letzte Überprüfung: 21.06.2022 Version 4.0

Klassifikation: intern

RA = Anforderung aus Risikoanalyse
CA = Compliance-Anforderung (Anforderungen aus Gesetzen, (Kunden)-Verträgen, sonstige Richtlinien/vorgaben)
GA = Geschäftsanforderung

Katja Siegemund

Control	Titel	Ziel	SOA Auswahl	SOA, Begründung Anwendbarkeit	RA	CA	GA
5.1	Vorgaben der Leitung für Informationssicherheit	Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften	Ja	Thema		x	x
5.1.1	Informationssicherheits-richtlinien	Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.	Ja	Setzt den Rahmen und definiert das Verständnis der Plusnet GmbH zum Thema Informationssicherheit.		x	
5.1.2	Überprüfung der Informationssicherheits-richtlinien	Die zentralen Dokumente werden jährlich und immer dann überprüft, wenn wesentliche Änderungen erfolgen, um ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.	Ja	Regelmäßige Überprüfung und Ergänzung der Richtlinie Informationssicherheit insbesondere bei Änderungen.		x	
6.1	Interne Organisation	Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.	Ja	Thema			
6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	Alle Informationssicherheitsverantwortlichkeiten sollten festgelegt und zugeordnet sein.	Ja	Informationssicherheitsmanagement muss insbesondere auch auf GF-Ebene mit einer hohen Priorität gelebt werden.	x		
6.1.2	Aufgabentrennung	Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sollten getrennt werden, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.	Ja	Eine unternehemsweite Umsetzung eines ISMS erfordert die Einbindung aller Betroffenen.	x		
6.1.3	Kontakt mit Behörden	Angemessene Kontakte mit relevanten Behörden sollten gepflegt werden.	Ja	Als TK Provider haben wir verschiedene Themenfelder, diese werden abgedeckt.		x	
6.1.4	Kontakt mit speziellen Interessensgruppe	Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden sollten gepflegt werden.	Ja	Vertretung Interessen und Bezug von Informationen	x		
6.1.5	Informationssicherheit im Projektmanagement	Informationssicherheit sollte im Projektmanagement berücksichtigt werden, ungeachtet der Art des Projekts.	Ja	Starkes Projektgeschäft, sowohl interne als auch Kundenprojekte.	x		
6.2	Mobilgeräte und Telearbeit	Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt.	Ja	Thema			
6.2.1	Richtlinie zu Mobilgeräten	Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sollten umgesetzt werden, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.	Ja	Absicherung der mobilen Arbeitsplätze entsprechen der EnBW Vorgaben und Kundenanforderungen.		x	
6.2.2	Telearbeit	Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sollten umgesetzt sein.	Ja	Es ist per Definiton erwünscht und notwendig, dass Telearbeit genutzt wird (Bereitschaft, Notfall, etc.)	x		x

A.7.0	A.7 Personalsicherheit	Das Personalmanagement und zugehörige organisatorische und verfahrenstechnische Abläufe sind im Plusnet GmbH Intranet dokumentiert.	Ja	Bereich			
7.1	Vor der Beschäftigung	Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.	Ja	Thema			
7.1.1	Sicherheitsüberprüfung	Alle Personen, die sich um eine Beschäftigung bewerben, werden einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.	Ja	Wird in Kundenverträgen gefordert und ist teilweise schon vereinbart. Wirklich erforderlich nur in Bezug auf einzelne Tätigkeitsfelder.		x	
7.1.2	Beschäftigungs- und Vertragsbedingungen	In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sind deren Verantwortlichkeiten und diejenigen der Organisation festgelegt.	Ja	Es gibt unterschiedliche Arten der Beschäftigung und die Größe des Unternehmens setzt eine strukturierte Verwaltung von personellen Ressourcen vorraus.	x		x
7.2	Während der Beschäftigung	Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.	Ja	Thema			
7.2.1	Verantwortlichkeiten der Leitung	Die Leitung verlangt von allen Beschäftigten und Auftragnehmern, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen.	Ja	Einfordern der Einhaltung von Richtlinien und einer aktiven Unterstützung zur Absicherung der Informationssicherheit.	x		
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, bekommen ein angemessenes Bewusstsein durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind.	Ja	Schaffen und Ausbauen des Bewusstseins für Informationssicherheit.	x		
7.2.3	Maßregelungsprozess	Ein formal festgelegter und bekanntgegebener Maßregelungsprozess sollte eingerichtet sein, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.	Ja	Es kann zu Sicherheitsverstössen kommen, bzw. gab es in der Vergangenheit welche, daher ist ein entsprechendes Verfahren notwendig und etabliert.	x		
7.3	Beendigung und Änderung der Beschäftigung	Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung.	Ja	Thema			
7.3.1	Beendigung und Änderung der Beschäftigung	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt werden.	Ja	Notwendig, um bspw. Kenntnisse in Bezug auf Kundenumgebungen oder auch unserer eigenen zu wahren.	x		
8.1	Verantwortlichkeit für Werte	Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.	Ja	Thema			
8.1.1	Inventarisierung der Werte	Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten erfasst und ein Inventar dieser Werte sollte erstellt und gepflegt werden.	Ja	Ohne diese Anforderung keine Möglichkeit die Qualität und Sicherheit in unseren komplexen IT-Umgebungen zu gewährleisten.	x		
8.1.2	Zuständigkeit für Werte	Für alle Werte, die im Inventar geführt werden, sollte es Zuständige geben.	Ja	Sicherstellung der Nachvollziehbarkeit des Eigentums von Systemen. Alle Informationen und organisationseigenen Werte (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen sollten Eigentum eines bestimmten Teils der Organisation sein.	x		

