Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.5.1.1	**Informationssicherheitsrichtlinie:** Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.		ja
A.5.1.2	**Überprüfung der Informationssicherheitsrichtlinien:** Die Informationssicherheitsrichtlinien werden in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.		ja
A.6.1.1	**Informationssicherheitsrollen und -verantwortlichkeiten:** Alle Informationssicherheitsverantwortlichkeiten sind festgelegt und zugeordnet.		ja
A.6.1.2	**Aufgabentrennung:** Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.		ja
A.6.1.3	**Kontakt mit Behörden:** Angemessene Kontakte mit relevanten Behörden werden gepflegt.		ja
A.6.1.4	**Kontakt mit speziellen Interessensgruppen:** Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden werden gepflegt.		ja
A.6.1.5	**Informationssicherheit im Projektmanagement:** Informationssicherheit wird im Projektmanagement berücksichtigt, ungeachtet der Art des Projekts.		ja
A.6.2.1	**Richtlinie zu Mobilgeräten:** Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sind umgesetzt, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.		ja
A.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, sind umgesetzt.		ja
A.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
A.7.1.2	**Beschäftigungs- und Vertragsbedingungen:** In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sind deren Verantwortlichkeiten und diejenigen der Organisation festgelegt.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.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
A.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
A.7.2.3	**Maßregelungsprozess:** Ein formal festgelegter und bekanntgegebener Maßregelungsprozess ist eingerichtet, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.		ja
A.7.3.1	**Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung:** Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sind festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt.		ja
A.8.1.1	**Inventarisierung der Werte:** Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sind erfasst und ein Inventar dieser Werte ist erstellt und wird gepflegt.		ja
A.8.1.2	**Zuständigkeit für Werte:** Für alle Werte, die im Inventar geführt werden, gibt es Zuständige.		ja
A.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, sind aufgestellt, dokumentiert und angewendet.		ja
A.8.1.4	**Rückgabe von Werten:** Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück.		ja
A.8.2.1	**Klassifizierung von Information:** Information ist anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert.		ja
A.8.2.2	**Kennzeichnung von Information:** Ein angemessener Satz von Verfahren zur Kennzeichnung von Information ist entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.		ja
A.8.2.3	**Handhabung von Werten:** Verfahren für die Handhabung von Werten sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt.		ja
A.8.3.1	**Handhabung von Wechseldatenträgern:** Verfahren für die Handhabung von Wechseldatenträgern sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.8.3.2	**Entsorgung von Datenträgern:** Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren entsorgt.		ja
A.8.3.3	**Transport von Datenträgern:** Datenträger, die Information enthalten, sind während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt.		ja
A.9.1.1	**Zugangssteuerungsrichtlinie:** Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.		ja
A.9.1.2	**Zugang zu Netzwerken und Netzwerkdiensten:** Benutzer haben ausschließlich Zugang zu denjenigen Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind.		ja
A.9.2.1	**Registrierung und Deregistrierung von Benutzern:** Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern ist umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.		ja
A.9.2.2	**Zuteilung von Benutzerzugängen:** Ein formaler Prozess zur Zuteilung von Benutzerzugängen ist umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.		ja
A.9.2.3	**Verwaltung privilegierter Zugangsrechte:** Zuteilung und Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird gesteuert.		ja
A.9.2.4	**Verwaltung geheimer Authentisierungsinformation von Benutzern:** Die Zuordnung von geheimer Authentisierungsinformation wird über einen formalen Verwaltungsprozess gesteuert.		ja
A.9.2.5	**Überprüfung von Benutzerzugangsrechten:** Die für Werte Zuständigen überprüfen in regelmäßigen Abständen die Benutzerzugangsrechte.		ja
A.9.2.6	**Entzug oder Anpassung von Zugangsrechten**: Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen werden bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst.		ja
A.9.3.1	**Gebrauch geheimer Authentisierungsinformation:** Benutzer sind verpflichtet, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.		ja
A.9.4.1	**Informationszugangsbeschränkung:** Zugang zu Information und Anwendungssystemfunktionen ist entsprechend der Zugangssteuerungsrichtlinie eingeschränkt.		ja
A.9.4.2	**sichere Anmeldeverfahren:** Soweit es die Zugangssteuerungsrichtlinie erfordert, wird der Zugang zu Systemen und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert.		ja
A.9.4.3	**System zur Verwaltung von Kennwörtern:** Systeme zur Verwaltung von Kennwörtern sind interaktiv und stellen starke Kennwörter sicher.		ja
