	Anforderungen	Basis-anforderungen	Zusatz-anforderungen		Ausschreibungskriterien
		alle Kategorien (Kat. 1-4) (Kat. 5 nicht beschrieben, da nicht angewendet)	Kat. 2 (Private Government Cloud)	Kat. 1 (Private Cloud)	
1	**Übergreifende Sicherheitsaspekte**				
1.1	Der AN verfügt über einen offiziell bestellten Datenschutzbeauftragten.	✓			Der CSP hat darzustellen, dass er über einen offiziell bestellten Datenschutzbeauftragten verfügt. Dieser muss über die gesetzlich geforderte Fachkunde im Bereich Datenschutz und IT-Sicherheit verfügen.
1.2	Der AN verfügt über ein formales Datenschutzkonzept, das die gesetzlichen Anforderungen erfüllt.	✓			Der CSP hat darzustellen, dass für den Geltungsbereich der bereitgestellten Cloud-Ressourcen ein formales Datenschutzkonzept existiert, welches die gesetzlichen Voraussetzungen (Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetz (LDSG)) erfüllt; bei gemeinsamer Datenverarbeitung mehrerer Länder ist ggf. § 11 EGovG zu nutzen. Die Einhaltung des Datenschutzkonzeptes kann durch ein Zertifikat über die Einhaltung des Datenschutzes bei Cloud Daten nachgewiesen werden.
1.3	Die eingesetzten Mitarbeiter sind bereit, sich nach dem örtlich geltenden Datenschutz-Gesetzen (LDSG oder vergleichbar) verpflichten zu lassen.	✓			Der CSP hat darzustellen, dass die Mitarbeiter des CSP mit Zugriff auf die bereitgestellten Cloud-Ressourcen nach dem LDSG verpflichtet werden können.
1.4	Die eingesetzten Mitarbeiter sind bereit, sich nach dem Landessicherheitsüberprüfungsgesetz (LSÜG) überprüfen zu lassen.		✓	✓	Der CSP hat darzustellen, dass die Mitarbeiter des CSP mit Zugriff auf die bereitgestellten Cloud-Ressourcen nach den Vorgaben des LSÜG des Landes überprüft werden können.

1.5	Der AN ist bereit, den behördlichen Datenschutzbeauftragten oder dessen Beauftragten, Vor-Ort-Auditierungen der Cloud-Ressourcen vornehmen zu lassen.		✓	✓	Der CSP hat darzustellen, dass und ggfls. unter welchen Bedingungen er dem Landesbeauftragen für den Datenschutz und die Informationsfreiheit des Landes (LfDI) oder dessen Beauftragten Vor-Ort-Auditierungen der bereitgestellten Cloud-Ressourcen gestattet
1.6	Alle Länder, in denen Daten verarbeitet, weitergeleitet oder gespeichert werden sind einsehbar. Die Daten werden im Geltungsbereich des BDSG verarbeitet.	✓			Es wird erwartet, dass die bereitgestellten Cloud-Ressourcen alle Daten vollständig und ausschließlich im Geltungsbereich des BDSG verarbeiten, d.h. in der Bundesrepublik Deutschland. Der Bieter hat offenzulegen, in welchen Ländern Daten verarbeitet, weitergeleitet oder gespeichert werden.
1.7	Regelmäßige Sicherheitsaudits werden durchgeführt	✓			Der CSP hat darzustellen, dass regelmäßige Sicherheitsaudits und Datenschutzaudits durch unabhängige Dritte stattfinden bzw. im Auftrag des Auftraggebers stattfinden können und wie diese sich ausgestalten. Die Trennung der Daten unterschiedlicher Kunden ist auch bei Sicherheitsprüfungen zu gewährleisten. Als Beleg ist den Ausschreibungsunterlagen ein Musterergebnisbericht aus einem solchen Audit beizulegen. Die Ergebnisse von Audits der bereitgestellten Cloud-Ressourcen sind dem Auftraggeber unaufgefordert mitzuteilen. Die Bereitschaft hierfür ist darzustellen.