8.1.3	Zulässiger Gebrauch von Werten	Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten aufgestellt, dokumentiert und angewendet werden.	Ja	Klare Regelungen für den Gebrauch der organisationseigenen Assets.	x		
8.1.4	Rückgabe von Werten	Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, sollten bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehörten, zurück geben.	Ja	Alle Arten von Werten (bspw. auch Computer, mobile Devices, Zutrittskarten,...) müssen berücksichtigt werden.	x		
8.2	Informationsklassifizierung	Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhält.	Ja	Liefert die Grundlage für die Auswahl der anzuwenden Sicherheitsmaßnahmen und Prozesse.	x		x
8.2.1	Klassifizierung von Information	Information sollte anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert werden.	Ja	Liefert die Grundlage für die Auswahl der anzuwenden Sicherheitsmaßnahmen und Prozesse.	x		
8.2.2	Kennzeichnung von Information	Ein angemessener Satz von Verfahren zur Kennzeichnung von Information sollte entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.	Ja	Alle Arten von Informationen müssen berücksichtigt werden, es bedarf eines Schemas zur Klassifizierung um generelle Regelungen zuzuweisen.	x		
8.2.3	Handhabung von Werten	Verfahren für die Handhabung von Werten sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.	Ja	Grundlage für die Anwendung von Sicherheitsmaßnahmen.	x		
8.3	Handhabung von Datenträgern	Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf Datenträgern gespeichert ist, wird unterbunden.	Ja	Einsatz und Entsorgung von Datenträgern gehört ist auch ein rechtlich gefordert (Datenschutz).	x	x	
8.3.1	Handhabung von Wechseldatenträgern	Verfahren für die Handhabung von Wechseldatenträgern sollten entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt werden.	Ja	Wird sowohl intern als auch in Kundenumgebungen benötigt.	x		
8.3.2	Entsorgung von Datenträgern	Nicht mehr benötigte Datenträger sollten sicher und unter Anwendung formaler Verfahren entsorgt werden.	Ja	Wird sowohl intern als auch in Kundenumgebungen benötigt	x		
8.3.3	Transport von Datenträgern	Datenträger, die Information enthalten, sollten während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden.	Ja	Wird sowohl intern als auch in Kundenumgebungen benötigt	x		
9.1	Geschäftsanforderungen an die Zugangssteuerung	Der Zugang zu Information und informationsverarbeitenden Einrichtungen ist eingeschränkt.	Ja	Zielsetzung: Beschränkung des Zugriffs auf Informationen und informationsverarbeitende Einrichtungen.	x	x	x
9.1.1	Leitlinie zur Zugangskontrolle	Eine Leitlinie zur Zugangskontrolle sollte auf Grundlage der geschäftlichen und der die Informationssicherheit betreffenden Anforderungen erstellt, dokumentiert und geprüft werden.	Ja	Regelt den Zutritt, Zugang und Zugriff innerhalb der Plusnet. Ziel Zusammenfassung der drei Punkte.	x		
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten	Benutzer sollten ausschließlich zu denjenigen Netzwerken und Netzwerkdiensten Zugang erhalten, zu deren Nutzung sie ausdrücklich autorisiert wurden.	Ja	Zugangsprofile müssen für einen Abgleich zwischen Soll und IST vorhanden sein	x		
9.2	Benutzerzugangssverwaltung	Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.	Ja	Gewährleistung der Zugriffssicherheit im Unternehmen und für die Kundensysteme.	x		

