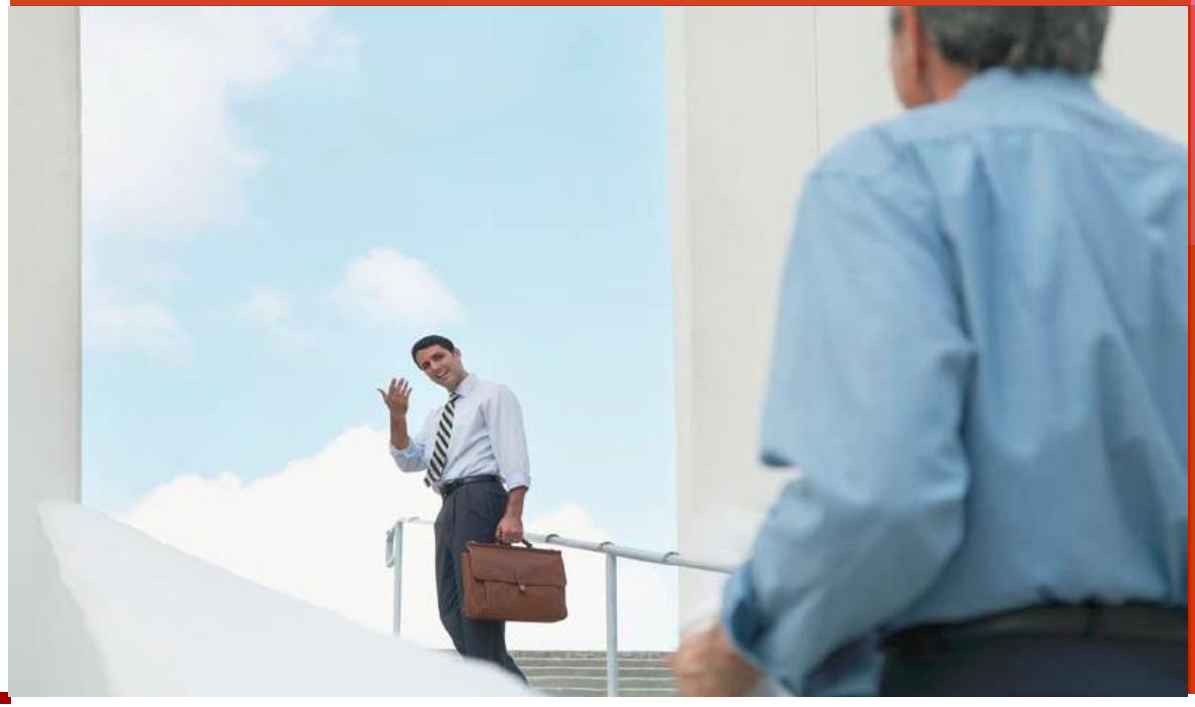
www.pwc.at/cloud

ERP Cloud Sourcing als Lösungsoption für die alten und neuen Herausforderungen im Bereich der IT Finanz- und Risikoarchitektur

Oktober 2014



pwc

Agenda

1. Anforderungen an die IT-Finanz und Risikoarchitektur

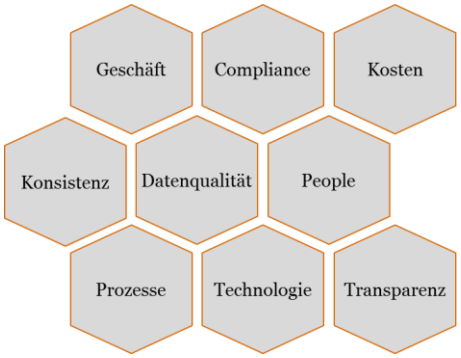
Steigende Anzahl von regulatorischen und geschäftlichen Anforderungen in die IT

Große Modernisierungs-projekte sind primär durch neue Regularien motiviert. Technologische Aspekte sind zweitrangig	Die Vielzahl und die Frequenz neuer Anforderungen setzen eine integrierte IT-Finanzarchitektur voraus, in welcher Anpassungen flexibel und effizient vorgenommen werden können	Die Voraussetzungen für eine zielgerichtete Gestaltung und das Management von IT-Finanzarchitekturen fehlen
• Bewusstsein für operationelle Risiken aus Altsystemen schaffen • Analyse Betriebs-investitionsplanung	• Standardisierung von Systemen und Prozessen • Schaffung einer darauf abgestimmten Organisation	• Transparenz über definierte Leistungsmerkmale • strategische Planung mit verschiedenen Szenarien

