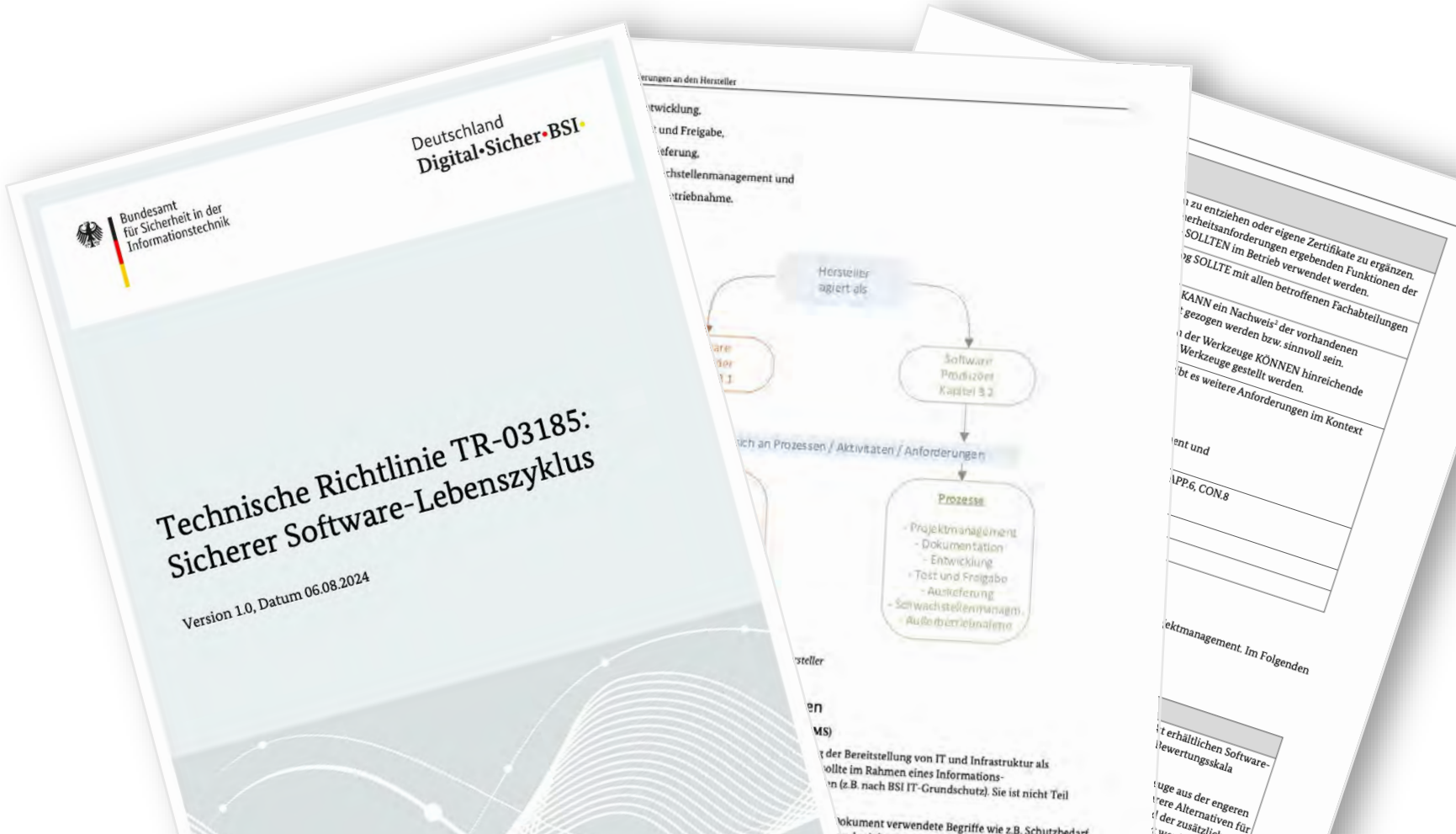
Weg von der BSI-Releaseprüfung mit der BSI TR-3185