9.2.1	Registrierung und Deregistrierung von Benutzern	Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern sollte umgesetzt werden, um die Zuordnung von Zugangsrechten zu ermöglichen.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
9.2.2	Zuteilung von Benutzerzugängen	Ein formaler Prozess zur Zuteilung von Benutzerzugängen sollte umgesetzt werden, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
9.2.3	Verwaltung privilegierter Zugangsrechte	Zuteilung und Gebrauch von privilegierten Zugangsrechten sollte eingeschränkt und gesteuert werden.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
9.2.4	Verwaltung geheimer Authentisierungsinformation von Benutzern	Die Zuordnung von geheimer Authentisierungsinformation sollte über einen formalen Verwaltungsprozess gesteuert werden.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
9.2.5	Überprüfung von Benutzerzugangsrechten	Die für Werte Zuständigen sollten in regelmäßigen Abständen die Benutzerzugangsrechte überprüfen.	Ja	Um sicherzustellen, dass Benutzer nur die benötigten Zugriffs- und Zutrittsrechte haben. Kundenanforderung.		x	
9.2.6	Entzug oder Anpassung von Zugangsrechten	Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen sollten bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst werden.	Ja	Für Berechtigungsmanagement intern und Kundenumgebungen notwendig	x		
9.3	Benutzerverantwortlichkeiten	Benutzer sind für den Schutz Ihrer Authentisierungsinformation verantwortlich gemacht.	Ja	In grösseren Unternehmen obligatorisch.			x
9.3.1	Gebrauch geheimer Authentisierungsinformation	Benutzer sollten verpflichtet werden, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
9.4	Zugangssteuerung für Systeme und Anwendungen	Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.	Ja	Für alle Arten Systeme und Applikationen anzuwenden	x		
9.4.1	Informationszugangssbeschränkung	Zugang zu Information und Anwendungssystemfunktionen sollte entsprechend der Zugangssteuerungs-richtlinie eingeschränkt sein.	Ja	Zugriffe werden nach dem need-to-know Prinzip behandelt.	x		
9.4.2	Sichere Anmeldeverfahren	Soweit es die Zugangssteuerungsrichtlinie erfordert, sollte der Zugang auf Systeme und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert werden.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.	x	x	
9.4.3	Kennwortmanagement-system	Kennwortmanagementsysteme sollten interaktiv sein und starke Kennwörter erfordern.	Ja	Vermeiden von Sicherheitslücken sowie Bestandteil der Vertreterregellung.	x		
9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, sollte eingeschränkt und streng überwacht werden.	Ja	Vermeidung von unkontrollierten Veränderungen an Systemen.	x		
9.4.5	Zugangssteuerung für Quellcode von Programmen	Zugang zu Quellcode von Programmen sollte eingeschränkt werden.	Ja	Zugriffe werden nach dem need-to-know Prinzip behandelt.	x		
A.10.1	Kryptographische Maßnahmen	Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt.	Ja	Gesetzliche Anforderung und Kundenanforderung		x	
A.10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	Eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information ist entwickelt und umgesetzt.	Ja	Umsetzung Anforderungen, Sicherstellen einheitlicher Standards und Vorgehensweisen.	x		