2. Handlungsfelder und Herausforderungen bei Umsetzung

Integrität, Verfügbarkeit und Verlässlichkeit der Finanz-und Risikodaten kritisch

Handlungsfelder durch Regulatorien / Geschäftsentwicklung bestimmt, Herausforderungen bei Umsetzung historisch gewachsen



Handlungsfelder & Herausforderungen

Die strategische Weiterentwicklung der IT-Finanzarchitekturen erfolgte in der Vergangenheit meist einem reaktiven Ansatz der bloßen Anpassung auf neue regulatorische Anforderungen.

Folgen dieser eher passiven Vorgehensweise und der geänderten Rahmenbedingungen sind nach unserer Erkenntnis häufig:

- Unzureichende Unterstützung der Anforderungen
- Unstimmiges fachlich-technisches Gesamtbild
- Veraltete Technologien und steigende Wartungs-Kosten
- Lange Umsetzungsdauer von neuen Anforderungen

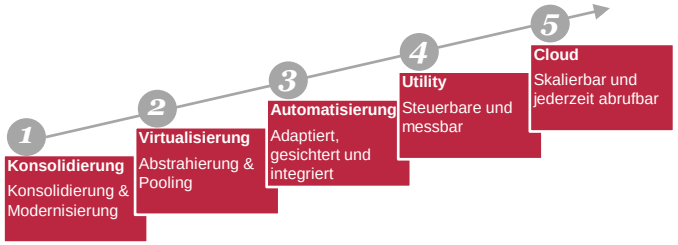
Zunehmendes operatives Risiko

Den jüngsten Trends am Markt und den Ergebnissen unserer Studie (siehe folgend sind wir der Meinung, dass ERP Cloud Sourcing das Potenzial bietet, die erwähnten Herausforderungen zu bewältigen.

3. ERP Cloud Sourcing als möglicher Lösungsansatz?

Neben den verbundenen Chancen sind auch die Risiken zu betrachten!

Abdeckung der Handlungsfelder durch Spezialisierung der Anbieter?



Evolutionsstufen Cloud Sourcing

Die Anforderungen der Finanzdienstleister im Finanz- und Risikoumfeld in Bezug auf Erfüllung der rechtlichen- und compliance Vorgaben, der Anforderungen in Bezug auf Performance und Datenkonsistenz sind hoch, jedoch zeigt unsere Studie aus dem Jahr 2013, dass der Reifegrad der Cloud Anbieter zugenommen hat.

Unsere Projekterfahrungen bestätigen diesen Trend der zunehmenden Professionalisierung und Spezialisierung auf Anbieterseite und der Zunahme des Reifegrades

Potenziale für Banken und Finanzdienstleister

Neben den allgemeinen Vorteilen von Cloud Services bieten sich unserer Einschätzung nach speziell für Banken bei kurz-mittel-langfrist-Betrachtung folgende Potenziale:

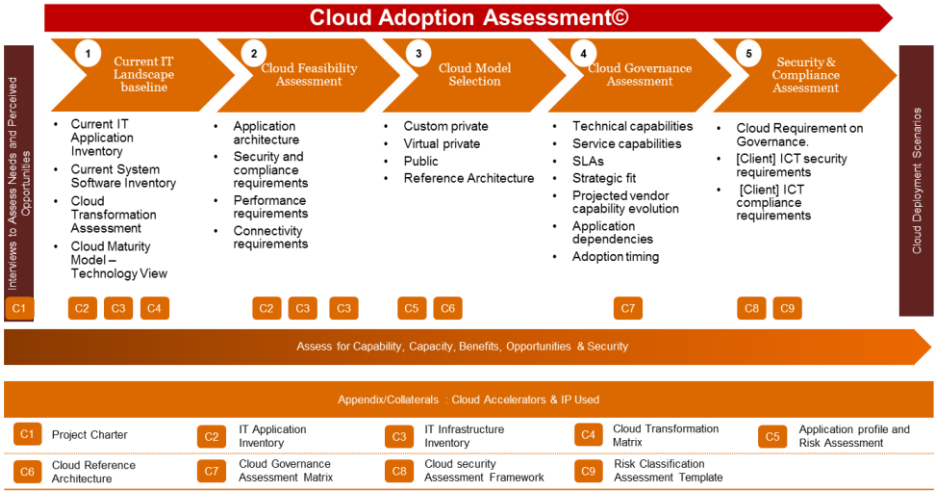
- Entlastung der Fachbereiche bei Umsetzung neuer gesetzlicher Anforderungen (IFRS9,13, Basel III)
- Standardisierung der Prozesse im Tagesgeschäft, effizienterer Ressourceneinsatz bzw. Kostensenkung
- Verkürzung der Durchlaufzeiten von Abschluss – Berichterstellung und Reduktion operationales Risiko
- Verlässliche Umsetzung von regulatorischen Anforderungen