1.8	Der AN verfügt über ein Sicherheitskonzept.	✓			Der CSP hat den Nachweis zu erbringen, dass er über ein dokumentiertes Sicherheitskonzept verfügt, das an den Vorgaben von mindestens ISO 27001, besser ISO 27001 auf Basis der BSI-Grundschutz-Standards orientiert ist. Dessen Umsetzung sollte durch Testate unabhängiger Stellen regelmäßig belegt werden. Den Ausschreibungsunterlagen ist ein Muster dieses Sicherheitskonzeptes beizulegen, aus dem eindeutig hervorgeht, welche organisatorischen, technischen und infrastrukturellen Bereiche Gegenstand des Sicherheitskonzeptes speziell ihrer Cloud-Infrastruktur sind.
2	**Fachliche Anforderungen**				
2.1	**Sicherheitstechnische und funktionale Anforderungen**				
2.1.1	**Organisatorisch**				
2.1.1.1	Es ist transparent, welche Unterauftragnehmer an dem Betrieb und dem Support der Cloud-Ressourcen beteiligt sind.	✓			Der CSP hat offenzulegen, welche Unterauftragnehmer im Rahmen des Betriebs und des Supports der bereitgestellten Cloud-Ressourcen im Auftrag des CSP beteiligt sind.
2.1.1.2	Es existiert ein formal definiertes Informationssicherheitsmanagementsystem nach ISO 27001.	✓			Der CSP hat darzustellen, dass ein formal definiertes ISMS für die bereitgestellten Cloud-Ressourcen existiert. Es wird erwartet, dass ein ISMS nach ISO 27001 existiert, das sich im Optimalfall an den Vorgaben des IT-Grundschutzes des BSI orientiert oder darauf basiert

2.1.1.3	Es gibt einen formalen Security Incidence Response Prozess. Ein CERT des Auftragebers kann angebunden werden.	✓			Der CSP hat sein Management von IT-Sicherheitsvorfällen in der Cloud-Infrastruktur darzustellen. Hierzu sollte der Security Incidence Response Prozess offengelegt werden. Weiterhin ist darzustellen, ob ein CERT des Auftraggebers an diesen Prozess angebunden werden kann.Es wird erwartet, dass IT-Sicherheitsvorfälle in der Cloud, die den Auftraggeber betreffen oder betreffen können, zeitnah offengelegt und auf abzustimmenden Wegen formal an den Auftraggeber gemeldet werden
2.1.2	**Sicherheit**				
2.1.2.1	Es existiert ein Schutz gegen Bruteforce-Angriffe.	✓			Der CSP hat darzustellen, dass und wie er die bereitgestellte Infrastruktur vor Bruteforce-Angriffen schützt
2.1.2.2	Intrusion Detection Systeme werden zur Abwehr von bekanntem, schädlichem Netzwerkverkehr eingesetzt.			✓	Der CSP hat darzustellen, dass und wo innerhalb der Cloud-Infrastruktur IDS eingesetzt werden und wie das IDS in das Sicherheitsmanagement der Cloud-Infrastruktur eingebunden ist
2.1.2.3	Konfigurierbare Firewallsysteme zur Abwehr von bekanntem, schädlichem Netzwerkverkehr werden innerhalb der Cloud-Infrastruktur eingesetzt.	✓			Der CSP hat darzustellen, dass und wo innerhalb der Cloud-Infrastruktur Firewall-Systeme eingesetzt werden und wie diese in das Sicherheitsmanagement der Cloud-Infrastruktur eingebunden sind
2.1.2.4	Eine getrennte Speicherung von Provider-Images und Anwender-Images findet statt.		✓	✓	Der CSP hat darzustellen, dass die Provider-Images (Datenträger-Sicherungen) getrennt von den Anwender-Images gespeichert werden und wie die Trennung sichergestellt wird
2.1.2.5	Es ist nicht möglich, auf Daten anderer Kunden zuzugreifen bspw. über Zugriff auf zufällige Bucket-Adressen oder Verzeichnisnamen, Ansteuern höherer Verzeichnisebenen.	✓			Der CSP hat darzustellen, dass und wie technisch sichergestellt wird, dass Kunden nicht auf Daten anderen Kunden zugreifen können (Trennung und Firewall-Absicherung virtueller Systeme untereinander und von den Hostsystemen erforderlich)