A.10.1.2	Schlüsselverwaltung	Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln ist entwickelt (siehe oben) und wird über deren gesamten Lebenszyklus umgesetzt.	Ja	Erfolgt Kundenprojektbezogen.	x		
11.1	Sicherheitsbereiche	Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informationsverarbeitenden Einrichtungen der Organisation sind verhindert.	Ja	Diverse Standorte mit unterschiedlichsten Gebäude und Raum-Anforderungen	x		
11.1.1	Physischer Sicherheitsperimeter	Zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitsperimeter festgelegt und verwendet werden.	Ja	Schutz sensibler Bereiche vor unberechtigten Zutritt.	x		
11.1.2	Physische Zutrittssteuerung	Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung geschützt werden um sicherzustellen, dass nur berechtigtes Personal Zutritt hat.	Ja	Umsetzung der Sicherheitsanforderungen.	x		
11.1.3	Sichern von Büros, Räumen und Einrichtungen	Die physische Sicherheit für Büros, Räume und Einrichtungen sollte konzipiert und angewendet werden.	Ja	Umsetzung der Sicherheitsanforderungen.	x		
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	Physischer Schutz vor Naturkatastrophen, bösartigen Angriffen oder Unfällen sollte konzipiert und angewendet werden.	Ja	Umsetzung der Sicherheitsanforderungen.	x		
11.1.5	Arbeiten in Sicherheitsbereichen	Verfahren für das Arbeiten in Sicherheitsbereichen sollten konzipiert und angewendet werden.	Ja	Umsetzung der Sicherheitsanforderungen.	x		
11.1.6	Anlieferungs- und Ladebereiche	Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, sollten überwacht und, falls möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um	Ja	Umsetzung der Sicherheitsanforderungen.	x		
11.2	Geräte und Betriebsmittel	Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.	Ja	Definition des sicheren Umgangs unternehmensweit.	x		
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln	Geräte und Betriebsmittel sollten so platziert und geschützt werden, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind.	Ja	Ist wesentlicher Bestandteil des Sicherheitskonzeptes.	x		
11.2.2	Versorgungseinrichtungen	Geräte und Betriebsmittel sollten vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.	Ja	Standard für Hochverfügbarkeit.	x		
11.2.3	Sicherheit der Verkabelung	Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung sollten vor Unterbrechung, Störung oder Beschädigung geschützt werden.	Ja	Standard für Hochverfügbarkeit.	x		
11.2.4	Instandhalten von Geräten und Betriebsmitteln	Geräte und Betriebsmittel sollten Instand gehalten werden, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen.	Ja	Schutz der Unternehmenswerte und Gewährleistung der Funktionsfähigkeit.	x		
11.2.5	Entfernen von Werten	Geräte, Betriebsmittel, Informationen oder Software sollten nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt werden.	Ja	Schutz der Unternehmenswerte und der Informationssicherheit.	x		
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	Werte außerhalb des Standorts sollten gesichert werden, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen.	Ja	Gilt für Notebooks / mobile Devices der Mitarbeiter der Plusnet, Homeoffice üblich.	x		x

11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, sollten überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.	Ja	Datenschutzgesetzte und Vertraulichkeitsverpflichtungen.		x	
11.2.8	Unbeaufsichtigte Benutzergeräte	Benutzer sollten sicherstellen, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
11.2.9	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen sollten angewendet werden.	Ja	Clean Desk fördert aktiv Sicherheit durch ordnungsgemäßen Umgang mit Informationen.	x		
12.1	Betriebsabläufe und -verantwortlichkeiten	Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.	Ja	Bestandteil Kerngeschäft			x
12.1.1	Dokumentierte Bedienabläufe	Die Betriebsverfahren sollten dokumentiert und allen Benutzern, die sie benötigen, zugänglich sein.	Ja	Nachvollziehbare Vorgehensweisen, Konzepte und Richtlinien zum Betrieb und der Weiterentwicklung der Systeme.	x		x
12.1.2	Änderungssteuerung	Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen sollten gesteuert werden.	Ja	Nachvollziehbarkeit und Risikovermeidung.	x		
12.1.3	Kapazitätssteuerung	Die Ressourcennutzung/Benutzung von Ressourcen wird überwacht und abgestimmt, und es werden Prognosen zu zukünftigen Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen.	Ja	Sicherstellung einer hohen Systemverfügbarkeit- und Performance entsprechend der Kundenforderungen.		x	
12.1.4	Trennung von Entwicklungs-, Test- und Betriebs-umgebungen	Entwicklungs-, Test- und Betriebsumgebungen sollten voneinander getrennt sein, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.	Ja	Vermeidung von Fehlern und Sicherheitsvorfällen in der Produktionsumgebung.	x		
12.2	Schutz vor Schadsoftware	Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.	x	x	
12.2.1	Maßnahmen gegen Schadsoftware	Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer sollten umgesetzt werden.	Ja	Absicherung der IT-Systeme und Applikationen erforderlich		x	
12.3	Datensicherung	Daten sind vor Verlust geschützt.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
12.3.1	Sicherung von Information	Sicherheitskopien von Information, Software und Systemabbildern sollten entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet werden.	Ja	Regelmäßige Erstellung Backup-Kopien von Informationen und von Software. Kundenanforderungen müssen berücksichtigt werden.		x	
12.4	Protokollierung und Überwachung	Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
12.4.1	Ereignisprotokollierung	Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, sollten erzeugt, aufbewahrt und regelmäßig überprüft werden.	Ja	Ist Basis für spätere Analysen und im speziellen auf Forderung der Kunden.	x	x	
12.4.2	Protokollinformation	Protokollierungseinrichtungen und Protokollinformation sollten vor Manipulation und unbefugtem Zugriff geschützt sein.	Ja	Forderungen der Sicherheitspolitik, Kunden und Gesetze.		x	

