

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
1	<p>Definitionen</p> <ul style="list-style-type: none"> <input type="checkbox"/> Die im Subvertrag 'Sicherheit outsourced Domain' erwähnten zentralen und wichtigen Ausdrücke sind ausformuliert und erklärt. 								<p>Beispiele sind:</p> <ul style="list-style-type: none"> <input type="checkbox"/> "Sicherheit outsourced Domain" ist derjenige Teil eines Outsourcing-Vertrages, der die Sicherheitsanforderungen an die in der Leistungsbeschreibung definierten Dienstleistungen spezifiziert. <input type="checkbox"/> Hinweis auf ein Glossarium, etc 	
2	<p>IT Sicherheits-Policy</p> <ul style="list-style-type: none"> <input type="checkbox"/> Anforderungen an die Sicherheit sind durch eine aktuelle Sicherheits-Policy für beide Vertragspartner verbindlich geregelt. <input type="checkbox"/> Aktualisierungen der Policy erfolgen in Übereinstimmung von beiden Vertragspartnern und werden rechtsgültig abgezeichnet. <input type="checkbox"/> In der Policy ist festgelegt, welche Sicherheitsanforderungen durch die Vertragspartner verbindlich eingehalten werden müssen. Die jeweiligen Anforderungen/Direktiven/Weisungen für beide Vertragspartner liegen schriftlich vor. <input type="checkbox"/> Das Verfahren für die Behandlung sowohl von Informations-Sicherheitsverletzungen als auch das Eskalationsverfahren für solche Fälle sind spezifiziert. 		D						<ul style="list-style-type: none"> <input type="checkbox"/> Standardwerke für die Entwicklung einer IT Sicherheits-Policy sind: <ul style="list-style-type: none"> <input type="checkbox"/> CobiT (Control Objectives for Information and related Technology) <input type="checkbox"/> 'Code of Practice for Information Security Management' der 'British Standards Institution' (BS7799) <input type="checkbox"/> IT-Sicherheitshandbuch (BSI 7105) vom Bundesamt für Sicherheit <input type="checkbox"/> Leistungsnehmer und Leistungsgeber führen einen zentralen Log mit allen die Informations-Sicherheit betreffenden Vorkommnissen, wie Zugriffsverletzungen, Manipulationen, Beweismittel für Betrugsfälle, Hacking etc. Dieser Log ist Basis für die Festlegung der Zusammenarbeit bei Verletzungen der Informationssicherheit und der Einführung von entsprechenden, neuen Kontrollen und Verfahren. 	

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
2	IT Sicherheits-Policy, Fortsetzung <input type="checkbox"/> Für die in den folgenden Paragraphen 3ff angeführten Kontrollziele für Kernaktivitäten sind je nach Art der 'outsourced Domain/Prozesse' immer zwingend entsprechende Vertragsvereinbarungen vorhanden (Minimalanforderung).									
3	Personal <input type="checkbox"/> Die bei der Anstellung von neuem Personal durchgeführten Personal-Recherchen beim Leistungsgeber sind konsistent zu Anforderungen an die Informations-Sicherheit beim Leistungsnehmer.									

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
4	<p>Katastrophen-Vorsorge/-Konzept beim Leistungserbringer</p> <ul style="list-style-type: none"> <input type="checkbox"/> Der Leistungserbringer unterhält einen aktuellen Katastrophenplan. Die darin eingebundenen Verfahren werden periodisch auf Aktualität und Angemessenheit überprüft und getestet. <input type="checkbox"/> Beim Leistungserbringer sind Prozeduren und Regelungen implementiert, die in einem Katastrophenfall dem Leistungsnehmer die Verfügbarkeit der vertraglich vereinbarten Service-Leistung garantieren. <input type="checkbox"/> Im Rahmen der Katastrophenvorsorge ausgelagerte Daten, Programme und Dokumentationen unterstehen den zwischen den beiden Vertragspartnern vereinbarten Geheimhaltungspflichten. 		D						<ul style="list-style-type: none"> <input type="checkbox"/> Prozeduren und Regelungen sind z.B.: <ul style="list-style-type: none"> <input type="checkbox"/> Alarmkonzepte <input type="checkbox"/> Hardware-Backup <input type="checkbox"/> Verfahren für die Sicherheits-Auslagerung von Daten, Applikations-Software, System-Software, Dokumentationen und anderer in einem Katastrophenfall benötigten Hilfsmittel (Backup) <input type="checkbox"/> Wiederanlauf-Verfahren bzw. -Plan zur Wiederherstellung des letzten produktiven Status vor Eintritt eines Vorkommnisses <input type="checkbox"/> Zugriffsregelung zu ausgelagerten Daten <input type="checkbox"/> Eskalationsverfahren zur verantwortlichen Stelle beim Leistungsnehmer inkl. Statusmeldungen an den Leistungsnehmer 	

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
4	<p>Katastrophen-Vorsorge/-Konzept beim Leistungserbringer, Fortsetzung</p> <ul style="list-style-type: none"> <input type="checkbox"/> Das Recht zur Einsichtnahme in die aktuelle Katastrophendokumentation sowie in Resultate periodischer Tests der Wiederanlaufverfahren ist, soweit sie Elemente der vertraglich vereinbarten Service-Leistung betreffen, durch den Subvertrag 'Revision outsourced Domain' geregelt. <input type="checkbox"/> Mit der Unterzeichnung des Rahmenvertrages wird der Leistungserbringer verpflichtet, in einem Katastrophenfall gemäss den im Katastrophenfallplan dokumentierten Verfahren, soweit sie Elemente der vertraglich vereinbarten Service-Leistung betreffen, zu handeln. 									

