Maßnahme				Bezug
Nummer	Bezeichnung	Beschreibung	Relevanz	Prozess
A.5	**Organisatorische Maßnahmen**			
A.5.1	Informationssicherheitspolitik und -richtlinien	Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.	J	Sicherheits-management
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.	J	Sicherheits-management
A.5.3	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.	J	Sicherheits-management
A.5.4	Verantwortlichkeiten der Leitung	Die Leitung muss vom gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik, und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.	J	Sicherheits-management
A.5.5	Kontakt zu Behörden	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.	J	Sicherheits-management
A.5.6	Kontakt mit speziellen Interessensgruppen	Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.	J	Sicherheits-management
A.5.7	Informationen über die Bedrohungslage	Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.	J	Sicherheits-management
A.5.8	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss in das Projektmanagement integriert werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.9	Inventar der Informationen und anderen damit verbundenen Werte	Ein Inventar der Informationen und anderen damit verbundenen Werte, einschließlich der Eigentümer, muss erstellt und gepflegt werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen damit verbundenen Werten müssen aufgestellt, dokumentiert und angewendet werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.11	Rückgabe von Werten	Das Personal und gegebenenfalls andere interessierte Parteien müssen alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.	J	Entwicklung, Bereitstellung, Betrieb
A.5.12	Klassifizierung von Informationen	Informationen müssen entsprechend den Informationssicherheitserfordernissen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.	J	Sicherheits-management
A.5.13	Kennzeichnung von Informationen	Ein angemessener Satz von Verfahren zur Kennzeichnung von Informationen muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.14	Informationsübermittlung	Für alle Arten von Übermittlungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.	J	Entwicklung, Bereitstellung, Betrieb
A.5.15	Zugangssteuerung	Regeln zur Steuerung des physischen und logischen Zugriffs auf Informationen und andere damit verbundene Werte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.	J	Betrieb
A.5.16	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.	J	Personal, Betrieb
A.5.17	Authentisierungsinformationen	Die Zuweisung und Verwaltung von Authentisierungsinformationen muss durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentisierungsinformationen umfasst.	J	Betrieb
A.5.18	Zugangsrechte	Zugangsrechte zu Informationen und anderen damit verbundenen Werten müssen in Übereinstimmung mit der themenspezifischen Richtlinie und den Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.	J	Betrieb

Maßnahme				Bezug
Nummer	Bezeichnung	Beschreibung	Relevanz	Prozess
A.5.19	Informationssicherheit in Lieferantenbeziehungen	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.	J	Entwicklung, Bereitstellung, Betrieb
A.5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Je nach Art der Lieferantenbeziehung müssen die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.21	Umgang mit der Informations- sicherheit in der Lieferkette der Informations- und Kommunika- tionstechnologie (IKT)	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.	J	Entwicklung, Bereitstellung, Betrieb
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Die Organisation muss regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.	J	Entwicklung, Bereitstellung, Betrieb
A.5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten müssen in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.24	Planung und Vorbereitung der Handhabung von Informations- sicherheitsvorfällen	Die Organisation muss die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.	J	Sicherheits- management
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Die Organisation muss Informationssicherheitsereignisse beurteilen und entscheiden, ob sie als Informationssicherheitsvorfälle eingestuft werden müssen.	J	Entwicklung, Bereitstellung, Betrieb
A.5.26	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.	J	Entwicklung, Bereitstellung, Betrieb
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse müssen zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.	J	Sicherheits- management
A.5.28	Sammeln von Beweismaterial	Die Organisation muss Verfahren für die Ermittlung, Sammlung, Beschaffung und Aufbewahrung von Beweismaterial im Zusammenhang mit Informationssicherheitsereignissen einführen und umsetzen.	J	Entwicklung, Bereitstellung, Betrieb
A.5.29	Informationssicherheit bei Störungen	Die Organisation muss planen, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau gehalten werden kann.	J	Entwicklung, Betrieb
A.5.30	IKT-Bereitschaft für Business- Continuity	Die IKT-Bereitschaft muss auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.	J	Compliance, Entwicklung, Bereitstellung, Betrieb
