Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Koordinierendes Informationssicherheits-management der Telematikinfrastruktur

Version:	1.2.0
Revision:	\main\rel_online\rel_ors1\5
Stand:	21.02.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_ISM]

Dokumentinformationen

Änderungen zur Vorversion

Losübergreifende Synchronisation

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	03.07.12		zur Abstimmung freigegeben	PL P77
			Einarbeitung der Kommentare	P77
0.6.0	07.09.12		zur Abstimmung freigegeben	PL P77
			Redaktionelle Anpassungen	QM
1.0.0	15.10.12		freigegeben	gematik
			Korrekturen	P77
1.0.9	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare LA	P77
1.1.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.1.0	06.06.13		freigegeben	gematik
			Einarbeitung laut Änderungsliste	gematik
			Losübergreifende Synchronisation	PL P77
1.2.0	21.02.14		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einführung 5

1.1 Zielsetzung 5

1.2 Zielgruppe 5

1.3 Geltungsbereich 5

1.4 Methodik 5

2 Kennzahlensystem des ISM in der TI 6

2.1 Kennzahlen zur Bewertung der Informationssicherheit 8

2.2 Kennzahlenmodell zur Bewertung der Informationssicherheit 8

2.2.1 Kennzahl 01: Budgetierung der Informationssicherheit 8

2.2.2 Kennzahl 02: Anzahl der Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter 8

2.2.3 Kennzahl 03: Anzahl der externen und internen informationssicherheitsbezogenen Audits 9

2.2.4 Kennzahl 04: Behebungszeit von in internen oder externen Audits festgestellten Abweichungen 9

2.2.5 Kennzahl 05: Vollständigkeit der Erfassung organisationseigener Werte (Assets) 10

2.2.6 Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management) 11

2.2.7 Kennzahl 07: Prozessablauf in der Änderungsverwaltung (Change Management) 11

2.2.8 Kennzahl 08: Anzahl privilegierter Benutzer 12

2.2.9 Kennzahl 09: Regeltests der Notfallpläne anhand von Notfallübungen 12

2.2.10 Kennzahl 10: Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter 13

3 Anforderungen an das ISM der Anbieter 14

3.1 Prozessdurchführung im Rahmen des übergreifenden Berichtsmanagements 14

3.2 Messung der Kennzahlen für den Security Report 14

3.3 Dokumentationsvorgaben des Informationssicherheits-Managements 15

3.4 Reports an das koordinierende ISM der TI 15

3.5 Berichtszeiträume der Security Reports 16

3.5.1 Format zur Bereitstellung des Security Reports 16

3.6 Kennzahlen und technische Struktur des Security Reports 17
3.6.1 Kennzahl 01: Budgetierung der Informationssicherheit 18
3.6.2 Kennzahl 02 Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter 19
3.6.3 Kennzahl 03 Anzahl der externen und internen Informationssicherheits-Audits 20
3.6.4 Kennzahl 04 Behebungszeit von in internen oder externen Audits festgestellten Abweichungen 20
3.6.5 Kennzahl 05 Vollständigkeit der Erfassung organisationseigener Werte (Assets) 21
3.6.6 Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management) 22
3.6.7 Kennzahl 07: Prozessablauf in der Änderungsverwaltung (Change Management) 23
3.6.8 Kennzahl 08: Anzahl privilegierter Benutzer 23
3.6.9 Kennzahl 09: Regeltests der Notfallpläne anhand von Notfallübungen 24
3.6.10 Kennzahl 10 Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter 25

3.7 Meldung von Kontaktinformationen zum übergreifenden ISM 26

3.8 Audit des Informationssicherheitsmanagements 26

3.9 Behandlung von gravierenden Informationssicherheitsvorfällen 27

3.10 Berücksichtigung von Informationen des koordinierenden ISM 28

3.11 Meldung von Informationssicherheitsrisiken 29

3.12 Gesamtübersicht Anbieterreporting für das koordinierende ISM 30

Anhang A – Verzeichnisse 31

A1 – Abkürzungen 31

A2 – Glossar 31

A3 – Tabellenverzeichnis 31

A4 – Referenzierte Dokumente 32
A4.1 – Dokumente der gematik 32
A4.2 – Weitere Dokumente 32

1 Einführung

1.1 Zielsetzung

Die vorliegende übergreifende Spezifikation definiert die Anforderungen für die Koordination des Informationssicherheitsmanagements (ISM) der Anbieter bei der übergreifenden Sicherstellung der Informationssicherheit in der TI. Diese Anforderungen sind als übergreifende Regelungen für Interoperabilität und Verfahrenssicherheit relevant.