Webinar SVDGV



7. Januar 2026

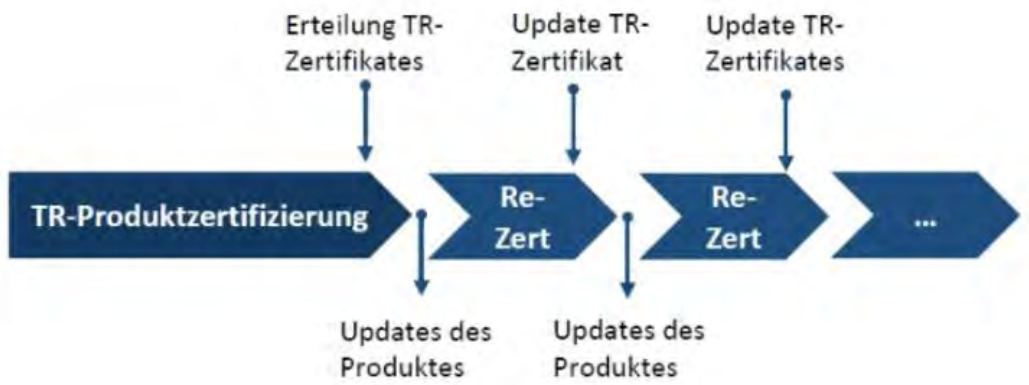
Christoph Twesten

Agenda

- Ausgangssituation nach BSI TR-03161-Zertifizierung
- Vorschlag des SVDGV
- Lösung des BSI
- Inhalt der BSI TR-03185
  - Hersteller als Anwender
  - Hersteller als Produzent
- Rahmenbedingungen der Zertifizierung
- Aktueller Stand

Ausgangssituation

- Nach erfolgreicher Zertifizierung gemäß BSI TR-3161 muss JEDES Release der App vom BSI geprüft werden
- Im „besten“ Fall kostet das 425,- Euro und Zeit (Maintenance-Verfahren)
- Im schlechtesten Fall stuft das BSI die Änderungen als sicherheitsrelevant ein und es erfolgt eine (Teil-)Rezertifizierung



