Anforderu	Bezeichnung	Normtext	Anwendb	Begründung E	Umsetzungsnachweis
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.	Ja	V, B, R	iteratec hat eine umfassende Informationssicherheitsleitlinie etabliert, die von der Geschäftsführung verabschiedet und kommuniziert wurde. Die Leitlinie definiert Ziele, Grundsätze und Verantwortlichkeiten für die Informationssicherheit. Ergänzend existieren 25+ spezifische Richtlinien zu Themen wie Zugriffskontrolle, Incident Management, Risikomanagement und Informationsklassifizierung. Alle Dokumente werden jährlich überprüft und bei Bedarf aktualisiert. Die Kommunikation erfolgt über das Confluence-ISMS-Portal mit Versionierung und Freigabeworkflow. Mitarbeiter werden beim Onboarding und durch regelmäßige Awareness-Maßnahmen über die Richtlinien informiert.
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.	Ja	B, R	iteratec hat klare Rollen und Verantwortlichkeiten für die Informationssicherheit definiert. Das ISMS-Team besteht aus dem Informationssicherheitsbeauftragten (ISB), dem Datenschutzbeauftragten (DSB) und weiteren Security und Compliance Spezialisten. Die Geschäftsführung trägt die Gesamtverantwortung und nimmt diese durch jährliche Managementbewertungen wahr. Fachbereichsverantwortliche (z.B. IT-Infrastruktur, Personal, Projektmanagement) sind für die Umsetzung in ihren Bereichen zuständig. Alle Rollen sind in der Informationssicherheitsleitlinie dokumentiert und werden bei Änderungen aktualisiert. Die Verantwortlichkeiten sind im Confluence-ISMS-Portal transparent dargestellt.
A.5.3	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.	Ja	G, B, R	iteratec hat Prinzipien zur Aufgabentrennung etabliert, um Interessenkonflikte und Missbrauch zu vermeiden. In der IT-Infrastruktur sind Entwicklungs-, Test- und Produktionsumgebungen getrennt. Administrative Rechte werden nach dem Need-to-know-Prinzip vergeben und regelmäßig überprüft. Kritische Prozesse wie Freigaben von Richtlinien erfordern Vier-Augen-Prinzip. In Projekten werden Rollen wie Entwickler, Tester und Reviewer getrennt. Die Berechtigungsvergabe erfolgt über definierte Gruppen mit dokumentierten Verantwortlichkeiten. Kompensationsmaßnahmen wie verstärkte Überwachung werden bei unvermeidbaren Rollenkonflikten
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.	Ja	B, R	iteratec hat die Verantwortlichkeiten der Geschäftsführung für die Informationssicherheit klar definiert. Die Geschäftsführung verabschiedet die Informationssicherheitsleitlinie und stellt erforderliche Ressourcen bereit. Jährlich findet eine Managementbewertung statt, in der KPIs, Audit-Ergebnisse, Vorfälle und Verbesserungspotenziale bewertet werden. Die Geschäftsführung fördert die Sicherheitskultur durch Kommunikation und Vorbildfunktion. Strategische Entscheidungen zu Sicherheitsinvestitionen und Risikoakzeptanz werden auf Leitungsebene getroffen. Die Dokumentation erfolgt in Protokollen der Managementbewertung mit nachverfolgbaren Maßnahmen.
A.5.5	Kontakt mit Behörden	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.	Ja	G, B, R	iteratec hat Prozesse für den Kontakt mit relevanten Behörden etabliert. Kontakte zu Datenschutzaufsichtsbehörden werden durch den Datenschutzbeauftragten gepflegt. Bei meldepflichtigen Datenschutzvorfällen erfolgt die Meldung gemäß DSGVO-Vorgaben innerhalb von 72 Stunden. Für IT-Sicherheitsvorfälle bestehen Kontakte zum BSI und CERT-Bund. Die Kontaktdaten sind im Notfallhandbuch dokumentiert und werden jährlich aktualisiert. Bei Bedarf werden auch Strafverfolgungsbehörden eingebunden. Die Verantwortlichkeiten für Behördenkontakte sind in der Incident-Management-Richtlinie geregelt.
A.5.6	Kontakt mit speziellen Interessensgruppen	Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.	Ja	B, R	iteratec pflegt Kontakte zu relevanten Interessensgruppen im Bereich Informationssicherheit. Dazu gehören Branchenverbände, Security-Communities und Fachforen. Der Austausch erfolgt über Konferenzen, Webinare und Online-Plattformen. iteratec nutzt Threat-Intelligence-Feeds und Security-Mailinglisten, um über aktuelle Bedrohungen informiert zu bleiben. Mitarbeiter nehmen an Fachveranstaltungen teil und bringen Erkenntnisse ins Unternehmen ein. Die Kontakte werden genutzt, um Best Practices zu teilen und von Erfahrungen anderer zu lernen. Relevante Informationen werden im ISMS-Team ausgewertet und bei Bedarf in Maßnahmen überführt.
A.5.7	Informationen über die Bedrohungslage	Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.	Ja	B, R	iteratec hat einen systematischen Prozess zur Erfassung und Bewertung von Bedrohungsinformationen etabliert. Threat-Intelligence-Feeds, BSI-Warnmeldungen und Vendor-Security-Advisories werden kontinuierlich überwacht. Das IT-Security-Team bewertet eingehende Informationen auf Relevanz und leitet bei Bedarf Maßnahmen ein. Schwachstellen-Scans und Penetrationstests liefern zusätzliche Erkenntnisse über potenzielle Bedrohungen. Informationen werden im Risikomanagement-Tool HitGuard dokumentiert und mit bestehenden Risiken abgeglichen. Regelmäßig erfolgt eine Auswertung der Bedrohungslage im ISMS-Team. Erkenntnisse fließen in die Sicherheitsmaßnahmen ein.

A.5.8	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss in das Projektmanagement integriert werden.	Ja	V, B, R	iteratec hat Informationssicherheit systematisch in das Projektmanagement integriert. Zu Projektbeginn erfolgt eine Kritikalitätsbewertung, die den Sicherheitsbedarf bestimmt. Sicherheitsanforderungen werden in Projektverträgen verankert und in der Planung berücksichtigt. Für kritische Projekte werden Bedrohungsanalysen und ggf. Pentests durchgeführt. Die Richtlinie "Sichere Software-Entwicklung" definiert Maßnahmen für Entwicklungsprojekte. Projektleiter werden zu Sicherheitsthemen geschult. Die Einhaltung wird durch Stichproben-Audits überprüft. Zugeordnete Maßnahmen und Kontrollen: - M_012 Verbesserung der Verankerung Security in den Projekten - M_044 ABW #2 Abweichung Sichere SW Entwicklung in Projekten - M_045 OFI #4 Sicherheit im Produkt
A.5.9	Inventar der Informationen und anderen damit verbundenen Werten	Ein Inventar der Informationen und anderen damit verbundenen Werte, einschließlich der Eigentümer, muss erstellt und gepflegt werden.	Ja	B, R	iteratec führt ein strukturiertes Inventar aller informationssicherheitsrelevanten Assets. Hardware-Assets (Server, Clients, Netzwerkkomponenten) werden im IT-Asset-Management-System erfasst. Software-Lizenzen und Anwendungen sind dokumentiert. Informationsassets werden nach der Informationsklassifizierung (Public, Internal, Confidential, Strictly Confidential) kategorisiert. Für jedes Asset sind Verantwortliche (Owner) benannt. Das Inventar wird bei Änderungen aktualisiert und jährlich vollständig überprüft. Kritische Assets werden im Risikomanagement besonders berücksichtigt. Die Dokumentation erfolgt in verschiedenen Systemen (Inventory360, Confluence, HitGuard) mit klaren Zuständigkeiten. Zugeordnete Maßnahmen und Kontrollen: - M_013 Initiale Befüllung der Assets in HitGuard - M_037 ABW #1 Abweichung Assetmanagement - M_049 OFI #8 Dokumentation der Verortung von Kundendaten in den Primary Assets - M_050 OFI #9 Überlegung zur Nachvollziehbarkeit der Bildung von Assetgruppen - M_051 OFI #10 Sicherstellen von Synchronität zwischen Risikotabelle und Confluence - M_052 OFI #11 Vereinfachung des Assetmanagement - M_053 OFI #12 Bewertung der Nützlichkeit von eigenen Assetgruppen für IOTs
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.	Ja	B, R	iteratec hat klare Regelungen zum zulässigen Gebrauch von Informationen und Assets definiert. Die Benutzerrichtlinien legen fest, wie Mitarbeiter mit Unternehmensinformationen, IT-Systemen und Geräten umgehen müssen. Die Informationsklassifizierung definiert Schutzanforderungen je Klassifizierungsstufe. Regelungen zur privaten Nutzung (COPE, BYOD) sind dokumentiert. Die Richtlinie "Externe Datenträger" regelt den Umgang mit USB-Sticks und mobilen Speichermedien. Mitarbeiter werden beim Onboarding über die Regelungen informiert und bestätigen die Kenntnisnahme. Verstöße werden im Incident-Management behandelt. Die Einhaltung wird durch technische Kontrollen (Endpoint-Management) und Stichproben überwacht. Zugeordnete Maßnahmen und Kontrollen: - M_089 25-29948:9 - Tomcat Shutdown Port Not Secured
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.	Ja	B, R	iteratec hat einen strukturierten Offboarding-Prozess etabliert, der die Rückgabe aller firmeneigenen Werte sicherstellt. Die Benutzerrichtlinien verpflichten Mitarbeiter zur Rückgabe von Schlüsseln, IT-Geräten, Zugangskarten und anderen Unternehmenswerten bei Beendigung oder Änderung des Beschäftigungsverhältnisses. Der Personalmanagement-Prozess sieht eine Checkliste für reguläre Beendigungen vor, die den Einzug aller Assets dokumentiert. Die IT-Infrastruktur deaktiviert Zugänge zeitnah und zieht Geräte ein. Externe Mitarbeiter und Dienstleister unterliegen denselben Regelungen. Die Vollständigkeit der Rückgabe wird dokumentiert und im HR-System nachgehalten.