2.1.2.6	Es kommen ausschließlich verschlüsselte Protokolle zur Datenübertragung zur Anwendung. Ausnahmen sind zu begründen.	✓			Der CSP muss offenlegen, welche Protokolle von seinem Produkt verwendet werden und welche Standards diesen Protokollen zugrunde liegen. Es sollten ausschließlich verschlüsselte Protokolle zur Anwendung kommen. Der Einsatz unverschlüsselter Kommunikation ist zu vermeiden und muss im Einzelfall begründet werden, falls er dennoch verwendet wird.
2.1.2.7	Es findet eine kryptografisch geschützte Authentifizierung zwischen den Cloud-Ressourcen statt.	✓			Der CSP hat darzustellen, dass eine kryptografisch geschützte Authentifizierung zwischen den Cloud-Ressourcen erfolgt und welche Authentifizierungsverfahren hier zum Einsatz kommen (einseitige oder zweiseitige Authentifizierung, Maßnahmen zur Vereitelung von Man-in-the-Middle)
2.1.2.8	Der AN verwendet verschlüsselte Verbindungen zwischen Cloud-Ressourcen.	✓			Der CSP hat darzustellen, dass verschlüsselte Verbindungen zwischen Cloud-Ressourcen unterstützt werden und welche Verschlüsselungsalgorithmen hier zum Einsatz kommen.
2.1.2.9	Für jeden Zugriff ist eine Authentisierung nötig.	✓			Alle Authentisierungs-Mechanismen der Cloud-Services müssen offengelegt werden.
2.1.2.10	Administrative Zugriffe erfordern eine Zwei-Faktor-Authentisierung		✓	✓	Für administrative Zugriffe ist eine Zwei-Faktor-Authentisierung wünschenswert.
2.1.2.11	Kundenseitige Richtlinien bezüglich Passwortsicherheit können umgesetzt werden.		✓	✓	Der CSP hat darzustellen, dass bezüglich passwortgesichertem Zugriff auf die bereitgestellten Cloud-Ressourcen kundenseitige Richtlinien bezüglich Passwortsicherheit (Passwort-Länge, Passwort-Komplexität, Gültigkeitsdauer, etc.) umgesetzt werden können.
2.1.2.12	Gehärtete Betriebssysteme werden auf den Virtualisierungshosts eingesetzt.	✓			Der CSP hat sein Härtungskonzept für die auf den Virtualisierungshosts eingesetzten Betriebssysteme darzustellen (Mindestanforderungen: Abschaltung nicht zwingend benötigter Dienste, Aktivierung Paketfilter mit Stateful Inspection Firewall).

2.1.2.13	Die Schlüsselerzeugung erfolgt in sicherer Umgebung z.B. auf Clientseite und unter Einsatz geeigneter Schlüsselgeneratoren (Schlüssellänge und Schlüsselkomplexität definiert).		✓	✓	Der CSP hat darzustellen, wie das Schlüsselmanagement für kryptographische Verfahren erfolgt und ob und wie Schlüssellängen und Schlüsselkomplexitäten definiert sind (Mindestanforderung: empfohlene Schlüssellängen des BSI).
2.1.2.14	Kryptographische Schlüssel dienen nur einem Einsatzzweck. Für jedes System / Dienst gibt es nur einen dedizierten Schlüssel.		✓	✓	Der CSP hat darzustellen, dass sichergestellt ist, dass kryptographische Schlüssel nur jeweils einem einzigen Einsatzzweck dienen.
2.1.2.15	Schlüssel werden redundant gesichert. Sind sie wiederherstellbar, um einen Verlust eines Schlüssels zu vermeiden.		✓	✓	Der CSP hat darzustellen, dass kryptographische Schlüssel redundant gesichert werden und welche Verfahren in diesem Zusammenhang eingesetzt werden. Weiterhin ist darzustellen, dass der Verlust eines Schlüssels durch mögliche Wiederherstellung vermieden werden kann.
2.1.2.16	Die Verteilung der Schlüssel erfolgt sicher (vertraulich, integer und authentisch).	✓			Der CSP hat darzustellen, dass die kryptographischen Schlüssel sicher verteilt werden, d.h. wie die Vertraulichkeit, Integrität und Authentizität verteilter Schlüssel sichergestellt wird.
2.1.2.17	Administratoren der Cloud haben keinen Zugriff auf Kundenschlüssel.	✓			Der CSP hat darzustellen, dass er als Administrator der Cloud keinen Zugriff auf vom Kunden generierte Schlüssel hat.
2.1.2.18	Eigene Sicherheitszone für das Management der Cloud.		✓	✓	Der CSP hat darzustellen, auf welche Weise das Management der Cloud von dem Management der Gastsysteme getrennt ist, ob also eine exklusive Sicherheitszone (z. B. ein dediziertes Management-Netz) für das Management der Cloud existiert.
2.1.2.19	Eigene Sicherheitszone für das Storage-Netz.		✓	✓	Der CSP hat darzustellen, auf welche Weise das Storage-Netz von den Gastsystemen und dem Management-Netz der Cloud getrennt ist, ob also eine exklusive Sicherheitszone (z. B. ein dediziertes Netz) für Storage existiert.