https://www.bsi.bund.de/dok/TR-03185

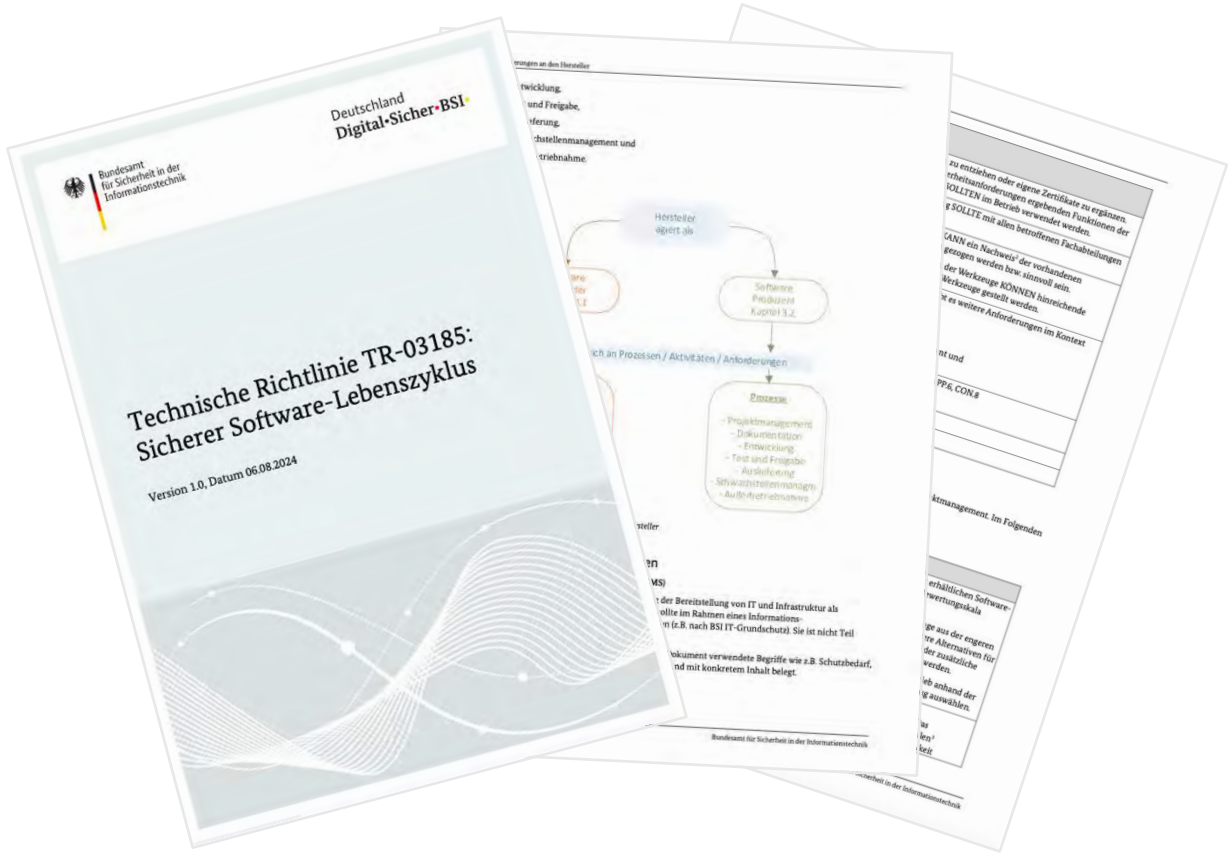
Vorschlag des SVDGV Juni 2025

- Prozesszertifizierung zur Aufrechterhaltung des 3161-Zertifikats
- Im Juni 2025 hatten wir einen Vorschlag eingereicht, der aus einigen Bausteinen des BSI IT-Grundschutz bestand

prozesszertifizierung_bsi_tr-03161.pdf (SVDGV Slack)