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
5	<p>Katastrophen-Vorsorge/-Konzept beim Leistungsempfänger</p> <ul style="list-style-type: none"> <input type="checkbox"/> Beim Leistungsempfänger sind Prozeduren und Regelungen implementiert, die in einem Katastrophenfall beim Leistungserbringer, die Fortführung der üblichen Geschäftstätigkeit garantieren. <input type="checkbox"/> Diese Prozeduren und Regelungen sind mit der Katastrophenvorsorge beim Leistungserbringer periodisch abgestimmt. Sie werden aktuell gehalten und periodisch getestet. <input type="checkbox"/> Der Leistungsnehmer trifft vorsorgliche Massnahmen um einer möglichen Vertragsauflösung vor Vertragsende zu begegnen. 		D						<ul style="list-style-type: none"> <input type="checkbox"/> Erstellung eine Wiederanlaufplanes <input type="checkbox"/> Archivieren aktueller Kopien von Applikations- und System-Software, Lizenzen und Dokumentationen oder Eigentumsrechte an solchen. 	

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
6 6.1	<p>Daten des Leistungsempfängers Datenverwaltung und Datennutzung</p> <ul style="list-style-type: none"> <input type="checkbox"/> Die Eigentümer der Daten sind benannt und deren Namen sind jederzeit aktuell. <input type="checkbox"/> Inhalt und Ort der Datenbestände des Leistungsnehmers sind aktuell dokumentiert. <input type="checkbox"/> Vertraulichkeitsklassierungen, Verfügbarkeits- und Integritätsanforderungen der Datenbestände sind spezifiziert. <input type="checkbox"/> Die Daten werden nur zur Erfüllung der vertraglich vereinbarten Dienstleistung genutzt. <input type="checkbox"/> Bekanntgabe, Verkauf, Vermietung der Daten oder anderweitige Verwendung derselben durch Drittparteien oder die kommerzielle Verwendung im Namen des Leistungsgebers sind verboten. <input type="checkbox"/> Der Leistungsgeber stellt die Einhaltung von vertraglich vereinbarten Anforderungen an die Datenverwaltung und Datennutzung sicher. 		D							

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
6 6.2	<p>Daten des Leistungsempfängers Datenschutz</p> <ul style="list-style-type: none"> <input type="checkbox"/> Der Leistungsgeber ist verantwortlich für einen angemessenen Schutz der ihm anvertrauten Daten. Insbesondere sind die die Daten gegen <ul style="list-style-type: none"> <input type="checkbox"/> unbefugte oder zufällige Zerstörung, <input type="checkbox"/> zufälligen Verlust, <input type="checkbox"/> technische Fehler, <input type="checkbox"/> Fälschung, Diebstahl oder widerrechtliche Verwendung, <input type="checkbox"/> unbefugtes Ändern, Kopieren oder andere unbefugte Bearbeitungen zu schützen. <input type="checkbox"/> Die Anforderungen an den Datenschutz beim Leistungsgeber erreichen im Minimum denselben Gütegrad wie derjenige beim Leistungsnehmer. <input type="checkbox"/> Der Leistungsnehmer zeichnet verantwortlich für die Durchsetzung von Art. 14 des DSGVO (Datenbearbeitung durch Dritte) beim Leistungsgeber <input type="checkbox"/> Die Anforderungen an den Datenschutz beim Leistungsnehmer sind bekannt, liegen schriftlich vor und sind vom Management genehmigt. 		D							

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
6 6.2	Daten des Leistungsempfängers Datenschutz, Fortsetzung <input type="checkbox"/> Der Zugriff zu ausgelagerten und insbesondere zu kommerziell sensitiven Datenbeständen und/oder Datensammlungen mit datenschutzwürdigen Personendaten ist konsistent zu dokumentierten Regelungen (Katastrophenkonzept (4) bzw. Sicherheitsmanagement (7.1, 8.1)).								<input type="checkbox"/> Massnahmen zum Schutz der Vertraulichkeit ausgelagerter Daten können sein: <input type="checkbox"/> Physischer Datenschutz durch Überwachung von Zugriff und Zugang <input type="checkbox"/> Kryptographischer Datenschutz	
7 7.1	Logische Zugriffe Sicherheits-Management <input type="checkbox"/> Zur Sicherung der Computer-Ressourcen gegen unauthorisierte Zugriffe, vor Schaden, Verlust oder Veränderungen sind Zugriffskontrollen installiert. Diese unterliegend einer laufenden Überwachung. <input type="checkbox"/> Verantwortlich für die Kontrolle der Zugriffssicherheit zeichnet das Management des Leistungsgebers.									