4. Potenzialbewertung von ERP Cloud Sourcing als Basis

PwC's Cloud Adaption Assessment zur objektiven Bewertung von Chancen & Risiken

PwC's Cloud Adoption Assessment© Methodologie als Basis zur Entscheidungsfindung

Auf Basis des erprobten Vorgehensmodells, welches an Ihre Bedürfnisse im Projekt maßgeschneidert wird, erfolgt die Identifikation und Bewertung der Potenziale in Bezug auf ERP-Cloud Sourcing im Finanz- und Risikobereich:



Neben den allgemeinen Kriterien werden folgende harte Kriterien und Methoden, welche speziell auf diesen Bereich zugeschnitten sind, in die Bewertung einbezogen der Ziellösung einbezogen:

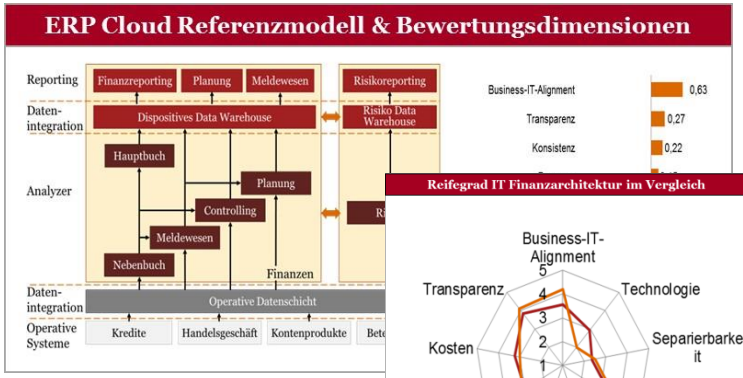
- Capability & Capacity
- Benefits & Opportunities
- Risk & IT / Information Security

Internationale Finanzdienstleister machen es vor und haben teile ihrer ERP und weitere Core-Systeme schon in die Cloud ausgelagert.

