

Elektronische Gesundheitskarte und Telematikinfrastruktur

TI Security Standard

Mitwirkungspflichten für Anbieter

Version: 1.0.0 CC
Revision: 1099314
Stand: 14.01.2025
Status: zur Abstimmung
freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemTI_SEC_Standard

Dokumentinformationen

Änderungen zur Vorversion

Erster initialer Entwurf zur Kommentierung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	10.07.202 4		Erster initialer Entwurf zur Kommentierung	gematik
0.6.0	03.11.202 4		Einarbeitung Kommentare Industrie	gematik
0.7.0	04.12.202 4		Version zur Vorabveröffentlichung	gematik
1.0.0 CC	14.01.202 5		Kommentierung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	5
1.1 Zielsetzung.....	5
1.2 Geltungsbereich.....	5
1.3 Abgrenzung des Dokuments.....	5
1.4 Methodik.....	6
2 Security Governance Level.....	7
3 TI Security Domains.....	10
4 Metadaten zu Controls.....	11
5 Übersicht Controls je Security Governance Level.....	12
6 Controls der Informationssicherheit und des Datenschutzes....	16
6.1 Organisation der Informationssicherheit (OIS).....	17
6.1.1 ISO-27001-Zertifikat.....	17
6.2 Sicherheitsrichtlinien und Arbeitsanweisungen (SP).....	19
6.2.1 Sicherheitskonzept.....	19
6.2.2 Sicherheitskonzeption in gematik Plattform.....	21
6.3 Personal (HR).....	23
6.3.1 Risikobasierte Sicherheitsüberprüfung.....	23
6.3.2 Schulungs- und Sensibilisierungsnachweise.....	24
6.3.3 Rollen- und Rechtekonzept.....	25
6.4 Asset Management (AM).....	27
6.4.1 Halbjährliche Assetübermittlung.....	27
6.4.2 Automatisierte monatliche Assetübermittlung.....	29
6.5 Physische Sicherheit (PS).....	31
6.5.1 Schutzzonenkonzept.....	31
6.6 Regelbetrieb (OPS).....	32
6.6.1 Schwachstellenscans.....	32
6.6.2 Zustimmung zu regelmäßigen Schwachstellenscans.....	33
6.6.3 Automatisierte Übermittlung Ergebnisse von Schwachstellenscans.....	34
6.6.4 Schwachstellenmanagement.....	35
6.6.5 Unverzögliche Bewertung von Schwachstellen.....	36
6.6.6 Meldung von erheblichen Schwachstellen und Bedrohungen.....	37
6.6.7 Entgegennahme und Prüfung von Meldungen der gematik.....	38
6.6.8 Security-Monitoring-Konzept.....	39
6.6.9 Überwachung, Auswertung und Reaktion auf Alarme.....	41
6.6.10 Weiterleitung erkannter Alarme an das TI-SIEM.....	43
6.6.11 Bearbeitungszeiten erkannter Alarme.....	45
6.6.12 Übermittlung an zentralen Log Aggregation Server.....	47

6.6.13 Weiterleitung von Logdaten (Rohdaten) an TI-SIEM.....	48
6.6.14 Weiterleitung von Reports an das TI-SIEM.....	49
6.7 Identitäts- und Berechtigungsmanagement (IDM).....	49
6.8 Kryptographie und Schlüsselmanagement (CRY).....	50
6.8.1 Kryptographie-Konzept.....	50
6.9 Kommunikationssicherheit (COS).....	52
6.9.1 Netzwerkkonzept.....	52
6.10 Portabilität und Interoperabilität (PI).....	53
6.11 Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV).....	53
6.12 Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)	54
6.12.1 Regelmäßiger Security Call.....	54
6.12.2 Teilnahme AK DIS.....	55
6.12.3 Teilnahme an Partnerworkshops.....	56
6.13 Gutachten, Audits und Sicherheitsanalysen.....	57
6.13.1 Bereitstellung Sicherheitsgutachten.....	57
6.13.2 Auditrechte der gematik.....	58
6.13.3 Recht der gematik auf Sicherheitsanalysen.....	60
6.13.4 Maßnahmenumsetzung.....	62
6.13.5 Supply Chain & Third Party Risk.....	64
6.14 Umgang mit Sicherheitsvorfällen (SIM).....	66
6.14.1 Meldung von Sicherheitsvorfällen und Datenschutzverstößen.....	66
6.15 Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM).....	68
6.15.1 Notfallkonzept.....	68
6.15.2 Notfallübungskonzept.....	70
6.15.3 Quartalsweise Notfallübung.....	71
6.16 Compliance (COM).....	72
6.17 Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ).....	72
6.18 Produktsicherheit (PSS).....	72
7 Anhang A.....	73
7.1 A1 - Zuordnung der Anbietertypen zu Security Governance Level.....	73
8 Anhang B - Verzeichnisse.....	75
8.1 B1 - Abkürzungen.....	75
8.2 B2 - Abbildungsverzeichnis.....	75
8.3 B4 - Tabellenverzeichnis.....	75
8.4 B5 - Referenzierte Dokumente.....	76
8.4.1 Dokumente der gematik.....	76
8.4.2 Weitere Dokumente.....	77

1 Einordnung des Dokuments

1.1 Zielsetzung

Das Dokument definiert Mitwirkungspflichten (Controls) die durch Anbieter der Telematikinfrastruktur im operativen Betrieb kontinuierlich, bei bestimmten Ereignissen ad hoc bzw. in regelmäßigen Intervallen zu erfüllen sind, damit die gematik auf dieser Basis die Aufrechterhaltung des erforderlichen Sicherheitsniveaus durch die Anbieter überprüfen kann. Hierdurch kommt die gematik ihrem gesetzlich festgelegten Überwachungs- und Steuerungsauftrag für die Telematikinfrastruktur (Security Governance) gemäß § 311 Nr.1c SGB V sowie § 331 SGB V nach.

Die Controls innerhalb des TI Security Standards orientieren sich eng am internationalen Standard der ISO 27001 und 27002 sowie der Handreichung zum "Stand der Technik" des Bundesverbandes IT Sicherheit e.V.-Teletrust in den jeweils gültigen Versionen. Daneben werden objektive Messkriterien (Key-Performance-Indicator = KPI) definiert, auf deren Basis die gematik ihrer Rolle als Governance Instanz für die Telematikinfrastruktur nachkommt und die Qualität der Mitwirkung im operativen Betrieb der TI bei Anbietern misst und bewertet.

1.2 Geltungsbereich

Dieses Dokument enthält normative Controls zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Das Dokument erlangt mit Veröffentlichung durch die gematik Gültigkeit und Verbindlichkeit. Für die Umsetzung der Controls werden Umsetzungsfristen gewährt, die je Control einzeln definiert sind.

Wichtiger Schutzrechts-/Patentrechtshinweis

Das nachfolgende Dokument ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.3 Abgrenzung des Dokuments

Der TI Security Standard (dieses Dokument) ist als Anhang zur Spezifikation [gemSpec_DS_Anbieter] zu verstehen. Der TI Security Standard ist daher selbst keine Spezifikation, sondern konkretisiert die Mitwirkungspflichten von Anbietern im operativen Betrieb der Telematikinfrastruktur. Daher wird in diesem Dokument als Abgrenzung zur Spezifikation bewusst von Controls statt Anforderungen gesprochen.

1.4 Methodik

Normative Controls werden durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

2 Security Governance Level

Die gematik hat gemäß § 311 Nr.1c SGB V sowie § 331 SGB V den gesetzlichen Auftrag, Vorgaben für den sicheren Betrieb der Telematikinfrastruktur (TI) zu erstellen und die Umsetzung dieser Vorgaben zu überwachen. Security Governance bezeichnet in diesem Kontext die Anforderungen und Controls bzgl. Informationssicherheit und Datenschutz, die die gematik an Anbieter der TI stellt und deren Einhaltung sie kontinuierlich überwacht.

Nicht alle Anbieter stellen gleichermaßen kritische Produkte für die TI bereit. Dies wird im Rahmen der Security Governance berücksichtigt. Daher ist ein Kriterium für die Security Governance der **Schutzbedarf** des Dienstes, der vom Anbieter betrieben wird bzw. werden soll. Da es sich bei den Daten innerhalb der Telematikinfrastruktur in hohem Maße um personenbezogene medizinische Daten handelt, ist die Wahrung der Vertraulichkeit und Integrität von essentieller Bedeutung. Aufgrund der sukzessiven Umstellung von relevanten Versorgungsprozessen im Gesundheitswesen auf digitale Prozesse der Telematikinfrastruktur kommt auch dem Schutzziel der Verfügbarkeit eine besondere Bedeutung zu. Die Bewertung der Kritikalität der Dienste, die von Anbietern betrieben werden, wird in regelmäßigen Abständen überprüft und kann sich auf die Einstufung in Security Governance Level auswirken.

Ein weiteres Kriterium bildet der Grad der **Verantwortung**, den die gematik beim Schutz der jeweiligen Produkte und Dienste trägt. Diese lassen sich in vier Kategorien unterteilen:

1. Von der gematik betriebene oder beauftragte Komponenten und Dienste
Hierbei handelt es sich um Komponenten und Dienste der Telematikinfrastruktur, die von der gematik auf Basis ihres gesetzlichen Auftrags selbst betrieben oder in deren direktem Auftrag betrieben werden.
2. Von der gematik zugelassene Komponenten und Dienste
Hierbei handelt es sich um Komponenten und Dienste der Telematikinfrastruktur, die von der gematik auf Basis ihres gesetzlichen Auftrags zugelassen werden.
3. Von der gematik bestätigte Komponenten und Dienste
Hierbei handelt es sich um Komponenten und Dienste der Telematikinfrastruktur, die von der gematik auf Basis ihres gesetzlichen Auftrags bestätigt werden.
4. Von der gematik registrierte Komponenten und Dienste
Hierbei handelt es sich um Komponenten und Dienste, die nicht direkt zur Telematikinfrastruktur gehören, jedoch über Schnittstellen mit der Telematikinfrastruktur interagieren.

Auf Basis der beiden Kriterien Schutzbedarf und gesetzliche Verantwortung der gematik wurde die nachfolgende Matrix der Security Governance Level entwickelt. Im weiteren Verlauf dient der **Security Governance Level** (nachfolgend SGL) dazu, den Grad der Steuerung und Überwachung der gematik im Security Kontext gegenüber den beauftragten, zugelassenen bzw. bestätigten Anbietern der Telematikinfrastruktur darzustellen.

Gesetzliche Verantwortung gematik	Sehr hoch <small>Dienst wird von gematik betrieben oder beauftragt</small>	3	2	1	1
	Hoch <small>Gesetzliche Anwendung, von der gematik zugelassen</small>	4	3	2	1
	Mittel <small>Mehrwertanwendung, von der gematik bestätigt</small>	5	4	3	2
	Niedrig <small>Anwendungen mit Schnittstellen zur TI</small>	5	5	4	3
		niedrig	mittel	hoch	Sehr hoch

Schutzbedarf des Produktes, das betrieben werden soll (Maximum Prinzip)

Security Governance Level

- 1 Kritisch
- 2 Sehr Hoch
- 3 Hoch
- 4 Mittel
- 5 Gering

Abbildung 1: Festlegung des Security Governance Levels

Jedes Produkt ist hierdurch eindeutig einem SGL zugeordnet. Jede Control innerhalb dieses TI Security Standards ist eindeutig einem Security Governance Level zugeordnet.

Ein Anbieter, der ein Produkt mit einem definierten SGL betreiben möchte, muss daher alle Controls erfüllen, die diesem SGL zugeordnet sind (Anbietertyp).

Im Ergebnis ergibt sich hieraus folgendes Bild:

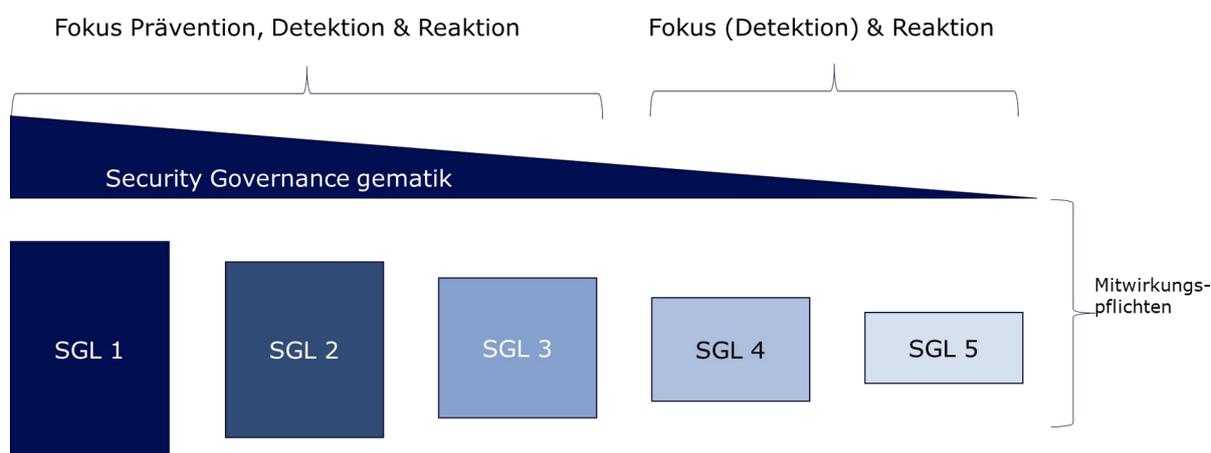


Abbildung 2: Mitwirkungspflichten in Abhängigkeit des SGL

Grundsätzlich gilt:

Je niedriger der SGL, desto mehr Mitwirkungspflichten ergeben sich für den Anbieter im operativen Betrieb und je stärker überwacht die gematik die Einhaltung der Mitwirkungspflichten. Bei SGL 1-3 liegt der Fokus der gematik auf der Kombination aus präventiven, detektiven als auch reaktiven Überwachungswerkzeugen, während bei den Stufen 4-5 der Fokus eher auf der (stichprobenartigen) Detektion und insbesondere Reaktion (z. B. Koordination von Sicherheitsvorfällen) liegt.