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
7 7.1	<p>Logische Zugriffe Sicherheits-Management, Fortsetzung</p> <ul style="list-style-type: none"> <input type="checkbox"/> Adäquate Richtlinien und Verfahren für die Administration von Zugriffsrechten sind definiert, liegen schriftlich vor und sind durch das Management des Leistungsgebers genehmigt. <input type="checkbox"/> Alle durch ihre Tätigkeit mit Zugriffen auf Daten des Leistungsnehmers betroffenen Personen haben eine Kopie der genannten Richtlinien unterzeichnet und übernehmen damit direkt die Verantwortung für jeden Zugriff mit ihrer Benutzer-Identifikation. 		D						<ul style="list-style-type: none"> <input type="checkbox"/> Beispiele dazu sind: <ul style="list-style-type: none"> <input type="checkbox"/> Policy und Verfahren der Zugriffsrechte <input type="checkbox"/> Administration der Zugriffsrechte <input type="checkbox"/> Standardisierung der Zugriffsrechte <input type="checkbox"/> Schutz der Zugriffskontrolldaten, wie: <ul style="list-style-type: none"> <input type="checkbox"/> Benutzer-Identifikatioenen <input type="checkbox"/> Passwörter <input type="checkbox"/> Zugriffsregeln <input type="checkbox"/> spezifische Zugriffsprivilegien <input type="checkbox"/> etc. 	
7.2	<p>Zugriffssicherheit</p> <ul style="list-style-type: none"> <input type="checkbox"/> Die Zugriffssicherheit umfasst im Minimum die folgenden Anforderungen: <ul style="list-style-type: none"> <input type="checkbox"/> Anmeldung (Sign-on) mit eindeutiger Benutzer-Identifikation <input type="checkbox"/> Verifizierung der Identität eines Benutzers (Authentisierung) <input type="checkbox"/> Aufzeichnung (Logging) und Auswertung bzw. periodische Überprüfung sicherheitsrelevanter Informationen 									

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
7 7.2	<p>Logische Zugriffe Zugriffssicherheit, Fortsetzung</p> <ul style="list-style-type: none"> <input type="checkbox"/> Durch automatisierte Zugriffseinschränkungen soll das Risiko von potentiellen Verlusten durch bewussten oder unbewussten Missbrauch, Diebstahl, Betrug, Veruntreuung, Manipulation oder Zerstörung von Daten bzw. sensitiven Zugriffsinformationen reduziert werden. 								<ul style="list-style-type: none"> <input type="checkbox"/> Beispiele dazu sind: <ul style="list-style-type: none"> <input type="checkbox"/> Automatischer Terminal Log-off <input type="checkbox"/> Access Control Software <input type="checkbox"/> Call-Back Verfahren 	
8 8.1	<p>Physische Sicherheit Sicherheits-Management</p> <ul style="list-style-type: none"> <input type="checkbox"/> Alle vom Auftraggeber an die physische Sicherheit gestellten Anforderungen werden vom Leistungsgeber an den davon betroffene örtlichen Stellen eingehalten. <input type="checkbox"/> Die Anforderungen an die physische Sicherheit beim Leistungsgeber erreichen im Minimum denselben Gütegrad wie derjenige beim Leistungsnehmer. <input type="checkbox"/> Die Anforderungen an die physische Sicherheit beim Leistungsnehmer sind bekannt, liegen schriftlich vor und sind vom Management genehmigt. <input type="checkbox"/> Zum Schutz der Computer-Ressourcen gegen unautorisierte Zutritte, unautorisierte physische Zugriffe und vor Schaden oder Verlust sind angemessene Sicherheitsmassnahmen getroffen. 		D							

KONTROLLZIELE		KONTROLLTECHNIKEN	COMP-LIANCE WP-REF	RISIKOBEWERTUNG					KOMMENTAR	REPORT W/P-REF
NR	BESCHREIBUNG	BESCHREIBUNG		C	B	L	M	H		
8 8.1	<p>Physische Sicherheit Sicherheits-Management, Fortsetzung</p> <p><input type="checkbox"/> Verantwortlich für die periodische Kontrolle der Umsetzung der Sicherheitsmassnahmen in wichtigen und schutzwürdigen Risikobereichen für Computer-Ressourcen zeichnet das Management des Leistungsgebers.</p>								<p><input type="checkbox"/> Wichtige und schutzwürdige Risikobereiche für Computer-Ressourcen umfassen insbesondere:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Zugang zu Computer-Ressourcen <input type="checkbox"/> Physische Zugriffe auf jedwelche Computer-Ressourcen, Daten, Datenfiles etc. <input type="checkbox"/> Gebäude und Gebäudeumgebung <input type="checkbox"/> Brandschutz <input type="checkbox"/> Schutz vor Wasser <input type="checkbox"/> Klima- und Kühlungsanlagen <input type="checkbox"/> Stromversorgung 	