Lösung des BSI

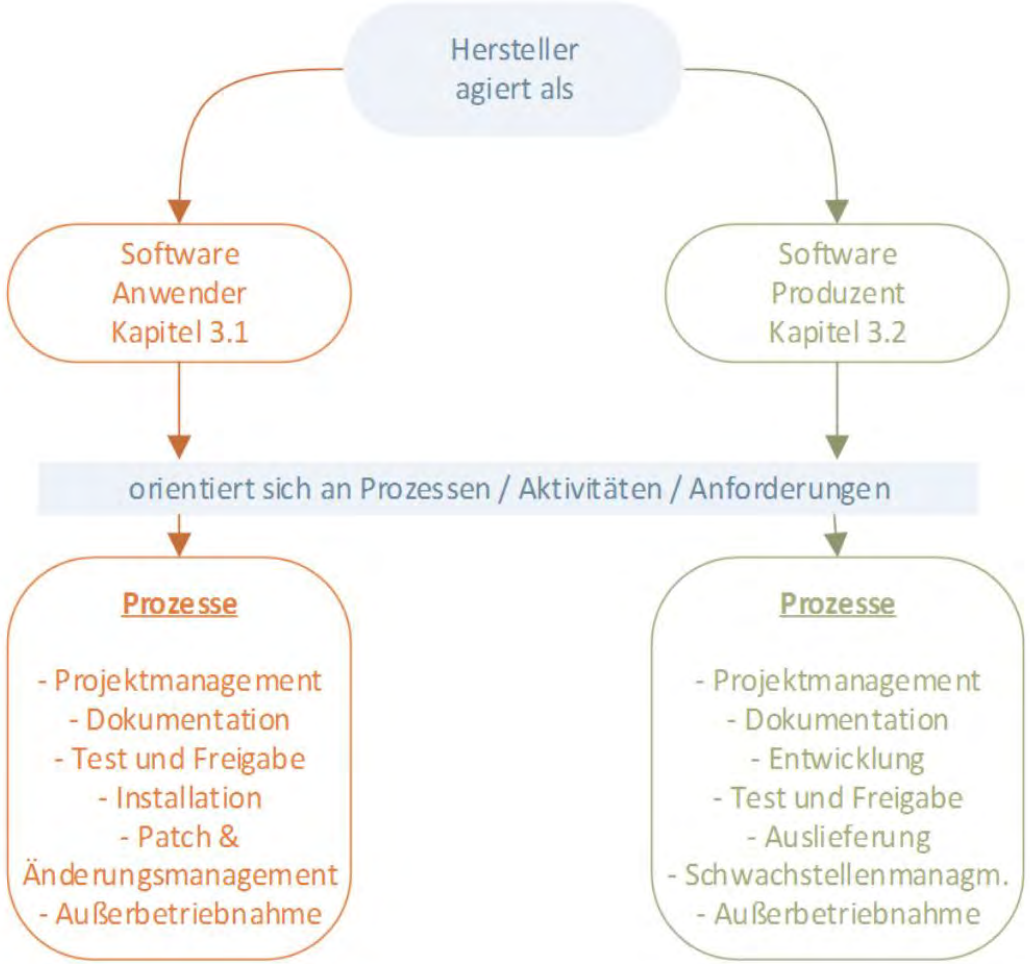
- Prozesszertifizierung zur Aufrechterhaltung des 3161-Zertifikats mit der TR-3185 „Sicherer Software-Lebenszyklus“
- Entwurf 2024 im Rahmen des Cyber-Resilience-Acts
- Besteht aus Bausteinen des BSI IT-Grundschutz