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.	Ja	B, R	iteratec hat eine umfassende Informationsklassifizierungsrichtlinie etabliert, die vier Vertraulichkeitsstufen definiert: offen, intern, vertraulich und geheim. Die Klassifizierung basiert auf Vertraulichkeit, Integrität und Verfügbarkeit sowie Schadenspotenzialen. Für jede Stufe sind klare Regeln für Kennzeichnung, Weitergabe, Speicherung, Übertragung und Entsorgung festgelegt. Die Richtlinie verknüpft Klassifizierungsstufen mit konkreten Schutzmaßnahmen und definiert Verantwortlichkeiten für die Klassifizierung. Mitarbeiter werden beim Onboarding und durch Awareness-Maßnahmen über die Klassifizierung informiert. Use Cases illustrieren die praktische Anwendung für verschiedene Informationstypen. Zugeordnete Maßnahmen und Kontrollen: - M_109 [OFI-14] [A5.12/A5.13] - Klassifizierung nach Integrität und Verfügbarkeit
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.	Ja	B, R	iteratec hat Verfahren zur Kennzeichnung von Informationen entsprechend dem Klassifizierungsschema implementiert. Die Informationsklassifizierungsrichtlinie fordert eine Kennzeichnung ab der Stufe "vertraulich" und außerhalb des Intranets auch für "intern". Die Richtlinie beschreibt detailliert, wie die Kennzeichnung auszusehen hat und wer dafür verantwortlich ist. Mitarbeiter werden geschult, Informationen korrekt zu kennzeichnen. Die Einhaltung wird durch Stichproben und Awareness-Kampagnen gefördert. Zugeordnete Maßnahmen und Kontrollen: - M_108 [OFI-15] [A5.13/A5.23] - Klassifizierung SaaS-Systeme - M_109 [OFI-14] [A5.12/A5.13] - Klassifizierung nach Integrität und Verfügbarkeit
A.5.14	Informationsübertragung	Für alle Arten von Übermittlungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.	Ja	R	iteratec hat klare Regeln für die Informationsübertragung in der Klassifizierungsrichtlinie und den Benutzerrichtlinien definiert. Je nach Klassifizierung sind unterschiedliche Schutzmaßnahmen vorgeschrieben. Die Nutzung sicherer interner Systeme wie OneDrive und SharePoint wird empfohlen. Für externe Übertragungen sind verschlüsselte Kanäle verpflichtend. Die Benutzerrichtlinien regeln den Umgang mit E-Mail-Versand, Cloud-Diensten und externen Datenträgern. Mitarbeiter werden über sichere Übertragungsmethoden informiert und geschult. Zugeordnete Maßnahmen und Kontrollen: - M_093 25-29948:13 - User Enumeration via Default Role Endpoint
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.	Ja	B, R	iteratec hat eine umfassende Zugriffskontrollrichtlinie etabliert, die physischen und logischen Zugriff auf Informationen und Assets regelt. Die Richtlinie basiert auf einem zweistufigen Prozess (Identifikation & Autorisierung) und einem Rollen-Rechte-Konzept. Die Verwaltung erfolgt primär über Gruppen im Active Directory und Azure AD. Prozesse für Einrichtung, Änderung und Entzug von Rechten sind definiert und folgen dem Need-to-Know-Prinzip. Jährliche Überprüfungen der AD-Gruppen stellen die Aktualität sicher. Physischer Zugang wird über Zutrittskontrollsysteme und Zonenpläne geregelt. Die Verantwortlichkeiten sind über RACI-Matrizen klar zugewiesen. Zugeordnete Maßnahmen und Kontrollen: - M_014 OFI #15 Überprüfung von BYOD-Risiko und -Maßnahmen - M_087 25-29948:7 - Stored Cross-Site Scripting (XSS) Mail - M_097 25-29948:1 - Same Default Password over Multiple Tenants - M_107 [OFI-16] [A5.15/A5.23] - Rezertifizierung SaaS-Systeme
A.5.16	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten muss verwaltet werden.	Ja	B, R	iteratec hat den gesamten Lebenszyklus von Identitäten in der Zugriffskontrollrichtlinie klar definiert. Identitäten werden zentral im Active Directory und Azure AD verwaltet. Der Lebenszyklus (Erstellung, Änderung, Löschung) ist an den HR-Prozess gekoppelt und wird automatisiert. Bei Eintritt werden Identitäten basierend auf der Rolle erstellt, bei Änderungen angepasst und bei Austritt zeitnah deaktiviert und später gelöscht. Der Personalmanagement-Prozess definiert die Schnittstellen zwischen HR und IT. Für externe Mitarbeiter und Dienstleister gelten spezielle Regelungen mit zeitlich begrenzten Identitäten. Die Verwaltung erfolgt zentral durch die IT-Infrastruktur.

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.	Ja	V, B, R	iteratec hat eine dedizierte Passwortrichtlinie sowie klare Regeln zum Umgang mit Authentisierungsinformationen etabliert. Die Verwendung eines Passwort-Managers ist verpflichtend. Anforderungen an Passwortkomplexität und -länge sind definiert. Multi-Faktor-Authentifizierung (MFA) wird gefordert, wo technisch möglich, und ist für administrative Zugänge verpflichtend. Die Benutzerrichtlinien enthalten detaillierte Regeln zum Umgang mit Passwörtern, API-Keys und anderen Authentisierungsinformationen. Mitarbeiter werden beim Onboarding und durch regelmäßige Awareness-Maßnahmen über sichere Authentifizierung informiert. Die Zugriffskontrollrichtlinie regelt die Verwaltung von Authentisierungsinformationen. Zugeordnete Maßnahmen und Kontrollen: - M_082 25-29948:2 - Vulnerable Dependencies - M_083 25-29948:3 - Broken Access Control on Database Configuration - M_084 25-29948:4 - Multiple Known Vulnerabilities in Tomcat - M_097 25-29948:1 - Same Default Password over Multiple Tenants
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.	Ja	B, R	iteratec hat einen detaillierten Prozess zur Verwaltung von Zugriffsrechten in der Zugriffskontrollrichtlinie implementiert. Der Prozess folgt dem Need-to-Know-Prinzip und basiert auf einem Rollen-Rechte-Konzept. Die Vergabe, Änderung und der Entzug von Rechten sind geregelt und werden über definierte Workflows abgewickelt. Eine jährliche Überprüfung der Zugriffsrechte durch die Verantwortlichen ist vorgeschrieben und wird über eine Kontrolle sichergestellt. Die Berechtigungsvergabe erfolgt über Gruppen mit dokumentierten Verantwortlichkeiten (Group Owner). Änderungen werden nachvollziehbar dokumentiert. Die Einhaltung wird durch regelmäßige AD-Gruppenprüfungen und Audits überwacht. Zugeordnete Maßnahmen und Kontrollen: - M_082 25-29948:2 - Vulnerable Dependencies - K_002 Überprüfung von Benutzerzugangsrechten - K_023 Überprüfung von Benutzerzugangsrechten in EntraID
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.	Ja	B, R	iteratec hat eine umfassende Lieferantenmanagement-Richtlinie etabliert, die einen systematischen Prozess zur Qualifizierung, Bewertung und Überwachung von Lieferanten definiert. Der Prozess basiert auf einer Kritikalitätsbewertung (gering, mittel, hoch, kritisch), die den Umfang der Sicherheitsanforderungen bestimmt. Vor der Beauftragung erfolgt eine Selbstauskunft mit Prüfung durch ISB und DSB. Anforderungen an die Informationssicherheit werden je nach Kritikalität in Verträge aufgenommen (NDAs, AVVs, Vertraulichkeitsvereinbarungen). Die Lieferantenbewertung wird in einer Excel-Datei dokumentiert und durch eine Kontrolle im GRC-Tool HitGuard jährlich überprüft. Zugeordnete Maßnahmen und Kontrollen: - M_015 Verbesserung der Lieferantenprüfung - K_038 Prüfung der Lieferantenliste
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.	Ja	B, R	iteratec integriert Informationssicherheitsanforderungen systematisch in Lieferantenvereinbarungen. Die Lieferantenmanagement-Richtlinie definiert Kritikalitätsstufen und zugehörige Sicherheitsanforderungen, die vertraglich vereinbart werden. Der Prozess zur Festlegung und vertraglichen Vereinbarung ist dokumentiert und wird angewendet. Eine RACI-Matrix definiert Verantwortlichkeiten. Vorgaben für NDAs, AVVs (DSGVO Art. 28) und Vertraulichkeitsvereinbarungen sind je nach Kritikalität festgelegt. Der Selbstauskunftsprozess vor Bestellung neuer IT-Systeme stellt die Prüfung durch DSB und ISB sicher. Dokumentierte Lieferantenbewertungen mit Kritikalitätseinstufung sind in der Excel-Datei vorhanden.
A.5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	Es müssen Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.	Ja	B, R	iteratec hat Prozesse zur Sicherstellung der Informationssicherheit in der IKT-Lieferkette etabliert. Die Richtlinie "Lieferantenmanagement" definiert Anforderungen an Lieferanten und deren Bewertung. Vor der Aufnahme neuer Lieferanten erfolgt eine Sicherheitsbewertung anhand definierter Kriterien.