2.1.2.20	Der AN bietet kundenexklusive Hardwareressourcen an.			✓	Der CSP hat darzustellen, dass es möglich ist, kundenexklusive Hardware-Ressourcen innerhalb der Cloud-Infrastruktur (gemäß Kategorie 2) bereitzustellen. Insbesondere sollte dargestellt werden, ob es möglich ist, virtuelle Maschinen des Kunden auf kundenexklusiven Virtualisierungsservern auszuführen.
2.1.3	**Monitoring, Logfiles**				
2.1.3.1	Zugriffsprotokolle werden revisionssicher aufbewahrt.	✓			Es muss nachvollziehbar sein, wer zu welchem Zeitpunkt Änderungen an den Systemen vorgenommen hat. Der CSP sollte die Protokolldaten der letzten sechs Monate revisionssicher vorhalten. Es ist hierbei darzustellen, welche Zugriffe protokolliert werden.
2.1.3.2	Alle Mitarbeiterzugriffe auf Cloud-Infrastrukturkomponenten werden protokolliert. Diese Protokollierung ist einsehbar.		✓	✓	Der CSP hat darzustellen, dass alle Zugriffe durch seine Mitarbeiter auf die Infrastrukturkomponenten der Cloud protokolliert werden und dass diese Protokollierung durch den Kunden einsehbar ist.
2.1.3.3	Administrative Operationen auf Betriebssystemebene (An- und Abmeldung am System, Installation von Anwendungen, Änderungen von Berechtigungen, Änderungen im Benutzermanagement, etc.) werden protokolliert.		✓	✓	Der CSP hat die Logmechanismen und deren Manipulationssicherheit darzustellen, die auf Betriebssystemebene der Virtualisierungshosts einerseits und der bereitgestellten Gastsysteme andererseits zum Einsatz kommen. Insbesondere ist darzustellen, dass administrative Operationen auf Betriebssystemebene (An- und Abmeldung am System, Installation von Anwendungen, Änderungen von Berechtigungen, Änderung im Benutzermanagement, etc.) geeignet protokolliert und datenschutzkonform befristet aufbewahrt und anschließend gelöscht werden.
2.1.3.4	Es existiert ein zentrales Monitoring für die Cloud-Umgebung. Eine Sicht auf das Monitoring wird dem Kunden bereitgestellt.		✓	✓	Der CSP hat das Monitoring des Sicherheitsstatus (Vertraulichkeit, Verfügbarkeit, Integrität) des Cloud-Managementsystems darzustellen. Insbesondere ist darzustellen, dass eine Sicht auf dieses Monitoring dem Kunden bereitgestellt werden kann und wenn ja, in welcher Form.