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03185/TR-03185_node.html

Inhalt der TR-3185: Zwei Blickwinkel

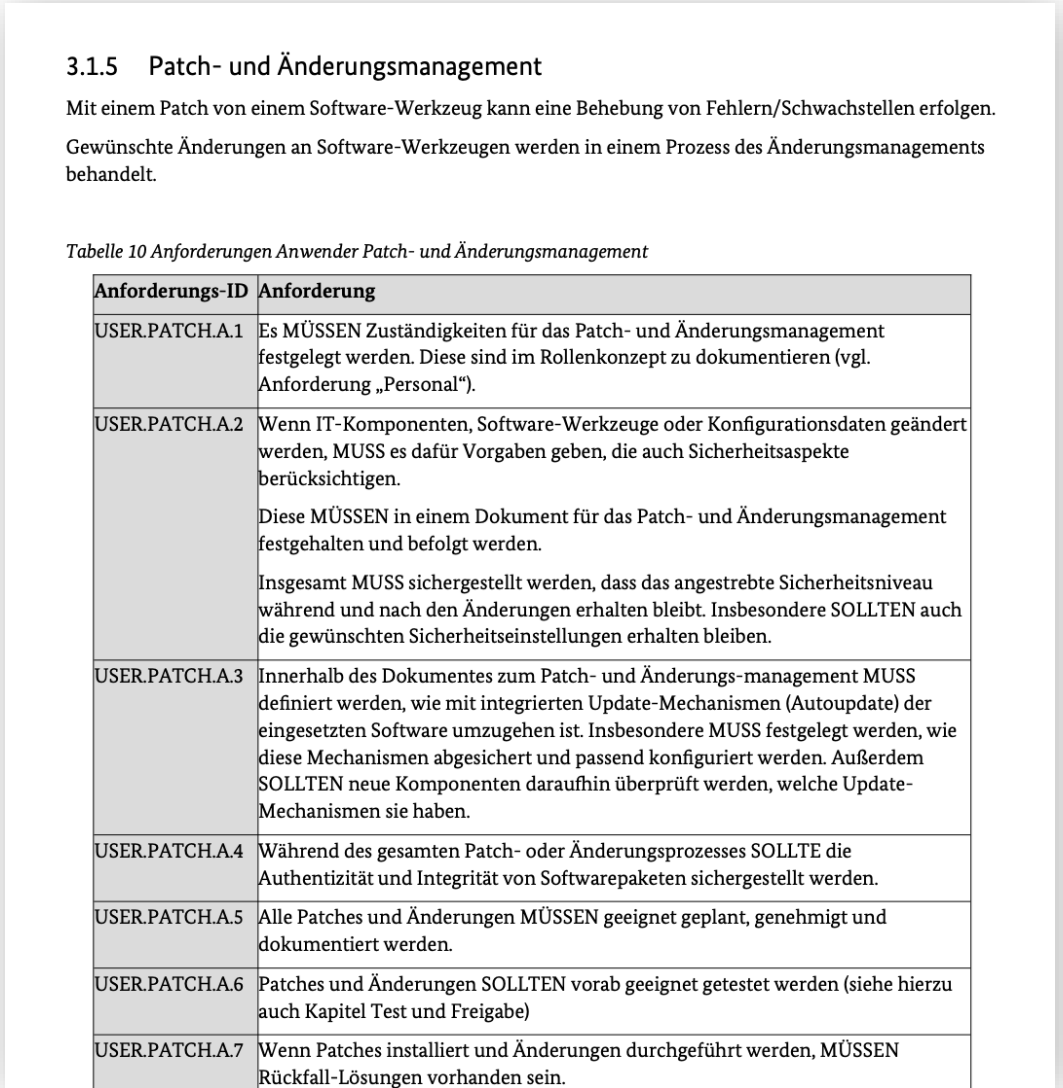
- Hersteller als Anwender
  - Bezieht sich auf Software, die im Entwicklungsprozess eingesetzt wird
- Hersteller als Produzent
  - Bezieht sich auf die eigentliche Herstellung von eigener Software



Hersteller als Anwender

Anforderungen an den Hersteller in der Perspektive als Anwender von Software. Damit sind konkret Werkzeuge zur Unterstützung des Software-Lebenszyklus (z.B. für Projektmanagement, Dokumentation, Entwicklung, Testen, CI/CD) gemeint.

- Projektmanagement (Allgemein, Beschaffung, IT-Betrieb, Personal),
- Dokumentation,
- Test und Freigabe,
- Installation,
- Patch- und Änderungsmanagement,
- Außerbetriebnahme



3.1.5 Patch- und Änderungsmanagement

Mit einem Patch von einem Software-Werkzeug kann eine Behebung von Fehlern/Schwachstellen erfolgen.