Im Anhang A ist die aktuelle Zuordnung der Anbietertypen zu den Security Governance Level dokumentiert.

3 TI Security Domains

Zum sicheren Betrieb der Produkte im Kontext der Telematikinfrastruktur ist es erforderlich, Informationssicherheit ganzheitlich zu betrachten und daher sowohl organisatorische, personelle, physische als auch technische Maßnahmen zu definieren. Hieraus leitet die gematik in Anlehnung an den ISO 27001 Standard sowie des C5-Kriterienkatalogs des BSI folgende TI Security Domains ab, die durch einen Anbieter im Betrieb von Produkten der Telematikinfrastruktur zu erfüllen sind:

- Organisation der Informationssicherheit (OIS)
- Sicherheitsrichtlinien und Arbeitsanweisungen (SP)
- Personal (HR)
- Asset Management (AM)
- Physische Sicherheit (PS)
- Regelbetrieb (OPS)
- Identitäts- und Berechtigungsmanagement (IDM) → aktuell keine Controls
- Kryptographie und Schlüsselmanagement (CRY)
- Kommunikationssicherheit (COS)
- Portabilität und Interoperabilität (PI) → aktuell keine Controls
- Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) → aktuell keine Controls
- Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)
- Umgang mit Sicherheitsvorfällen (SIM)
- Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)
- Compliance (COM) → aktuell keine Controls
- Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ) → aktuell keine Controls
- Produktsicherheit (PSS) → aktuell keine Controls

Bei der Ausgestaltung der Controls wird soweit möglich auf etablierte Standards verwiesen und diese nur (soweit erforderlich) um Konkretisierungen zur Umsetzung des Security Governance Auftrages der gematik ergänzt.

4 Metadaten zu Controls

Jede Control setzt sich neben der Beschreibung Control-Text aus den nachfolgend beschriebenen Informationen/Metadaten zusammen. Diese Metadaten lehnen sich stark an den ISO 27002 Standard (ISO/IEC 27002:2022) an und werden zusätzlich um einige gematik spezifische Metadaten ergänzt:

- Control Type
- Information Security Properties
- Cybersecurity Concepts
- Operational Capabilities
- Security Domain
- Purpose
- Other Information.

Daneben werden folgende gematik spezifische Metadaten mit erhoben:

- Verpflichtend umzusetzen ab Security Governance Level
- Verpflichtende Umsetzung bis
- Referenz (Referenzen auf gängige Standards und Normen)
- gematik KPI (Art der Messung der Erfüllung der Control durch die gematik)
- Verfehlung (Konsequenz der Verfehlung des KPI auf den Security Score bzw. monetäre Sanktion)
- Lieferintervall

5 Übersicht Controls je Security Governance Level

Die nachfolgende Tabelle gibt einen Überblick über die Controls und soll Anbieter dabei unterstützen, die umzusetzenden Controls in Abhängigkeit des Security Governance Levels auf einen Blick zu erfassen. Ein X in der Tabelle bedeutet, dass diese Control auf diesem SGL verbindlich umzusetzen ist. Der Lieferintervall gibt an, in welchen Zeitabständen ein Anbieter den zu einem Control gehörenden Liefergegenstand der gematik zur Verfügung stellen muss.

Tabelle 1: Übersicht der Controls

Control	SGL 1	SGL 2	SGL 3	SGL 4	SGL 5	Lieferintervall
Organisation der Informationssicherheit (OIS)						
ISO-27001-Zertifikat	X	X	X	-	-	jährlich
Sicherheitsrichtlinien und Arbeitsanweisungen (SP)						
Sicherheitskonzept		X	X	-	-	jährlich
Sicherheitskonzeption in gematik Plattform	X	-	-	-	-	jährlich
Personal (HR)						
Risikobasierte Sicherheitsüberprüfung	X	-	-	-	-	Auditprüfung
Schulungs- und Sensibilisierungsnachweise	X	X	X	-	-	Auditprüfung
Rollen- und Rechtekonzept	X	X	X	-	-	Auditprüfung
Asset Management (AM)						
Halbjährliche Assetübermittlung	-	-	-	X	X	halbjährlich
Automatisierte monatliche Assetübermittlung	X	X	X	-	-	monatlich

Physische Sicherheit (PS)						
Schutzzonenkonzept	X	X	X	-	-	Auditprüfung
Regelbetrieb (OPS)						
Zustimmung zu regelmäßigen Schwachstellenscans	X	X	X	X	X	jährlich (Bestätigung)
Automatisierte Übermittlung Ergebnisse von Schwachstellenscans	X	X	X	-	-	monatlich
Unverzögliche Bewertung von Schwachstellen	X	X	X	-	-	ad hoc bei Bedarf
Meldung von erheblichen Schwachstellen und Bedrohungen	X	X	X	X	X	ad hoc bei Bedarf
Entgegennahme und Prüfung von Meldungen der gematik	X	X	X	X	X	Ad hoc bei Bedarf
Security Monitoring Konzept	X	X	X	-	-	jährlich
Überwachung, Auswertung und Reaktion auf Alarme	X	X	X	-	-	ad hoc bei Bedarf
Weiterleitung erkannter Alarme an das TI-SIEM	X	X	X	-	-	kontinuierlich
Bearbeitungszeiten erkannter Alarme	X	X	X	-	-	gemäß Tabelle
Kontinuierliche Weiterleitung von Logdaten auf zentralen Log Aggregation Server	X	-	-	-	-	kontinuierlich
Weiterleitung von Logdaten (Rohdaten) an TI-SIEM	X	X	X	-	-	ad hoc bei Bedarf binnen 48h
Weiterleitung von Reports an das TI-SIEM	X	X	X	-	-	kontinuierlich
Identitäts- und Berechtigungsmanagement (IDM)						

Aktuell keine Controls						
Kryptographie und Schlüsselmanagement (CRY)						
Kryptographie-Konzept	X	X	X	-	-	jährlich
Kommunikationssicherheit (COS)						
Netzwerkkonzept	X	X	X	-	-	jährlich
Portabilität und Interoperabilität (PI)						
Aktuell keine Controls						
Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)						
Aktuell keine Controls						
Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)						
Regelmäßiger Security Call	X	X	X	-	-	monatlich
Teilnahme AK DIS	X	X	X	-	-	halbjährlich
Teilnahme an Partnerworkshops	X	X	X	-	-	jährlich
Bereitstellung Sicherheitsgutachten	X	X	X	-	-	alle drei Jahre
Auditrechte der gematik	X	X	X	X	X	jährlich
Recht der gematik auf Sicherheitsanalysen	X	X	X	X	X	jährlich
Maßnahmenumsetzung	X	X	X	X	X	Gemäß Umsetzungsfristen
Supply Chain & Third Party Risk	X	X	X	X	X	jährlich
Umgang mit Sicherheitsvorfällen (SIM)						
Meldung von Sicherheitsvorfällen und Datenschutzverstößen	X	X	X	X	X	ad hoc gemäß Meldefrist
Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)						

Notfallkonzept	X	X	X	-	-	jährlich
Notfallübungskonzept	X	X	X	-	-	jährlich
Quartalsweise Notfallübung	X	X	X	-	-	quartalsweise
Compliance (COM)						
Aktuell keine Controls						
Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)						
Aktuell keine Controls						
Produktsicherheit (PSS)						
Aktuell keine Controls						

6 Controls der Informationssicherheit und des Datenschutzes

In diesem Kapitel werden die Controls der Informationssicherheit und des Datenschutzes mit allen dazugehörigen Metadaten, sortiert nach den Domains, aufgeführt.

6.1 Organisation der Informationssicherheit (OIS)

6.1.1 ISO-27001-Zertifikat

Tabelle 2: ISO-27001-Zertifikat

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify	Operational Capabilities #Governance	Security Domain #Governance_and_Ecosystem
Control	Der Anbieter MUSS mit der Inbetriebnahme seines TI-Dienstes ein ISO-27001-Zertifikat vorweisen, welches alle Systeme und Prozesse des TI-Produktes abdeckt, die Zertifizierung kontinuierlich aufrechterhalten und der gematik das jeweils aktuell gültige Zertifikat bereitstellen.			
Purpose	Durch die Bereitstellung des ISO-27001-Zertifikats attestiert der Anbieter gegenüber der gematik die Umsetzung eines Informationssicherheitsmanagements.			
Verpflichtend umzusetzen ab Security Governance Stufe	1-3	Verpflichtende Umsetzung bis:	31.12.2025	
Other information	Die Bereitstellung des Zertifikats stellt eine Security Baseline aus Sicht der gematik dar. Für Cloud-Dienste kann auch ein C5-Testat eingereicht werden.			
Referenz	[gemSpec_DS_Anbieter] GS-A_5554 - Aufrechterhaltung der Informationssicherheit und des Datenschutzes [gemSpec_DS_Anbieter] GS-A_4980-02 - Umsetzung der Norm ISO/IEC 27001 [gemSpec_DS_Anbieter] GS-A_4981-01 - Erreichen der Ziele der Norm ISO/IEC 27001 Annex A [gemSpec_DS_Anbieter] GS-A_4982-01 - Umsetzung der Maßnahmen der Norm ISO/IEC 27002 [gemSpec_DS_Anbieter: GS-A_4983-01 - Umsetzung der Maßnahmen aus dem BSI-Grundschutz [ISO/IEC 27001:2022] [C5] OIS-01 Informationssicherheitsmanagementsystem (ISMS) [Teletrust] 3.3.1 Standards und Normen			
Gematik KPI	Aktuell gültiges ISO_27001-Zertifikat des Anbieters liegt vor.			
Verfehlung	To be defined	Lieferintervall	jährlich	

	(tbd)		
--	-------	--	--

6.2 Sicherheitsrichtlinien und Arbeitsanweisungen (SP)

6.2.1 Sicherheitskonzept

Tabelle 3: Sicherheitskonzept

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Governance #Legal_and_compliance #Information_security – assurance	Security Domain #Governance_and – Ecosystem #Resilience
Control	Der Anbieter MUSS eine aktuelle und nachvollziehbare Dokumentation erstellen, pflegen, kontinuierlich weiterentwickeln und der gematik jährlich als PDF bereitstellen. Folgende Mindestinhalte werden erwartet: <ul style="list-style-type: none"> • Systembeschreibung • Asseeterfassung • Dokumentation des Schutzbedarfs • Dokumentation des Business Impacts (BIA) • Sicherheitsanalyse (Verifikation, ob die ergriffenen Sicherheitsmaßnahmen zum Schutz der Assets in Hinblick auf den Schutzbedarf angemessen und ausreichend sind) • (Rest-) Risikoabschätzung 			
Purpose	Die Sicherheitsdokumentation dient dazu sicherzustellen, dass eine Dokumentation der erforderlichen Sicherheitsmaßnahmen zum Schutz des TI-Dienstes beim TI-Anbieter vorliegt und regelmäßig überprüft wird.			
Verpflichtend umzusetzen für Security Governance Stufen	2-3	Verpflichtende Umsetzung bis:	01.08.2025	
Other information	Das Sicherheitskonzept kann auch weitere konzeptionelle Inhalte wie das Rollen- und Rechtekonzept (siehe 6.3.3) enthalten bzw. darauf verweisen.			
Referenz	[ISO 27002:2022] 5.1 Policies for information security [ISO 27002:2022] 5.36 Compliance with policies, rules and standards for information security [C5] SP-01 Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen [C5] SP-02 Überprüfung und Freigabe von Richtlinien und Anweisungen [Teletrust] Management von Informationssicherheitsrisiken			
Gematik KPI	Produktspezifisches Sicherheitskonzept wird jährlich der gematik bereitgestellt.			
Verfehlung	tbd	Lieferintervall	jährlich	