12.4.3	Administratoren- und Bedienerprotokolle	Tätigkeiten von Systemadministratoren und Systembedienern sollten aufgezeichnet und die Protokolle sollten geschützt und regelmäßig überprüft werden.	Ja	Nachvollziehbarkeit von System- und Konfigurationsänderungen.	x		
12.4.4	Uhrensynchronisation	Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder einem Sicherheitsbereich sollten mit einer einzigen Referenzzeitquelle synchronisiert sein.	Ja	Voraussetzung für den ordnungsgemäßen Betrieb der Systeme und des sicheren VPN-Zugangs, Verlässlichkeit bei Logfile Analysen.	x		x
12.5	Steuerung von Software im Betrieb	Die Integrität von Systemen im Betrieb ist sichergestellt.	Ja	Anforderungen in EnBW Vorgaben.		x	
12.5.1	Installation von Software auf Systemen im Betrieb	Verfahren zur Steuerung der Installation von Software auf Systemen im Betrieb sind umgesetzt.	Ja	Etablierung von Verfahren zur Kontrolle von Software im Betrieb.	x		
12.6	Handhabung technischer Schwachstellen	Die Ausnutzung technischer Schwachstellen ist verhindert.	Ja	Anforderungen in EnBW Vorgaben und Anforderungen seitens der Kunden.		x	
12.6.1	Handhabung von technischen Schwachstellen	Informationen über technische Schwachstellen verwendeter Informationssysteme sollte rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen sollte bewertet und angemessene Maßnahmen ergriffen werden, um das dazugehörige Risiko zu behandeln.	Ja	Minimieren von Risiken und Sicherheitsvorfällen.	x		
12.6.2	Einschränkung von Softwareinstallation	Regeln für die Softwareinstallation durch Benutzer sollten festgelegt und umgesetzt werden.	Ja	Etablierung von Verfahren zur Kontrolle von Software im Betrieb.	x		
12.7	Audit von Informationssystemen	Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhaltet, sollten sorgfältig geplant und vereinbart werden, um Störungen der Geschäftsprozesse zu minimieren.	Ja	Anforderung Sicherheitsrichtlinien, Bestandteil Kerngeschäft		x	x
12.7.1	Maßnahmen für Audits von Informationssystemen	Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhaltet, sollten sorgfältig geplant und vereinbart werden, um Störungen der Geschäftsprozesse zu minimieren.	Ja	Ist ein Baustein im Rahmen des Risikomanagements und wird von Kunden z.T. gefordert.	x	x	
A.13.1	Netzwerksicherheits-management	Der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen ist sichergestellt.	Ja	Anforderung Sicherheitsrichtlinien, Bestandteil Kerngeschäft	x	x	x
A.13.1.1	Netzwerksteuerungs-maßnahmen	Netzwerke werden verwaltet und gesteuert, um Information in Systemen und Anwendungen zu schützen.	Ja	Ein Betrieb der Netze in heterogenen Umgebungen erfordert klare Regelungen und Sicherheitsmaßnahmen.	x		x
A.13.1.2	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Anforderungen an die Verwaltung aller Netzwerkdienste sind bestimmt und werden sowohl für interne als auch für ausgegliederte Netzwerkdienste in Vereinbarungen aufgenommen.	Ja	Komplexe Netzwerkumgebungen bedürfen zu Betrieb angemessene Sicherheitsregellungen.	x		