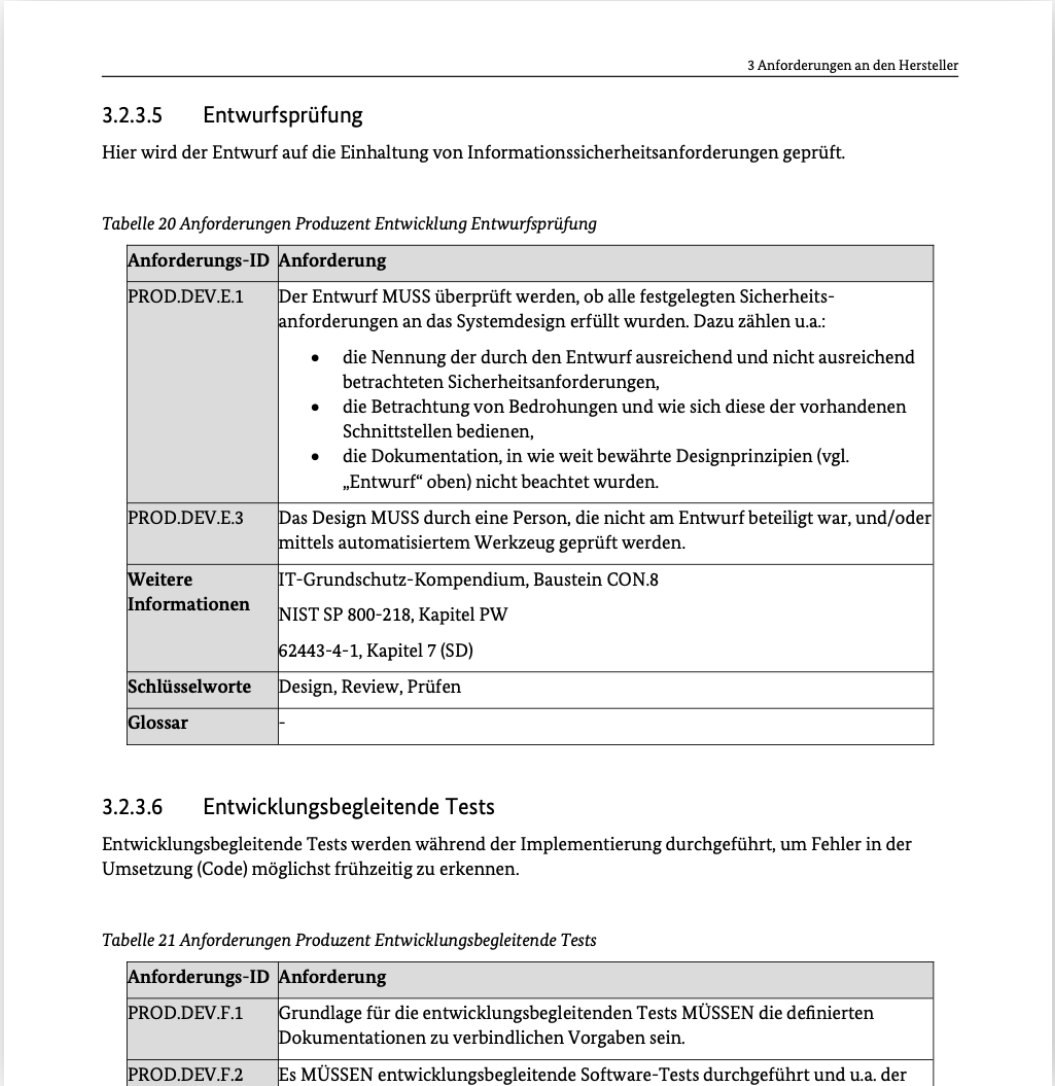
Gewünschte Änderungen an Software-Werkzeugen werden in einem Prozess des Änderungsmanagements behandelt.

Tabelle 10 Anforderungen Anwender Patch- und Änderungsmanagement

Anforderungs-ID	Anforderung
USER.PATCH.A.1	Es MÜSSEN Zuständigkeiten für das Patch- und Änderungsmanagement festgelegt werden. Diese sind im Rollenkonzept zu dokumentieren (vgl. Anforderung „Personal“).
USER.PATCH.A.2	Wenn IT-Komponenten, Software-Werkzeuge oder Konfigurationsdaten geändert werden, MUSS es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Diese MÜSSEN in einem Dokument für das Patch- und Änderungsmanagement festgehalten und befolgt werden. Insgesamt MUSS sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt. Insbesondere SOLLTEN auch die gewünschten Sicherheitseinstellungen erhalten bleiben.
USER.PATCH.A.3	Innerhalb des Dokumentes zum Patch- und Änderungs-management MUSS definiert werden, wie mit integrierten Update-Mechanismen (Autoupdate) der eingesetzten Software umzugehen ist. Insbesondere MUSS festgelegt werden, wie diese Mechanismen abgesichert und passend konfiguriert werden. Außerdem SOLLTEN neue Komponenten daraufhin überprüft werden, welche Update-Mechanismen sie haben.
USER.PATCH.A.4	Während des gesamten Patch- oder Änderungsprozesses SOLLTE die Authentizität und Integrität von Softwarepaketen sichergestellt werden.
USER.PATCH.A.5	Alle Patches und Änderungen MÜSSEN geeignet geplant, genehmigt und dokumentiert werden.
USER.PATCH.A.6	Patches und Änderungen SOLLTEN vorab geeignet getestet werden (siehe hierzu auch Kapitel Test und Freigabe)
USER.PATCH.A.7	Wenn Patches installiert und Änderungen durchgeführt werden, MÜSSEN Rückfall-Lösungen vorhanden sein.