2.1.3.5	Die historischen Daten über den Sicherheitsstatus des Cloud-Managementsystems sind vollständig, über einen ausreichen langen Zeitraum einsehbar.		✓	✓	Der CSP hat darzustellen, dass er einen regelmäßigen Report über den vollständigen Sicherheitsstatus (Vertraulichkeit, Verfügbarkeit, Integrität) des Cloud-Management-Systems über einen bestimmten Berichtszeitraum (z.B. eine Woche, einen Monat, ein Jahr) liefern kann.
2.1.3.6	Für den Kunden ist einsehbar, wie viele Cloud-Ressourcen (Virtueller Speicher, Virtuelles Netzwerk, Virtuelle CPU-Last, Virtuelles Storage) aktuell in Gebrauch sind (d.h. eine Darstellung der Auslastung der aktuell sich in Gebrauch befindlichen Cloud-Ressourcen). Diese Daten werden regelmäßig für den Kunden bereitgestellt.	✓			Der CSP hat darzustellen, dass für den Kunden einsehbar ist, wie viele Cloud-Ressourcen (Virtueller Speicher, Virtuelles Netzwerk, Virtuelle CPU-Last, Virtuelles Storage) aktuell in Gebrauch sind (d.h. eine Darstellung der Auslastung der aktuell sich in Gebrauch befindlichen Cloud-Ressourcen). Es ist darzustellen, wie diese Daten regelmäßig monatlich für den Auftraggeber bereitgestellt werden.
2.1.3.7	Alle Operationen (Image-Erzeugung, -Duplizierung, Löschung) werden protokolliert.		✓	✓	Der CSP hat die Logmechanismen darzustellen, die im Rahmen des Lebenszyklus einer virtuellen Maschine zum Einsatz kommen.
2.1.3.8	Protokolldaten werden dem Kunden zur Verfügung gestellt und können an das SIEM des Kunden weitergeleitet werden.			✓	Der CSP hat darzustellen, dass und welche Protokolldaten in welchem Format und auf welche Weise an das SIEM (Security Information and Event Management) des Auftraggebers weitergeleitet werden können.
2.1.4	**Update- und Patchmanagement**				
2.1.4.1	Für jede Cloud-Ressource ist eine aktuelle Liste mit installierter Software vorhanden.		✓	✓	Der CSP hat darzustellen, dass er eine Software-Inventarisierung für die installierte Software für jede bereitgestellte Cloud-Ressource vorhält und in dieser auch die aktuell zum Einsatz kommenden Versionen dokumentiert sind.
2.1.4.2	Alle vorhandenen Sicherheitsupdates für die installierte Hypervisor-Software werden installiert (Patchlevel).	✓			Der CSP hat den Nachweis zu erbringen, dass existierende Sicherheitsupdates für die zum Einsatz kommende Software grundsätzlich zeitnah installiert werden. Dabei ist ein Vetorecht des Kunden zumindest für dedizierte Systeme erforderlich, bei shared Systemen ggf. gegen Zusatzentgelt für Beibehaltung der bisherigen Plattform

2.1.4.3	Regelmäßige Überprüfung über verfügbare Sicherheitspatches der installierten Software finden statt.		✓	✓	Der CSP hat darzustellen, dass eine regelmäßige Überprüfung über verfügbare Sicherheitspatches der installierten Software stattfindet.
2.1.4.4	Es existiert ein Benachrichtigungsmechanismus, ob Sicherheitsmaßnahmen noch aktuell sind (bspw. Ablaufzeiten von Zertifizierungen).		✓	✓	Der CSP hat darzustellen, dass und welchen regelmäßigen Zertifzierungsprozessen (Datenschutzzertifizierung, ISO 27001, ggf. weitere Zertifizierungen) er für den Geltungsbereich der bereitgestellten Cloud-Ressourcen unterliegt und wie sichergestellt wird, dass Zertifizierungen aufrechterhalten bleiben. Es wird erwartet, dass der Auftraggeber über den aktuellen Zertifizierungsstatus in regelmäßigen Abständen unaufgefordert benachrichtigt wird. Die Bereitschaft hierfür ist darzustellen.
2.1.4.5	Alle Sicherheitsupdates der verwendeten Storagemanagement-Software werden installiert.		✓	✓	Der CSP hat darzustellen, dass die Storagemanagementsoftware einem Patchmanagementprozess unterliegt.
2.1.4.6	Der Kunde wird über durchgeführte Sicherheitsupdates informiert.		✓	✓	Der CSP hat darzustellen, dass und ggfls. wie der Kunde über durchgeführte Sicherheitsupdates informiert wird.
2.1.5	**Backup**				
2.1.5.1	Es existiert ein Backup-Konzept für das Cloud-Management-System	✓			Der CSP hat sein Backup-Konzept für das Cloud-Management-System ausführlich und nachvollziehbar darzustellen.