A.13.1.3	Trennung in Netzwerken	Informationsdienste, Benutzer und Informationssysteme werden in Netzwerken gruppenweise voneinander getrennt gehalten.	Ja	Zum Schutz der Vertraulichkeit und Integrität der Kundendaten.	x		
A.13.2	Informationsübertragung	Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen Stelle, ist aufrechterhalten.	Ja	Bestandteil Kerngeschäft			x
A.13.2.1	Richtlinien und Verfahren zur Informationsübertragung	Formale Übertragungsrichtlinien, -verfahren und -maßnahmen sind vorhanden, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen.	Ja	Schaffung von Leitlinien und Verfahren zum Austausch von Informationen.	x		
A.13.2.2	Vereinbarungen zur Informationsübertragung	Vereinbarungen behandeln die sichere Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien.	Ja	Zusammenarbeit mit diversen Lieferanten und Partnern, daher erforderlich.		x	
A.13.2.3	Elektronische Nachrichtenübermittlung	Information in der elektronischen Nachrichtenübermittlung ist angemessen geschützt.	Ja	Einhaltung der gesetzlichen Vorgaben für den Versand von geschäftlichen E-Mails.		x	
A.13.2.4	Vertraulichkeits- oder Geheimhaltungsverein-barungen	Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, werden identifiziert, regelmäßig überprüft und sind dokumentiert.	Ja	Umsetzen der Forderungen aus der Sicherheitspolitik und dem Datenschutzgesetzen.		x	
A.14.0	Anschaffung, Entwicklung und Instandhalten von Systemen	Definition von Anforderungen, Maßnahmen und Bedingungen um Systeme bei der Plusnet GmbH qualifiziert auszuwählen, zu entwickeln und sie ständig auf einem sicheren Stand zu halten.	Ja	Bestandteil Kerngeschäft	x		x
A.14.1	Sicherheitsanforderungen an Informationssysteme	Es ist sichergestellt, dass Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen ist. Dies beinhaltet auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze bereitstellen.	Ja	Notwendig zur Risikominimierung im Kerngeschäft der Plusnet	x		
A.14.1.1	Analyse und Spezifikation von Informationssicherheits-anforderungen	Die Anforderungen, die sich auf Informationssicherheit beziehen, sind in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen.	Ja	Hierdurch werden die Lieferanten in die Pflicht genommen, um die Sicherheits- und Verfügbarkeitsstandards zu gewährleisten.	x		
A.14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	Information, die durch Anwendungsdienste über öffentliche Netzwerke übertragen wird, ist vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter Offenlegung sowie Veränderung geschützt.	Ja	IOT, Webplattformen und Selfservices im EInsatz.	x		
A.14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	Information, die an Transaktionen bei Anwendungsdiensten beteiligt ist, ist so geschützt, dass unvollständige Übertragung, Fehlleitung, unbefugte Offenlegung, unbefugte Vervielfältigung oder unbefugte Wiederholung von Nachrichten verhindert ist.	Ja	Z.B. SAP und andere Applikationen	x		
A.14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	Es ist sichergestellt, dass Informationssicherheit im Entwicklungszyklus von Informationssystemen geplant und umgesetzt ist.	Ja	Bestandteil Kerngeschäft			x
A.14.2.1	Richtlinie für sichere Entwicklung	Regeln für die Entwicklung von Software und Systemen sind festgelegt und werden bei Entwicklungen innerhalb der Organisation angewendet.	Ja	Neuentwicklung / Evaluation von Lösungen und Systemen	x		
A.14.2.2	Verfahren zur Verwaltung von Systemänderungen	Änderungen an Systemen innerhalb des Entwicklungszyklus werden durch formale Verfahren zur Verwaltung von Änderungen gesteuert.	Ja	Nachvollziehbarkeit und Risikobetrachtung für die Gewährleistung der SLA's.	x	x	