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.	Ja	B, R	iteratec überwacht und überprüft Lieferantendienstleistungen regelmäßig. Eine entsprechende Kontrolle zur Überwachung und Überprüfung von Lieferantendienstleistungen ist im HitGuard GRC-Tool dokumentiert. Kritische Lieferanten werden jährlich neu bewertet. Änderungen an Lieferantendienstleistungen werden über das Change-Management-Verfahren gesteuert. Die Überwachung umfasst SLA-Compliance, Sicherheitsvorfälle und Zertifizierungsstatus. Zugeordnete Maßnahmen und Kontrollen: - K_014 Überwachung und Überprüfung von Lieferantendienstleistungen
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.	Ja	B, R	iteratec nutzt Cloud-Dienste unter Berücksichtigung von Informationssicherheitsanforderungen. Cloud-Dienste werden vor der Nutzung bewertet und freigegeben. Die Authentifizierung erfolgt i.A über SSO mit MFA. Datenklassifizierung bestimmt die zulässige Cloud-Nutzung. Zugeordnete Maßnahmen und Kontrollen: - M_016 Konzept für den Ausstieg aus Cloud-Diensten - M_107 [OFI-16] [A5.15/A5.23] - Rezertifizierung SaaS-Systeme - M_108 [OFI-15] [A5.13/A5.23] - Klassifizierung SaaS-Systeme
A.5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	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.	Ja	B, R	iteratec hat ein strukturiertes Incident-Management etabliert. Eine Richtlinie definiert Prozesse zur Handhabung von Sicherheitsvorfällen. Das Security Team ist für die Vorfallbearbeitung verantwortlich. Rollen und Verantwortlichkeiten sind in der Informationssicherheitsleitlinie definiert. Eskalationswege und Kontakte sind dokumentiert. Mitarbeiter werden über das Vorgehen bei Sicherheitsvorfällen geschult. Notfallpläne für verschiedene Szenarien sind vorhanden.
A.5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Die Organisation muss Informationssicherheitsereignisse beurteilen und entscheiden, ob sie als Informationssicherheitsvorfälle eingestuft werden müssen.	Ja	B, R	iteratec bewertet Sicherheitsereignisse systematisch. Eine Richtlinie definiert Kriterien zur Bewertung und Klassifizierung von Ereignissen. Ereignisse werden nach Schweregrad (Critical, High, Medium, Low) priorisiert. Das Security Team entscheidet über die weitere Behandlung basierend auf Auswirkung und Dringlichkeit. Die Bewertung umfasst Betroffenheit, Schadensausmaß und Eskalationsbedarf. Alle Ereignisse werden im Ticketsystem dokumentiert.
A.5.26	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.	Ja	B, R	iteratec reagiert strukturiert auf Sicherheitsvorfälle. Eine Richtlinie definiert Reaktionsprozesse für verschiedene Vorfalltypen. Das Security Team koordiniert die Vorfallbearbeitung und leitet Sofortmaßnahmen ein. Dokumentierte Verfahren existieren für häufige Szenarien (Phishing, Datenverlust, unberechtigter Zutritt). Die Reaktion umfasst Eindämmung, Analyse, Behebung und Wiederherstellung. Betroffene Stakeholder werden informiert. Alle Vorfälle werden dokumentiert und nachverfolgt. Zugeordnete Maßnahmen und Kontrollen: - M_042 Security Event Management (SIEM / SOD)
A.5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse müssen zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.	Ja	B, R	iteratec nutzt Sicherheitsvorfälle zur kontinuierlichen Verbesserung. Nach Abschluss von Vorfällen erfolgt eine Post-Mortem-Analyse zur Identifikation von Verbesserungspotenzialen. Erkenntnisse werden dokumentiert und im Security Team besprochen. Aus Vorfällen abgeleitete Maßnahmen werden erfasst und nachverfolgt. Trends und wiederkehrende Probleme werden analysiert. Lessons Learned fließen in Schulungen und Prozessverbesserungen ein.
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.	Ja	G, B, R	iteratec hat Verfahren zur Beweissicherung etabliert. Eine Richtlinie definiert Prozesse zur forensisch korrekten Sicherung von Beweismaterial. Bei schwerwiegenden Vorfällen erfolgt die Beweissicherung unter Wahrung der Chain of Custody. Logs und Systemzustände werden gesichert. Die IT-Infrastruktur verfügt über umfassende Logging-Mechanismen. Beweismaterial wird geschützt aufbewahrt.
A.5.29	Informationssicherheit bei Störungen	Die Organisation muss planen, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau gehalten werden kann.	Ja	B, R	iteratec stellt Informationssicherheit auch bei Störungen sicher. Eine Richtlinie integriert Sicherheitsanforderungen in die Notfallplanung. Notfallszenarien berücksichtigen Sicherheitsaspekte. Bei Störungen bleiben Zugangskontrollen und Protokollierung aktiv. Notfallprozeduren sind dokumentiert und getestet. Die Wiederherstellung erfolgt unter Berücksichtigung von Sicherheitsanforderungen. Das BCM ist mit dem ISMS verzahnt.

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.	Ja	B, R	iteratec hat IKT-Bereitschaft für Business Continuity etabliert. Eine Richtlinie definiert Anforderungen an die IKT-Verfügbarkeit. Eine Business Impact Analysis (BIA) identifiziert kritische Geschäftsprozesse und deren IKT-Abhängigkeiten. Für kritische Systeme existieren Redundanzen und Backup-Strategien. Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) sind definiert. Wiederherstellungspläne werden regelmäßig getestet. Die Backup-Richtlinie stellt Datenverfügbarkeit sicher. Eine entsprechende Maßnahme zur IKT-Bereitschaft für Business-Continuity ist im HitGuard GRC-Tool dokumentiert. Zugeordnete Maßnahmen und Kontrollen: - M_073 Umsetzung A5.30 IKT-Bereitschaft für Business-Continuity
A.5.31	Rechtliche, 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.	Ja	G, B, R	iteratec hat einen systematischen Prozess zur Identifizierung, Dokumentation und Aktualisierung von rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen etabliert. Ein Rechtskataster wird für die Standorte in Deutschland und Polen geführt und regelmäßig aktualisiert. Die Anforderungen werden systematisch erfasst und ihre Einhaltung wird überwacht. Verantwortlichkeiten für die Überwachung und Umsetzung der verschiedenen Anforderungskategorien sind klar definiert und zugewiesen. Änderungen in relevanten Rechtsvorschriften werden zeitnah identifiziert und in die Compliance-Prozesse integriert. Zugeordnete Maßnahmen und Kontrollen: - M_106 [OFI-17] [A5.31] - Delegation Vertragswesen an Controlling
A.5.32	Geistige Eigentumsrechte	Die Organisation muss geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.	Ja	G, B, R	iteratec hat etablierte Praktiken zum Schutz von geistigem Eigentum implementiert. Dies umfasst sowohl den Schutz des eigenen geistigen Eigentums als auch die Einhaltung der Rechte Dritter. Lizenzmanagement-Prozesse stellen sicher, dass Software und andere urheberrechtlich geschützte Materialien ordnungsgemäß lizenziert und verwendet werden. Mitarbeiter werden über die Bedeutung des Schutzes geistiger Eigentumsrechte informiert und geschult. Vertragliche Regelungen mit Mitarbeitern und Dienstleistern adressieren die Handhabung von geistigem Eigentum. Eine entsprechende Richtlinie regelt die Anforderungen und Verfahren. Laufende Verbesserungsarbeiten zielen darauf ab, die Prozesse weiter zu optimieren. Zugeordnete Maßnahmen und Kontrollen: - M_017 Maßnahmen zur Verbesserung der geistigen Eigentumsrechte verbessern
A.5.33	Schutz von Aufzeichnungen	Aufzeichnungen müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.	Ja	G, B, R	iteratec hat umfassende Maßnahmen zum Schutz von Aufzeichnungen implementiert. Eine entsprechende Richtlinie regelt die Anforderungen an Erstellung, Speicherung, Schutz, Aufbewahrung und Vernichtung von Aufzeichnungen. Aufzeichnungen werden vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unerlaubter Freigabe geschützt. Aufbewahrungsfristen werden entsprechend gesetzlicher, regulatorischer und geschäftlicher Anforderungen definiert und eingehalten. Zugriffskontrollmechanismen stellen sicher, dass nur autorisierte Personen auf Aufzeichnungen zugreifen können. Backup- und Archivierungsprozesse gewährleisten die Verfügbarkeit und Integrität von Aufzeichnungen über den erforderlichen Zeitraum. Zugeordnete Maßnahmen und Kontrollen: - M_089 25-29948:9 - Tomcat Shutdown Port Not Secured
A.5.34	Datenschutz und Schutz personenbezogener 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.	Ja	G, B, R	iteratec hat ein umfassendes Datenschutz-Managementsystem etabliert. Ein Datenschutzbeauftragter (DSB) ist benannt und nimmt seine Aufgaben gemäß DSGVO wahr. Prozesse zur Identifizierung und Erfüllung datenschutzrechtlicher Anforderungen sind implementiert. Verzeichnisse von Verarbeitungstätigkeiten werden geführt und aktualisiert. Datenschutz-Folgenabschätzungen werden bei risikobehafteten Verarbeitungen durchgeführt. Betroffenenrechte können systematisch wahrgenommen werden. Mitarbeiter werden regelmäßig zu Datenschutzthemen geschult. Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sind implementiert und werden kontinuierlich überprüft. Eine entsprechende Richtlinie regelt die Umsetzung von Datenschutzmaßnahmen.
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.	Ja	G, B, R	iteratec hat ein System zur unabhängigen Überprüfung der Informationssicherheit etabliert. Interne Audits werden regelmäßig durch qualifizierte interne Auditoren durchgeführt, die unabhängig von den geprüften Bereichen sind. Externe Audits durch akkreditierte Zertifizierungsstellen finden im Rahmen der ISO 27001-Zertifizierung statt. Penetrationstests werden regelmäßig durch externe Sicherheitsexperten durchgeführt, um die Wirksamkeit der technischen Sicherheitsmaßnahmen zu überprüfen. Die Ergebnisse aller Überprüfungen werden dokumentiert, analysiert und führen zu Verbesserungsmaßnahmen. Ein Auditprogramm stellt die systematische Planung und Durchführung der Überprüfungen sicher.