Hersteller als Produzent von Software

- Projektmanagement (Allgemein, Personal),
- Dokumentation (Projektdokumentation, Benutzerdokumentation),
- Entwicklung (Entwicklungsmanagement, Entwurf, Bedrohungsmodellierung, Entwurf/ Architektur, Entwurfsprüfung, Entwicklungsbegleitende Tests, Drittkomponenten, Code Management, Werkzeuge, Inventarisierung),
- Test und Freigabe (Patches und Updates),
- Auslieferung,
- Schwachstellenmanagement,
- Außerbetriebnahme



3.2.3.5 Entwurfsprüfung

Hier wird der Entwurf auf die Einhaltung von Informationssicherheitsanforderungen geprüft.

Tabelle 20 Anforderungen Produzent Entwicklung Entwurfsprüfung

Anforderungs-ID	Anforderung
PROD.DEV.E.1	Der Entwurf MUSS überprüft werden, ob alle festgelegten Sicherheits-anforderungen an das Systemdesign erfüllt wurden. Dazu zählen u.a.: • die Nennung der durch den Entwurf ausreichend und nicht ausreichend betrachteten Sicherheitsanforderungen, • die Betrachtung von Bedrohungen und wie sich diese der vorhandenen Schnittstellen bedienen, • die Dokumentation, in wie weit bewährte Designprinzipien (vgl. „Entwurf“ oben) nicht beachtet wurden.
PROD.DEV.E.3	Das Design MUSS durch eine Person, die nicht am Entwurf beteiligt war, und/oder mittels automatisiertem Werkzeug geprüft werden.
Weitere Informationen	IT-Grundschutz-Kompendium, Baustein CON.8 NIST SP 800-218, Kapitel PW 62443-4-1, Kapitel 7 (SD)
Schlüsselworte	Design, Review, Prüfen
Glossar	-

3.2.3.6 Entwicklungsbegleitende Tests

Entwicklungsbegleitende Tests werden während der Implementierung durchgeführt, um Fehler in der Umsetzung (Code) möglichst frühzeitig zu erkennen.

Tabelle 21 Anforderungen Produzent Entwicklungsbegleitende Tests

Anforderungs-ID	Anforderung
PROD.DEV.F.1	Grundlage für die entwicklungsbegleitenden Tests MÜSSEN die definierten Dokumentationen zu verbindlichen Vorgaben sein.
PROD.DEV.F.2	Es MÜSSEN entwicklungsbegleitende Software-Tests durchgeführt und u.a. der

Rahmenbedingungen der Zertifizierung

- Prozesszertifizierung nach TR-3185 ist prinzipiell **freiwillig**, angesichts der Ausgangssituation aber **quasi alternativlos**.
- Liegt eine Zertifizierung nach der TR-3185 vor, **entfallen Re-Zertifizierungen und Maintenance-Verfahren** nach der TR-3161 sowie die üblichen Änderungsmitteilungen bei Updates/Patches.
- Start des Verfahrens noch für den **Januar 2026** geplant.
- Laufzeit der Zertifikate nach der TR-3185: **3 Jahre** mit jährlichen Überwachungs-Audits (Managementsystemzertifizierung).
- Für die Auditierung wird auf **BSI-Grundschutz-Auditoren** zurückgegriffen, eine Liste der möglichen Auditoren wird zeitnah vom BSI bereitgestellt.