A.9.4.4	**Gebrauch von Hilfsprogrammen mit privilegierten Rechten:** Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.9.4.5	**Zugangssteuerung für Quellcode von Programmen:** Zugang zu Quellcode von Programmen ist eingeschränkt.		ja
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
A.10.1.2	**Schlüsselverwaltung:** Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln ist entwickelt und wird über deren gesamten Lebenszyklus umgesetzt.		ja
A.11.1.1	**physischer Sicherheitsperimeter:** Zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitsperimeter festgelegt und werden verwendet.		ja
A.11.1.2	**physische Zutrittssteuerung:** Sicherheitsbereiche sind durch eine angemessene Zutrittssteuerung geschützt, um sicherzustellen, dass nur berechtigtes Personal Zugang hat.		ja
A.11.1.3	**Sichern von Büros, Räumen und Einrichtungen:** Die physische Sicherheit für Büros, Räume und Einrichtungen ist konzipiert und wird angewendet.		ja
A.11.1.4	**Schutz vor externen und umweltbedingten Bedrohungen:** Physischer Schutz vor Naturkatastrophen, bösartigen Angriffen oder Unfällen ist konzipiert und wird angewendet.		ja
A.11.1.5	**Arbeiten in Sicherheitsbereichen:** Verfahren für das Arbeiten in Sicherheitsbereichen sind konzipiert und werden angewendet.		ja
A.11.1.6	**Anlieferungs- und Ladebereiche:** Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, werden überwacht und sind, falls möglich, von informationsverarbeitenden Einrichtungen getrennt, um unbefugten Zutritt zu verhindern.		ja
A.11.2.1	**Platzierung und Schutz von Geräten und Betriebsmitteln:** Geräte und Betriebsmittel sind so platziert und geschützt, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind.		ja
A.11.2.2	**Versorgungs- und Entsorgungseinrichtungen:** Geräte und Betriebsmittel sind vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt.		ja
A.11.2.3	**Sicherheit der Verkabelung:** Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung sind vor Unterbrechung, Störung oder Beschädigung geschützt.		ja
A.11.2.4	**Instandhalten von Geräten und Betriebsmitteln:** Geräte und Betriebsmittel werden ordnungsgemäß Instand gehalten, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.11.2.5	**Entfernen von Werten:** Geräte, Betriebsmittel, Information oder Software werden nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt.		ja
A.11.2.6	**Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten:** Werte außerhalb des Standorts werden gesichert, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen.		ja
A.11.2.7	**sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln:** Alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, werden überprüft, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.		ja
A.11.2.8	**unbeaufsichtigte Benutzergeräte:** Benutzer stellen sicher, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind.		ja
A.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 werden angewendet.		ja
A.12.1.1	**Dokumentierte Bedienabläufe:** Die Bedienabläufe sind dokumentiert und allen Benutzern, die sie benötigen, zugänglich.		ja
A.12.1.2	**Änderungssteuerung:** Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen werden gesteuert.		ja
A.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
A.12.1.4	**Trennung von Entwicklungs-, Test- und Betriebsumgebungen:** Entwicklungs-, Test- und Betriebsumgebungen sind voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.		ja
A.12.2.1	**Maßnahmen gegen Schadsoftware:** Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer sind umgesetzt.		ja
A.12.3.1	**Sicherung von Information:** Sicherheitskopien von Information, Software und Systemabbildern werden entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet.		ja
A.12.4.1	**Ereignisprotokollierung:** Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, werden erzeugt, aufbewahrt und regelmäßig überprüft.		ja
A.12.4.2	**Schutz der Protokollinformation:** Protokollierungseinrichtungen und Protokollinformation sind vor Manipulation und unbefugtem Zugriff geschützt.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.12.4.3	**Administratoren- und Bedienerprotokolle:** Tätigkeiten von Systemadministratoren und Systembedienern werden aufgezeichnet und die Protokolle sind geschützt und werden regelmäßig überprüft.		ja
A.12.4.4	**Uhrensynchronisation**: Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder eines Sicherheitsbereichs werden mit einer einzigen Referenzzeitquelle synchronisiert.		ja
A.12.5.1	**Installation von Software auf Systemen im Betrieb:** Verfahren zur Steuerung der Installation von Software auf Systemen im Betrieb sind umgesetzt.		ja
A.12.6.1	**Handhabung von technischen Schwachstellen:** Information über technische Schwachstellen verwendeter Informationssysteme wird rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen wird bewertet und angemessene Maßnahmen werden ergriffen, um das dazugehörige Risiko zu behandeln.		ja
A.12.6.2	**Einschränkung von Softwareinstallation:** Regeln für die Softwareinstallation durch Benutzer sind festgelegt und umgesetzt.		ja
A.12.7.1	**Maßnahmen für Audits von Informationssystemen:** Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhalten, werden sorgfältig geplant und vereinbart, um Störungen der Geschäftsprozesse zu minimieren.		ja