In diesem Dokument wird ein Kennzahlenmodell festgelegt, mit dem die Einhaltung der Anforderungen der Informationssicherheit bei den Anbietern von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten kontrolliert werden kann.

1.2 Zielgruppe

Das Dokument richtet sich an Anbieter von Produkten der TI.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Herausgeber von HBA und SMC-B sind nicht Bestandteil des Geltungsbereiches.

Die Anforderungen dieses Dokumentes beziehen sich ausschließlich auf die vom Anbieter verantworteten Systeme der TI.

1.4 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Kennzahlensystem des ISM in der TI

Diese Kapitel beschreibt das Kennzahlensystem des Informationssicherheitsmanagements (ISM) der TI. Ziel der Kennzahlen ist es, den Erfolg des ISM zu messen, um Entscheidungen über die Wirksamkeit und die Fortentwicklung des ISM treffen zu können. Das Kennzahlensystem soll dabei dem „SMART"-Grundsatz folgen, d. h. die einzelnen Kennzahlen sind zielgerichtet (specific), messbar (measurable), erlangbar (attainable), reproduzierbar (repeatable) und beziehen sich auf einen bestimmten Zeitraum (time-dependent) [Jelen00].

Dazu müssen entsprechende Messzahlen und adäquate Messpunkte festgelegt werden, die die Nachhaltigkeit der *physischen*, *personellen*, *technischen* und *organisatorischen* Sicherheitskontrollen des ISM berücksichtigen.

Die ermittelten Kennzahlen liefern Aufschluss über

- die Funktionsfähigkeit des ISM (die Wirksamkeit des Zusammenspiels zwischen Prozessen und Abläufen des eigentlichen ISM),
- die technische Dimension der Informationssicherheit (die Wirksamkeit der Sicherheitskontrollen),
- die zielgerichtete Entwicklung des Risikomanagements, und
- die Auswirkungen des Erfolgs des ISM auf die Ziele der Telematikinfrastruktur.

Die Kennzahlen sind dabei dermaßen gestaltet, dass sie sowohl die Kontrollziele der [ISO/IEC27002] unterstützen, als sich auch gegenseitig über die zugeordneten Kontrollziele hinaus unterstützen, und somit helfen, ein übergeordnetes Bild der Aktivitäten im Bereich der Informationssicherheit wiederzugeben, um so eine Steuerung und Verbesserung im Informationssicherheitsmanagements zu ermöglichen.

Da auch innerhalb der einzelnen Kontrollziele verschiedene Bereiche der Informationssicherheit adressiert werden, müssen die jeweiligen Kennzahlen einen Eindruck der Sicherheit in diesen Bereichen wiedergeben. Die Kennzahlen sind daher über den Kontrollzielen hinaus auch den folgenden Bereichen zugeordnet:

- **Physische Sicherheit**

  Die physische Sicherheit schließt den Schutz der Gebäude, den Schutz der unternehmenseigene Werte (*Assets*) und den Schutz der Betriebsprozesse mit ein.

- **Personelle Sicherheit**

  Die personelle Sicherheit umfasst die Verantwortung der Mitarbeiter zu Themen der Informationssicherheit, die Zuverlässigkeit von Mitarbeitern (bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit), die Kompetenz und Weiterbildung von Mitarbeitern, die Funktionstrennung (s*eparation of duties*) und die Bewertung der gesamten Organisationsstruktur (*workforce analysis*).

- **IT-Sicherheitskontrollen**

  Als IT-Sicherheitskontrollen werden die logische Zugangskontrollen zu IT-Systemen, die Identifizierung und Authentisierung im Rahmen der Zugangs- und Zugriffskontrolle, die Authentizität und Nichtabstreitbarkeit von Zugriffen, die Unterstützung von Kryptographie und Verschlüsselung, die Etablierung von Informationsflusskontrollen und die generelle Administration und Wartung der IT-Infrastruktur, aber auch das technische Datenschutz- und Sicherheitsmanagement verstanden.

- **IT-Sicherheitsmaßnahmen**

  Sicherheitsmaßnahen der IT-Infrastruktur adressieren die Auditierung und Alarmierung innerhalb der Infrastruktur, den Schutz der Verfügbarkeit, die Fehler- und Vorfallsbehandlung und die Fehlerabwicklung. Die IT-Sicherheitsmaßnahmen umfassen auch den Schutz der Integrität, eine Domänen-Separierung innerhalb der Infrastruktur und das Ressourcen-Management.