5. Überblick Hauptergebnistypen aus Potenzialbewertung

Bewertung von Capability & Capacity, Benefits & Opportunities, Risk & Security

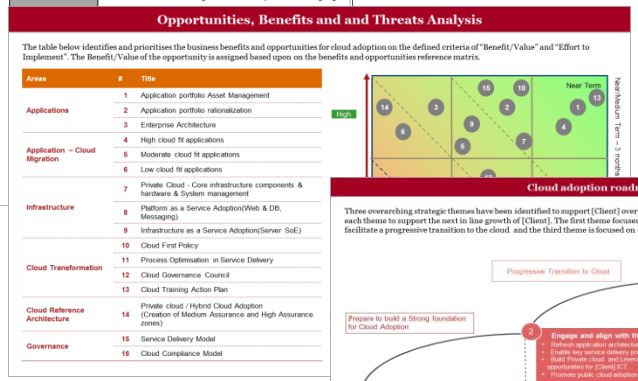
ERP Cloud Referenzmodell



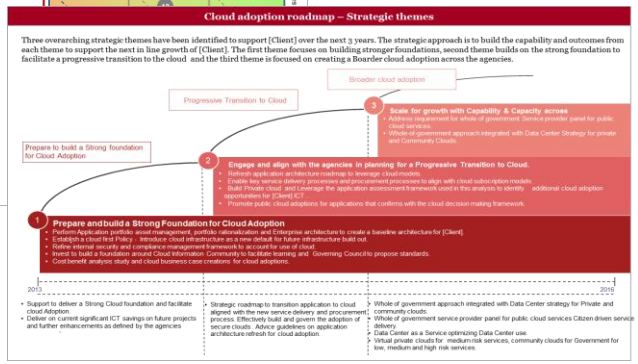
Reifegrad-modell

Dimension	Inhalt
Business-IT-Alignment	Haben Fach- und IT-Bereich ein gemeinsames Verständnis über Zielbilder, Vorgehensmodelle und ihre Zusammenarbeit, welches über Jahre Bestand hat?
Technology	Wird der technologische Modernisierungsbedarf erkannt und wie gut werden fachliche Anforderungen vom IT-Bereich abgedeckt?
Separierbarkeit	Wie flexibel lässt sich die Finanzarchitektur bei Mergers & Acquisitions integrieren bzw. bei Ausgründungen von Geschäftsbereichen trennen?
Konsistenz	Stehen den Anwendern eine bereichsübergreifende Datenbasis und ein homogener Methodenpool zur Verfügung?

Opportunities & Threats



Definierte Roadmap

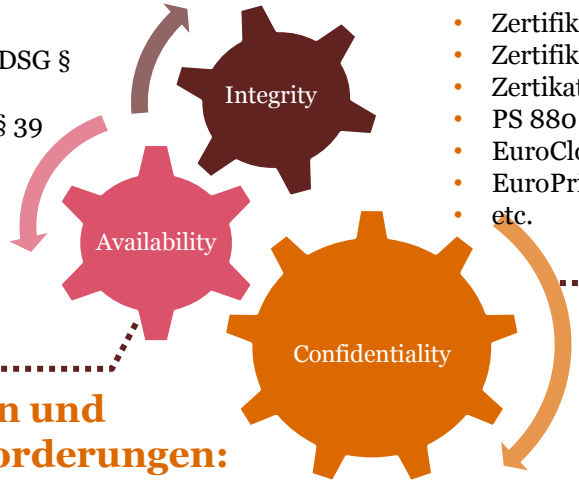


6. Überblick Herausforderungen bei Potenzialbewertung

Neben geschäftlichen Anforderungen sind auch diese aus Compliance zu berücksichtigen

Sicherstellung rechtlicher Anforderungen:

- Datenschutzgesetz: DSG § 4, DSG § 10, DSG § 11, DSG § 14
- Bankwesengesetz:BWG § 38 und BWG § 39
- Wertpapiergesetz WAG § 25
- Bundesabgabenordnung BOA § 131 und § 132
- Fachgutachten KFS , DV 2



Sicherstellung von Compliance Anforderungen:

- Zertifikat ISAE 3402: IT Security und Dateschutz
- Zertifikat ISO 27001: IT Sicherheitsstandard
- Zertikat PCIDSS: Regelwerk zu Zahlungsverkehr
- PS 880: Softwareprüfung zur Buchführung
- EuroCloud Zerfitizierung
- EuroPrise Datenschutz
- etc.

Technische Anforderungen und organisatorische Herausforderungen:

- Integration von Cloud Services in die bestehende IT Landschaft
- Lokation des Rechenzentrums
- Datenmigration und Datenarchivierung
- Übernahme der Cloud Architektur
- SLA Gestaltung und Einhaltung der Servicelevels
- Maintenance und Verfügbarkeit von Services sowie Einführung von Helpdesk Strukturen

Weitere Herausforderungen:

- IT Security: Verschlüsselung von Daten und Schutz der Cloud Computing Umgebung vor Hackern
- Datenschutz und Informationssicherheit: Entscheidungsfreiheit über die Nutzung der Daten und Lokation der Daten sowie Kontrollierbarkeit, Transparenz und Rückholbarkeit der Daten
- Bestehende Kultur/fehlende Akzeptanz im Unternehmen

7. Studien & weitere Informationen als Download verfügbar

Ausgewählte Studien zum Thema Sourcing, Cloud Computing & IT Finanzarchitektukr

IT-Finanzarchitektur – Zufallsprodukt oder gezielte Weiterentwicklung?