A.5.31	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen müssen ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.	J	Compliance
A.5.32	Geistige Eigentumsrechte	Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.	J	Compliance
A.5.33	Schutz von Aufzeichnungen	Aufzeichnungen müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.	J	Sicherheits- management
A.5.34	Datenschutz und Schutz von personenbezogenen Daten(PbD)	Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.	J	Compliance
A.5.35	Unabhängige Überprüfung der Informationssicherheit	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien müssen auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.	J	Compliance
A.5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Die Einhaltung der Informationssicherheitspolitik der Organisation und ihrer themenspezifischen Richtlinien, Regeln und Normen muss regelmäßig überprüft werden.	J	Compliance
A.5.37	Dokumentierte Betriebsabläufe	Die Betriebsverfahren für Informationsverarbeitungsanlagen müssen dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.	J	Bereitstellung, Betrieb

Maßnahme				Bezug
Nummer	Bezeichnung	Beschreibung	Relevanz	Prozess
A.6	**Personenbezogene Maßnahmen**			
A.6.1	Sicherheitsüberprüfung	Alle Personen, die in die Belegschaft aufgenommen werden, müssen vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und diese Überprüfung muss in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Informationen und den wahrgenommenen Risiken stehen.	J	Personal
A.6.2	Beschäftigungs- und Vertragsbedingungen	In den arbeitsvertraglichen Vereinbarungen müssen die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.	J	Personal
A.6.3	Informationssicherheits- bewusstsein, -ausbildung und -schulung	Das Personal der Organisation und relevante interessierte Parteien müssen ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet relevant sind.	J	Personal
A.6.4	Maßregelungsprozess	Ein Maßregelungsprozess muss formalisiert und kommuniziert werden, um Schritte gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.	J	Personal
A.6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung von Beschäftigungsverhältnissen bestehen bleiben, müssen festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.	J	Personal
A.6.6	Vertraulichkeits- oder Geheim-haltungsvereinbarungen	Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche den Bedarf der Organisation am Schutz von Informationen widerspiegeln, müssen identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.	J	Personal, Betrieb
A.6.7	Remote-Arbeit	Es müssen Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter aus der Ferne arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.	J	Betrieb
A.6.8	Meldung von Informationssicherheitsereignissen	Die Organisation muss einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Informationssicherheitsereignisse über geeignete Kanäle rechtzeitig zu melden.	J	Sicherheits-management
A.7	**Physische Maßnahmen**			
A.7.1	Physische Sicherheitsperimeter	Zum Schutz von Bereichen, in denen sich Informationen und andere damit verbundene Werte befinden, müssen Sicherheitsperimeter festgelegt und verwendet werden.	J	Betrieb
A.7.2	Physischer Zutritt	Sicherheitsbereiche müssen durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.	J	Betrieb
A.7.3	Sichern von Büros, Räumen und Einrichtungen	Die physische Sicherheit von Büros, Räumen und Einrichtungen muss konzipiert und umgesetzt werden.	J	Betrieb
A.7.4	Physische Sicherheitsüberwachung	Die Räumlichkeiten müssen ständig auf unbefugten physischen Zugang überwacht werden.		Betrieb
A.7.5	Schutz vor physischen und umweltbedingten Bedrohungen	Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur muss geplant und umgesetzt werden.	J	Betrieb
A.7.6	Arbeiten in Sicherheitsbereichen	Es müssen Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.	J	Betrieb
A.7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Es müssen klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.	J	Betrieb
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen sicher und geschützt aufgestellt werden.	J	Betrieb
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Werte außerhalb des Standorts müssen geschützt werden.	J	Betrieb
A.7.10	Speichermedien	Speichermedien müssen während ihres gesamten Lebenszyklus– Erwerb, Verwendung, Transport und Entsorgung– in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.	J	Betrieb

Maßnahme				Bezug
Nummer	Bezeichnung	Beschreibung	Relevanz	Prozess
A.7.11	Versorgungseinrichtungen	Informationsverarbeitungseinrichtungen müssen vor Stromausfällen und anderen Störungen, die durch Ausfälle von unterstützenden Versorgungseinrichtungen verursacht werden, geschützt werden.	J	Betrieb
A.7.12	Sicherheit der Verkabelung	Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Abhören, Störung oder Beschädigung geschützt werden.	J	Betrieb
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.	J	Betrieb
A.7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, müssen überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.	J	Betrieb
A.8	**Technologische Maßnahmen**			
A.8.1	Endpunktgeräte des Benutzers	Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.	J	Betrieb