Aktueller Stand

- **Start** des Verfahrens wird **im Laufe des Januars** 2026 bekanntgegeben.
- Anmeldung beim BSI analog zur TR-3161.
- Liste der Auditoren wird im Laufe des Januars veröffentlicht.
- **Umfang und Art** des Audits: voraussichtlich **Stage 1** (Dokumentenaudit) und **Stage 2** (Prozessprüfung, im direkten Gespräch).
- Aktuell noch **finale Abstimmungen** zwischen BSI und BfArM / BMG
- **Update** der TR-3185 geplant, aber keine grundlegenden Änderungen erwartet.
- **„Pilot“-Projekt** anders als von uns erwartet: bedeutet für das BSI, dass 2-3 Zertifizierungen begleitet werden, um den Prozess zügig zu verbessern.

Schneller und einfacher zur TR-3185

Mit unserer
Experten-Lösung

Praxisnahe KI entwickelt im Herstellerverbund

.PM.C2	werden, welche Arten von So...		teilweise	durch die Supplier-List und SOP...	Approved_Supplier_list, QMSP-SOP-240_Rele...	(Toolchain-Doku...
ER.PM.C3	Bei Verteilung, Betrieb und Pflege der Werkzeu...	SOLLTE	teilweise	Einzelne SOPs und Guidelines beziehen sich auf...	QMSP-SOP-251_Coding_Guidelines, QMSP-SOP-240_R...	Klarstellung und Nach... zur Beachtung des
ER.PM.C4	Es SOLLTEN nur unbedingt notwendige Plug-ins u...	SOLLTE	nicht abgedeckt	Keine explizite Regelung oder Dokumentation bz...	nicht vorhanden	Verbindliche Anweisung Auswahl, Freigab
ER.PM.C5	Das zu entwickelnde Software-Produkt MUSS im E...	MUSS	vollständig	Prozesse zum Datenschutz, sichere Speicherung,...	QMSP-SOP-250_Code_Review, QMSP-SOP-252_Data_Sa...	Keine (Kriterium ert

perfood sidekick LangChain Pinecone Confluence

Schneller und einfacher zur TR-3185

Zügig zum Zertifikat:

Auditfähige Implementierung, strukturiert und mit deutlich reduziertem Aufwand

Effizient:

Analyse und Erweiterung bestehender Managementsysteme (ISMS, QM, MDR)

Höchste Standards:

Identifizierte Lücken systematisch schließen auf BSI-IT-Grundschutz-Niveau

Blended Intelligence:

KI-gestützte Analyse kombiniert mit fundiertem Expertenwissen

16 Jahre DiGA-Expertise

Dr. Tobias Lorenz

Mitgründer und CTO aidhere GmbH

Verantwortung für Produkt, Technik und Regulatorik

Aufbau und Leitung von Software-Entwicklungsteams

Entwicklung von Machine Learning Lösungen für Unternehmen

Dr. Christoph Twesten

Mitgründer und CTO Perfood GmbH

Vorstandsmitglied SVDGV für Ressort Datenschutz / Datensicherheit)

Langjährige Erfahrung mit DiGA, MDR, BSI-Richtlinien und DSGVO

Auditor für KRITIS-Infrastruktur

Blended Intelligence für TR-3185

Jetzt unverbindlich anfragen

Kostenlose GAP-Analyse inklusive
fundierter Experteneinschätzung
(limitiert auf die ersten 5 Anfragen)

slack: DM an Christoph Twesten

mail: info@team3185.de

web: team3185.de

LinkedIn Tobias
LinkedIn Christoph

Danke für die Aufmerksamkeit!

Fragen?