Abstract: Banken und Finanzdienstleister sehen sich seit einigen Jahren mit einer immer größeren Zahl an regulatorischen Vorgaben konfrontiert, welche eine Modernisierung der IT-Finanzarchitekturen erfordern. Die Studie nimmt eine Standortbestimmung der IT-Finanzarchitekturen von Banken und Finanzdienstleistern vor und zeigt Chancen und Risiken auf.

IT-Sourcing-Studie 2012-Aktuelle IT-Sourcing-Perspektiven erkennen und nutzen

Abstract: Vor dem Hintergrund aktueller Trends wie Cloud Computing und Multi-Vendor-Sourcing möchte die vorliegende Studie Klarheit über den heutigen Stand des IT-Sourcing und die zukünftigen Entwicklungen in diesem Umfeld geben. Befragt wurden für die strategischen IT-Entscheidungen verantwortliche Führungskräfte, die einen umfassenden Überblick über die IT-Sourcing-Aktivitäten haben.

Cloud Computing – Evolution in der Wolke

Abstract *(in German only)*: Cloud Computing im deutsch-sprachigen Raum ist weiter im Aufwind und wird zunehmend strategisch eingesetzt. Die Herausforderungen auf der Anbieterseite bleiben trotz vieler Verbesserungen im Kern weiter bestehen.

Ihr Reifegrad unter der Effizienzlupe

Abstract : Unsere Studie informiert Sie über den Status quo und Reifegrad bankfachlicher Dienstleister und gibt Handlungsempfehlungen für ein nachhaltiges Wachstum.

8. Haben wir Ihr Interesse geweckt - Kontaktdaten

Ich freue mich über Ihre Kontaktaufnahme und weitere Diskussion

Für Detailfragen kontaktieren Sie bitte...

Günther Seyer
Senior Manager
Technology Consulting & IT-Project Management

Tel: +43 1 501 88 5118
Mob: +43 676 833 77 5118
Mail: guenther.seyer@at.pwc.com

Cloud Glossary 1/6

The following are a list of common terms and acronyms.

Term/Acronym	Definition
IaaS	Infrastructure as a service.
PaaS	Platform as a Service.
SaaS	Software as a Service.
Public cloud	Hosted by external provider follows the Multi-tenacy model of cloud delivery services.
Private cloud	Cloud Services offered on a single Tenancy model.
Hybrid cloud	Cloud Service offered on a hybrid model, with Private burst to borrow provisions from Public or vice versa.
Custom Private cloud	Typically created as on-premise Private cloud.
Virtual Private cloud	Private cloud created in a cloud provider location with the single-tenacy model.
Reference Architecture	A reference architecture provides a proven template solution for an architecture for a particular domain.
Converged Infrastructure	Rapid Provisioning the infrastructure components like Storage, Server/Compute, Network from a service lifecycle workflow.
AAA	Authentication, authorization and accounting, security architecture for distributed systems.
Application dependency	Dependency of an application with another application in the landscape.
BCP	Business Continuity Planning, an interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption.

Cloud Glossary 2/6

The following are a list of common terms and acronyms.

Term/Acronym	Definition
CAPEX	Capital expenditure
CBA	Cost benefit analysis
Cloud platform	A system where software applications may be run in an environment composed of utility cloud services in a logically abstract environment.
Cloud provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organisations and/or individuals, usually for a fee.
Cloud Security Alliance (CSA)	The Cloud Security Alliance (CSA) is a nonprofit organization that promotes research into best practices for securing cloud computing and the ability of cloud technologies to secure other forms of computing.
CMDB	Configuration management database, is a repository of information related to all the components of an information system.
Elastic computing	The ability to dynamically provision and de-provision processing, memory, and storage resources to meet demands of peak usage without worrying about capacity planning and engineering for peak usage.
G2B	Service provided by government to business
G2C	Service provided by government to citizens
G2G	Service provided by government to government
GRC	Governance, risk and compliance.
I/O	Input/Output, the communication between an information processing system (such as a computer), and the outside world.

Cloud Glossary 3/6

The following are a list of common terms and acronyms.