A.13.1.1	**Netzwerksteuerungsmaßnahmen:** Netzwerke werden verwaltet und gesteuert, um Information in Systemen und Anwendungen zu schützen.		ja
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
A.13.1.3	**Trennung in Netzwerken:** Informationsdienste, Benutzer und Informationssysteme in Netzwerken werden gruppenweise voneinander getrennt gehalten.		ja
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
A.13.2.2	**Vereinbarungen zur Informationsübertragung:** Vereinbarungen behandeln die sichere Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien.		ja
A.13.2.3	**elektronische Nachrichtenübermittlung:** Information in der elektronischen Nachrichtenübermittlung ist angemessen geschützt.		ja
A.13.2.4	**Vertraulichkeits- oder Geheimhaltungsvereinbarungen:** Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, werden identifiziert, regelmäßig überprüft und sind dokumentiert.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.14.1.1	**Analyse und Spezifikation von Informationssicherheitsanforderungen:** Die Anforderungen, die sich auf Informationssicherheit beziehen, sind in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen.		ja
A.14.1.2	**Sicherung von Anwendungsdiensten in öffentlichen Netzwerken:** Information, die durch Anwendungsdiensten über öffentliche Netzwerke übertragen wird, ist vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter Offenlegung sowie Veränderung geschützt.		ja
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
A.14.2.1	**Richtlinie für sichere Entwicklung:** Regeln für die Entwicklung von Software und Systemen sind festgelegt und bei Entwicklungen innerhalb der Organisation angewendet.		ja
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
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
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
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
A.14.2.6	**sichere Entwicklungsumgebung:** Organisationen schaffen sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus und schützen diese angemessen.		ja
A.14.2.7	**ausgegliederte Entwicklung:** Die Organisation beaufsichtigt und überwacht die Tätigkeit ausgegliederter Systementwicklung.		ja
A.14.2.8	**Testen der Systemsicherheit:** Die Sicherheitsfunktionalität wird während der Entwicklung getestet.		ja
A.14.2.9	**Systemabnahmetest:** Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt.		ja
A.14.3.1	**Schutz von Testdaten:** Testdaten werden sorgfältig ausgewählt, geschützt und gesteuert.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
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
A.15.1.2	**Behandlung von Sicherheit in Lieferantenvereinbarungen:** Alle relevanten Informationssicherheitsanforderungen werden mit jedem Lieferanten, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt, festgelegt und sind vereinbart.		ja
A.15.1.3	**Lieferkette für Informations- und Kommunikationstechnologie:** Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, werden in Vereinbarungen mit Lieferanten aufgenommen.		ja
A.15.2.1	**Überwachung und Überprüfung von Lieferantendienstleistungen:** Organisationen überwachen, überprüfen und auditieren die Dienstleistungserbringung durch Lieferanten regelmäßig.		ja
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
A.16.1.1	**Verantwortlichkeiten und Verfahren:** Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.		ja
A.16.1.2	**Meldung von Informationssicherheitsereignissen:** Informationssicherheitsereignisse werden so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet.		ja
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 melden.		ja
A.16.1.4	**Beurteilung von und Entscheidung über Informationssicherheitsereignisse:** Informationssicherheitsereignisse werden beurteilt, und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.16.1.5	**Reaktion auf Informationssicherheitsvorfälle:** Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert.		ja
A.16.1.6	**Erkenntnisse aus Informationssicherheitsvorfällen:** Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse werden dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.		ja
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
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
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
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
A.17.2.1	**Verfügbarkeit von informationsverarbeitenden Einrichtungen:** Informationsverarbeitende Einrichtungen werden mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert.		ja
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
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 die Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.		ja

Nr.	Maßnahme (Forderung der Norm)		SOA ja / nein
A.18.1.3	**Schutz von Aufzeichnungen:** Aufzeichnungen sind gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt.		ja
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
A.18.1.5	**Regelungen bezüglich kryptographischer Maßnahmen:** Kryptographische Maßnahmen werden unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt.		ja
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
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
A.18.2.3	**Überprüfung der Einhaltung von technischen Vorgaben:** Informationssysteme werden regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft.		ja