertes Managementsystem

Das Qualitätsmanagement der T-Systems ist als integriertes Managementsystem konzipiert, das gewährleistet, dass alle bestehenden und zukünftigen Normanforderungen in ein einheitliches Managementsystem integriert werden und die vorhandenen Synergien zwischen den bestehenden Normen, Standards und Systemen optimal genutzt werden.

Das integrierte Managementsystem der T-Systems umfasst das Qualitäts-, Informationssicherheits-, IT-Service-, Umwelt- und Arbeitsschutzmanagement.

Zum Integrierten Managementsystem der T-Systems gehören die Strategien, Organisationsstrukturen, Zuständigkeiten, Verfahren, Prozesse und Mittel, die für eine kundenorientierte und geschäftlich erfolgreiche Arbeit notwendig sind. Darüber hinaus fasst es die relevanten Normanforderungen zusammen.

T-Systems stellt die folgenden Anforderungen an sein Managementsystem:

- Kundenorientierung steht im Mittelpunkt aller Geschäftsprozesse:
  Die externe Schnittstelle zum Kunden ist das Service Management (bei T-Systems getragen vom Service Delivery Manager). Über das Service Management werden die Kundenanforderungen in die Prozesse und das Qualitätsmanagement eingebracht.
- Kunden werden regelmäßig aufgefordert, den Service zu bewerten und Rückmeldungen zur Leistungsqualität zu geben (Kundenzufriedenheitsbefragung nach der TRI*M-Methode). Die daraus abgeleiteten Maßnahmen werden konsequent umgesetzt. Mit

regelmäßigen Monitorings werden Implementierung, Fortschritt und Zielerreichung der Maßnahmen überwacht.

- Geschäftsprozesse werden ziel- und qualitätsorientiert und mit definierten Verantwortlichkeiten durchgeführt.
- Prozesse und Methoden werden zentral definiert und global in alle Ländereinheiten eingeführt. Über einheitliche Prozesse und Methoden wird eine fortlaufende Serviceverbesserung gewährleistet
- Mitarbeiter werden über Ziele und Arbeitsprozesse umfassend informiert und für die anstehenden Aufgaben geschult.
- Interne Organisationseinheiten kommunizieren in geeigneter Weise miteinander.
- Geschäftsprozesse und deren Ergebnisse werden laufend bewertet und verbessert.

1.2 Qualitätssicherung

Alle Geschäftsprozesse werden kontinuierlich auf Verbesserungsmöglichkeiten hin überprüft unter der Leitung der Prozess-Verantwortlichen und mit Einbindung des Verantwortlichen für den jeweiligen Geschäftsbereich. Hiermit wird die Möglichkeit geschaffen, auf der Basis der gemessenen Prozessleistung und der ermittelten Prozessreife Ursachen zu erforschen, Optimierungspotenzial abzuleiten sowie konkrete Verbesserungsmaßnahmen zu projektieren und durchzuführen.

Die interne Qualitätssicherung wird von einem übergreifenden Lenkungsausschuss (PQ-Board) für Prozesse, Qualität und Sicherheit gesteuert, dessen Mitglieder aus den verschiedenen organisatorischen Einheiten der T-Systems kommen.

1.3 Normative Standards der T-Systems

Standard	Thema	Zertifiziert seit
ISO/IEC 9001:2008	Quality Management	1995
ISO/IEC 14001:2009	Environmental Management Systems	2010
OHSAS 18001	Occupational Health and Safety Management	2010
ISO/IEC 20000-1:2011	IT Service Management	2008
ISO/IEC 22301:2012	Business Continuity Management	2015
ISO 27001:2013	Information Security Management	2005
SAS 70	Internal Control System	2005-2011
ISAE 3402 (vormals SAS 70)	Internal Control System	2011