--	--	--	--

6.2.2 Sicherheitskonzeption in gematik Plattform

Tabelle 4: Sicherheitskonzeption in gematik Plattform

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Governance #Legal_and_compliance #Information_security - assurance	Security Domain #Governance_and - Ecosystem #Resilience
Control	<p>Der Anbieter MUSS eine aktuelle und nachvollziehbare Dokumentation innerhalb der von der gematik bereitgestellten Plattform erstellen, pflegen und kontinuierlich weiterentwickeln. Folgende Mindestinhalte werden erwartet:</p> <ul style="list-style-type: none"> • Systembeschreibung • Asseterfassung (Aufteilung des Produkttyps in mehrere Assets, sofern sinnvoll) • Dokumentation des Schutzbedarfs • Dokumentation des Business Impacts (BIA) • Sicherheitsanalyse (Verifikation, ob die ergriffenen Sicherheitsmaßnahmen zum Schutz der Assets in Hinblick auf den Schutzbedarf angemessen und ausreichend sind) • (Rest-) Risikoabschätzung 			
Purpose	<p>Die Sicherheitsdokumentation dient dazu sicherzustellen, dass es eine Dokumentation der erforderlichen Sicherheitsmaßnahmen zum Schutz des TI-Dienstes beim TI-Anbieter gibt, die regelmäßig überprüft wird.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1	Verpflichtende Umsetzung bis:	01.08.2025	
Other information	<p>Das Sicherheitskonzept kann auch weitere konzeptionelle Inhalte wie das Rollen- und Rechtekonzept (siehe 6.3.3) enthalten bzw. darauf verweisen.</p>			
Referenz	<p>[ISO 27002:2022] 5.1 Policies for information security [ISO 27002:2022] 5.36 Compliance with policies, rules and standards for information security [C5] SP-01 Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen [C5] SP-02 Überprüfung und Freigabe von Richtlinien und Anweisungen [Teletrust] Management von Informationssicherheitsrisiken</p>			
Gematik KPI	<p>Produktspezifisches Sicherheitskonzept wird mindestens jährlich in der Plattform der gematik aktualisiert.</p>			
Verfehlung	tbd	Lieferintervall	jährlich (Überarbeitung)	

--	--	--	--

6.3 Personal (HR)

6.3.1 Risikobasierte Sicherheitsüberprüfung

Tabelle 5: Risikobasierte Sicherheitsüberprüfung

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect	Operational Capabilities #Human_resource _security	Security Domain #Governance_and_Ecosystem
Control	Der Anbieter muss jährlich eine dokumentierte Risikobewertung durchführen, ob und wenn ja für welche Mitarbeitenden (die mit Entwicklungs- oder Betriebsaspekten eines TI-Produktes betreut sind) eine Sicherheitsüberprüfung erforderlich ist.			
Purpose	Der Einsatz von vertrauenswürdigen und zuverlässigem Personal ist eine Grundvoraussetzung für die sichere Entwicklung und den sicheren Betrieb von TI-Diensten.			
Verpflichtend umzusetzen für Security Governance Stufen	1	Verpflichtende Umsetzung bis:	30.06.2025	
Other information	Die Bewertung muss alle Rollen umfassen, die im Rollen- und Rechtekonzept aufgeführt sind.			
Referenz	[ISO 27002 2022] 6.2 Terms and conditions of employment [ISO 27002 2022] 6.6 Confidentiality or non-disclosure agreements [C5] HR-01 Überprüfung der Qualifikation und Vertrauenswürdigkeit [Teletrust] 3.3.2 Prozesse			
Gematik KPI	Wird im Rahmen von Audits der gematik geprüft. Sofern keine Abweichung aus einem Audit vorliegt, wird der KPI standardmäßig als erfüllt anerkannt.			
Verfehlung	tbd	Lieferintervall	Anlassbezogen im Rahmen von Audits	

6.3.2 Schulungs- und Sensibilisierungsnachweise

Tabelle 6 : Schulungs- und Sensibilisierungsnachweise

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect	Operational Capabilities #Human_resource - security	Security Domain #Governance_and_ Ecosystem
Control	Der Anbieter MUSS die im Kontext der Entwicklung und des Betriebs eingesetzten Mitarbeitenden initial und nachfolgend regelmäßig (mindestens jährlich) sowohl fachlich als auch in Bezug auf Datenschutz sowie Informationssicherheit schulen und sensibilisieren sowie der gematik einen geeigneten Nachweis bereitstellen.			
Purpose	Der Einsatz von fachlich und in Fragen der Informationssicherheit und des Datenschutzes geschultem Personal ist eine Grundvoraussetzung für die sichere Entwicklung und den sicheren Betrieb von TI-Diensten.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	30.06.2025	
Other information	Der Nachweis kann (sofern aus Datenschutz- oder innerbetrieblichen Erfordernissen erforderlich) in pseudonymisierter Form bereitgestellt werden. Die Bewertung muss alle Rollen umfassen, die im Rollen- und Rechtekonzept aufgeführt sind.			
Referenz	[ISO 27002 2022] 6.3 Information security awareness, education and training [C5] HR-03 Programm zur Sicherheitsausbildung und Sensibilisierung [Teletrust] 3.3.2.12 Schulungen & Awareness [Teletrust] 3.3.7 Personenzertifizierung			
Gematik KPI	Wird im Rahmen von Audits der gematik geprüft. Sofern keine Abweichung aus einem Audit vorliegt wird der KPI standardmäßig als erfüllt anerkannt.			
Verfehlung	tbd	Lieferintervall	Anlassbezogen im Rahmen von Audits	

6.3.3 Rollen- und Rechtekonzept

Tabelle 7: Rollen- und Rechtekonzept

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify	Operational Capabilities #Governance	Security Domain #Governance and Ecosystem #Protection #Resilience
Control	<p>Der Anbieter MUSS sicherstellen, dass einzelne Mitarbeitende (z.B. im Rahmen der Administration verschiedener TI-Produkte) nicht in die Lage versetzt werden, missbräuchlich auf personenbezogene medizinische Daten zuzugreifen.</p> <p>Der Anbieter MUSS auf Basis eines Rollen- und Rechtekonzeptes Identitäten und die Berechtigungen für die Entwicklung und den Betrieb des von ihm verantworteten TI-Produktes an Mitarbeitende vergeben, die vergebenen Identitäten und Berechtigungen regelmäßig hinsichtlich der Erfordernisse überprüfen und bei Bedarf anpassen.</p> <p>Der Anbieter MUSS der gematik eine Dokumentation der im Rahmen der Entwicklung und des Betriebs des TI Betriebs beteiligten Rollen (Rollenkonzept) zur Verfügung stellen. Rollen, deren gleichzeitige Wahrnehmung durch einen Mitarbeitenden nicht erlaubt ist, sind dabei besonders zu kennzeichnen.</p>			
Purpose	<p>Sofern Mitarbeitenden im Rahmen ihrer Tätigkeit im Unternehmen gleichzeitig mehrere Rollen ausfüllen, kann es zu Interessenskonflikten und der Unvereinbarkeit bestimmter Rollenkombinationen kommen. Um diese Unvereinbarkeiten und Interessenskonflikte zu erkennen und wirksam aufzulösen, sollte eine dokumentierte Rollen- und Rechteübersicht inkl. der nicht miteinander vereinbaren Rollen sowie der Mitarbeitenden, die diese Rollen bekleiden, bestehen.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	30.06.2025	
Other information	<p>Neben Rollenausschlüssen und der damit verbundenen Verteilung sicherheitskritischer Aktivitäten auf verschiedene Mitarbeitenden aus unterschiedlichen Geschäftseinheiten sind auch andere wirksame Maßnahmen wie die technische Durchsetzung das Vier-Augen-Prinzips (ggf. auch durch Unterstützung der gematik) oder die von unabhängigen Dritten durchgeführte technische Überwachung von Zugriffen (im Rahmen des Security Monitorings) oder organisatorische Maßnahmen (Audits und Innenrevision) im Rahmen des Konzeptes zu beschreiben.</p> <p>Der Nachweis kann (sofern aus Datenschutz- oder innerbetrieblichen Erfordernissen nicht anders möglich) in pseudonymisierter Form bereitgestellt werden.</p>			
Referenz	<p>[ISO 27002:2022] 5.2 Information security roles and responsibilities [Teletrust] 3.3.10 Absicherung von privilegierten Accounts</p>			

Gematik KPI	Wird im Rahmen von Audits der gematik geprüft. Sofern keine Abweichung aus einem Audit vorliegt wird der KPI standardmäßig als erfüllt anerkannt.		
Verfehlung	tbd	Lieferintervall	Anlassbezogen im Rahmen von Audits

6.4 Asset Management (AM)

6.4.1 Halbjährliche Assetübermittlung

Tabelle 8: Halbjährliche Assetübermittlung

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify	Operational Capabilities #Asset_management	Security Domain #Governance_and_Ecosystem #Protection
Control	Der Anbieter MUSS der gematik halbjährlich eine aktuelle Liste der zur Leistungserbringung von Diensten der TI verwendeten Hard- und Softwareprodukte sowie den zugehörigen TI-Produkttyp übermitteln. Der Anbieter MUSS der gematik regelmäßig und bei Änderungen eine Übersicht über die Außenschnittstellen der Telematikinfrastruktur (IP-Adresse bzw. FQDN), die aus dem Internet erreichbar sind, zur Verfügung stellen.			
Purpose	Die Bereitstellung der Produktinformationen stellt eine Grundlage dar, damit die gematik auf dieser Basis anbieterunabhängig relevante Schwachstellen im TI-Kontext erkennen und bei besonderer Kritikalität eskalieren kann. Die Bereitstellung der Außenschnittstellen ist eine Voraussetzung, damit die gematik auf dieser Basis regelmäßige anbieterunabhängige Schwachstellenscans durchführen kann. Weiterhin kann die gematik diese Informationen für Threat-Intelligence-Maßnahmen verwenden.			
Verpflichtend umzusetzen für Security Governance Stufen	4-5	Verpflichtende Umsetzung bis:	01.02.2025	
Other information	Die zur Verfügung gestellten Produktinformationen (z. B. Betriebssystem, eingesetzte Webserver, Datenbanken, Netzwerkkomponenten inkl. jeweils aktueller Version) dienen dazu, bei Schwachstellen und Sicherheitsvorfällen die Sicherheitslage der TI besser einschätzen und mit Anbietern gezielt Maßnahmen zur Beseitigung der Schwachstellen zeitnah abstimmen zu können. Von Interesse sind hierbei insbesondere exponierte Systeme der TI und Spezialkomponenten, die für die Sicherheit der TI eine besondere Bedeutung haben. Der Detailgrad und das zu verwendende Format der bereitzustellenden Liste der Produktinformationen sind vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte sowie bei Änderungen an bestehenden Produkten mit der gematik abzustimmen. Außenschnittstellen der Telematikinfrastruktur in diesem Kontext sind alle Schnittstellen zum Internet, die direkt oder indirekt zur Bereitstellung des TI-Produktes notwendig sind (z. B. Beantragungsschnittstelle bei TSPs, Zertifikatsaustauschschnittstellen zwischen TSP und Personalisierer).			
Referenz	[ISO 27002 2022] 5.9 Inventory of information and other associated assets			

	[Teletrust] 3.3.2.11 Asset Management [Teletrust] 3.3.12 Software Bill of Materials (SBOM)		
Gematik KPI	Halbjährliche Bereitstellung der Produktinformationen		
Verfehlung	tbd	Lieferintervall	halbjährlich

6.4.2 Automatisierte monatliche Assetübermittlung

Tabelle 9: Automatisierte monatliche Assetübermittlung

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify	Operational Capabilities #Asset_management	Security Domain #Governance_and_Ecosystem #Protection
Control	Der Anbieter MUSS der gematik monatlich CPEs (common platform enumeration) der zur Leistungserbringung von Diensten der TI verwendeten Hard- und Softwareprodukte sowie den zugehörigen TI-Produkttyp automatisiert über den von der gematik bereitgestellten Eingangskanal zur Verfügung stellen. Der Anbieter MUSS der gematik eine abgestimmte maschinenverarbeitbare Übersicht über die Außenschnittstellen der Telematikinfrastruktur (IP-Adresse bzw. FQDN), die aus dem Internet erreichbar sind, automatisiert über den von der gematik bereitgestellten Eingangskanal zur Verfügung stellen.			
Purpose	Die Bereitstellung der Produktinformationen stellt eine Grundlage dar, damit die gematik auf dieser Basis anbieterunabhängig relevante Schwachstellen im TI Kontext erkennen und bei besonderer Kritikalität eskalieren kann.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.08.2025	
Other information	Die zur Verfügung gestellten Produktinformationen (z.B. Betriebssystem, eingesetzte Webserver, Datenbanken, Netzwerkkomponenten inkl. jeweils aktueller Version) dienen dazu, bei Schwachstellen und Sicherheitsvorfällen die Sicherheitslage der TI besser einschätzen zu können und mit Anbietern gezielt Maßnahmen zur Beseitigung der Schwachstellen zeitnah abstimmen zu können. Von Interesse sind hierbei insbesondere exponierte Systeme der TI und Spezialkomponenten, die für die Sicherheit der TI eine besondere Bedeutung haben. Der Detailgrad und das zu verwendende Format der Produktinformationen sind vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten mit der gematik abzustimmen. Die Bereitstellung kann auch kombiniert mit dem Control „Automatisierte Übermittlung Ergebnisse von Schwachstellenscans“ erfolgen.			
Referenz	[ISO 27002 2022] 5.9 Inventory of information and other associated assets [Teletrust] 3.3.2.11 Asset Management [Teletrust] 3.3.12 Software Bill of Matterials (SBOM)			
Gematik KPI	Monatliche automatisierte Bereitstellung der CPE und Außenschnittstellen Informationen liegt vor.			
Verfehlung	tbd	Lieferintervall	monatlich	