2.1.5.2	Verschiedene Versionen des Backups einer VM werden ausreichend lange gespeichert.	✓			Der CSP hat das Backup-Konzept (bei datei- und verzeichnisbasiertem Backup) für bereitgestellte virtuelle Maschinen darzustellen. Der CSP muss dem Auftraggeber Datensicherungen in ausreichendem und angemessenem Rahmen auch auf physikalischen Medien zur Verfügung stellen können, um auch im Falle einer Insolvenz des CSP die Verfügbarkeit möglichst schnell wiederherstellen zu können. Für das datei- und verzeichnisbasierte Backup ist insbesondere offenzulegen, über welchen Zeitraum und über wie viele Generationen Backups angelegt, gespeichert und wiederhergestellt werden können, welches Backup-Tool eingesetzt und welche Backup-Parameter verwendet werden. Für ein image-basiertes Backup ist eine Beschreibung vorzulegen, welches Image-Tool eingesetzt wird. Das Image-Backup erfolgt initial nach Absprache mit dem Auftraggeber, es erfolgt eine längstens halbjährliche Image-Erneuerung nach Absprache mit dem Auftraggeber.
2.1.5.3	Der Zugriff auf Backupdaten wird protokolliert.		✓	✓	Der CSP hat darzustellen, dass der Zugriff auf mit dem Backup-System gesicherte Daten protokolliert wird.
2.1.6	**Datenlöschung**				
2.1.6.1	Daten werden sicher gelöscht.	✓			Der CSP hat seinen Prozess zum sicheren Löschen von Daten darzustellen. Das Löschverfahren ist explizit offenzulegen. Für den Fall, dass Speichermedien im Rahmen des Löschprozesses vernichtet werden, ist auch das Verfahren zum Vernichten offenzulegen. Die Übereinstimmung mit entsprechenden DIN-Standards / Zertifizierungen sollte dokumentiert werden,

2.1.6.2	Das Löschen von beliebig ausgewählten Daten und anschließende Suche nach verfügbaren Replikaten ist möglich.			✓	Der CSP hat darzustellen, welche Möglichkeiten zum Löschen von Daten in der Cloud-Infrastruktur für den Nutzer besteht und dass die anschließende Suche nach verfügbaren Replikaten möglich ist.
2.1.7	**Funktionalität**				
2.1.7.1	Eine Skalierung der VMs ist möglich.	✓			Der CSP hat darzustellen, dass und inwieweit eine Skalierung (d.h. Änderung der Parameter der virtuellen Hardware, wie CPU-Leistung, Größe des zugeteilten virtuellen Speichers) vorgesehen ist und dass bestehende Skalierungsgrenzen dabei berücksichtigt werden.
2.1.7.2	Eine Integritätsprüfung des Exports der in der Cloud gespeicherten Daten ist möglich.	✓			Der CSP hat darzustellen, dass und ggfls. wie eine Integritätsprüfung der in der Cloud gespeicherten Daten möglich ist.
2.1.7.3	Images virtueller Maschinen können in die Cloud exportiert und aus ihr importiert werden.	✓			Der CSP hat darzustellen, dass und ggf. wie Images virtueller Maschinen aus der Infrastruktur des Kunden in die bereitgestellten Cloud-Ressourcen exportiert und aus ihr importiert werden können und welche Formate hierfür unterstützt werden. Die verfügbare Bandbreite sollte ebenfalls dargestellt werden
2.1.7.4	APIs und Serviceschnittstellen zum Datenexport aus der Cloud sind transparent.			✓	Der CSP hat seine Schnittstellen und APIs zum Export und Daten aus der Cloud darzustellen.
3	**Betriebliche Anforderungen** (Die betrieblichen Anforderungen variieren von Auftraggeber zu Auftraggeber und sollen hier nur beispielhaft aufgeführt werden.)				
3.1	Storage - Transparenz der RAID-Level, der Anbindung und weiterer Leistungsparameter	✓			Es ist transparent, welcher RAID-Level, welche Festplatten-Technik und welche Anbindungstechnologie zu den Virtualisierungshosts eingesetzt wird und wieviel IOPS diese Lösung erzielt. Eine zentralisierte Storagelösung mit einer Mindest-IO-Leistung von 5000 IOPS (Workload von 100% random bei 70% read und 30% write) und einem RAID-Level mit Redundanz wird eingesetzt.

3.2	CPU - Transparenz der Leistungsparameter	✓			Der CSP hat eine Beschreibung vorzulegen, welche physikalischen Prozessoren (Hersteller/Typ) bei den Virtualisierungs-Hosts verwendet werden. Jeder Virtualisierungshost hat eine CPU-Leistung von mindestens 400 Bench-markpunkten (Benchmark-Result SPEC-Intrate 2006 (Baseline)).
3.3	Host - Transparenz der Technik und Leistungsparameter	✓			Durch den CSP ist eine Beschreibung vorzulegen, welche Technik beim Host eingesetzt wird und wie er die Verfügbarkeit gewährleistet. Die Virtualisierungsumgebung besteht aus mindestens zwei Virtalisierungsknoten, zwischen denen eine Live-Migration / Live-Replikation der Virtuellen Maschinen möglicht ist.
3.4	Virtualisierungsschicht - Zonenkonzept		✓	✓	Der CSP hat als Virtualisierungsplattform VSphere und/oder HYPER-V bereitzustellen. Die Gewährleistung einer ausreichenden Absicherung der Virtuellen Plattformen verschiedener Kunden bzw. unterschiedlicher Schutzbedarfe gegeneinander ist zu beschreiben.
3.5	zentrales Management der Cloud-Services	✓			Der Zugriff auf den durch den CSP bereitzustellenden Cloud-Service und erforderliches Management erfolgt über eine vom Auftraggeber betriebene zentrale Management-Plattform. Der CSP hat darzustellen, wie eine weitgehend transparente Integration des Zugriffs über das zentrale Cloud-Management des Auftraggebers erfolgen kann.