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.	Ja	B, R	iteratec hat ein umfassendes System zur Überprüfung der Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit implementiert. Key Performance Indicators (KPIs) und Metriken werden systematisch erfasst und ausgewertet, um die Compliance zu überwachen. Regelmäßige Reviews stellen sicher, dass die implementierten Maßnahmen den definierten Anforderungen entsprechen. Abweichungen werden identifiziert, dokumentiert und durch Korrekturmaßnahmen adressiert. Das Management wird regelmäßig über den Compliance-Status informiert. Eine entsprechende Richtlinie regelt die Messung und Überwachung der Wirksamkeit. Automatisierte Monitoring-Tools unterstützen die kontinuierliche Überwachung der Einhaltung technischer Sicherheitsanforderungen.
A.5.37	Dokumentierte Betriebsabläufe	Die Betriebsverfahren für Informationsverarbeitungsanlagen müssen dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.	Ja	B, R	iteratec hat umfassende Dokumentationen der Betriebsabläufe erstellt und implementiert. Das Betriebshandbuch der IT-Infrastruktur dokumentiert alle wesentlichen Betriebsprozesse und -verfahren. Arbeitsanweisungen und Prozessbeschreibungen sind für kritische Tätigkeiten verfügbar und werden den betroffenen Mitarbeitern zugänglich gemacht. Eine entsprechende Richtlinie regelt die Anforderungen an die Dokumentensteuerung, einschließlich Erstellung, Prüfung, Genehmigung, Verteilung und Aktualisierung von Dokumenten. Versionskontrolle stellt sicher, dass immer die aktuellen Versionen verwendet werden. Regelmäßige Reviews gewährleisten die Aktualität und Relevanz der Dokumentationen. Die Dokumentationen werden in einem zentralen System verwaltet und sind für autorisierte Personen jederzeit verfügbar.
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.	Ja	B, R	iteratec hat ein strukturiertes risikobasiertes Screening-Verfahren für neue Mitarbeitende etabliert. Das Verfahren umfasst mehrstufige Prüfungen, die sich an der Kritikalität der Position und den damit verbundenen Zugangsrechten orientieren. Die Überprüfungen erfolgen vor Vertragsabschluss und beinhalten die Validierung von Qualifikationen, Referenzen und beruflichen Hintergründen. Eine entsprechende Richtlinie regelt die Anforderungen, Verantwortlichkeiten und Prozesse für die Durchführung von Sicherheitsüberprüfungen. Die Dokumentation der Prüfungsergebnisse erfolgt vertraulich in den Personalakten.
A.6.2	Beschäftigungs- und Vertragsbedingungen	In den arbeitsvertraglichen Vereinbarungen müssen die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.	Ja	G, B, R	Bei iteratec werden alle Mitarbeitenden vertraglich auf die Einhaltung von Informationssicherheitsanforderungen verpflichtet. Die Arbeitsverträge enthalten explizite Klauseln zur Vertraulichkeit, zum Datenschutz und zur Einhaltung interner Sicherheitsrichtlinien. Mitarbeitende werden auf das Betriebsgeheimnis verpflichtet und bestätigen die Kenntnisnahme der DSGVO-Anforderungen. Die vertraglichen Vereinbarungen umfassen auch Regelungen zu akzeptabler Nutzung von IT-Ressourcen, Umgang mit Geschäftsgeheimnissen und Konsequenzen bei Verstößen. Standardvorlagen für Arbeitsverträge werden regelmäßig auf Aktualität und Vollständigkeit geprüft. Zugeordnete Maßnahmen und Kontrollen: - M_113 [OFI-10] [A6.2] - HR-Standardvorlagen Polen
A.6.3	Informationssicherheitsbewusstsein, -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.	Ja	B, R	iteratec hat ein umfassendes rollenbasiertes Schulungs- und Sensibilisierungskonzept für Informationssicherheit etabliert. Alle Mitarbeitenden durchlaufen verpflichtende jährliche Awareness-Trainings, die aktuelle Bedrohungen, Sicherheitsrichtlinien und Best Practices abdecken. Neue Mitarbeitende erhalten im Rahmen des Onboardings eine dedizierte Einführung in die Informationssicherheit. Zusätzlich werden regelmäßige Phishing-Simulationen durchgeführt, um das Sicherheitsbewusstsein zu testen und zu stärken. Für spezielle Rollen (z.B. Entwickler, Administratoren) werden zielgruppenspezifische Schulungen angeboten. Die Teilnahme an Schulungen wird dokumentiert und die Wirksamkeit der Maßnahmen wird regelmäßig evaluiert. Zugeordnete Maßnahmen und Kontrollen: - M_039 Etablierung regelmäßiger Awareness-Maßnahmen (Phishing-Simulation)
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.	Ja	B, R	Bei iteratec ist ein formelles Disziplinarverfahren für Verstöße gegen Informationssicherheitsrichtlinien etabliert. Der Prozess definiert abgestufte Sanktionen abhängig von der Schwere und Häufigkeit der Verstöße. Das Verfahren umfasst die Dokumentation von Vorfällen, die Untersuchung durch die zuständigen Stellen (HR, ISMS-Team, Führungskräfte), die Anhörung der betroffenen Person und die Festlegung angemessener Maßnahmen. Mögliche Sanktionen reichen von Verwarnungen über Schulungsmaßnahmen bis hin zu arbeitsrechtlichen Konsequenzen. Der Prozess stellt sicher, dass Verstöße konsistent und fair behandelt werden und gleichzeitig eine abschreckende Wirkung entfalten.

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.	Ja	B, R	iteratec hat einen strukturierten OffBoarding-Prozess etabliert, der die Informationssicherheit bei Beendigung oder Änderung von Beschäftigungsverhältnissen gewährleistet. Eine Checkliste stellt sicher, dass alle sicherheitsrelevanten Schritte durchgeführt werden: Entzug von Zugangsrechten, Rückgabe von Firmeneigentum (Geräte, Zugangskarten, Schlüssel), Löschung von Zugangsdaten, Erinnerung an fortbestehende Vertraulichkeitsverpflichtungen und Durchführung von Exit-Gesprächen. Bei Rollenwechseln innerhalb des Unternehmens werden Berechtigungen entsprechend angepasst. Der Prozess wird durch HR koordiniert und die Durchführung wird dokumentiert.
A.6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	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.	Ja	V, R	Bei iteratec werden systematische Vertraulichkeitsverpflichtungen für alle relevanten Parteien eingesetzt. Mitarbeitende unterzeichnen Vertraulichkeitsvereinbarungen als Teil ihrer Arbeitsverträge. Externe Dienstleister, Berater und Lieferanten werden vor Zugang zu vertraulichen Informationen zur Unterzeichnung von NDAs (Non-Disclosure Agreements) verpflichtet. Die Vereinbarungen definieren klar den Umfang der vertraulichen Informationen, die Pflichten der Parteien, die Dauer der Vertraulichkeit und die Konsequenzen bei Verstößen. Standardvorlagen für verschiedene Szenarien (Mitarbeitende, Lieferanten, Geschäftspartner) sind verfügbar und werden von der Rechtsabteilung gepflegt.
A.6.7	Telearbeit (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.	Ja	G, B, R	iteratec hat eine umfassende Richtlinie für Homeoffice, Coworking-Spaces und mobiles Arbeiten etabliert. Die Richtlinie definiert Sicherheitsanforderungen für Remote-Arbeitsplätze, einschließlich physischer Sicherheit, Netzwerksicherheit (VPN-Nutzung), Gerätesicherheit (Endpoint Protection, Verschlüsselung) und Datenschutz. Mitarbeitende werden über sichere Arbeitspraktiken informiert, wie z.B. die Vermeidung von Einsichtnahme durch Dritte, sichere Aufbewahrung von Geräten und Dokumenten sowie die Nutzung sicherer Netzwerkverbindungen. Die Richtlinie berücksichtigt verschiedene Arbeitsszenarien und wird regelmäßig an neue Arbeitsformen angepasst. Zugeordnete Maßnahmen und Kontrollen: - M_054 OFI #14 Prüfung der Dokumente bzgl. des sprachlichen Verbindlichkeitsgrads
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.	Ja	G, B, R	Bei iteratec ist ein strukturierter Meldemechanismus für Informationssicherheitsereignisse etabliert. Alle Mitarbeitenden sind verpflichtet und befähigt, Sicherheitsvorfälle, Schwachstellen oder verdächtige Aktivitäten umgehend zu melden. Der Meldeweg erfolgt über den Security Service Desk oder direkt an das Security Operations Desk (SOD). Eine entsprechende Richtlinie definiert, was als meldepflichtiges Ereignis gilt, wie die Meldung zu erfolgen hat und welche Informationen bereitzustellen sind. Der Prozess stellt sicher, dass Meldungen vertraulich behandelt werden und keine negativen Konsequenzen für Meldende entstehen (No-Blame-Culture). Alle Meldungen werden dokumentiert, bewertet und entsprechend der Incident-Management-Prozesse behandelt.
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.	Ja	V, R	iteratec hat ein 5-Zonen-Sicherheitsmodell zur Strukturierung der physischen Sicherheit an allen Standorten implementiert. Die Zonen reichen von Zone 0 (öffentlicher Bereich) bis Zone 5 (Sicherheitsbereich wie Rechenzentrum). Für jede Zone sind spezifische Zutrittsbeschränkungen und Sicherheitsmaßnahmen definiert. Das Zonenmodell wird standortspezifisch umgesetzt und berücksichtigt die jeweiligen baulichen Gegebenheiten. Elektronische Zutrittskontrollsysteme, Sicherheitspersonal und physische Barrieren sichern die definierten Perimeter. Das externe Rechenzentrum in München ist als Zone 5 mit höchster Sicherheitsstufe klassifiziert. Zugeordnete Maßnahmen und Kontrollen: - M_100 [OFI-06] [A7.1] - Regeln für Untermieter in Zonen ab Zone 3 - M_118 [OFI-02] [A7.1] - Physische Sicherheit Netzwerkraum Wrocław
A.7.2	Physischer Zutritt	Sicherheitsbereiche müssen durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.	Ja	V, R	iteratec hat umfassende Zutrittskontrollmaßnahmen basierend auf dem 5-Zonen-Modell implementiert. Elektronische Zutrittskontrollsysteme mit Chipkarten und Transpondern regeln den Zugang zu den verschiedenen Bereichen. Differenzierte Berechtigungen sind für unterschiedliche Personenkreise definiert (Mitarbeitende, externe Nutzer, Besucher, Dienstleister). Ein digitales Besucherbuch dokumentiert alle Besuchereinträge. Für Technikräume gilt eine Protokollierungspflicht für jeden Zutritt. Besucher werden registriert, erhalten farbcodierte Ausweise und müssen begleitet werden. Standortspezifische Sicherheitsmaßnahmen sind für alle Geschäftsstellen dokumentiert. Zugeordnete Maßnahmen und Kontrollen: - M_102 [OFI-07] [A7.2] - Regelmäßige Prüfung Zutrittsrechte München - K_040 Prüfung Zutrittsrechte München