--	--	--	--

6.5 Physische Sicherheit (PS)

6.5.1 Schutzzonenkonzept

Tabelle 10: Schutzzonenkonzept

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect	Operational Capabilities #Physical_security #Identity_and_Access – Management	Security Domain #Protection #Resilience
Control	Der Anbieter muss ein Schutzzonenkonzept für den physischen Zutrittsschutz zu seinen Systemen und Versorgungseinrichtungen erstellen und pflegen sowie die daraus abgeleiteten Maßnahmen umsetzen und regelmäßig kontrollieren.			
Purpose	Anbieter müssen angemessene Maßnahmen zum physischen Schutz der Systeme und Versorgungseinrichtungen vor unberechtigtem Zutritt und physischen Schäden (Brand, Wasser, Stromversorgung etc.) treffen. Der physische Schutz von Systemen und Versorgungseinrichtungen, die für die Aufrechterhaltung des Betriebs der Systeme (insbesondere Energie, Kühlung und Brandschutz) erforderlich sind, ist elementar für die Verfügbarkeit aber auch Wahrung der Vertraulichkeit und Integrität der Datenverarbeitung.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.08.2025	
Other information	Das Schutzzonenkonzept muss alle Standorte beinhalten, die für den Betrieb des Produktes erforderlich sind. Das Schutzzonenkonzept kann auch mit anderen Dokumenten wie (Geo-) Redundanzkonzepten kombiniert werden.			
Referenz	ISO 27002 2022: 7.1 Physical security perimeters ISO 27002 2022: 7.2 Physical entry ISO 27002 2022: 7.3 Securing offices, rooms and facilities ISO 27002 2022: 7.6 Working in secure areas ISO 27002 2022: 7.11 Supporting utilities ISO 27002 2022: 7.12 Cabling security ISO 27002 2022: 7.13 Equipment maintenance			
Gematik KPI	Wird im Rahmen von Audits der gematik geprüft. Sofern keine Abweichung aus einem Audit vorliegt, wird der KPI standardmäßig als erfüllt anerkannt.			
Verfehlung	tbd	Lieferintervall	Anlassbezogen im Rahmen von Audits	

--	--	--	--

6.6 Regelbetrieb (OPS)

6.6.1 Schwachstellenscans

Ziel von Schwachstellenscans ist es, ein möglichst vollständiges Bild der aktuellen Schwachstellensituation auf allen Systemen der Telematikinfrastruktur zu erhalten. Dies stellt eine wichtige Basis für die kritikalitätsbasierte Beseitigung von Schwachstellen dar (siehe 6.13.4).

6.6.2 Zustimmung zu regelmäßigen Schwachstellenscans

Tabelle 11: Zustimmung zu regelmäßigen Schwachstellenscans

Control type #Preventive #Detective #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Detect #Respond	Operational Capabilities #Threat_and_vulnerability - management	Security Domain #Defence #Resilience
Control	Der Anbieter MUSS zustimmen, dass die gematik monatliche nicht-invasive Schwachstellenscans auf die Außenschnittstellen ihrer TI-Produkte durchführen darf.			
Purpose	Die regelmäßige anbieterunabhängige Überprüfung der Außenschnittstellen der Telematikinfrastruktur soll dazu beitragen, Schwachstellen und Konfigurationsfehler (z. B. im Zuge eines Changes) rechtzeitig zu erkennen und nachfolgend darauf zu reagieren.			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.12.2024	
Other information	<p>Als Außenschnittstellen werden alle Systeme bezeichnet, die offene eingehende Netzwerkverbindungen aus dem Internet herauslassen und hierdurch auch für einen potenziellen Angreifer unmittelbar erreichbar sind.</p> <p>Die gematik führt die Schwachstellenscans nach initialer Abstimmung mit dem Anbieter und einem Probelauf vollautomatisiert (in der Regel) in den Nebenzeiten durch.</p> <p>Sofern durch den Anbieter gewünscht, stellt die gematik vor dem initialen Scan eine durch beide Seiten zu unterschreibende Vereinbarung zur Durchführung von Schwachstellenscans (Permission to Attack) bereit.</p>			
Referenz	ISO 27002 2022: 5.7 Threat intelligence ISO 27002 2022: 8.8 Management of technical vulnerabilities [Teletrust] 3.3.2.19 Technische Systemaudits			
Gematik KPI	Freigabe vom Anbieter zur Durchführung der Scans ist schriftlich erfolgt.			
Verfehlung	tbd	Lieferintervall	jährlich (Bestätigung)	

6.6.3 Automatisierte Übermittlung Ergebnisse von Schwachstellenscans

Tabelle 12: Automatisierte Übermittlung Ergebnisse von Schwachstellenscans

Control type #Preventive #Detective #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Detect #Respond	Operational Capabilities #Threat_and_vulnerability management	Security Domain #Defence #Resilience
Control	<p>Der Anbieter MUSS mindestens monatlich authentisierte Schwachstellenscans oder vergleichbare Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen („vulnerabilities“) in den vom ihm betriebenen Dienst der TI bzw. RZ-Consumer durchführen.</p> <p>Der Anbieter MUSS der gematik die Ergebnisse von durchgeführten Schwachstellenscans oder der vergleichbaren Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen in maschinenlesbarer Form über eine von der gematik vorgegebene automatisierte Schnittstelle an das TI SIEM der gematik zur Verfügung stellen.</p> <p>Dabei MÜSSEN mindestens die folgenden Inhalte enthalten sein:</p> <ul style="list-style-type: none"> • Scandatum • Titel der Schwachstelle aus dem Schwachstellenscanner • betroffene Umgebung (PU/RU/TU) • betroffenes System Name (interner/externer Name) • betroffenes System Adresse (IP-Adresse) • betroffene Software • eindeutige Bezeichnung der Schwachstelle als CVE oder anderen Identifier • Schweregrad der Schwachstelle als CVSS Score und Severity (nach nist CVSS v3.x/4.0 Ratings) <p>Weitere optionale Daten:</p> <ul style="list-style-type: none"> • Erster Auftritt / Finding der Schwachstelle (first_detected) • Zuletzt entdeckter Auftritt / Finding der Schwachstelle (last_detected) • Information zum Umgang mit der Schwachstelle <p>Wenn keine Schwachstellen gefunden wurden, müssen die Systeme (IP/Name) und Scandatum übertragen werden, die gescannt wurden.</p>			
Purpose	<p>Durch die Bereitstellung der Schwachstellenergebnisse erhält die gematik einen regelmäßigen Überblick über die Gesamtschwachstellensituation der Telematikinfrastruktur.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	3108.2025	

Other information	Durch die automatisierte Übermittlung der Scanergebnisse werden sowohl auf Seiten des Anbieters als auch auf Seiten der gematik Ressourcen eingespart. Weiterhin reduziert die automatische Übermittlung die Wahrscheinlichkeit menschlicher Fehler bei der Bereitstellung.		
Referenz	ISO 27002 2022: 5.7 Threat intelligence ISO 27002 2022: 8.8 Management of technical vulnerabilities [Teletrust] 3.3.2.19 Technische Systemaudits		
Gematik KPI	Pünktliche automatisierte mindestens monatliche Bereitstellung		
Verfehlung	tbd	Lieferintervall	monatlich

6.6.4 Schwachstellenmanagement

Ziel des Schwachstellenmanagements ist es, neue Schwachstellen bzw. Schwachstellen, bei denen sich aufgrund neuer Erkenntnisse (z. B. Exploits) eine signifikante Veränderung der Kritikalität ergibt, zu erkennen, zu analysieren und anschließend risikobasiert zu beheben. Die nachfolgende Abbildung gibt einen Überblick über den Prozess.

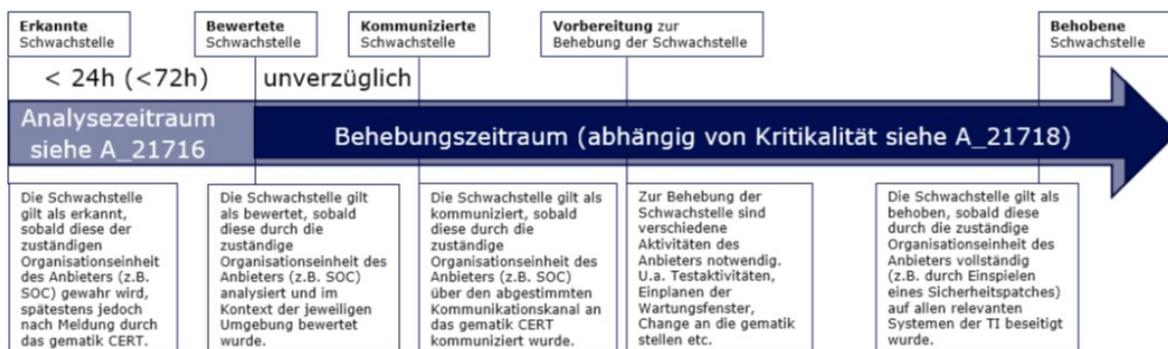


Abbildung 3: Schwachstellenprozess

6.6.5 Unverzögliche Bewertung von Schwachstellen

Tabelle 13: Unverzögliche Bewertung von Schwachstellen

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Threat_and_vulnerability management	Security Domain #Governance_and_Ecosystem #Protection #Defence
Control	Anbieter der TI MÜSSEN erkannte Software-Schwachstellen in den von Ihnen betriebenen Umgebungen der TI unverzüglich nach dem international etablierten Standard Common Vulnerability Scoring System (CVSS) in der jeweils aktuellen Fassung bewerten. Hierbei MUSS eine Reaktionszeit von <24h zur Bewertung der Schwachstellen an Werktagen sowie Bewertung der Schwachstellen an Wochenenden und Feiertagen von <72 h gewährleistet werden.			
Purpose	Die unverzügliche Bewertung von Schwachstellen ist erforderlich, um auf dieser Basis eine risikobasierte Entscheidung anhand des bewerteten CVSS treffen zu können, ob die Schwachstelle im Rahmen des Regelpatchzyklus oder ad hoc im Rahmen eines außerplanmäßigen Patchfensters geschlossen werden muss.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Von der gematik werden in Ausnahmefällen auch vom CVSS-Standard abweichende Bewertungssysteme zur Schwachstellenbewertung akzeptiert, sofern vom Anbieter Transparenz über die Bewertungskriterien hergestellt werden kann.			
Referenz	ISO 27002 2022: 5.7 Threat intelligence ISO 27002 2022: 8.8 Management of technical vulnerabilities [Teletrust] 3.3.5 Schwachstellen- und Patchmanagement			
Gematik KPI	Einhaltung der Fristen zur Bewertung der Schwachstellen. Die Frist startet, sobald die Schwachstelle im Rahmen eines anbieterinternen Schwachstellenscans erkannt wurde oder auf Basis einer Meldung der gematik (siehe Control „Entgegennahme und Prüfung von Meldungen der gematik“).			
Verfehlung	tbd	Lieferintervall	Ad hoc bei Bedarf	

6.6.6 Meldung von erheblichen Schwachstellen und Bedrohungen

Tabelle 14: Meldung von erheblichen Schwachstellen und Bedrohungen

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Threat_and_vulnerability - management	Security Domain #Governance_and_Ecosystem #Protection #Defence
Control	Der TI-Anbieter MUSS kritische und hochbewertete Schwachstellen (CVSS ab 7) und erhebliche Bedrohungen unverzüglich nach Abschluss der Bewertung direkt an die gematik melden.			
Purpose	Die Meldung von kritischen und hochbewerteten Schwachstellen an die gematik ist erforderlich, damit die gematik ihren gesetzlichen Governance-Auftrag für die Telematikinfrastruktur erfüllen kann. Anbieter der Telematikinfrastruktur sind gemäß §329 Abs 2 SGB V verpflichtet, Beeinträchtigungen der Sicherheit unverzüglich an die gematik zu melden. Die gematik ist wiederum verpflichtet, daraus resultierende Beeinträchtigungen der Sicherheit an das BSI zu melden.			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Von der gematik werden in Ausnahmefällen auch vom CVSS-Standard abweichende Bewertungssysteme zur Schwachstellenbewertung akzeptiert, sofern vom Anbieter Transparenz über die Bewertungskriterien hergestellt werden kann. Schwachstellen, die bereits über die automatisierte Übermittlung der Ergebnisse von Schwachstellenscans (siehe 6.6.3) an die gematik gemeldet wurden, müssen nicht zusätzlich manuell gemeldet werden.			
Referenz	ISO 27002 2022: 5.7 Threat intelligence ISO 27002 2022: 8.8 Management of technical vulnerabilities [Teitrust] 3.3.5 Schwachstellen- und Patchmanagement			
Gematik KPI	Unverzügliche Meldefristen von kritischen und hochbewerteten Schwachstellen werden eingehalten.			
Verfehlung	tbd	Lieferintervall	Ad hoc bei Bedarf	