3.6	Betriebssysteme		✓	✓	Der CSP hat dem Auftraggeber folgende Betriebssysteme bereitzustellen: - SLES 11 (32-Bit), SLES 11 (64-Bit), - Windows 2008 SE/EE deutsch (32-Bit), Windows 2008 SE/EE deutsch (64-Bit), Windows 2008R2 SE/EE deutsch (64-Bit), Windows 2012 (Standard und Datacenter) deutsch (64-Bit). Zum Zeitpunkt des Erscheinens neuer Versionen dieser Betriebssysteme sind jeweils die 3 neuesten Versionen jeweils in der 32- und 64 bit-Version (sofern verfügbar) bereitzustellen
3.7	Datenbanken		✓	✓	##
3.8	Betriebshandbuch		✓	✓	Der AN führt ein Betriebshandbuch, das mindestens folgende Informationen enthält: o Installationsanweisungen o Hardwarebeschreibungen o Administrationsvorgaben o Backup und Restore o Störungsmanagement o Änderungsmanagement o und weitere zum Betrieb notwendige Einträge
3.9	Bereitstellung einer deutschsprachigen Hotline	✓			Eine kostenfreie deutschsprachige Hotline zu den angefragten Servicezeiten (5x9 und 7x24) mit einer erreichbaren E-Mail-Adresse sowie Telefonnummer im deutschen Festnetz steht bereit. Anfragen per E-Mail sind, soweit nicht ausdrücklich etwas anderes vereinbart wurde, jeweils bis zum Ende des nächsten Arbeitstages zu beantworten.

3.10	Systemverfügbarkeit	✓			Der AN stellt durch eine entsprechende Betreuung in den angefragten Betriebszeiten eine hohe Verfügbarkeit der Systemlandschaft in den Betriebszeiten sicher. Innerhalb dieser Betriebszeit bietet der AN eine über den Vertragszeitraum geltende durchschnittliche technische Verfügbarkeit der Cloud-Services von 99,9 % per anno an. Nachfolgend Aufgelistetes geht nicht in die Berechnung der Ausfallzeit ein: o Unterbrechungen während des vertraglich vereinbarten regulären Wartungsfensters, auch wenn diese nicht besonders angekündigt wurden. o geplante Unterbrechungen wegen Wartungsarbeiten innerhalb eines sonstigen Wartungsfensters außerhalb der vereinbarten Zeiten, sofern vom Auftragnehmer mit einem Vorlauf von sieben Kalendertagen angekündigt.

3.11	Wartungen		✓	✓	Zur Vermeidung von Inkompatibilitäten, Unterbrechungen oder Störungen beim Betrieb der Anwendung unterrichtet der AN den Auftraggeber frühzeitig über die Absicht, im Rechenzentrum des Auftragnehmers neue Programmversionen (z.B.: Betriebssystem, systemnahe Softwarekomponenten, Datenbankverwaltungssystem o. ä.) zu implementieren. Bei der Verwendung gemeinsamer Infrastrukturen für mehrere Kunden unterrichtet der CSP den Kunden, mit welchen Zusatzkosten der Kunde zu rechnen hat, wenn er auf einem Weiterbetrieb der bisherigen Programmversion besteht. Geplante Unterbrechungen wegen Wartungsarbeiten innerhalb eines sonstigen Wartungsfensters werden mit einer Vorlaufzeit von sieben Kalendertagen angekündigt. Außerordentliche Wartungsarbeiten, die kurzfristig zu erledigen sind, werden - soweit möglich - nach Information des Auftraggebers durchgeführt.
3.12	Anbindung an die Cloud-Infrastruktur	✓			Die Anbindung des Auftraggebers an die Cloud-Infrastruktur des CSP ist über eine verschlüsselte VPN-Anbindung zu realisieren. Es ist transparent, mit welchen Technologien, welcher Bandbreite und Verfügbarkeit im Jahresmittel die VPN-verschlüsselte Anbindung an die Cloud aus der Infrastruktur des Kunden realisiert wird. Dazu sollten nach Möglichkeit offene, im Quellcode prüfbare Transportprotokolle eingesetzt werden.
4	**Datenschutzanforderungen**				
4.1	**Transparenz**				
4.1.1	Verständlichkeit	✓			Werden sämtliche Vertragsbedingungen dem Kunden in verständlicher Weise erklärt?
4.1.2	Vollständigkeit	✓			Sind die Leistungen des Cloudanbieters ausführlich und vollständig definiert?