- **Service Life Cycle**

  Der Service Life Cycle umfasst die Entwicklung von Konzepten einschließlich der Analyse der Sicherheitsmaßnahmen, die Beschreibung von Architektur und Design, Entwicklung, Test, Deployment von Komponenten und Diensten und schließlich der Wirkbetrieb der IT-Infrastruktur bis zur Außerbetriebnahme.

- **Organisation der Informationssicherheit**

  Die Organisation der Informationssicherheit deckt Stakeholder-Strategien und Maßnahmen zur Sensibilisierung, wie auch das Configuration und Patch Management, Schwachstellenanalysen und das Richtlinien-Management ab. Es schließt dabei eigene und beauftragte Audits mit ein.

Die im folgenden Kapitel beschriebenen Kennzahlen sind vom **ISM der Beteiligten** der zugelassenen wie beauftragten Anbietern von zentralen Produkten (Diensten) der TI zu erheben und an das **koordinierende ISM** der TI zu berichten. Hierfür sind Format und Kennzeichnung entsprechend der „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL_Betr_TI] zu wählen.

Von Anbietern bereitgestellte Kennzahlen werden vom koordinierenden ISM auf Auffälligkeiten hin überprüft. Dazu werden Vergleiche der Anbieter untereinander als auch aus zurückliegende Kennzahlenreports (des gleichen Anbieters) miteinander verglichen. Bei erkannten Auffälligkeiten werden die Gründe hierfür beim Anbieter näher hinterfragt. Der Anbieter muss in diesem Fall entsprechende Dokumente bereitstellen, die eine Klärung der Auffälligkeit unterstützen. Im Zweifel kann durch das koordinierende ISM ein Audit des Anbieters beauftragt oder selbst durchgeführt werden, um eine Klärung herbeizuführen.

Die in [gemSpec_ISM] festgelegten Pflichten für Anbieter sind Bestandteil der verbindlichen Vergabebedingungen. Werden die in [gemSpec_ISM] festgelegten Pflichten, insbesondere die termingerechte und vollständige Lieferung der Reports von Kennzahlen, verletzt, so greifen die Sanktionsmechanismen der Vergabe.

Nach der Vergabe übernimmt die Linie der gematik den Wirkbetrieb und damit die Überwachung der Einhaltung.

2.1 Kennzahlen zur Bewertung der Informationssicherheit

Im Folgenden werden die einzelnen Kennzahlen detailliert beschrieben, die vom jeweiligen Anbieter an das koordinierende ISM der gematik in den jeweils beschriebenen Regelzyklen zu liefern sind. Die für die Kennzahlen erwarteten Informationen orientieren sich dabei an den folgenden inhaltlichen Eckpunkten:

1. eine **Zuordnung** der Kennzahl zur [ISO/IEC27001]
2. eine Beschreibung der Methode zur **Messung** oder zum Erhalt der Kennzahl
3. der (vom ISM der Beteiligten festgelegte) zu **erwartende Kennzahlenwert** (der angestrebte Idealwert), einschließlich der verwendeten Skala und Einheiten
4. der tatsächlich festgestellte **Kennzahlenwert** und der **Berichtszeitraum** (falls dieser vom beschriebenen Berichtszeitraum abweicht)
5. die **Interpretation** des festgestellten Kennzahlenwertes

2.2 Kennzahlenmodell zur Bewertung der Informationssicherheit

2.2.1 Kennzahl 01: Budgetierung der Informationssicherheit

Vom Top Management sollten explizit Ressourcen für die Aufrechterhaltung und Verbesserung des Niveaus der Informationssicherheit bereitgestellt werden.

Erwartete Werte

Verhältniswert aus dem Budget die Informationssicherheit betreffende Investitionen im Vergleich zum gesamten IT-Budget je Anbieter.

Ziel der Kennzahl

Anhand der Kennzahl soll der Koordinator des übergreifenden ISM einen Eindruck von der Planung und Budgetierung im Rahmen erforderlicher Maßnahmen zur Aufrechterhaltung und Verbesserung der Informationssicherheit in der Organisation erhalten. Ein budgetierter Wert liefert Hinweise auf einen funktionierenden Prozess zur Ermittlung und Bewertung von die Informationssicherheit betreffenden Risiken, denen durch geplante und budgetierte Maßnahmen gezielt begegnet werden soll.

2.2.2 Kennzahl 02: Anzahl der Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter

Effektives Informationssicherheitsmanagement ist in aller Regel nicht gesichert, wenn die mit der TI befassten Mitarbeiter des Anbieters nicht ausreichend in Datenschutz und informationssicherheitsrelevanten Aspekten sowie deren Umsetzung und Anwendung geschult worden sind und darin kontinuierlich weitergebildet werden.