A.7.3	Sichern von Büros, Räumen und Einrichtungen	Die physische Sicherheit von Büros, Räumen und Einrichtungen muss konzipiert und umgesetzt werden.	Ja	R	iteratec hat Sicherheitsmaßnahmen für Büros, Räume und Einrichtungen sowohl an den Bürostandorten als auch für Homeoffice und mobiles Arbeiten implementiert. Standortspezifische Maßnahmen umfassen elektronische Zutrittskontrollsysteme, Sicherheitspersonal, Brandschutzmaßnahmen und die physische Sicherung von Technikräumen. Standort-Koordinatoren aus dem Security-Team überwachen die Einhaltung der Clean Desk Policy und anderer Sicherheitsmaßnahmen. Für Homeoffice und mobiles Arbeiten sind Risikobewertungen für verschiedene Arbeitsumgebungen durchgeführt und entsprechende Sicherheitsanforderungen definiert. Eine entsprechende Richtlinie regelt die Anforderungen an physische Sicherheit, Netzwerksicherheit und Datenschutz in verschiedenen Arbeitsszenarien.
A.7.4	Physische Sicherheitsüberwachung	Die Räumlichkeiten müssen ständig auf unbefugten physischen Zugang überwacht werden.	Ja	B, R	iteratec hat Überwachungsmaßnahmen für die physische Sicherheit implementiert. Zutrittsprotokolle für Technikräume dokumentieren jeden Zutritt. Ein digitales Besucherbuch registriert alle Besucher. An ausgewählten Standorten (Frankfurt, Wrocław) ist Videoüberwachung installiert. Elektronische Zutrittskontrollsysteme protokollieren Zutrittsereignisse. Sicherheitspersonal und Concierge-Dienste an mehreren Standorten fungieren als zusätzliche Überwachungsinstanz. Das externe Rechenzentrum in München verfügt über professionelle Überwachungsmaßnahmen entsprechend der höchsten Sicherheitsstufe. Zugeordnete Maßnahmen und Kontrollen: - M_103 [OFI-08] [A7.4] - Videoüberwachung Serverräume München - M_116 [OFI-04] [A7.4] - Physisches Monitoring Wrocław
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.	Ja	R	iteratec hat grundlegende Schutzmaßnahmen gegen physische und umweltbedingte Bedrohungen implementiert. Brandschutzmaßnahmen sind an allen Standorten vorhanden, einschließlich definierter Brandschutzhelfer und Evakuierungssammelstellen. Ein Notfallhandbuch beschreibt Verfahren bei physischen Notfällen. Das Risikomanagement umfasst einen Gefährdungskatalog nach BSI Grundschutz, der physische Bedrohungen wie Feuer, Wasser, Naturkatastrophen und Stromausfälle berücksichtigt. Das externe Rechenzentrum in München verfügt über professionelle Schutzmaßnahmen gegen umweltbedingte Risiken. Eine entsprechende Richtlinie regelt die Backup-Strategie zum Schutz gegen Datenverlust durch physische Schäden.
A.7.6	Arbeiten in Sicherheitsbereichen	Es müssen Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.	Ja	R	iteratec hat Regelungen für das Arbeiten in Sicherheitsbereichen etabliert, mit Fokus auf Technikräume. Für Technikräume (Zone 5) sind definierte Zutrittsberechtigte festgelegt (IT-Infrastruktur-Team). Eine Protokollierungspflicht gilt für jeden Zutritt, sowohl für interne als auch externe Personen. Externe Personen müssen begleitet werden. Das externe Rechenzentrum in München unterliegt der höchsten Sicherheitsstufe mit entsprechenden Zutrittsbeschränkungen. Physische Zutrittskontrollmaßnahmen umfassen elektronische Schlösser, mechanische Schlösser mit Schlüsseltresoren und Chipkarten-Systeme. Zutrittsprotokolle dokumentieren die Anwesenheit in Sicherheitsbereichen.
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.	Ja	B, R	iteratec hat Clear Desk und Clear Screen Policies für Büroarbeitsplätze, Homeoffice und mobiles Arbeiten implementiert. Bildschirmsperren sind beim Verlassen des Arbeitsplatzes verpflichtend. Blickschutzfolien werden für Arbeit in öffentlichen Bereichen empfohlen. Die Clear Desk Policy fordert die sichere Aufbewahrung und Entsorgung schützenswerter Dokumente. Aktenvernichter mit Sicherheitsstufe 4+ sind an allen Standorten verfügbar. Das Endpoint Management erzwingt Bildschirmsperre-Einstellungen auf verwalteten Geräten und führt Compliance-Prüfungen durch. Festplattenverschlüsselung bietet zusätzlichen Schutz. Stichprobenartige Überprüfungen durch ISB und IT-Infrastruktur-Team stellen die Einhaltung sicher.
A.7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen sicher und geschützt aufgestellt werden.	Ja	B, R	iteratec hat grundlegende Maßnahmen zur Platzierung und zum Schutz von Geräten implementiert. Server und Netzwerkinfrastruktur sind in definierten Technikräumen mit Zutrittskontrolle untergebracht. Das externe Rechenzentrum in München bietet professionelle Schutzmaßnahmen für kritische Infrastruktur. Client-Geräte werden über Endpoint Management verwaltet, mit dokumentierter Ausgabe und Rücknahme durch das IT-Infrastruktur-Team. Laptops verfügen über Kensington-Lock-Möglichkeiten. Verschlüsselung schützt bei Diebstahl. Mobile Device Management sichert Smartphones. Das Asset-Management-System dokumentiert Gerätestandorte. Technikräume sind physisch gesichert und in geschützten Bereichen der Gebäude platziert.
A.7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Werte außerhalb des Standorts müssen geschützt werden.	Ja	R	iteratec hat umfassende Sicherheitsmaßnahmen für Assets außerhalb der Unternehmensräume implementiert. Eine entsprechende Richtlinie regelt Homeoffice, mobiles Arbeiten, Coworking-Spaces und Geräte auf Reisen. Risikobewertungen für verschiedene Arbeitsumgebungen sind durchgeführt und differenzierte Sicherheitsanforderungen definiert. Das Endpoint Management erzwingt Verschlüsselung, Bildschirmsperre-Konfiguration und bietet Remote-Wipe-Möglichkeit bei Verlust oder Diebstahl. VPN-Zugang sichert Netzwerkverbindungen. Anti-Malware-Schutz ist auf allen Geräten installiert. BYOD/COPE-Konzepte regeln die Trennung zwischen privater und dienstlicher Nutzung. Compliance-Reports überwachen Verschlüsselung und Sicherheitskonfigurationen. Das Asset-Management dokumentiert ausgegebene Geräte und deren Rücknahme.

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.	Ja	B, R	iteratec hat Regelungen für Speichermedien über deren Lebenszyklus implementiert. Eine entsprechende Richtlinie fordert die Verschlüsselung externer Datenträger für Firmendaten. Unverschlüsselte USB-Sticks sind für Firmendaten nicht zugelassen. Cloud-Speicher wird als Alternative zu USB-Sticks empfohlen. Eine Löschrichtlinie definiert Löschklassen (Klasse 1-4) und Verfahren für die sichere Löschung bei Außerbetriebnahme. Aktenvernichter mit Sicherheitsstufe 4+ sind für Dokumente verfügbar. Externe Festplatten werden zentral in München durch einen externen Dienstleister entsorgt. Das Asset-Management verwaltet externe Festplatten. Festplattenverschlüsselung ist auf allen Geräten implementiert. Eine Backup-Strategie sichert Server und Clients. Zugeordnete Maßnahmen und Kontrollen: - M_115 [OFI-05] [A7.10] - Entsorgungsrichtlinie Wrocław IT-Geräte
A.7.11	Versorgungseinrichtungen	Informationsverarbeitungseinrichtungen müssen vor Stromausfällen und anderen Störungen, die durch Ausfälle von unterstützenden Versorgungseinrichtungen verursacht werden, geschützt werden.	Ja	B, R	iteratec hat grundlegende Maßnahmen für unterstützende Versorgungseinrichtungen implementiert. Das externe Rechenzentrum in München verfügt über professionelle Stromversorgung mit Redundanz, Klimatisierung und Brandschutz. An den Standorten sind elektrische Sicherheit und Brandschutzeinrichtungen vorhanden. Das Risikomanagement berücksichtigt den Ausfall der Stromversorgung als Gefährdung. Ein Notfallhandbuch beschreibt Verfahren bei Infrastrukturausfällen. Kontaktdaten für Notfälle sind dokumentiert. Das externe Rechenzentrum ist durch SLA mit Wartungsvereinbarungen abgesichert. Die Standortdokumentation erwähnt elektrische Sicherheit und Brandschutzmaßnahmen für alle Geschäftsstellen.
A.7.12	Sicherheit der Verkabelung	Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Abhören, Störung oder Beschädigung geschützt werden.	Ja	B, R	iteratec hat Maßnahmen für Kabelsicherheit durch Farbkodierung und logische Segmentierung implementiert. Netzwerkkabel sind standortspezifisch nach Funktion und Sicherheitsstufe farbcodiert (z.B. Server, DMZ, Internet, Gast-Leitung). Die Farbschemata sind für alle Standorte dokumentiert. Logische Netzwerksegmentierung über VLANs und Firewall-Regeln trennt sensible Segmente. Ein Zero Trust Ansatz verhindert direkte Kommunikation zwischen Geräten im internen Netz. Das externe Rechenzentrum verfügt über professionelle Verkabelung mit Etikettierung besonderer Kabel. Netzwerkpläne sind dokumentiert. Switch-Konfigurationen werden versioniert verwaltet. Firewall-Logs überwachen den Netzwerkverkehr. Zugeordnete Maßnahmen und Kontrollen: - M_117 [OFI-03] [A7.12] - Kabelführung Büro Wrocław
A.7.13	Instandhaltung von Geräten und Betriebsmitteln	Geräte und Betriebsmittel müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.	Ja	B, R	iteratec hat Wartungsprozesse für Geräte etabliert. Software-Wartung erfolgt über automatische Updates durch das Endpoint Management für alle Plattformen (Windows, macOS, iOS, Android). Patchmanagement mit Update-Ringen ermöglicht gestaffelte Verteilung. Dell Command Update verwaltet Firmware-Updates für Dell-Geräte. Malware-Schutz-Updates erfolgen automatisch. Hardware-Wartung umfasst Ausgabe und Rücknahme durch das IT-Infrastruktur-Team. Das Asset-Management-System dokumentiert Geräte und Seriennummern. Das externe Rechenzentrum verfügt über professionelle Wartung durch den Betreiber mit SLA-Vereinbarungen. Endpoint Management Compliance-Reports überwachen Patch-Levels und Update-Status für alle Plattformen.
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.	Ja	R	iteratec hat Prozesse für die sichere Entsorgung und Wiederverwendung von Geräten implementiert. Eine Löschrichtlinie definiert Löschklassen (Klasse 1-4) und Verfahren je nach Sensibilität der Daten (Überschreiben, physische Zerstörung, verschlüsseltes Löschen). Die Dokumentation der Löschvorgänge umfasst Art, Datum und ausführende Person. Geräterücknahme erfolgt bei Beendigung des Arbeitsverhältnisses oder Gerätewechsel und wird über die OffBoarding-Checkliste dokumentiert. Das Endpoint Management bietet Remote-Wipe-Möglichkeit für mobile Geräte. Festplattenverschlüsselung ermöglicht sicheres Löschen durch Entfernen des Verschlüsselungsschlüssels. Aktenvernichter mit Sicherheitsstufe 4+ sind für Dokumente verfügbar. Externe Datenträger werden vor Wiederverwendung sicher gelöscht oder bei Entsorgung physisch zerstört.
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.	Ja	B, R	iteratec hat ein umfassendes Endpoint Management über Microsoft Endpoint Manager (Intune) für alle Gerätekategorien und Plattformen implementiert. Security Baselines, Verschlüsselung (BitLocker, FileVault), Malware-Schutz (Malwarebytes/ThreatDown), automatisches Patch-Management und Screen-Lock-Policies sind standardisiert ausgerollt. Der Compliance-Status aller Geräte wird in Intune überwacht mit automatischer Durchsetzung bei Non-Compliance. Zugeordnete Maßnahmen und Kontrollen: - M_014 OFI #15 Überprüfung von BYOD-Risiko und -Maßnahmen - M_054 OFI #14 Prüfung der Dokumente bzgl. des sprachlichen Verbindlichkeitsgrads - M_060 Patch-Management für Betriebssysteme verbessern