4.1.3	Verbindlichkeit	✓			Werden Angaben zu Verfügbarkeit, Reaktionszeiten, Rechenleistung, Speicherplatz und Support gemacht?
4.1.4	Kontrollbefugnis	✓			Der CSP ermöglicht dem Kunden, die Verfügbarkeit und andere im SLA vereinbarte Messgrößen zu kontrollieren
4.1.5	Statistische Auswertungen	✓			Stellt der Cloud-Anbieter dazu Statistiken bereit?
4.2	**Portabilität**				
4.2.1	Portabilität	✓			Ist die Portabilität der Cloud Dienste gewährleistet?
4.2.2	Migration	✓			Ist eine Migration der Daten zu einem anderen Cloud-Anbieter jederzeit möglich?
4.2.3	Migrationsunterstützung	✓			Stellt der Cloud-Anbieter Unterstützungsleistungen bei der Migration auf andere Anbieter zur Verfügung
4.2.4	Schnittstellen	✓			Verwendet der CSP geeignete Schnittstellen, die eine Migration der Daten in und aus der Cloud ermöglichen?
4.2.5	offene Standards	✓			Verwendet der CSP offene Standarts, die die Portabilität der Daten z.B. zu einem anderen Anbieter ermöglichen?
4.3	**Schulung**				
4.3.1	Personal	✓			Stellt der Cloud-Anbieter sicher, dass ausreichend geschultes Personal zur Verfügung steht?
4.3.2	Schulungen	✓			Werden regelmäßig Schulungen im Bereich Datenschutz und Datensicherheit für eigene Mitarbeiter angeboten?
4.3.3	Schulungsnachweise	✓			Müssen Mitarbeiter den Besuch von Schulungsmaßnahmen nachweisen?
4.4	**Mitarbeiterüberprüfung**				
4.4.1	Führungszeugnis	✓			Wird bei allen Mitarbeitern des CSP geprüft, ob diese über ein Führungszeugnis ohne relevante Einträge verfügen?
4.4.2	Embargoprüfung		✓	✓	Wird geprüft, ob der CSP von einem Embargo der EU betroffen ist (zb EU-Finanzembargo?)
4.4.3	Verfassungsprüfung		✓	✓	Wird geprüft, ob der CSP verfassungsfeindliche Organisationen unterstützt?
4.5	**Verarbeitungsbeschränkungen**				

4.5.1	Zulässigkeit der Auftragsdatenverarbeitung	✓			Ist Auftragsdatenverarbeitung datenschutzrechtlich zulässig? (Beschränkungen ergeben sich z.B. aus Landeskrankenhausgesetzen)
4.5.2	Rechtfertigung der Weitergabe bei Daten im Sinne des § 203 StGB	✓			Ist eine Befugnisnorm für die Weitergabe bei Daten im Sinne des § 203 StGB vorhanden?
4.5.3	Einwilligung	✓			Liegen alle notwendigen Einwilligungen der Betroffenen vor?
4.6	**Revisionssicherheit**				
4.5.1	Langzeitarchivierung	✓			Der CSP hat darzustellen, wie die Langzeitsicherung von Daten gewährleistet werden kann
4.5.2	Verschlüsselung/Digitale Signaturen	✓			Der CSP hat darzustellen, ob und wie kryptographische Methoden zur Sicherung von Dokumenten gegen Veränderung eingesetzt werden
4.5.3	Werden die Vorgaben der BSI-Richtlinie TR-ESOR dabei beachtet?	✓			Der CSP hat zu erklären, ob er die in der TR ESOR festgelegten Methoden zur Zeitstempelung und Nachsignierung von Dokumenten bereithält