6.6.7 Entgegennahme und Prüfung von Meldungen der gematik

Tabelle 15: Entgegennahme und Prüfung von Meldungen der gematik

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Threat_and_vulnerability _management	Security Domain #Governance_and_Ecosystem #Protection #Defence
Control	Der Anbieter MUSS von der gematik übermittelte Meldungen zu kritischen und hochbewerteten Schwachstellen annehmen, bewerten und der gematik das Ergebnis der Bewertung mit einer Reaktionszeit von <24h Werktagen sowie <72 h an Wochenenden und Feiertagen bereitstellen. Weiterhin MÜSSEN Anbieter der TI das Coordinated Vulnerability Disclosure Programm der gematik aktiv durch ihre Beteiligung unterstützen.			
Purpose	Die Entgegennahme und Prüfung von kritischen und hochbewerteten Schwachstellen der gematik ist erforderlich, um sicherzustellen, dass Schwachstellen nicht unerkannt bleiben und hierdurch eine Gefährdung für die Telematikinfrastruktur entsteht.			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Die Bereitstellung der Bewertungsergebnis gegenüber der gematik erfolgt in der Regel auf Basis des durch den Anbieter angepassten CVSS Scores			
Referenz	ISO 27002 2022: 5.7 Threat intelligence ISO 27002 2022: 8.8 Management of technical vulnerabilities https://nvd.nist.gov/vuln-metrics/cvss [Teletrust] 3.3.5 Schwachstellen- und Patchmanagement			
Gematik KPI	Fristen zur Prüfung inkl. Rückmeldung werden eingehalten.			
Verfehlung	tbd	Lieferintervall	Ad hoc bei Bedarf	

6.6.8 Security-Monitoring-Konzept

Tabelle 16: Security-Monitoring-Konzept

Control type #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security - event_management	Security Domain #Defence
Control	<p>Der Anbieter MUSS vor der Inbetriebnahme seines Produkts die technische Umsetzung des Security Monitorings, die zu überwachenden Systeme, die zu detektierenden Ereignisse auf den jeweiligen Systemen, sowie die begleitenden organisatorischen Maßnahmen (z. B. Vorhaltefristen der detektierten Ereignisse) mit der gematik abstimmen, in einem Security-Monitoring-Konzept dokumentieren und umsetzen.</p> <p>Der Anbieter MUSS regelmäßig und in Abstimmung mit der gematik (mindestens jährlich) die Umsetzung des Security Monitorings überprüfen, erkannte Verbesserungspotenziale etablieren und alle fachlichen Änderungen im Security-Monitoring-Konzept dokumentieren.</p>			
Purpose	<p>Die Abstimmung und Fixierung der Rahmenbedingungen für das Security Monitoring in Form eines Konzeptes dient dazu, ein gemeinsames Verständnis bezüglich der Prozesse und zu übermittelnden Daten zu gewinnen.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	<p>Ziel des Security Monitoring ist es präventive Maßnahmen zur Erkennung, Analyse und Mitigation von Bedrohungen (z. B. über Korrelation und Auswertung von Log-Daten) durchführen.</p> <p>Zu überwachende Systeme sind einerseits insbesondere Firewalls, Application Level Gateways, Proxies und andererseits relevante technische Komponenten zur Absicherung von Übergängen zwischen der Telematikinfrastruktur und dem Internet, da sie neuralgische Punkte für die Sicherheit des Gesamtsystems darstellen und daher besonders geschützt werden müssen. Neben der Absicherung bedeutet dies vor allem auch, dass die Schnittstellen mittels geeigneter Sensoren dahingehend überwacht werden, dass alle sicherheitsrelevanten Aktivitäten erfasst, kontinuierlich und echtzeitnah analysiert sowie erkannte Anomalien eskaliert werden.</p> <p>Darüber hinaus werden auch innerhalb der TI durch verschiedene Systeme besondere sicherheitsrelevante Aktionen durchgeführt. Dazu gehören hauptsächlich Aktionen, bei denen Identitäten zugewiesen, entzogen oder in sonstiger Form verändert werden bzw. der Zugriff(-versuch) auf besonders kritische Systembestandteile (z. B. Nutzung von privatem Schlüsselmaterial). Da eine unautorisierte Nutzung dieser Aktionen die Sicherheitsarchitektur in besonderem Maße gefährdet, müssen auch diese Aktionen kontinuierlich und echtzeitnah auf Anomalien hin überwacht werden.</p>			

Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022 7.4 Physical security monitoring ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM) [Teletrust] 3.2.17 Netzwerküberwachung mittels Intrusion Detection System [Teletrust] 3.2.19 Schutz von Webanwendungen		
Gematik KPI	Das Security-Monitoring-Konzept wird der gematik jährlich in aktualisierter Form zur Verfügung gestellt.		
Verfehlung	tbd	Lieferintervall	jährlich

6.6.9 Überwachung, Auswertung und Reaktion auf Alarme

Tabelle 17: Überwachung, Auswertung und Reaktion auf Alarme

Control type #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security - event_management	Security Domain #Defence
Control	Der Anbieter MUSS die in seinem Security-Monitoring-Konzept festgelegten Systeme hinsichtlich sicherheitsrelevanter Ereignisse kontinuierlich und echtzeitnah überwachen. Der Anbieter MUSS die Ergebnisse der Überwachung der in seinem Security-Monitoring-Konzept festgelegten Systeme an zentraler Stelle aggregieren, korrelieren und analysieren. Der Anbieter SOLL dabei mindestens die im Leitfaden Security Monitoring aufgeführten Monitoring Use Cases (Basic) umsetzen. Der Anbieter KANN zusätzlich die im Leitfaden Security Monitoring aufgeführten Monitoring Use Cases (Erweitert) umsetzen. Der Anbieter MUSS auf detektierte Ereignisse (Alarmer) unverzüglich reagieren und verifizieren, ob das Ereignis einen Sicherheitsvorfall darstellt.			
Purpose	Um Anomalien und potenzielle Angriffsversuche zeitnah zu erkennen, ist eine Überwachung, Auswertung und die darauf ggf. folgende Reaktion auf Alarme von entscheidender Bedeutung.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Sofern sich Rahmen der Auswertung der Alarme der Verdacht eines Angriffsversuchs erhärtet, sind diese als Sicherheitsvorfälle an die gematik zu eskalieren. Die Überprüfung der Anforderung erfolgt auf Basis der weitergeleiteten Alarme, Reports und Rohdaten an die gematik.			
Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022 7.4 Physical security monitoring ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM)			
Gematik KPI	Der Anbieter stellt einen Überblick der umgesetzten Security Monitoring Use Cases bereit.			
Verfehlung	tbd	Lieferintervall	jährlich	

--	--	--	--

6.6.10 Weiterleitung erkannter Alarme an das TI-SIEM

Tabelle 18: Weiterleitung erkannter Alarme an das TI-SIEM

Control type #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security _event_management	Security Domain #Defence
Control	Der Anbieter MUSS für in seinem Security-Monitoring-Konzept festgelegten Systeme erkannte Anomalien technisch automatisiert über die von der gematik angebotene Schnittstelle an das TI-SIEM System übermitteln.			
Purpose	<p>Die Weiterleitung erkannter Alarme dient dazu, dass die gematik anbieterübergreifend Anomalien und Angriffsversuche umgehend erkennen kann. Weiterhin dient die Weiterleitung der Alarme der Verifikation durch die gematik, dass Alarme durch den Anbieter zeitnah und kritikalitätsbasiert bewertet und bei Bedarf eskaliert werden. Muss über eine von der gematik vorgegebene automatisierte Schnittstelle zur Verfügung gestellt werden. Dabei MÜSSEN mindestens die folgenden Inhalte enthalten sein:</p> <ul style="list-style-type: none"> • Eindeutiger Identifier für dieses Event (ID) • Title des Alarms • Bewertung des Schweregrades als Severity (Critical, High, Medium, Low, None) • betroffene Umgebung (PU/RU/TU) • betroffenes System Name (interner/externer Name) • betroffenes System Adresse (IP-Adresse), • Status (z.B. open, pending, reopen, closed) • Timestamp der Änderung des Status • Bemerkung (Beschreibung der Analyse und des Ergebnisses) 			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Neben dem Alarm sind auch der Bearbeitungsstatus sowie die Bewertung des Alarms durch den Security-Analysten mit zu übermitteln, wobei jede Statusaktualisierung ebenfalls mit zu übermitteln ist.			

Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022: 7.4 Physical security monitoring ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM)		
Gematik KPI	Alarmer werden kontinuierlich an das TI-SIEM-System übertragen		
Verfehlung	tbd	Lieferintervall	Kontinuierlich

6.6.11 Bearbeitungszeiten erkannter Alarme

Tabelle 19: Bearbeitungszeiten erkannter Alarme

Control type #Detective #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security_event_management	Security Domain #Defence																				
Control	Der Anbieter MUSS die nachfolgenden Bearbeitungszeiten für die Bewertung und Reaktion von Alarmen in Abhängigkeit der Kritikalität der Alarme umsetzen.																							
	<table border="1"> <thead> <tr> <th data-bbox="371 786 560 875">Kritikalität</th> <th data-bbox="560 786 842 875">Analyse innerhalb</th> <th data-bbox="842 786 1193 875">Abschluss innerhalb</th> <th data-bbox="1193 786 1386 875">Fristverletzung</th> </tr> </thead> <tbody> <tr> <td data-bbox="371 875 560 994">Kritisch</td> <td data-bbox="560 875 842 994">24 h an Werktagen 72 h an Wochenenden und Feiertagen</td> <td data-bbox="842 875 1193 994">48 h an Werktagen 120 h an Wochenenden und Feiertagen</td> <td data-bbox="1193 875 1386 994">Gematik stellt Sicherheitsvorfallsticket an Anbieter</td> </tr> <tr> <td data-bbox="371 994 560 1093">Hoch</td> <td data-bbox="560 994 842 1093">48 h an Werktagen 120 h an Wochenenden und Feiertagen</td> <td data-bbox="842 994 1193 1093">1 Woche</td> <td data-bbox="1193 994 1386 1093">Gematik stellt Sicherheitsvorfallsticket an Anbieter</td> </tr> <tr> <td data-bbox="371 1093 560 1182">Normal</td> <td data-bbox="560 1093 842 1182">2 Wochen</td> <td data-bbox="842 1093 1193 1182">2 Wochen</td> <td data-bbox="1193 1093 1386 1182">Gematik spricht Verletzung im Sec-Call an</td> </tr> <tr> <td data-bbox="371 1182 560 1283">Niedrig</td> <td data-bbox="560 1182 842 1283">Keine Vorgabe</td> <td data-bbox="842 1182 1193 1283">4 Wochen</td> <td data-bbox="1193 1182 1386 1283">Gematik spricht Verletzung im Sec-Call an</td> </tr> </tbody> </table>				Kritikalität	Analyse innerhalb	Abschluss innerhalb	Fristverletzung	Kritisch	24 h an Werktagen 72 h an Wochenenden und Feiertagen	48 h an Werktagen 120 h an Wochenenden und Feiertagen	Gematik stellt Sicherheitsvorfallsticket an Anbieter	Hoch	48 h an Werktagen 120 h an Wochenenden und Feiertagen	1 Woche	Gematik stellt Sicherheitsvorfallsticket an Anbieter	Normal	2 Wochen	2 Wochen	Gematik spricht Verletzung im Sec-Call an	Niedrig	Keine Vorgabe	4 Wochen	Gematik spricht Verletzung im Sec-Call an
Kritikalität	Analyse innerhalb	Abschluss innerhalb	Fristverletzung																					
Kritisch	24 h an Werktagen 72 h an Wochenenden und Feiertagen	48 h an Werktagen 120 h an Wochenenden und Feiertagen	Gematik stellt Sicherheitsvorfallsticket an Anbieter																					
Hoch	48 h an Werktagen 120 h an Wochenenden und Feiertagen	1 Woche	Gematik stellt Sicherheitsvorfallsticket an Anbieter																					
Normal	2 Wochen	2 Wochen	Gematik spricht Verletzung im Sec-Call an																					
Niedrig	Keine Vorgabe	4 Wochen	Gematik spricht Verletzung im Sec-Call an																					
Purpose	Die zeitnahe und kritikalitätsbasierte Analyse sowie der Abschluss der Bewertung des Alarms ist erforderlich, um potenzielle Angriffe schnell zu erkennen und im Bedarfsfall darauf zu reagieren.																							
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:		31.03.2025																				
Other information	keine																							
Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022: 7.4 Physical security monitoring																							

	ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM)		
Gematik KPI	Keine Verletzungen der Bewertungs- und Abschlusszeiten		
Verfehlung	tbd	Lieferintervall	Gemäß Tabelle

6.6.12 Übermittlung an zentralen Log Aggregation Server

Tabelle 20: Übermittlung an zentralen Log Aggregation Server

Control type #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security - event_management	Security Domain #Defence
Control	Der Anbieter MUSS die innerhalb der TI-Umgebung entstehenden Logdaten auf ein von der gematik bereitgestelltes zentrales System (Log Aggregation Server) übertragen.			
Purpose	Die Übermittlung von Logdaten auf den Log Aggregation Server dient dazu, der gematik eine anbieterunabhängige Überwachung der Telematikinfrastruktur und Analyse der Daten jederzeit zu ermöglichen, um Anbieter bei Fehleranalysen und Anomalien situativ unverzüglich unterstützen zu können. Weiterhin soll hierdurch die Möglichkeit geschaffen werden, jederzeit Stichproben der Logdaten für Sicherheitsanalysen ziehen zu können.			
Verpflichtend umzusetzen für Security Governance Stufen	1	Verpflichtende Umsetzung bis:	31.08.2025	
Other information	Die zu übermittelnden Logdaten werden bilateral zwischen gematik und dem Anbieter abgestimmt. Im Fokus stehen insbesondere Firewalls an den Außenschnittstellen zum Internet, sowie Webserver, die Anfragen aus dem Internet annehmen.			
Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022: 7.4 Physical security monitoring ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM)			
Gematik KPI	Kontinuierliche Übermittlung der Daten wird seitens des Anbieters gewährleistet.			
Verfehlung	tbd	Lieferintervall	kontinuierlich	

6.6.13 Weiterleitung von Logdaten (Rohdaten) an TI-SIEM

Tabelle 21: Weiterleitung von Logdaten (Rohdaten) an TI-SIEM

Control type #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security - event_management	Security Domain #Defence
Control	Der Anbieter MUSS der gematik auf Nachfrage Rohdaten für die in seinem Security-Monitoring-Konzept festgelegten Systeme automatisiert über die von der gematik angebotene Schnittstelle an das TI-SIEM-System übermitteln.			
Purpose	Die Übermittlung der Rohdaten dient der Verifikation und kontinuierlichen Verbesserung der bestehenden Schwell- und Messwerte. Weiterhin können hierdurch potenzielle Sicherheitsvorfälle auch auf Seiten der gematik analysiert werden.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	keine			
Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022: 7.4 Physical security monitoring ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM)			
Gematik KPI	Übermittlung wird innerhalb von 48h nach Anforderung der gematik umgesetzt.			
Verfehlung	tbd	Lieferintervall	Ad hoc bei Bedarf binnen 48h	

6.6.14 Weiterleitung von Reports an das TI-SIEM

Tabelle 22: Weiterleitung von Reports an das TI-SIEM

Control type #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Detect #Respond	Operational Capabilities #Information_security - event_management	Security Domain #Defence
Control	Der Anbieter MUSS für die in seinem Security-Monitoring-Konzept festgelegten Systeme aggregierte Informationen (Reports) technisch automatisiert über die von der gematik angebotene Schnittstelle an das TI-SIEM-System übermitteln.			
Purpose	Die Übermittlung der Reports dient der zusammengefassten Übermittlung von Logdaten mit dem Ziel, sicherheitsrelevante Trends (z. B. Anzahl abgelehnter Zugriffe über einen bestimmten Zeitraum) erkennen und bewerten zu können.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	keine			
Referenz	ISO 27002: 2022: 5.25 Assessment and decision on information security events ISO 27002 2022: 5.28 Collection of evidence ISO 27002 2022: 7.4 Physical security monitoring ISO 27001 2022: 8.7 Protection against malware ISO 27001 2022: 8.12 Data leakage prevention ISO 27001 2022: 8.15 Logging ISO 27001 2022: 8.16 Monitoring activities [Teletrust] 3.2.24 Angriffserkennung und Auswertung (SIEM)			
Gematik KPI	Fristgerechte monatliche Übermittlung der abgestimmten Reports.			
Verfehlung	tbd	Lieferintervall	kontinuierlich	

6.7 Identitäts- und Berechtigungsmanagement (IDM)

Aktuell keine Controls.

6.8 Kryptographie und Schlüsselmanagement (CRY)

6.8.1 Kryptographie-Konzept

Tabelle 23: Kryptographie-Konzept

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect	Operational Capabilities #Secure_configuration	Security Domain #Protection
Control	<p>Der Anbieter MUSS die im Rahmen der TI verwendeten kryptographischen Verfahren sowie die Prozesse zum sicheren Einsatz dieser Verfahren in einem Kryptographie-Konzept dokumentieren, umsetzen und regelmäßig auf Aktualität und Wirksamkeit überprüfen. Folgende Aspekte MÜSSEN mindestens innerhalb des Konzeptes dokumentiert werden:</p> <ul style="list-style-type: none"> • Eingesetzte kryptographische Verfahren inkl. Ausprägung (Schlüssellängen, Modus) • Eingesetzte kryptographische Systeme (insbesondere HSMs) • Beschreibung der Prozesse zur Erzeugung, Einsatz und Außerbetriebnahme von kryptographischen Schlüsseln (Life-Cycle-Management) • Besondere Maßnahmen zum Schutz privater Schlüssel 			
Purpose	<p>Kryptographische Verfahren leisten innerhalb der Telematikinfrastruktur einen erheblichen Beitrag zum Schutz medizinischer personenbezogener Informationen. Daher ist es erforderlich, dass Anbieter der TI die Verfahren und deren Prozesse zum Einsatz im Kontext der TI beschreiben und umsetzen.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.08.2025	
Other information	keine			
Referenz	ISO 27002 2022: 8.24 Use of cryptography [Teletrust] 3.2.4 Kryptographische Verfahren gemSpec_Krypt			
Gematik KPI	Jährliche Bereitstellung des Kryptographie-Konzeptes gegenüber der gematik			
Verfehlung	tbd	Lieferintervall	jährlich	

6.9 Kommunikationssicherheit (COS)

6.9.1 Netzwerkkonzept

Tabelle 24: Netzwerkkonzept

Control type #Preventive #Detective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect #Detect	Operational Capabilities #System_and_network - security	Security Domain #Protection
Control	Der Anbieter MUSS Maßnahmen zur Absicherung und Segmentierung der Netzbereiche, in denen Dienste der TI betrieben werden, treffen. Der Anbieter MUSS Netzwerke, in denen Produkte der TI betrieben werden, einschließlich deren Sicherheitsmaßnahmen in einem Netzwerkkonzept beschreiben. Folgende Aspekte MÜSSEN mindestens innerhalb des Konzeptes dokumentiert werden: <ul style="list-style-type: none"> • Netzwerkplan als grafischer Überblick • Absicherung der Netzwerkgrenzen und Netzsegmentierung • Absicherung administrativer Zugriffsmöglichkeiten • Netzwerkmanagement • Eingesetzte Systeme zur Gewährleistung der Netzwerksicherheit (Firewalls, ALG, NIDS etc.) • Maßnahmen zur Netzwerküberwachung 			
Purpose	Die Absicherung von Netzen, in denen Produkte der TI betrieben werden, sowohl in Richtung WAN als auch in Richtung anderer interner (Management) Netze/LAN, ist ein elementarer Aspekt zum Schutz der Produkte der TI innerhalb dieser Netze.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.08.2025	
Other information	keine			
Referenz	ISO 27002 2022: 8.20 Networks security ISO 27002 2022: 8.21 Security of network services ISO 27002 2022: 8.22 Segregation of networks ISO 27002 2022: 8.23 Web filtering [Teletrust] 3.2.30 Netzwerksegmentierung und Separierung			
Gematik KPI	Jährliche Bereitstellung des Netzwerkkonzeptes gegenüber der gematik			
Verfehlung	tbd	Lieferintervall	jährlich	

6.10 Portabilität und Interoperabilität (PI)

Aktuell keine Controls.

6.11 Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)

Aktuell keine Controls.

6.12 Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)

6.12.1 Regelmäßiger Security Call

Tabelle 25: Regelmäßiger Security Call

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect #Respond #Recover	Operational Capabilities #Governance	Security Domain #Defence #Resilience
Control	Der Anbieter muss die Teilnahme an regelmäßigen Security Calls (i. d. R. monatlich virtuell) ermöglichen.			
Purpose	Die regelmäßige Abstimmung zwischen Anbietern und gematik im Kontext der Informationssicherheit und des Datenschutzes ist erforderlich, um kontinuierlich die Sicherheitslage abzugleichen, die partnerschaftliche Zusammenarbeit und den kontinuierlichen Verbesserungsprozess zu fördern.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3		Verpflichtende Umsetzung bis:	31.03.2025
Other information	Sofern die Ziele der Zusammenarbeit und des Austausches auch auf anderem Wege erreicht werden können, kann die gematik auf die Teilnahme des Anbieters an den Security Calls verzichten.			
Referenz	ISO 27002:2022 5.5 Contact with authorities			
Gematik KPI	Teilnahme durch den Anbieter wird gewährleistet (maximal 2 Terminabsagen pro Jahr seitens des Anbieters).			
Verfehlung	tbd		Lieferintervall	monatlich

6.12.2 Teilnahme AK DIS

Tabelle 26: Teilnahme AK DIS

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect #Respond #Recover	Operational Capabilities #Governance	Security Domain #Defence #Resilience
Control	Der Anbieter muss die Teilnahme am Arbeitskreis Datenschutz und Informationssicherheit (AK DIS) (i. d. R. halbjährlich in Präsenz) ermöglichen.			
Purpose	Die regelmäßige Abstimmung zwischen Anbietern und gematik innerhalb des AK DIS ist erforderlich, um den anbieterübergreifenden Austausch zu fördern.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Sofern die Ziele der Zusammenarbeit und des Austausches auch auf anderem Wege erreicht werden können, kann die gematik auf die Teilnahme des Anbieters an den Präsenzveranstaltungen verzichten.			
Referenz	ISO 27002:2022 5.5 Contact with authorities			
Gematik KPI	Teilnahme durch den Anbieter wird gewährleistet (keine Verfehlung i. d. R. 2/2)			
Verfehlung	tbd	Lieferintervall	halbjährlich	

6.12.3 Teilnahme an Partnerworkshops

Tabelle 27: Teilnahme an Partnerworkshops

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect #Respond #Recover	Operational Capabilities #Governance	Security Domain #Defence #Resilience
Control	Der Anbieter muss die Teilnahme Partnerworkshops (i. d. R. einmal pro Jahr in Präsenz) ermöglichen.			
Purpose	Die persönliche intensive Abstimmung zwischen Anbieter und gematik im Rahmen des Partnerworkshops ist erforderlich, um Verbesserungspotenziale zu erkennen und die Zusammenarbeit zu fördern.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Der Partnerworkshop findet sofern nicht anders besprochen in den Geschäftsräumen des Anbieters statt.			
Referenz	ISO 27002:2022 5.5 Contact with authorities			
Gematik KPI	Teilnahme durch den Anbieter wird gewährleistet (keine Verfehlung i. d. R. 1/1)			
Verfehlung	tbd	Lieferintervall	jährlich	

6.13 Gutachten, Audits und Sicherheitsanalysen

6.13.1 Bereitstellung Sicherheitgutachten

Tabelle 28: Bereitstellung Sicherheitgutachten

Control type #Preventive	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify	Operational Capabilities #Legal_and_compliance	Security Domain #Governance_and_Ecosystem #Protection
Control	Der Anbieter MUSS der gematik erstmalig (für Zulassungsnehmer im Rahmen der Zulassung), anschließend alle drei Jahre und bei signifikanten Änderungen ein betriebliches Sicherheitgutachten einreichen.			
Purpose	Das Vorlegen von Nachweisen ist zur Verifikation der erfolgreichen Maßnahmenumsetzung durch die gematik erforderlich.			
Verpflichtend umzusetzen für Security Governance Stufen	1-4	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	keine			
Referenz	Zulassungsvertrag			
Gematik KPI	Sicherheitgutachten werden der gematik fristgerecht bereitgestellt.			
Verfehlung	tbd	Lieferintervall	Alle drei Jahre	

