Finanz & Versicherungswesen

Standards	ISO27001, ISO 27018, ISO 27017, PCI-DSS, C5:2020, (BSI Standards, BSI-IT Grundschutz), IDW PS 951, IDW PS880
Regulierung	DSGVO, IT Sicherheitsgesetz, BSI-Gesetz, BSI-KritisV, Bankengesetzgebung (Bafin), VAIT, BAIT, MA Risk, Basel3
Standards RZ	ISO/IEC 27001, EN 50600, TSI.Standard, DCSA eco

Typische Use Case 1	**Investmentbanking**
TSI Level	Level 4
Verfügbarkeit	99.999%
Dauer Ausfallzeit pro Störung / Jahr	ca. 5 Minuten
Beispielhafte Anwendungen	Investment-Plattformen, Börsensysteme, Clearing-Plattformen
Maßnahmen zur Erreichung der Verfügbarkeit	Backup, Disaster Recovery, LoadBalancer, Fail-Over Cluster mit eventueller Geo-Redundanz und active-active Sync

Typische Use Case 2	**Retailbanking und Payment**
TSI Level	Level 3
Verfügbarkeit	99.99%
Dauer Ausfallzeit pro Störung / Jahr	< 1 Stunde
Beispielhafte Anwendungen	Online-Banking, Payment-Systeme, Big Data für Fraud-Analysen, KI
Maßnahmen zur Erreichung der Verfügbarkeit	Backup, Disaster Recovery, LoadBalancer, Fail-Over Cluster mit eventueller Geo-Redundanz und active-passive Sync

Typische Use Case 3	**Office IT**
TSI Level	Level 3
Verfügbarkeit	99.99%
Dauer Ausfallzeit pro Störung / Jahr	< 1 Stunde
Beispielhafte Anwendungen	Office, Mail, CRM, CRM, V-IT, Projektmanagement, Collaboration, Webanwendungen, Dokumentenverwaltung, Kommunikation, Netzwerk, Security, Virtualisierung, Storage, Backup
Maßnahmen zur Erreichung der Verfügbarkeit	Backup, Disaster Recovery, LoadBalancer, Fail-Over Cluster mit eventueller Geo-Redundanz und active-passive Sync

Standards	Beschreibung
ISO 27001	Internationale Norm: “Information technology – Security techniques – Information security management systems – Requirements” spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des jeweiligen Organisation. Anforderungen zur Beurteilung und Behandlung von Informationssicherheitsrisiken und Bedürfnissen der Organisationen.
ISO 27018	Erster internationale Standard über den Datenschutz bei Cloud-Computing-Diensten, der von der Industrie gefördert wurde. Dieser wurde 2014 als Zusatz zu ISO/IEC 27001, dem ersten internationalen Verhaltenskodex für den Datenschutz in der Cloud, erstellt. Unterstützt Cloud-Service-Anbietern, die personenbezogene Daten (PII) verarbeiten, bei der Risikobewertung und der Implementierung von Kontrollen zum Schutz von PII. Er wurde von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) veröffentlicht.
ISO 27017	Internationale Norm und Richtlinien zur Unterstützung und Implementierung von Informationssicherheitskontrollen für Cloud-Service-Kunden, die Kontrollen implementieren, sowie Cloud-Service-Provider, die Implementierung dieser Kontrollen unterstützen. Sicherheitsstandard für Anbieter und Nutzer von Cloud-Diensten, um eine sichere Cloud-basierte Umgebung zu schaffen und das Risiko von Sicherheitsproblemen zu verringern.
BSI Standards	BSI-Standards sind ein essentieller Bestandteil der IT-Grundschutz-Methodik und beinhalten Empfehlungen zu Methoden, Prozessen und Verfahren, sowie Maßnahmen und deren Vorgehensweisen zu den Aspekten der Informationssicherheit. Nutzer aus Behörden, Unternehmen, Hersteller, Dienstleister können mit den BSI-Standards die Geschäftsprozesse und Daten sicherer gestalten.
BSI-IT Grundschutz	IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik.
C5:2020	Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) definiert die Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, Prüfer und Kunden.
IDW PS 951	Prüfungsstandard des Institut der Wirtschaftsprüfer in Deutschland e.V., ist ein Prüfungsstandard, in dem die Prüfung eines ausgelagerten internen Kontrollsystems auf ein Dienstleistungsunternehmen geregelt ist.
IDW PS880	Prüfungsstandard unterstützt Wirtschaftsprüfer bei der Prüfung und Erteilung von Bescheinigungen zu Softwareprodukten. Prüfungen, die darauf ausgerichtet sind, Prüfungsaussagen mit hinreichender Sicherheit zu treffen. Die Vorgehensweise der Prüfung von Softwareprodukten folgt der Systematik von Systemprüfungen bei Einsatz von Informationstechnologie. Der Informationstechnologie und den Ordnungsmäßigkeits- und Sicherheitsanforderungen beim Einsatz von IT. Prüfungsstandard zur Verwertung der Ergebnisse und Prüfung von Softwareprodukten im Rahmen einer Abschlussprüfung beim Softwareanwender, sowie Beurteilung der Ordnungsmäßigkeit und Sicherheit der Buchführung.
PCI-DSS	“Payment Card Industry Data Security Standard”, ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.
TSI EN 50600	“Trusted Site Infrastructure” (TSI) EN50600 - ist eine länderübergreifende Norm und beinhaltet die RZ-Vorgaben für die Planung, Neubau und den Betrieb eines Rechenzentrums und ist ein Prüfzeichen vom TÜV. Das Prüfzeichen beinhaltet eine Untersuchung der physischen Infrastruktur eines Rechenzentrums (Standort, Baukonstruktion, Sicherheitstechnik, Energieversorgung und Kältetechnik) sowie der organisatorischen Prozesse des Betreibers und dokumentiert die Eignung für Sicherheitsbereiche, die eine hohe Verfügbarkeit verlangt wird.

Standards	Beschreibung
TSI.Standard	Der “TSI.STANDARD” ist die klassische TSI-Zertifizierung seit 2002 und Grundlage für die Untersuchung und Zertifizierung bildet ein regelmäßig aktualisierter Kriterienkatalog, welcher auf langjährige Erfahrungen in der Prüfung von Rechenzentren als auch auf Regelwerken und Normen aufbaut. Level 1 – mittlerer Schutzbedarf, Level 2 – erweiterter Schutzbedarf, Level 3 – hoher Schutzbedarf, Level 4 – sehr hoher Schutzbedarf.
DCSA eco	Das Datacenter Star Audit (DCSA) ist ein Projekt von eco – Verband der Internetwirtschaft e.V. und als Gütesiegel für Rechenzentren konzipiert. DCSA prüft und beurteilt objektiv Infrastruktur und Leistungen. Die Sterne (DC Stars) informieren über die Qualität und Umfang des jeweiligen Leistungsspektrum.