Term/Acronym	Definition
ISP	Internet service provider, is a company which primarily offers their customers access to the Internet
ITIL	Information Technology Infrastructure Library
LAN	Local area network, a computer network covering a small physical area.
LPAR	Logical partition, a subset of computer's hardware resources, virtualized as a separate computer. In effect, a physical machine can be partitioned into multiple LPARs, each housing a separate operating system.
NAS	Network area storage.
OPEX	Operating expenditure
Pay as you go	A cost model for cloud services that encompasses both subscription-based and consumption-based models, in contrast to traditional IT cost model that requires up-front capital expenditures for hardware and software.
Cloud provisioning	Cloud provisioning is the allocation of a cloud provider's resources to a customer.
Dynamic provisioning	Dynamic provisioning, the provider allocates more resources as they are needed and removes them when they are not.
SSAE	Statement of Standards for Attestation Engagements
AT101	AT-101 was developed to put requirements in place for CPAs examining and issuing reports on controls over subject matter other than financial reporting. These standards are codified within AT section 101, Attest Engagements, of the attestation standards.

Cloud Glossary 4/6

The following are a list of common terms and acronyms.

Term/Acronym	Definition
RDBMS	Relational database management system, a database management system that is based on the relational model.
ROI	Return on investment
RPC	Remote procedure call.
SAN	An architecture to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached
Service Level Agreement (SLA)	A contractual agreement between a service provider and a consumer where the consumer's requirements are specified and a service provider defines the level of service, responsibilities, priorities, private and security and guarantees regarding availability, performance, and other aspects of the service.
SOC 1/2	Service Organization Controls, while the SOC 1 report is mainly concerned with examining controls over financial reporting, the SOC 2 and SOC 3reports focus more on the pre-defined, standardized benchmarks for controls related to security, processing integrity, confidentiality, or privacy of the data center's system and information.
SOE	Standard Operating Environment, an IT industry term used to describe a standard implementation of an operating system and its associated software
Software as a Service (SaaS)	Cloud application services, whereby applications are delivered over the Internet by the provider, so that the applications don't have to be purchased, installed, and run on the customer's computers. SaaS providers were previously referred to as ASP (application service providers). SaaS removes the need for organisations to handle the installation, set-up and often daily upkeep and maintenance.

Cloud Glossary 5/6

The following are a list of common terms and acronyms.

Term/Acronym	Definition
Virtual machine (VM)	A file (typically called an image) that, when executed, looks to the user like an actual machine. Infrastructure as a Service is often provided as a VM image that can be started or stopped as needed. Changes made to the VM while it is running can be stored to disk to make them persistent. (NIST)
Software as a Service (SaaS)	Cloud application services, whereby applications are delivered over the Internet by the provider, so that the applications don't have to be purchased, installed, and run on the customer's computers. SaaS providers were previously referred to as ASP (application service providers). SaaS removes the need for organisations to handle the installation, set-up and often daily upkeep and maintenance.
Subscription-based pricing model	A pricing model that lets customers pay a fee to use the service for a particular time period, often used for SaaS services. See also Consumption-based pricing model.
System management components	Components for IT systems management like server, storage, network, performance, capacity, change,
Third Party	Any relationship between two parties or entities to refer to some other person or entity with some involvement.
Threat and vulnerability	Threat: the expressed potential for the occurrence of a harmful event such as an attack; vulnerability: a weakness that makes targets susceptible to an attack.
Virtual private cloud	A private cloud that exists within a shared or public cloud, e.g., the Amazon VPC that allows Amazon EC2 to connect to legacy infrastructure on an IPsec VPN.

Cloud Glossary 6/6

The following are a list of common terms and acronyms.

Term/Acronym	Definition
Virtualization	Virtualization is the creation of a virtual version of something, such as an operating system, a server, a storage device or network resources. Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power. (NIST)
Virtualised resources	Computer resources like compute, storage, network made available by using virtualization technology.
VLAN	Virtual storage access method, an IBM disk file storage access method.
VSAM	Virtual Storage Access Method, is one of the access methods used to process data.
WAN	Wide Area Network is a computer network that covers a broad area i.e. any network whose communications links cross metropolitan, regional, or national boundaries.
AICPA	American Institute of Certified Public Accountants.