A.8.2	Privilegierte Zugangsrechte	Zuteilung und Gebrauch von privilegierten Zugangsrechten müssen eingeschränkt und verwaltet werden.	Ja	B, R	iteratec hat ein strukturiertes Privileged Access Management mit LAPS (7-Tage-Rotation für lokale Admin-Passwörter), Privileged Identity Management (PIM) für temporäre Rechteerhöhungen im Security Team und rollenbasierter Zugriffskontrolle (RBAC) über Berechtigungs-Gruppen implementiert. Cloud-Provider-Zugriffe erfolgen ausschließlich über Autorisierungsgruppen ohne individuelle IAM-User. Administrative Passwörter werden zentral im Enterprise Password Manager (1Password) verwaltet. Jährliche Access Rights Reviews werden dokumentiert und durch Asset Owner durchgeführt. Die LAPS-Rotation wird automatisch durchgesetzt und protokolliert. Zugeordnete Maßnahmen und Kontrollen: - M_087 25-29948:7 - Stored Cross-Site Scripting (XSS) Mail - M_097 25-29948:1 - Same Default Password over Multiple Tenants
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.	Ja	B, R	iteratec hat eine Informationsklassifizierung mit Personenkreisen und Schutzbedarfskategorien (C-I-A) etabliert. Zugriffskontrolle erfolgt über RBAC mit Berechtigungs-Gruppen, SSO via Azure AD/Entra ID und rollenbasierte Zugriffsrechte. Asset Owner führen jährliche Access Reviews durch. Das Asset-Inventar mit CIA-Bewertungen ist vorhanden. Asset Owner sind definiert und zugewiesen, die Klassifizierung ist in der Asset-Datenbank erfasst. Zugeordnete Maßnahmen und Kontrollen: - M_085 25-29948:5 - Broken Access Control on Groups Endpoint - M_087 25-29948:7 - Stored Cross-Site Scripting (XSS) Mail - M_089 25-29948:9 - Tomcat Shutdown Port Not Secured - M_095 25-29948:15 - Password Exposure via User-Management - M_097 25-29948:1 - Same Default Password over Multiple Tenants
A.8.4	Zugriff auf den Quellcode	Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken müssen angemessen verwaltet werden.	Ja	R	iteratec nutzt GitLab als zentrale DevServices-Plattform für Source Code Management mit gruppenbasierter Zugriffskontrolle. Infrastructure as Code (IaC) für Netzwerkkonfigurationen, Versionskontrolle für alle Konfigurationen und integrierte Security-Scanning-Tools (SAST/DAST, Dependency Management via Dependabot/Snyk/RenovateBot) sind etabliert. Code Reviews sind im Entwicklungsprozess verankert. GitLab-Zugriffe werden über Gruppen gesteuert und sind nachvollziehbar. Security Scanning Ergebnisse werden in CI/CD Pipelines erfasst, Dependency-Schwachstellen automatisch erkannt und gemeldet.
A.8.5	Sichere Authentisierung	Sichere Authentisierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.	Ja	V, B, R	iteratec hat eine umfassende Multi-Faktor-Authentisierung (MFA) über Azure AD/Entra ID implementiert, die, wo technisch möglich, erzwungen wird. Single Sign-On (SSO) via Azure AD mit SAML2 und OpenIDConnect, Windows Hello for Business und Microsoft Authenticator für MFA sind etabliert. Eine SIEM-basierte Risky User Detection mit Azure AD Identity Protection erkennt verdächtige Anmeldeversuche automatisch und löst bei Risk Level medium oder höher automatische Passwort-Resets via Conditional Access Policy aus sowie Tickets im Security Service Desk. Automatische Meldekette: Azure AD Identity Protection → SSD-Ticket → Analyse → Remediation ist etabliert. Zugeordnete Maßnahmen und Kontrollen: - M_082 25-29948:2 - Vulnerable Dependencies - M_083 25-29948:3 - Broken Access Control on Database Configuration - M_084 25-29948:4 - Multiple Known Vulnerabilities in Tomcat
A.8.6	Kapazitätssteuerung	Die Nutzung von Ressourcen muss überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.	Ja	B, R	iteratec hat Monitoring-Tools für Infrastruktur (Azure Sentinel als SIEM, Zabbix) implementiert. Kapazitätsmanagement ist in der IT-Infrastruktur-Richtlinie referenziert. Cloud-Provider-native Monitoring-Tools (AWS CloudWatch, Azure Monitor, GCP Monitoring) sind verfügbar. Monitoring-Daten werden erfasst, Ressourcennutzung überwacht und Alerts bei Schwellwertüberschreitungen konfiguriert.
A.8.7	Schutz gegen Schadsoftware	Schutz gegen Schadsoftware muss umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.	Ja	V, B, R	iteratec hat Malwarebytes/ThreatDown als zentrale Anti-Malware-Lösung über Microsoft Endpoint Manager (Intune) auf allen verwalteten Geräten ausgerollt. Automatische Updates, zentrale Verwaltung und Überwachung sind implementiert. Eine Schadsoftware Management Richtlinie ist etabliert. Der Malware-Schutz-Status wird in Intune zentral überwacht, der Compliance-Status für Anti-Malware getrackt. Malware-Erkennungen werden geloggt und ausgewertet. Ein Incident Management Prozess für Malware-Vorfälle ist etabliert. Zugeordnete Maßnahmen und Kontrollen: - M_043 Einrichten von Virenschutzsoftware auf Clients und Servern

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.	Ja	B, R	iteratec hat ein umfassendes Vulnerability Management mit JIRA/DefectDojo als zentrale Plattform, secureCodeBox für automatisierte Scans, SAST/DAST-Tools (SonarQube, Semgrep, Checkmarx, Fortify) und Dependency Management (Dependabot, Snyk, RenovateBot) implementiert. Automatische Schwachstellenerkennung in CI/CD-Pipelines ist integriert. Schwachstellen werden in JIRA/DefectDojo zentral erfasst und getrackt. Der Patch-Status wird zentral in Intune überwacht (Update-Ringe). Dependency-Schwachstellen werden automatisch erkannt und gemeldet, Risikobewertung erfolgt systematisch. Zugeordnete Maßnahmen und Kontrollen: - M_091 25-29948:11 - Broken Access Control on LDAP Config
A.8.9	Konfigurationsmanagement	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.	Ja	B, R	iteratec hat ein strukturiertes Konfigurationsmanagement mit dokumentierten Prozessen für Identifikation, Konzeption, Implementierung und Verifikation etabliert. Infrastructure as Code (IaC) für Netzwerkkonfigurationen und Versionskontrolle über Git sind implementiert. Zentrale Systeme wie Firewall, ThreatDown und Object Sync werden systematisch verwaltet. Jährliche Reviews der Konfigurationen sind dokumentiert. Versionskontrolle ermöglicht Audit-Trail für alle Konfigurationsänderungen. Der Compliance-Status von Client-Konfigurationen wird in Intune überwacht. Zugeordnete Maßnahmen und Kontrollen: - M_088 25-29948:8 - Broken Access Control on Authentication Configuration - M_093 25-29948:13 - User Enumeration via Default Role Endpoint - K_016 Konfigurationsmanagement - Prüfung Firewall - K_017 Konfigurationsmanagement - Prüfung ThreatDown/Malwarebytes - K_020 Konfigurationsmanagement - Object Sync
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.	Ja	B, R	iteratec hat eine umfassende Richtlinie zur sicheren Löschung von Daten mit 4 Löschklassen und definierten Aufbewahrungsfristen etabliert. Gesetzliche Aufbewahrungspflichten (6-10 Jahre) werden berücksichtigt. SharePoint-Versionsverwaltung ist auf unter 1 Jahr oder maximal 100 Versionen begrenzt. Sichere Löschverfahren für Datenträger (Überschreiben, physische Zerstörung) sind definiert. Remote Wipe für mobile Geräte via MDM ist verfügbar. Regelmäßige Audits durch Datenschutzbeauftragten sind vorgesehen, Offboarding-Checklisten mit Löschnachweis vorhanden. Zugeordnete Maßnahmen und Kontrollen: - M_019 Erstellung eines Löschkonzepts - M_084 25-29948:4 - Multiple Known Vulnerabilities in Tomcat - M_101 [OFI-18] [A8.10] - Datenlöschung auf Endgeräten
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.	Ja	R	iteratec hat eine Datenmaskierungs-Richtlinie mit vier definierten Methoden etabliert: Pseudonymisierung, synthetische Daten, Verschlüsselung und Zugriffsbeschränkungen. Verantwortlichkeiten sind klar definiert. Die Richtlinie ist in Entwicklungs- und Testprozesse integriert. Technische Maßnahmen umfassen Pseudonymisierung in Test-/Entwicklungsumgebungen, synthetische Testdaten-Generierung, Field-Level Encryption für sensible Datenfelder und RBAC für Datenzugriff. Kontinuierliche Überwachung der Effektivität und Projektaudits zur Prüfung der Datenmaskierung sind etabliert. Zugeordnete Maßnahmen und Kontrollen: - M_020 Konzept zur Datenmaskierung - M_089 25-29948:9 - Tomcat Shutdown Port Not Secured
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.	Ja	B, R	iteratec hat mehrere Maßnahmen zur Verhinderung von Datenlecks implementiert: Informationsklassifizierung mit Schutzmaßnahmen, Endpoint-Schutz via MDM mit Verschlüsselung und Remote Wipe, Netzwerksegmentierung, SIEM-basiertes Monitoring (Azure Sentinel) und Zugriffskontrolle via RBAC/MFA. Ein umfassendes DLP-Konzept wurde erstellt, das kritische Systeme identifiziert und DLP-Lösungen evaluiert hat. Aktuell wird ein SIEM-basierter Ansatz für die Erkennung großer Datenabflüsse verfolgt mit Alerting bei verdächtigen Datenübertragungen. Awareness-Maßnahmen zu visuellen Datenlecks (Blickschutzfolie, Screen Lock) sind dokumentiert. Zugeordnete Maßnahmen und Kontrollen: - M_021 Verhinderung von Datenlecks