6.13.2 Auditrechte der gematik

Tabelle 29: Auditrechte der gematik

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Information_security – assurance	Security Domain #Governance_and – Ecosystem
Control	Der Anbieter MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt ist: <ul style="list-style-type: none"> • pro Kalenderjahr maximal ein Regelaudit durchzuführen. Hiervon unbenommen ist das Recht der gematik, anlassbezogene Audits durchzuführen, • im Rahmen eines Audits beim Anbieter die konkrete Umsetzung der an den Anbieter gestellten Anforderungen der TI zu überprüfen, • im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Anbieters zu betreten und • im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu erhalten. 			
Purpose	Audits (in der Regel vor Ort beim Anbieter) dienen dazu, die Einhaltung der an den Anbieter gestellten Anforderungen zu verifizieren.			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Die gematik wird ein Regelaudit standardmäßig drei Monate vor der Durchführung beim Anbieter ankündigen. Die Terminvereinbarung erfolgt im gegenseitigen Einvernehmen. Die gematik erstellt im Vorfeld einen Auditplan, in dem der Umfang und die zu betrachtenden Themenbereiche festgelegt sind und stimmt den Auditplan mit dem Anbieter ab. Die gematik muss das Auditrecht nicht notwendigerweise jedes Jahr wahrnehmen. Der Anbieter MUSS die Berechtigung zur Durchführung und Unterstützung von Audits im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Anbieter durch diese Mitwirkungspflichten entstehen, trägt der Anbieter selbst.			
Referenz	gemSpec_DS_Anbieter GS-A_27099 Audits und Sicherheitsanalysen ISO 27002_2022: 5.35 Independent review of information security [Teletrust] 3.3.2.20 Interne und externe Audits, ISMS-Zertifizierung			
Gematik KPI	Auditrecht wird durch den Anbieter fristgerecht (mit Vorlauf von 3 Monaten) eingeräumt.			
Verfehlung	tbd	Lieferintervall		jährlich

--	--	--	--

6.13.3 Recht der gematik auf Sicherheitsanalysen

Tabelle 30: Recht der gematik auf Sicherheitsanalysen

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Information_security – assurance	Security Domain #Governance_and – Ecosystem
Control	<p>Der Anbieter MUSS für sein Produkt zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt ist,</p> <ul style="list-style-type: none"> • pro Kalenderjahr maximal eine Sicherheitsanalyse (z. B. Penetrationstests) zu seinem Produkt durchzuführen; hiervon unbenommen ist das Recht der gematik, eine anlassbezogene Sicherheitsanalyse durchzuführen, • die konkrete Umsetzung der an das Produkt gestellten Anforderungen zu überprüfen, • die Sicherheitsanalysen zu unterstützen. 			
Purpose	<p>Sicherheitsanalysen haben das Ziel, die sichere technische Umsetzung der Produkte mit besonderem Fokus auf Angriffe zu überprüfen.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	<p>Die gematik wird Sicherheitsanalysen in der Regel drei Monate vor der Durchführung beim Anbieter ankündigen. Die Terminvereinbarung erfolgt im gegenseitigen Einvernehmen. Die gematik erstellt im Vorfeld einen Plan, in dem der Umfang und die zu betrachtenden Produkte festgelegt sind und stimmt diesen Plan mit dem Anbieter ab. Die gematik muss das Recht zur Durchführung von Sicherheitsanalysen nicht notwendigerweise jedes Jahr wahrnehmen. Zur Unterstützung der Sicherheitsanalysen zählt u. a. die Teilnahme an vorbereitenden Abstimmungsterminen sowie die Bereitstellung aller für die Durchführung benötigten Informationen, insbesondere Informationen über das zu testende System inkl. Zugriffsmöglichkeiten sowie Zugangsdaten. Der Anbieter MUSS die Berechtigung zur Durchführung und Unterstützung von Sicherheitsanalysen im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Anbieter durch diese Mitwirkungspflichten entstehen, trägt der Anbieter selbst.</p>			
Referenz	<p>gemSpec_DS_Anbieter GS-A_27099 Audits und Sicherheitsanalysen ISO 27002 2022: 5.35 Independent review of information security [Teletrust] 3.3.2.19 Technische Systemaudits</p>			

Gematik KPI	Recht zur Durchführung von Sicherheitsanalysen wird durch den Anbieter fristgerecht (mit Vorlauf von 3 Monaten) eingeräumt.		
Verfehlung	tbd	Lieferintervall	jährlich

6.13.4 Maßnahmenumsetzung

Tabelle 31 : Maßnahmenumsetzung

Control type #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Threat_and_vulnerability _management	Security Domain #Governance_and_Ecosystem #Protection #Defence																				
Control	<p>Der Anbieter MUSS von der gematik übermittelte Feststellungen aus Sicherheitsanalysen, Audits und Notfallübungen annehmen, bewerten und der gematik das Ergebnis der Bewertung mit einer Reaktionszeit von 10 Werktagen bereitstellen.</p> <p>Der Anbieter MUSS Maßnahmen (insbesondere zur Behebung von Feststellungen aus Sicherheitsanalysen, Audits, Notfallübungen sowie Sicherheitsvorfällen und Schwachstellen)</p> <ul style="list-style-type: none"> • mit der gematik abstimmen • die erforderlichen Maßnahmen fristgerecht umsetzen, • den Abschluss der Maßnahmenumsetzung an die gematik melden, • der gematik auf Verlangen Nachweise der erfolgreichen Umsetzung von abgestimmten Maßnahmen bereitstellen. <p>Dabei SOLL die Einhaltung folgender Umsetzungsfristen in Abhängigkeit der Kritikalität gewährleistet werden:</p> <table border="1" data-bbox="379 1205 1385 1832"> <thead> <tr> <th>Kategorie</th> <th>Feststellung</th> <th>CVSS (bewertet)</th> <th>Umsetzungsfrist</th> </tr> </thead> <tbody> <tr> <td>Kritisch</td> <td>Kritische Abweichung</td> <td>9,0 - 10</td> <td>Unverzüglich, Individualvereinbarung mit gematik</td> </tr> <tr> <td>Schwer</td> <td>Hauptabweichung</td> <td>7,0 - 8,9</td> <td>1 Monat</td> </tr> <tr> <td>Mittel</td> <td>Nebenabweichung</td> <td>4,0 - 6,9</td> <td>1 Quartal</td> </tr> <tr> <td>Niedrig</td> <td>Hinweis</td> <td>0,1 - 3,9</td> <td>Individualvereinbarung ggf. optional</td> </tr> </tbody> </table>				Kategorie	Feststellung	CVSS (bewertet)	Umsetzungsfrist	Kritisch	Kritische Abweichung	9,0 - 10	Unverzüglich, Individualvereinbarung mit gematik	Schwer	Hauptabweichung	7,0 - 8,9	1 Monat	Mittel	Nebenabweichung	4,0 - 6,9	1 Quartal	Niedrig	Hinweis	0,1 - 3,9	Individualvereinbarung ggf. optional
Kategorie	Feststellung	CVSS (bewertet)	Umsetzungsfrist																					
Kritisch	Kritische Abweichung	9,0 - 10	Unverzüglich, Individualvereinbarung mit gematik																					
Schwer	Hauptabweichung	7,0 - 8,9	1 Monat																					
Mittel	Nebenabweichung	4,0 - 6,9	1 Quartal																					
Niedrig	Hinweis	0,1 - 3,9	Individualvereinbarung ggf. optional																					
Purpose	<p>Die fristgerechte Umsetzung von abgestimmten Maßnahmen dient dazu, etwaige Angriffe auf TI-Produkte und damit Schäden für die Telematikinfrastruktur zu minimieren und sicherzustellen, dass keine (Folge-) Schäden oder vergleichbaren Vorfälle eintreten.</p> <p>Das Vorlegen von Nachweisen ist zur Verifikation der erfolgreichen</p>																							

	Maßnahmenumsetzung durch die gematik erforderlich.		
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.03.2025
Other information	<p>Die Umsetzungsfrist der Maßnahmen wird auf Basis der Kritikalität der Umsetzung festgelegt. Dabei beginnt die Frist nach Abschluss der Bewertungszeit. Die gematik ist auf Basis ihres gesetzlichen Auftrags (§329 Absatz 3 SGB V) berechtigt, Anbietern im Zuge der Gefahrenabwehr verbindliche Anweisungen zu erteilen.</p> <p>Bei kritischen Feststellungen oder sofern (z. B. aufgrund fehlender bereitgestellter Sicherheitspatches des Herstellers) eine Behebung innerhalb der definierten Fristen nicht erfolgen kann, ist eine Risikoanalyse in Abstimmung mit der gematik durchzuführen und sind mögliche alternative mitigierende Maßnahmen mit der gematik festzulegen.</p> <p>Nachweise können in Form von zur Verfügung gestellten Dokumentationen, neuen Regelungen oder Prozessen sowie anhand von Auszügen aus der Konfiguration oder Logdaten erbracht werden.</p>		
Referenz	<p>§ 329 SGB V Maßnahmen zur Abwehr von Gefahren für die Funktionsfähigkeit und Sicherheit der Telematikinfrastruktur Art-33-dsgvo ISO 27002 2022: 8.8 Management of technical vulnerabilities https://nvd.nist.gov/vuln-metrics/cvss [Teletrust] 3.3.2.21 Verbesserungsmanagement (kontinuierlicher Verbesserungsprozess)</p>		
Gematik KPI	Festgelegte Frist zur Umsetzung der Maßnahme(n) wird eingehalten. Nachweis der Maßnahmenumsetzung wird bereitgestellt.		
Verfehlung	tbd	Lieferintervall	Gemäß Umsetzungsfristen

6.13.5 Supply Chain & Third Party Risk

Tabelle 32 : Supply Chain & Third Party Risk

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Identify #Protect	Operational Capabilities #Information_security – assurance	Security Domain #Governance_and – Ecosystem
Control	<p>Der Anbieter MUSS (sofern relevant) für externe Dienstleister (und insbesondere Auftragsverarbeiter im Sinne der DSGVO), die im Rahmen der Entwicklung oder im Betrieb des TI-Produktes Leistungen bzw. die Umsetzung von Anforderungen übernehmen, die Rechte und Pflichten im Kontext des Datenschutzes und der Informationssicherheit vertraglich festlegen.</p> <p>Der Anbieter MUSS (sofern relevant) externe Dienstleister (und insbesondere Auftragsverarbeiter im Sinne der DSGVO), die Im Rahmen der Entwicklung oder im Betrieb des TI-Produktes Leistungen bzw. die Umsetzung von Anforderungen übernehmen, kontinuierlich steuern und die Einhaltung der vertraglichen Aspekte des Datenschutzes und der Informationssicherheit kontrollieren.</p> <p>Der Anbieter MUSS der gematik eine Übersicht der externen Dienstleister, Hersteller und Partner die im Rahmen der Entwicklung und des Betriebs des TI-Produktes (Teil-) Leistungen übernehmen, bereitstellen.</p> <p>Der Anbieter MUSS in regelmäßigen Abständen Nachweise erbringen, dass er seine TI-relevanten Dienstleister wirksam überwacht und steuert.</p>			
Purpose	<p>Sofern Anbieter Teile ihrer Entwicklungsarbeiten oder Betriebsleistungen im Kontext der TI-Produkte an externe Dienstleister auslagern, müssen die gegenüber der gematik eingegangenen vertraglichen Verpflichtungen an den externen Dienstleister vertraglich mit übergeben werden. Weiterhin muss der Anbieter die Einhaltung der vertraglich fixierten Verpflichtungen des Dienstleisters in angemessener Art und Weise regelmäßig überprüfen, um sicherzustellen, dass diese durch den Dienstleister auch in hoher Qualität fortlaufend eingehalten werden.</p> <p>Die Übermittlung der Dienstleister- und Kooperationsbeziehungen zur Erbringung der Leistungen in und für die TI sind erforderlich, um die "supply chains" für diese Dienste nachvollziehen, mögliche übergreifende Abhängigkeiten identifizieren zu können und die Erkenntnisse in den Kritikalitätsbewertungen berücksichtigen zu können. Darüber hinaus ist der Nachweis der wirksamen Steuerung von Dienstleistern notwendig, um mögliche Risiken (Third Party Risk) für die TI zu minimieren.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.08.2025	
Other information	keine			

Referenz	ISO 27002 2022: 5.19 Information security in supplier relationships ISO 27002 2022: 5.20 Addressing information security within supplier agreements ISO 27002 2022: 5.21 Managing information security in the ICT supply chain ISO 27002 2022: 5.22 Monitoring, review and change management of supplier services ISO 27002 2022: 5.23 Information security for use of cloud services ISO 27002 2022: 6.6 Confidentiality or non-disclosure agreements [Teletrust] 3.3.8 Umgang mit Dienstleistern		
Gematik KPI	Jährliche Übermittlung einer vollständigen, zur Erbringung der jeweiligen Dienste und Leistungen für die TI relevanten Dienstleister, Hersteller und Partner sowie eines Nachweises der wirksamen Steuerung dieser Dienstleister.		
Verfehlung	tbd	Lieferintervall	jährlich