A.14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	Bei Änderungen an Betriebsplattformen, werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder Organisationssicherheit gibt.	Ja	Sicherstellung der Verfügbarkeit und Korrektheit.	x		
A.14.2.4	Beschränkung von Änderungen an Softwarepaketen	Änderungen an Softwarepaketen werden nicht gefördert, sind auf das Erforderliche beschränkt und alle Änderungen unterliegen einer strikten Steuerung.	Ja	Softwareentwicklung, umfangreiche Patchaktivitäten, Notwendigkeit bspw. Kunden spezif. Frozen Zones zu berücksichtigen, etc	x	x	
A.14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sind festgelegt, dokumentiert, werden aktuell gehalten und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet.	Ja	Neuentwicklung / Evaluation von Lösungen und Systemen	x		
A.14.2.6	Organisationen schaffen sichere Entwicklungs-umgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus und schützen diese angemessen.	Organisationen schaffen sichere Entwicklungs-umgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus und schützen diese angemessen.	Ja	Neuentwicklung / Evaluation von Lösungen und Systemen	x		
A.14.2.7	Ausgegliederte Entwicklung	Die Organisation beaufsichtigt und überwacht die Tätigkeit ausgegliederter Systementwicklung.	Ja	Neuentwicklung / Evaluation von Lösungen und Systemen auch mit Partnern	x		
A.14.2.8	Testen der Systemsicherheit	Die Sicherheitsfunktionalität wird während der Entwicklung getestet.	Ja	Zentrale Softwareentwicklung und Entwicklung von Betriebsskripten	x		
A.14.2.9	Systemabnahmetest	Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt.	Ja	Zentrale Softwareentwicklung und Entwicklung von Betriebsskripten. Auch Abnahme von Änderungen durch DL.	x		
A.14.3	Testdaten	Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.	Ja	Im Rahmen interner Betrieb und Kundenlösungen	x		
A.14.3.1	Schutz von Testdaten	Testdaten werden sorgfältig ausgewählt, geschützt und gesteuert.	Ja	Im Rahmen interner Betrieb und Kundenlösungen	x		
A.15.1	Informationssicherheit in Lieferantenbeziehungen	Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.	Ja	Weitergabe der Kundenanforderungen an Lieferanten vertraglich zugesichert (z.B. BAIT, MaRisk)		x	
A.15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	Die Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation werden mit dem Zulieferer vereinbart und sind dokumentiert.	Ja	Hierdurch soll der Schutz der Unternehmenswerte den gesetzlichen- und Kundenregellungen entsprechend juristisch durchsetzbar geregelt werden.		x	
A.15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	Alle relevanten Informationssicherheitsanforderungen werden mit jedem Lieferanten festgelegt, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt und sind vereinbart.	Ja	Hierdurch soll der Schutz der Unternehmenswerte den gesetzlichen- und Kundenregellungen entsprechend juristisch durchsetzbar geregelt werden.	x	x	
A.15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produkt-lieferkette verbunden sind, werden in Vereinbarungen mit Lieferanten aufgenommen.	Ja	Hierdurch soll der Schutz der Unternehmenswerte den gesetzlichen- und Kundenregellungen entsprechend juristisch durchsetzbar geregelt werden.	x	x	
A.15.2.0	Steuerung der Dienstleistungserbringung von Lieferanten	Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung ist im Einklang mit Lieferantenverträgen aufrechterhalten.	Ja	Weitergabe der Kundenanforderungen an Lieferanten vertraglich zugesichert (z.B. BAIT, MaRisk)		x	

A.15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen	Organisationen überwachen, überprüfen und auditieren die Dienstleistungserbringung durch Lieferanten regelmäßig.	Ja	Rechtliche Absicherung der Anforderungen in den Verträgen mit Dritten.	x	x	
A.15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen	Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten werden gesteuert. Solche Änderungen umfassen auch die Pflege und Verbesserung bestehender Informationssicherheitsrichtlinien, -verfahren und -maßnahmen. Dabei werden die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet.	Ja	Geordnete Fortschreibung der Verträge mit Dritten.		x	
A.16.0	Handhabung von Informationssicherheits-vorfällen	Erst denken dann handeln.	Ja	U.a. Gesetzliche Vorgabe, Kundenanforderung, Management der Informationssicherheit der Plusnet, Risikominimierung bzw. -eindämmung.	x	x	x
A.16.1	Handhabung von Informationssicherheits-vorfällen und Verbesserungen	Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt.	Ja	Standardisierung und Weitergabe an Kunden			x
A.16.1.1	Verantwortlichkeiten und Verfahren	Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.	Ja	Klare Verantwortlichkeiten gewährleisten eine schnelles, zielgerichtetes Vorgehen.			x
A.16.1.2	Meldung von Informationssicherheits-ereignissen	Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet.	Ja	Eine schnelle, zielgerichtete Kommunikation ist Voraussetzung für die Einhaltung der SLA's. Kundenanforderung.	x	x	
A.16.1.3	Meldung von Schwächen in der Informationssicherheit	Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, werden angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu	Ja	Ein schnelles Erkennen ist für den Betriebs unabdingbar. Kundenanforderung.	x	x	
A.16.1.4	Beurteilung von und Entscheidung über Informationssicherheits-ereignisse	Informationssicherheitsereignisse werden beurteilt, und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind.	Ja	Vertragliche Verpflichtung und nach dem IT-Sicherheitsgesetz Vorgabe		x	
A.16.1.5	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert.	Ja	Vertragliche Verpflichtung und nach dem IT-Sicherheitsgesetz Vorgabe		x	
A.16.1.6	Erkenntnisse aus Informationssicherheits-vorfällen	Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse werden dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.	Ja	Eine strukturierte Nachbereitung von Vorfällen hilft die Informationssicherheit der Plusnet sowie die Servicequalität für alle Kunden zu verbessern.	x		
A.16.1.7	Sammeln von Beweismaterial	Die Organisation legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, fest und wendet diese an.	Ja	Aufgrund der Komplexität werden individuelle Vorgehensweisen mit den Kunden vereinbart.		x	
A.17.1	Aufrechterhalten der Informationssicherheit	Die Aufrechterhaltung der Informationssicherheit ist in das Business Continuity Managementsystem der Organisation eingebettet.	Ja	Vertragliche Verpflichtung zum Bestand der ISO27001 während Kundenvetragslaufzeit		x	