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.	Ja	B, R	iteratec hat eine umfassende Backup-Richtlinie mit drei definierten Backup-Methoden (Full, Incremental, Differential) etabliert. Halbjährliche Recovery-Tests sind dokumentiert und werden durchgeführt. Asset-Liste mit Backup-Anforderungen ist vorhanden. Für Infrastruktur-Server ist Veeam im Einsatz, für Clients sind OneDrive for Business und lokale Backups (TimeMachine, Veeam) vorgesehen. Backup-Verantwortlichkeiten sind klar definiert (IT-Infrastruktur für Server-Backups, Mitarbeitende für Client-Backups). Verschlüsselung aller Backup-Datenträger ist vorgeschrieben. Backup-Rotation mit definierten Aufbewahrungsfristen und Offsite-Backup für kritische Systeme sind implementiert. Der Backup-Status wird für Server-Systeme überwacht. Zugeordnete Maßnahmen und Kontrollen: - K_005 Sicherung von Information (Wiederherstellungstests von Backups)
A.8.14	Redundanz von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen realisiert werden.	Ja	B, R	iteratec hat Redundanzkonzepte für kritische Systeme implementiert: Cloud-basierte Dienste mit Provider-SLAs (Microsoft 365 mit Multi-Geo-Redundanz, Azure mit Availability Zones und Geo-Redundanz, AWS/GCP mit Hochverfügbarkeitsoptionen). Verfügbarkeitsanforderungen sind im Asset-Inventar mit RTO-Werten dokumentiert. Notfall-Szenarien mit Redundanzüberlegungen sind dokumentiert (z.B. zusätzliche Azure AD Connectoren). Backup-Systeme dienen als Redundanz für kritische Daten. VMware-Umgebung mit Redundanzoptionen, mehrere Internet-Anbindungen an Standorten und redundante Netzwerkkomponenten (Firewall, Switches) sind vorhanden. Monitoring von Systemverfügbarkeit via Zabbix sowie Cloud-Provider SLA-Monitoring sind etabliert.
A.8.15	Protokollierung	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.	Ja	G, B, R	iteratec hat eine umfassende Ereignisprotokoll-Richtlinie mit risikobasiertem Logging-Ansatz etabliert: Azure Sentinel als zentrales SIEM-System für kritische und hohe Risiken, lokale Protokollierung für mittlere und niedrige Risiken. SOC-Prozesse sind definiert mit Überwachung, Bedrohungserkennung und Reaktion. Der Logging-Scope umfasst Netzwerkkomponenten, Server, Cloud-Dienste, Sicherheitssysteme und kritische Business-Anwendungen. Zeitsynchronisation über zentrale NTP-Server ist etabliert. Automatische Alerts bei Sicherheitsereignissen sind konfiguriert. Risky User Detection mit automatischer Meldung an Security Service Desk ist aktiv. Zugeordnete Maßnahmen und Kontrollen: - M_090 25-29948:10 - Email Credentials Leaked To Frontend
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.	Ja	B, R	iteratec hat mehrere Monitoring-Systeme implementiert: Azure Sentinel als SIEM für Security Event Monitoring mit Anomalie-Erkennung, Zabbix für Infrastruktur-Monitoring. Azure AD Identity Protection mit Risky User Detection ist aktiv und meldet automatisch an den Security Service Desk. Incident Management Prozesse mit Überwachung und Reaktion sind etabliert. Der Monitoring-Scope umfasst Netzwerkkomponenten, Server, Cloud-Dienste, Sicherheitssysteme und kritische Business-Anwendungen. Monitoring ist in IT-Infrastruktur-Richtlinie und Messung/Überwachung der Wirksamkeit verankert. Zugeordnete Maßnahmen und Kontrollen: - M_083 25-29948:3 - Broken Access Control on Database Configuration - M_090 25-29948:10 - Email Credentials Leaked To Frontend
A.8.17	Uhrensynchronisation	Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme müssen mit zugelassenen Zeitquellen synchronisiert werden.	Ja	B, R	iteratec hat Zeitsynchronisierung für Systeme implementiert. Die Verwendung eines einheitlichen Zeitservers bzw. Zeitserverpools ist im IT-Infrastruktur Betriebshandbuch dokumentiert. NTP-basierte Zeitsynchronisation wird eingesetzt. Konfigurationsmanagement-Richtlinie fordert Synchronisierung der Uhren als Grundvorgabe. Zeitsynchronisation wird technisch durchgesetzt und ist für Logging-Korrelation im SIEM-System relevant.
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.	Ja	R	iteratec hat Maßnahmen zur Kontrolle privilegierter Zugriffe implementiert: Getrennte administrative Accounts für privilegierte Tätigkeiten, LAPS (Local Administrator Password Solution) für Windows-Clients mit automatischer Rotation, sudo-Konfiguration mit Passworteingabe für Linux-Clients, No-Admin Windows-Clients für nicht-technische Rollen. Endpoint Management mit Konfigurationsprofilen für Admin-Rechte ist etabliert. Passwortrichtlinie definiert Anforderungen für administrative Accounts. Konfigurationsmanagement fordert Deaktivierung nicht benötigter Zugangsrechte. Abdeckungsgrad Domain-User ohne lokale Admin-Rechte wird dokumentiert.

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.	Ja	B, R	iteratec hat umfassende Prozesse zur Kontrolle der Software-Installation implementiert. Benutzerrichtlinien regeln Software-Installation für Mitarbeiter. Kostenpflichtige Software muss über IISD-Ticket angefordert werden. Endpoint Management (Microsoft Intune) für alle Plattformen mit automatischer Installation definierter Standard-Anwendungen und Unternehmensportal für optionale Anwendungen. No-Admin Windows-Clients für nicht-technische Rollen, LAPS für temporäre Admin-Rechte bei Bedarf. ThreatDown zur Erkennung unerwünschter Software und Schwachstellen, Inventory360 zur Erfassung installierter Software. Compliance-Richtlinien für alle Client-Plattformen (Windows, macOS, iOS, Android). Monatliche Überprüfung des Systemstands der Client-Devices und KPI-Messung des Patch-Stands installierter Software. Zugeordnete Maßnahmen und Kontrollen: - M_091 25-29948:11 - Broken Access Control on LDAP Config
A.8.20	Netzwerksicherheit	Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.	Ja	R	iteratec hat umfassende Netzwerksicherheitsmaßnahmen implementiert: Firewall bzw. Firewall-Cluster an jedem Standort, VLAN-basierte Netzwerktrennung mit Zonierung (Client, Server, Management, DMZ, Gäste), Site-to-Site VPN für Standortvernetzung, Client VPN mit EntraID-Authentifizierung (Cisco AnyConnect). Firewall-Regeln nach Least-Privilege-Prinzip. Netzwerk-Dokumentation als Infrastructure as Code im Git-Repository. Changemanagement für Netzwerkänderungen, jährliche Überprüfung der Firewall-Konfiguration geplant. Externer Red-Team-Pentest 2025 (modzero) bestätigt hohe Wirksamkeit: Netzwerksegmentierung hat Angreifer erfolgreich aufgehalten, Backup- und Management-Netzwerke blieben vollständig isoliert.
A.8.21	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste müssen ermittelt, umgesetzt und überwacht werden.	Ja	R	iteratec hat Sicherheitsmaßnahmen für Netzwerkdienste implementiert: Client VPN mit Cisco AnyConnect (TLS 1.3, DTLS 1.2), E-Mail-Server mit STARTTLS, TLS 1.2, DKIM, SPF, SSL/TLS-Zertifikate von Digicert und LetsEncrypt mit jährlicher SSL-Labs Überprüfung (Ziel: Bewertung A). Site-to-Site VPN für Kunden und Dienstleister mit Protokollierung. Dokumentierte Netzwerkdienste umfassen Domain Controller, Fileserver, Terminalserver, Monitoring (Zabbix), Gitlab, Proxy, Firewall Management, Zeitserver (NTP), DNS, DHCP, RADIUS. Server- und Dienstsegmentierung mit C-I-A-Bewertung ist dokumentiert. Kryptographie-Richtlinie definiert Anforderungen für
A.8.22	Trennung von Netzwerken	Informationsdienste, Benutzer und Informationssysteme müssen in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.	Ja	R	iteratec hat umfassende Netzwerksegmentierung implementiert: Dedizierte Netzwerksegmentierung-Richtlinie definiert standortbezogene Netze (München, Hamburg, Stuttgart, Frankfurt, Düsseldorf, Wien, Wrocław) und Zonierung nach Schutzbedarf (Client, Server, Management, DMZ, Gäste). VLAN-basierte Netzwerktrennung mit Firewall-Kontrolle zwischen allen Segmenten. Dedizierte Gäste-VLANs mit eigenem Router und Firewall, Management-Zonen nur für privilegierte Administratoren, DMZ für Internet-exponierte Dienste mit Perimeter-Firewall. Infrastructure as Code für Netzwerk-Provisionierung (DellOS6 Switches). Changemanagement für Netzwerkänderungen. Externer Red-Team-Pentest 2025 bestätigt Wirksamkeit: Backup- und Management-Segmente blieben vollständig isoliert, Netzwerksegmentierung reduzierte lateral movement opportunities.
A.8.23	Webfilterung	Der Zugang zu externen Websites muss verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.	Ja	R	iteratec hat Web-Filtering über ThreatDown (ehemals Malwarebytes) Endpoint Security implementiert. Der integrierte Webfilter ist auf allen verwalteten Clients aktiv und blockiert bösartige Websites. Automatische Installation über Endpoint Management (MDM) auf Windows und macOS. Abdeckungsgrad Endpoint Security wird monatlich dokumentiert. Jährliche Wirksamkeitsprüfung von ThreatDown durch IT-Infrastruktur und Security Kernteam. ThreatDown-Portal für Monitoring und Incident-Response vorhanden. Zugeordnete Maßnahmen und Kontrollen: - M_088 25-29948:8 - Broken Access Control on Authentication Configuration
A.8.24	Verwendung von Kryptographie	Es müssen Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.	Ja	B, R	iteratec hat umfassende Kryptographie-Richtlinie implementiert mit Referenz zu den aktuellen BSI Richtlinien. Jährliche Aktualisierung der Vorgaben anhand BSI-Standards. Definierte kryptographische Verfahren: Symmetrisch (AES-256, Serpent), Asymmetrisch (RSA-4096, ECC-256, Ed25519), Hash (SHA-256 oder höher, SHA-3), Digitale Signaturen (RSA-3072, ECDSA-256), Schlüsselaustausch (Diffie-Hellman-3072, ECDH-256). Schlüssel-Lifecycle und Schlüsselverantwortliche dokumentiert. Technische Umsetzung: Festplattenverschlüsselung (BitLocker, FileVault, LUKS), Client VPN (TLS 1.3, DTLS 1.2), E-Mail (STARTTLS, TLS 1.2, S/MIME), SSL/TLS-Zertifikate, SSH Keys, WLAN (WPA2, WPA3). SSL-Labs Überprüfung für Webdienste, monatliche Überprüfung der Client-Verschlüsselung, Wiederherstellungsschlüssel in Intune/AAD gespeichert. Zugeordnete Maßnahmen und Kontrollen: - M_023 Aktualisierung der Kryptographie-Richtlinie - M_093 25-29948:13 - User Enumeration via Default Role Endpoint - M_094 25-29948:14 - Credentials Exposed in Bash History