A.8.2	Privilegierte Zugangsrechte	Zuteilung und Gebrauch von privilegierten Zugangsrechten müssen eingeschränkt und verwaltet werden.	J	Betrieb
A.8.3	Informationszugangsbeschränkung	Der Zugang zu Informationen und anderen damit verbundenen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.	J	Betrieb
A.8.4	Zugriff auf den Quellcode	Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken müssen angemessen verwaltet werden.	J	Entwicklung
A.8.5	Sichere Authentisierung	Sichere Authentisierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.	J	Entwicklung, Betrieb
A.8.6	Kapazitätssteuerung	Die Nutzung von Ressourcen muss überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.7	Schutz gegen Schadsoftware	Schutz gegen Schadsoftware muss umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.	J	Betrieb
A.8.8	Handhabung von technischen Schwachstellen	Es müssen Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.9	Konfigurationsmanagement	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.10	Löschung von Informationen	Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, müssen gelöscht werden, wenn sie nicht mehr benötigt werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.11	Datenmaskierung	Die Datenmaskierung muss in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.12	Verhinderung von Datenlecks	Maßnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übermitteln.	J	Entwicklung, Betrieb
A.8.13	Sicherung von Informationen	Sicherungskopien von Informationen, Software und Systemen müssen in Übereinstimmung mit der vereinbarten themenspezifischen Richtlinie zu Datensicherungen aufbewahrt und regelmäßig geprüft werden.	J	Betrieb
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen realisiert werden.	J	Entwicklung, Betrieb
A.8.15	Protokollierung	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.	J	Entwicklung, Bereitstellung, Betrieb

Maßnahme				Bezug
Nummer	Bezeichnung	Beschreibung	Relevanz	Prozess
A.8.16	Überwachung von Aktivitäten	Netzwerke, Systeme und Anwendungen müssen auf anormales Verhalten überwacht und geeignete Maßnahmen müssen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.	J	Entwicklung, Betrieb
A.8.17	Uhrensynchronisation	Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit zugelassenen Zeitquellen synchronisiert werden.	J	Betrieb
A.8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmaßnahmen zu umgehen, muss eingeschränkt und streng überwacht werden.	J	Bereitstellung, Betrieb
A.8.19	Installation von Software auf Systemen im Betrieb	Es müssen Verfahren und Maßnahmen umgesetzt werden, um die Installation von Software auf in Betrieb befindlichen Systemen sicher zu verwalten.	J	Bereitstellung, Betrieb
A.8.20	Netzwerksicherheit	Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.	J	Entwicklung, Betrieb
A.8.21	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste müssen ermittelt, umgesetzt und überwacht werden.	J	Entwicklung, Betrieb
A.8.22	Trennung von Netzwerken	Informationsdienste, Benutzer und Informationssysteme müssen in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.	J	Entwicklung, Betrieb
A.8.23	Webfilterung	Der Zugang zu externen Websites muss verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.	J	Betrieb
A.8.24	Verwendung von Kryptographie	Es müssen Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.	J	Entwicklung, Betrieb
A.8.25	Lebenszyklus einer sicheren Entwicklung	Regeln für die sichere Entwicklung von Software und Systemen müssen festgelegt und angewendet werden.	J	Entwicklung
A.8.26	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit sollten bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.	J	Entwicklung
A.8.27	Sichere Systemarchitektur und Entwicklungsgrundsätze	Grundsätze für die Entwicklung sicherer Systeme müssen festgelegt, dokumentiert, aufrechterhalten und bei allen Aktivitäten der Informationssystemsentwicklung angewendet werden.	J	Entwicklung
A.8.28	Sichere Codierung	Bei der Softwareentwicklung müssen die Grundsätze der sicheren Codierung angewandt werden.	J	Entwicklung
A.8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	Sicherheitsprüfverfahren müssen definiert und in den Entwicklungslebenszyklus integriert werden.	J	Entwicklung, Bereitstellung
A.8.30	Ausgegliederte Entwicklung	Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgegliederten Systementwicklung leiten, überwachen und überprüfen.	J	Entwicklung, Betrieb
A.8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Entwicklungs-, Test- und Produktionsumgebungen müssen getrennt und gesichert werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.32	Änderungssteuerung	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.	J	Bereitstellung, Betrieb
A.8.33	Testdaten	Die Testdaten müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.	J	Entwicklung, Bereitstellung, Betrieb
A.8.34	Schutz der Informationssysteme während Tests im Rahmen von Audits	Tests im Rahmen von Audits und andere Sicherheitstätigkeiten, die eine Beurteilung der in Betrieb befindlichen Systeme beinhalten, sollten zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.	J	Sicherheits-management