Rechtliche Anforderungen 1/2

§	Beschreibung
DSG § 4	Definition: Daten können nach Intensität des Personenbezugs unterschieden werden in direkt personenbezogene Daten, indirekt personenbezogene Daten und nicht personenbezogene (anonymisierte) Daten. Außerdem können Daten nach dem Grad der Schutzwürdigkeit unterteilt werden in: sensible (= besonders schutzwürdige) Daten und nicht-sensible Daten.
DSG § 10	Datensicherheitsmaßnahmen: Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dies umfasst unter anderem die Aufgabenverteilung bei der Datenverwendung, Zutritts- und Zugriffsberechtigungen.
DSG § 11	Auskunftsrecht: Dem Betroffenen sind bei Nachweis seiner Identität auf schriftlichen Antrag beim Auftraggeber seine Daten in allgemein verständlicher Form sowie deren Herkunft und die Rechtsgrundlage für deren Ermittlung, Verarbeitung, Benützung und Übermittlung binnen vier Wochen schriftlich mitzuteilen
DSG § 14	Rechtsschutz des Betroffenen: Die Datenschutzkommission erkennt über Beschwerden von Personen, die behaupten, in ihren Rechten nach diesem Bundesgesetz oder den hierzu ergangenen Verordnungen verletzt zu sein.
BWG § 38	Bankgeheimnis: Kreditinstitute, ihre Gesellschafter, Organmitglieder, Beschäftigte sowie sonst für Kreditinstitute tätige Personen dürfen Geheimnisse, die ihnen ausschließlich auf Grund der Geschäftsverbindung mit Kunden oder auf Grund des § 75 Absatz 3 BWG anvertraut oder zugänglich gemacht worden sind, nicht offenbaren oder verwerten.
BWG § 38	Allgemeine Sorgfaltspflichten: Die Geschäftsleiter eines Kreditinstitutes haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters im Sinne des § 84 Abs. 1 AktG anzuwenden. Dabei haben sie sich insbesondere über die bankgeschäftlichen und bankbetrieblichen Risiken zu informieren, diese durch angemessene Strategien und Verfahren zu steuern, zu überwachen und zu begrenzen sowie über Pläne und Verfahren gemäß § 39a zu verfügen. Weiters haben sie auf die Gesamtertragslage des Kreditinstitutes Bedacht zu nehmen.

Rechtliche Anforderungen 2/2

§ / Fachgutachten	Beschreibung
WAG § 25	Auslagerung von wesentlichen betrieblichen Aufgaben an Dienstleister: Ein Rechtsträger hat sicherzustellen, dass beim Rückgriff auf Dritte (Dienstleister) zur Wahrnehmung betrieblicher Aufgaben, die für die kontinuierliche und zufrieden stellende Erbringung von Dienstleistungen für Kunden und Ausübung von Anlagetätigkeiten wesentlich sind, angemessene Vorkehrungen gemäß Anlage 1 zu § 25 getroffen werden, um unnötige zusätzliche Geschäftsrisiken zu vermeiden.
BAO § 131	Bücher, die gemäß den §§ 124 oder 125 zu führen sind oder die ohne gesetzliche Verpflichtung geführt werden, und Aufzeichnungen der in den §§ 126 bis 128 bezeichneten Art dürfen, wenn nicht anderes gesetzlich angeordnet ist, auch im Ausland geführt werden.
BOA § 132	Bücher und Aufzeichnungen sowie die zu den Büchern und Aufzeichnungen gehörigen Belege sind sieben Jahre aufzubewahren.
Fachgutachten KFS	Fachgutachten über Grundsätze ordnungsgemäßer Bilanzierung von Pensionsverpflichtungen nach den Vorschriften des Rechnungslegungsgesetzes
Fachgutachten DV 2	Abschlussprüfung bei Einsatz von Informationstechnik

Compliance Anforderungen

Zertifikat / Bescheinigung	Beschreibung
Zertifikat ISAE 3402	Berichtserstattungsmöglichkeit für Dienstleistungsorganisationen mit einem weltweit einheitlichen Berichtsaufbau.
Zertifikat ISAE 27001	Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.
Zertifikat PCI-DSS	Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.
PS 880	Softwarebescheinigung: Die Prüfung der Ordnungsmäßigkeit von Softwareprodukten richtet sich auf die notwendigen Verarbeitungsfunktionen (Beleg-, Journal- und Kontenfunktion), die programmierten Verarbeitungsregeln, die Softwaresicherheit sowie die Dokumentation.