A.8.25	Lebenszyklus einer sicheren Entwicklung	Regeln für die sichere Entwicklung von Software und Systemen müssen festgelegt und angewendet werden.	Ja	R	iteratec hat umfassende Richtlinien für sichere Softwareentwicklung etabliert: Richtlinie Sicherheit im Entwicklungsprozess für alle Entwicklungsprojekte, Richtlinie Sichere Software-Entwicklung in IT-Projekten mit den Prozessschritten: Projektkritikalität, Risikoanalyse, Sicherheitsanforderungen, Maßnahmen-Identifikation, Umsetzung, Wirksamkeitsprüfung, Assetmanagement, Richtlinie Sicherheit in der Produktentwicklung für interne Produkte. Kritikalitätsbewertung mit 5 Stufen und daraus abgeleiteten Maßnahmen. Rollenkonzept mit Projektverantwortlichen, Security Champions und Sicherheitsbeauftragten je nach Projektkritikalität. Technische Maßnahmen: Versionsverwaltung, Code-Review-Prozesse, CI/CD-Pipeline mit Schutz gegen Manipulation, statische Code-Analyse, Bedrohungsanalyse für hochkritische Projekte. Allgemeine Praktiken zur sicheren Programmierung mit Guides für Java, JavaScript, TypeScript, Python, Go, HTML. Projektaudit-Checkliste und OWASP ASVS Checkliste für hochkritische Projekte. Zugeordnete Maßnahmen und Kontrollen: - M_044 ABW #2 Abweichung Sichere SW Entwicklung in Projekten
A.8.26	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit müssen bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.	Ja	B, R	Sicherheitsanforderungen sind als verpflichtender Prozessschritt in Entwicklungsrichtlinien verankert. Systematische Ermittlung aus drei Quellen: Projektkritikalität, Projektrisiken und explizite Anforderungen. Berücksichtigung von Kundenanforderungen, firmeneigenen Anforderungen und DSGVO. Template ISMS Projektinformationen zur strukturierten Dokumentation. Kritikalitätsbewertung mit daraus abgeleiteten Mindestanforderungen. OWASP ASVS als Referenz für hochkritische Projekte. Verantwortlichkeiten klar definiert (RACI-Matrix). Zugeordnete Maßnahmen und Kontrollen: - M_044 ABW #2 Abweichung Sichere SW Entwicklung in Projekten
A.8.27	Sichere Systemarchitektur und Entwicklungsgrundsätze	Grundsätze für die Entwicklung sicherer Systeme müssen festgelegt, dokumentiert, aufrechterhalten und bei allen Aktivitäten der Informationssystementwicklung angewendet werden.	Ja	B, R	Umfassende Grundsätze für sichere Systemarchitektur nach Projektkritikalität gestuft. Grundprinzipien: Validierung aller Eingabedaten, server-seitige Validierung, Least Privilege, vertrauenswürdige Bibliotheken. Ab Kritikalität mäßig: Fail-Safe Defaults, sichere Standardkonfigurationen, Privacy by Design/Default, Bedrohungsanalyse. Ab Kritikalität hoch: Verpflichtende Bedrohungsanalyse, Sicherheitsbeauftragter, OWASP ASVS. Secure Coding Guidelines ab Kritikalität mäßig. Guides für Java, JavaScript, TypeScript, Python, Go, HTML verfügbar.
A.8.28	Sichere Codierung	Bei der Softwareentwicklung müssen die Grundsätze der sicheren Codierung angewandt werden.	Ja	B, R	Secure Coding Guidelines dokumentiert, ab Projektkritikalität mäßig verpflichtend. Allgemeine Guides für 7 Programmiersprachen verfügbar. Code-Review-Prozess: empfohlen ab niedrig, verpflichtend ab mäßig. Security Champion koordiniert sicherheitsrelevante Aspekte. Qualitätssicherungsprozess mit Sicherheitsaspekten (Guidelines, statische Code-Analyse). CI/CD-Pipeline mit Sicherheitsprüfungen. Zugeordnete Maßnahmen und Kontrollen: - M_024 Coding Guidelines für Sprachen/Technologien erstellen - M_085 25-29948:5 - Broken Access Control on Groups Endpoint - M_086 25-29948:6 - Remote Code Execution in Administration - M_088 25-29948:8 - Broken Access Control on Authentication Configuration - M_090 25-29948:10 - Email Credentials Leaked To Frontend - M_091 25-29948:11 - Broken Access Control on LDAP Config - M_092 25-29948:12 - Broken Access Control on REST Application Configuration
A.8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	Sicherheitsprüfverfahren müssen definiert und in den Entwicklungslebenszyklus integriert werden.	Ja	B, R	Sicherheitsprüfverfahren als verpflichtender Prozessschritt in Entwicklungslebenszyklus integriert. Projektaudit-Checkliste zur systematischen Überprüfung. Ab Kritikalität niedrig: Code-Reviews empfohlen. Ab Kritikalität mäßig: Tests vor Freigabe, Qualitätssicherung mit Sicherheitsaspekten, regelmäßige Bibliotheken-Prüfung. Ab Kritikalität hoch: Bedrohungsanalyse, OWASP ASVS. Projektaudit durch ISB/DSB mit SECKT-Unterstützung. Testsysteme für Changes mit mehr als niedrigem Risiko.
A.8.30	Ausgegliederte Entwicklung	Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgegliederten Systementwicklung leiten, überwachen und überprüfen.	Ja	B, R	Prozesse für ausgegliederte Entwicklung dokumentiert, insbesondere für Kundenprojekte. Drei-Stufen-Regelung: 1) Bei Einfluss greift sicherere Vorgabe, 2) Bei Abweichungen: Kunde auf Risiko aufmerksam machen, 3) Bei Risiken für iteratec: Information an Security-Champion, Risikoanalyse. Überwachung: Projektverantwortlicher informiert über Änderungen, Neubewertung bei wesentlichen Änderungen, Dokumentation von Widersprüchen. Unterauftragnehmer: Information des Kunden, DSB-Prüfung auf Datenschutzniveau.

A.8.31	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	Entwicklungs-, Test- und Produktionsumgebungen müssen getrennt und gesichert werden.	Ja	V, B, R	Trennung von Umgebungen in Entwicklungsrichtlinien verankert. Testsysteme bei Changes mit mehr als niedrigem Risiko. Testdaten (ab Kritikalität mäßig): Möglichst keine personenbezogenen Daten, sonst Anonymisierung/Pseudonymisierung. Datenmaskierungs-Richtlinie definiert Verfahren (Pseudonymisierung, synthetische Daten, Verschlüsselung). Zugriffsrechte: Dokumentation und halbjährliche Prüfung. Separate Umgebungen für Entwicklung, Test und Produktion mit Zugriffssteuerung.
A.8.32	Änderungssteuerung	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen müssen Gegenstand von Änderungsmanagementverfahren sein.	Ja	B, R	Umfassendes Change-Management etabliert. 4 Change-Arten: Redaktionell, Standard, Normal, Emergency. 7 Prozessschritte: Antrag, Bewertung, Freigabe, Planung, Umsetzung, Wirksamkeitsprüfung, Kommunikation. Bewertung: Auswirkungen, Schadenshöhe, Risiko, ISB/DSB-Einbeziehung. Freigabe: ISB/DSB haben Vetorecht bei Normal-Changes. Rückfallpläne bei mehr als niedrigem Risiko verpflichtend. Ticketsystem zur Dokumentation, Testsysteme für risikoreichere Changes.
A.8.33	Testdaten	Die Testdaten müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.	Ja	B, R	Anforderungen an Testdaten nach Projektkritikalität gestuft. Grundprinzip (ab mäßig): Möglichst keine personenbezogenen Daten, sonst Anonymisierung/Pseudonymisierung. Datenmaskierung: Identifikation sensibler Daten, Auswahl geeigneter Methoden (Pseudonymisierung, synthetische Daten, Verschlüsselung), Zugriffsbeschränkung, kontinuierliche Überwachung. Schulung aller Mitarbeiter über Bedeutung der Datenmaskierung. Dokumentation aller Schritte, zentrale Ablage. Regelmäßige Überprüfungen der korrekten Anwendung.
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, müssen zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.	Ja	B, R	Audit-Tests nach definierten Prozessen zum Schutz von Produktionssystemen. Projektaudit: ISB/DSB führen Audit durch, Audit-Bericht als Dokumentation. Audit-Vorführung: Ausschließlich in Entwicklungsumgebungen, kein Zugriff auf Produktionssysteme, Vertraulichkeitsschutz durch NDAs. Change-Management für Tests: Bei mehr als niedrigem Risiko Testsystem erforderlich, sonst Begründung und Fallback-Lösung. Bewertung, Freigabe und Wirksamkeitsprüfung verpflichtend. Kommunikation bei mehr als unwesentlichen Auswirkungen.
			Legende:	G	gesetzliche Anforderung
				V	vertragliche Verpflichtung
				B	Anforderung aus Geschäftsprozessen (Business) bzw. der beteiligten Parteien
				R	Aufgrund der Risikobewertung