6.14 Umgang mit Sicherheitsvorfällen (SIM)

6.14.1 Meldung von Sicherheitsvorfällen und Datenschutzverstößen

Tabelle 33: Meldung von Sicherheitsvorfällen und Datenschutzverstößen

Control type #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Respond #Recover	Operational Capabilities #Governance #Information_security _event_management	Security Domain #Defence
Control	<p>Der Anbieter MUSS erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die zum Ausfall oder zur Beeinträchtigung der Sicherheit oder Funktionsfähigkeit des Dienstes der TI oder zum Ausfall oder zur Beeinträchtigung der Sicherheit oder Funktionsfähigkeit der Telematikinfrastruktur führen können oder bereits geführt haben sowie bei Datenschutzverstöße, nach Art. 34 DSGVO,</p> <ul style="list-style-type: none"> • Sofortmaßnahmen ergreifen, um Schäden zu begrenzen bzw. zu verhindern, • Unverzüglich, jedoch spätestens innerhalb von 72 Stunden nach Bekanntwerden nach bekannt werden direkt der gematik melden, • Maßnahmen zur Behebung des Sicherheitsvorfalls inkl. Umsetzungsfristen mit der gematik abstimmen, • Die erforderlichen Maßnahmen fristgerecht umsetzen, • Den Abschluss der Umsetzung an die gematik melden, • der gematik Nachweise der Umsetzung bereitstellen sowie • Nachweise im Zusammenhang mit dem Sicherheitsvorfall mindestens drei Jahre für Zwecke der Verifikation vorzuhalten. <p>Bei einer hohen Kritikalität des Sicherheitsvorfalls ist eine Root Cause Analyse durchführen und mit der gematik zu besprechen.</p>			
Purpose	<p>Die gematik übernimmt im Zuge auftretender Störungen, Sicherheitsvorfälle, Datenschutzverstöße und Notfälle eine koordinierende Rolle und steuert den oder die beteiligten Akteure. Weiterhin ist die unverzügliche Meldung von Sicherheitsvorfällen an die gematik ist erforderlich, damit die gematik ihrer gesetzlichen Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesministerium für Gesundheit (BMG) nachkommen kann.</p>			
Verpflichtend umzusetzen für Security Governance Stufen	1-5	Verpflichtende Umsetzung bis:	31.03.2025	

Other information	keine		
Referenz	ISO 27002 2022: 5.24 Information security incident management planning and preparation ISO 27002 2022: 5.26 Response to information security incidents ISO 27002 2022: 6.8 Information security event reporting § 329 SGB V Maßnahmen zur Abwehr von Gefahren für die Funktionsfähigkeit und Sicherheit der Telematikinfrastruktur Art-33-dsgvo [Teletrust] 3.3.2.14 Incident Management		
Gematik KPI	Sicherheitsvorfälle werden unverzüglich (spätestens nach 72h) an die gematik gemeldet.		
Verfehlung	tbd	Lieferintervall	Ad Hoc gemäß Meldefrist

6.15 Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)

6.15.1 Notfallkonzept

Tabelle 34: Notfallkonzept

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect #Respond	Operational Capabilities #Continuity	Security Domain #Protection #Resilience
Control	Der Anbieter MUSS die von ihm betriebenen Dienste der TI in seine bestehende Notfallkonzeption einbinden oder ein betreiberspezifisches Notfallkonzept erstellen. Der Anbieter SOLL sich hierbei am BSI Standard 200-4 orientieren. Folgende Inhalte MÜSSEN mindestens dokumentiert werden: <ul style="list-style-type: none"> • Übergeordnete Notfallstrategie und Einordnung der Dienste der TI • Gesetzliche und vertragliche Anforderungen • Rollen und Verantwortliche in Bezug auf das Notfall-Management • Dokumentation zur Notfallvorsorge inkl. durchgeführter Auswirkungsanalyse (BIA oder vergleichbar) • Szenario-unabhängige Notfallbewältigungsstrategie (hierbei ist insbesondere auch die TI-spezifische Eskalation zu weiteren Anbietern und zur gematik zu beschreiben) • Dokumentation der Szenario-spezifischen Notfallpläne (hierbei sind neben allgemeinen Notfallplänen für Brand und Wassereinbruch etc. insbesondere auch TI-spezifische Notfallszenarien wie der Ausfall verfügbarkeitskritischer TI-Produkte, Schwächung oder Kompromittierung von kryptographischen Schlüsselmaterial etc. zu dokumentieren) • Nachbereitung von Notfällen • Prävention und Vorbeugung von Notfällen, inklusive Fachkunde und Schulungen 			
Purpose	Für eine erfolgreiche Notfallprävention ist es erforderlich, die wesentlichen Aspekte der Geschäftsvorführung bzw. des Notfallmanagements in Form einer Notfallkonzeption zusammenzufassen. Mittels der Notfallkonzeption werden die zentralen Eckpunkte der Notfallvorsorge festgelegt.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Die Notfallkonzeption für Produkte der TI soll sich soweit möglich optimal in die bestehende anbieterweite Notfalldokumentation eingliedern und nur bedarfsgerecht um die relevanten Aspekte des TI-Dienstes erweitert werden.			

	Die Notfalldokumentation kann zusammen mit der Sicherheitskonzeption erstellt und übermittelt werden.		
Referenz	ISO 27002 2022: 5.29 Information security during disruption ISO 27002 2022: 5.30 ICT readiness for business continuity BSI Standard 200-4 [Teletrust] 3.3.2.15 Continuity Management		
Gematik KPI	Jährliche Bereitstellung der Notfalldokumentation gegenüber der gematik.		
Verfehlung	tbd	Lieferintervall	jährlich

6.15.2 Notfallübungskonzept

Tabelle 35: Notfallübungskonzept

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect #Respond	Operational Capabilities #Continuity	Security Domain #Protection #Resilience
Control	Der Anbieter MUSS jährlich ein Notfallübungskonzept inkl. eines Test- und Übungsplans erarbeiten, in dem die innerhalb des TI-Notfallkonzeptes beschriebenen Notfallszenarien in angemessener Form getestet bzw. geübt werden.			
Purpose	Im Rahmen regelmäßiger Risikoanalysen identifiziert der Anbieter relevante Notfallszenarien für die Dienste, die er innerhalb der TI erbringt. Durch das regelmäßige Durchführen von Tests und Übungen überprüft der Anbieter die Wirksamkeit seiner Notfallvorsorge sowie seiner Handlungsfähigkeit im Notfall.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	keine			
Referenz	ISO 27002 2022: 5.29 Information security during disruption ISO 27002 2022: 5.30 ICT readiness for business continuity BSI Standard 200-4 [Teletrust] 3.3.2.15 Continuity Management			
Gematik KPI	Notfallübungskonzept wird fristgerecht bis zum 31.01 des jeweiligen Jahres zur Verfügung gestellt.			
Verfehlung	tbd	Lieferintervall	jährlich	

6.15.3 Quartalsweise Notfallübung

Tabelle 36: Quartalsweise Notfallübung

Control type #Preventive #Corrective	Information security Properties #Confidentiality #Integrity #Availability	Cybersecurity Concepts #Protect #Respond	Operational Capabilities #Continuity	Security Domain #Protection #Resilience
Control	Der Anbieter MUSS in Abstimmung mit der gematik mindestens eine quartalsweise Notfallübung für die im Rahmen der BIA und Risikobewertungen als kritisch identifizierten Notfallszenarien durchführen und die gematik in die Übung auf Wunsch mit einbinden.			
Purpose	Das Vorlegen von Nachweisen ist zur Verifikation der erfolgreichen Maßnahmenumsetzung durch die gematik erforderlich.			
Verpflichtend umzusetzen für Security Governance Stufen	1-3	Verpflichtende Umsetzung bis:	31.03.2025	
Other information	Der Anbieter erstellt hierzu einen jährlichen Übungs- und Testplan und stimmt diesen mit der gematik ab. Für die jeweiligen Übungen und Tests erstellt der Anbieter Übungskonzepte, die er der gematik im Vorfeld der Durchführung zur Verfügung stellt. Die Komplexität der Übungen kann dabei von einfachen Alarmierungstests bis hin zu anbieterübergreifenden drehbuchbasierten technischen Ausfallsimulationen (z. B. Redundanzüberprüfungen und Lastschwenks) reichen.			
Referenz	ISO 27002 2022: 5.29 Information security during disruption ISO 27002 2022: 5.30 ICT readiness for business continuity BSI Standard 200-4 [Teletrust] 3.3.2.15 Continuity Management			
Gematik KPI	Mindestens eine quartalsweise durchgeführte Notfallübung.			
Verfehlung	tbd	Lieferintervall	quartalsweise	

6.16 Compliance (COM)

Aktuell keine Controls.

6.17 Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)

Aktuell keine Controls.

6.18 Produktsicherheit (PSS)

Wird im Rahmen der Produktzulassung geprüft.

7 Anhang A

7.1 A1 - Zuordnung der Anbietertypen zu Security Governance Level

Tabelle 37: Zuordnung der Produkttypen zu Security Governance Level

SGL	Anbietertypen
1	zentrale Plattform Dienste (FHIR) Verzeichnisdienst DEMIS Federation Master eRp-Fachdienst IDP Dienst CVC Root CA POPP ePA Fachdienst
2	SGD 1&2 (ePA) Signaturdienst TI Gateway VPN Zugangsdienst TSP HBA / SMC-B Sektorale IDP Sektorale IDP Kostenträger NCPEH
3	KIM TI-Messenger TSP eGK CardLink
4	VSDM Highspeed-Konnektor (Anbieter) Basis Consumer KTR Consumer
5	WANDA / PATs

8 Anhang B - Verzeichnisse

8.1 B1 - Abkürzungen

Kürzel	Erläuterung
SGL	Security Governance Level

8.2 B2 - Abbildungsverzeichnis

Abbildung 1: Festlegung des Security Governance Levels.....	8
Abbildung 2: Mitwirkungspflichten in Abhängigkeit des SGL.....	8
Abbildung 3: Schwachstellenprozess.....	35

8.3 B4 - Tabellenverzeichnis

Tabelle 1: Übersicht der Controls.....	12
Tabelle 2: ISO-27001-Zertifikat.....	17
Tabelle 3: Sicherheitskonzept.....	19
Tabelle 4: Sicherheitskonzeption in gematik Plattform.....	21
Tabelle 5: Risikobasierte Sicherheitsüberprüfung.....	23
Tabelle 6 : Schulungs- und Sensibilisierungsnachweise.....	24
Tabelle 7: Rollen- und Rechtekonzept.....	25
Tabelle 8: Halbjährliche Assetübermittlung.....	27
Tabelle 9: Automatisierte monatliche Assetübermittlung.....	29
Tabelle 10: Schutzzonenkonzept.....	31
Tabelle 11: Zustimmung zu regelmäßigen Schwachstellenscans.....	33
Tabelle 12: Automatisierte Übermittlung Ergebnisse von Schwachstellenscans.....	34
Tabelle 13: Unverzögliche Bewertung von Schwachstellen.....	36
Tabelle 14: Meldung von erheblichen Schwachstellen und Bedrohungen.....	37
Tabelle 15: Entgegennahme und Prüfung von Meldungen der gematik.....	38

Tabelle 16: Security-Monitoring-Konzept.....39
 Tabelle 17: Überwachung, Auswertung und Reaktion auf Alarme.....41
 Tabelle 18: Weiterleitung erkannter Alarme an das TI-SIEM.....43
 Tabelle 19: Bearbeitungszeiten erkannter Alarme.....45
 Tabelle 20: Übermittlung an zentralen Log Aggregation Server.....47
 Tabelle 21: Weiterleitung von Logdaten (Rohdaten) an TI-SIEM.....48
 Tabelle 22: Weiterleitung von Reports an das TI-SIEM.....49
 Tabelle 23: Kryptographie-Konzept.....50
 Tabelle 24: Netzwerkkonzept.....52
 Tabelle 25: Regelmäßiger Security Call.....54
 Tabelle 26: Teilnahme AK DIS.....55
 Tabelle 27: Teilnahme an Partnerworkshops.....56
 Tabelle 28: Bereitstellung Sicherheitsgutachten.....57
 Tabelle 29: Auditrechte der gematik.....58
 Tabelle 30: Recht der gematik auf Sicherheitsanalysen.....60
 Tabelle 31 : Maßnahmenumsetzung.....62
 Tabelle 32 : Supply Chain & Third Party Risk.....64
 Tabelle 33: Meldung von Sicherheitsvorfällen und Datenschutzverstößen.....66
 Tabelle 34: Notfallkonzept.....68
 Tabelle 35: Notfallübungskonzept.....70
 Tabelle 36: Quartalsweise Notfallübung.....71
 Tabelle 37: Zuordnung der Produkttypen zu Security Governance Level.....73

8.4 B5 - Referenzierte Dokumente

8.4.1 Dokumente der gematik

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_DS_Anbieter]	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter

8.4.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

[ISO/IEC 27001]	ISO/IEC Third edition 2022-10 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[ISO/IEC 27002]	ISO/IEC 2022 Third edition 2022-02 Information security, cybersecurity and privacy protection — Information security controls
[Teletrust]	Handreichung zum "Stand der Technik" Technische und organisatorische Maßnahmen
[C5]	Cloud Computing Compliance Criteria Catalogue -C5: 2020