A.17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit	Die Organisation bestimmt ihre Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements bei widrigen Situationen, z. B. Krise oder Katastrophe.	Ja	Entwicklung, Einführung und Pflege der Notfallplanung für die Plusnet.		x	
A.17.1.2	Umsetzen der Aufrechterhaltung der Informationssicherheit	Die Organisation legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert, setzt sie um und erhält diese aufrecht, um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können.	Ja	Ein Risikomanagement muß regelmäßig die betrieblichen Risiken erfassen, bewerten und entsprechende Maßnahmen einleiten.	x		
A.17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	Die Organisation überprüft in regelmäßigen Abständen die festgelegten und umgesetzten Maßnahmen zur Aufrechterhaltung der Informationssicherheit, um sicherzustellen dass diese gültig und in widrigen Situationen wirksam sind.	Ja	Pläne zur Sicherstellung des Geschäftsbetriebs müssen regelmäßig überprüft und getestet werden.	x		
A.17.2	Redundanzen	Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sichergestellt.	Ja	In großen Teilen Bestandteil Kundenverträge, Anforderungen laut Vertrag (differieren)		x	
A.17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen werden mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert.	Ja	Vertragliche Verpflichtung und interne Notwendigkeit		x	
A.18.1	Einhaltung gesetzlicher Vorgaben	Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit und gegen jegliche Sicherheitsanforderungen sind vermieden.	Ja	Compliance		x	
A.18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	Alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen der Organisation zur Einhaltung dieser Anforderungen sind für jedes Informationssystem und die Organisation ausdrücklich bestimmt und dokumentiert und werden auf dem neuesten Stand gehalten.	Ja	Voraussetzung für Compliance.		x	
A.18.1.2	Geistige Eigentumsrechte	Es sind angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.	Ja	Vermeidung von Regressansprüchen von Rechteinhabern wie SAP oder MS.		x	
A.18.1.3	Schutz von Aufzeichnungen	Aufzeichnungen sind gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter	Ja	Ist Basis für die Sicherheit des Geschäftsbetriebes.		x	x
A.18.1.4	Privatsphäre und Schutz von personenbezogener Information	Die Privatsphäre und der Schutz von personenbezogener Information sind, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt.	Ja	Um Gesetzen, Vorschriften und Vertragsklauseln gerecht zu werden.		x	
A.18.1.5	Regelungen bezüglich kryptographischer Maßnahmen	Kryptographische Maßnahmen werden unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt.	Ja	Vertragliche Zusicherung gegenüber Kunden, intern muss die Summe implementiert werden. Vorgaben auch seitens DSGVO / TKG		x	
A.18.2	Überprüfungen der Informationssicherheit	Informationssicherheit ist in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und wird entsprechend angewendet.	Ja	Vertragliche Anforderung Kunden und Gesetze		x	

A.18.2.1	Unabhängige Überprüfung der Informationssicherheit	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung (d. h. Maßnahmenziele, Maßnahmen, Richtlinien, Prozesse und Verfahren zur Informationssicherheit) werden auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft.	Ja	Erkennen von Risiken und Schwachstellen.	x		
A.18.2.2	Einhaltung von Sicherheitsrichtlinien und -standards	Leitende Angestellte überprüfen regelmäßig die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstiger Sicherheitsanforderungen bei der Informationsverarbeitung und den Verfahren in ihrem Verantwortungsbereich.	Ja	Grundvoraussetzung für den sicheren IT-Betrieb.			x
A.18.2.3	Überprüfung der Einhaltung von technischen Vorgaben	Informationssysteme werden regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft.	Ja	Hierdurch werden die aktuellen Sicherheitsstandards der System umgesetzt und überwacht.	x		