Erwartete Werte

Durchschnittliche Anzahl der Schulungen der mit der TI befassten Mitarbeiter und die durchschnittliche Dauer der Informationssicherheitsschulungstage pro mit der TI befassten Mitarbeiter im Berichtszeitraum.

Personenbezogene Daten sind dabei nicht zu übermitteln.

Ziel der Kennzahl

Diese Kennzahl gibt Aufschluss über das Engagement eines Anbieters, seine Mitarbeiter hinsichtlich informationssicherheitsrelevanter Themen zu schulen. Werden regelmäßig und in angemessenem Umfang solche Schulungen durchgeführt, ist zumindest davon auszugehen, dass die Mitarbeiter auf das Thema Informationssicherheit sensibilisiert sind. Diese Kennzahl gibt jedoch nicht zwingend eine Auskunft über den Umfang und die Qualität des vermittelten Wissens. Insofern kann auch bei vielen Schulungstagen kein direkter Rückschluss auf tatsächlich vorhandene Kenntnisse der Mitarbeiter gezogen werden. Andererseits liegt die Annahme jedoch nahe, dass die Kenntnisse gering sein werden, wenn ein Anbieter keine solchen Schulungen durchführt.

2.2.3 Kennzahl 03: Anzahl der externen und internen informationssicherheitsbezogenen Audits

Durch externe oder interne Audits mit Bezug zur Informationssicherheit wird die Einhaltung der Vorgaben zur Informationssicherheit im laufenden Betrieb kontrolliert. Die bei einem Audit festgestellten Befunde sollten durch entsprechend geplante und budgetierte Maßnahmen behoben werden, um dem Regelkreis des ISM zu entsprechen.

Erwartete Werte

Anzahl der durchgeführten Audits im Rahmen des Betriebs seines ISM und Anzahl aller gefundenen Schwachstellen.

Falls Anbieter Betreiber beauftragen, sind die Angaben zusätzlich auch für die beauftragten Betreiber mit Bezug zum spezifischen Dienst der TI mit anzugeben.

Es ist zu beachten, dass hier diejenigen Audits gemeint sind, die im Ergebnis einen Berichtscharakter aufweisen, daher gefundene Schwachstellen, eine Risikobewertung und eine Maßnahme zur Mitigation beinhalten. Auch externe Berichte über z.B. durchgeführte Penetration Testings zählen hierzu.

Ziel der Kennzahl

Diese Kennzahl zeigt, welche Anbieter die geforderten Aktivitäten zur eigenständigen Regelprüfung im Rahmen ihres ISM etabliert haben. Dabei wird angenommen, dass eine Kontrolle der etablierten Maßnahmen durch Audits zu einer nachhaltigen Verbesserung bzw. Aufrechterhaltung des Informationssicherheitsniveaus führt.

Die Anzahl der Audits lässt jedoch keinen Rückschluss auf den Umgang mit Ergebnissen der Audits zu.

2.2.4 Kennzahl 04: Behebungszeit von in internen oder externen Audits festgestellten Abweichungen

Während eines Audits beim Anbieter wird die Einhaltung eigener Richtlinien und Standards überprüft und es werden Abweichungen identifiziert. Diese Abweichungen sollten

innerhalb eines realistischen Zeitplanes behoben werden. Die Kennzahl erfasst den korrekten Umgang mit identifizierten Abweichungen und somit die kontinuierliche Verbesserung der Informationssicherheit.

Erwartete Werte

Zeitspanne zwischen der Identifikation der Abweichung (FIA) und der Behebung der Abweichung (FIB) in Tagen für alle innerhalb des Berichtszeitraumes umgesetzten Maßnahmen zur Behebung von Abweichungen (FI) vorangegangener Audits.

Ermittelt und berichtet wird die mittlere Zeitspanne (MC) zur Behebung dieser Abweichungen.

Ziel der Kennzahl

Der mittlere Wert sollte die Zeitspanne zwischen den durch das ISM der Beteiligten geplanten internen Überprüfungszyklen (in der Regel spätestens alle 12 Monate) nicht überschreiten. Dieses sollte nur in Ausnahmefällen passieren, wenn die erforderlichen Maßnahmen zur Umsetzung entsprechenden zeitintensiven Umfang besitzen.

2.2.5 Kennzahl 05: Vollständigkeit der Erfassung organisationseigener Werte (Assets)

Innerhalb der Verwaltung organisationseigener Werte (Assets) sollte eine vollständige Erfassung aller (geschäftskritischen) Werte, einschließlich den Aspekten Benennung und Kategorisierung, zugeordnete Verantwortlichkeiten, Klassifizierung, Schutzbedarfsfeststellung, Risikobewertung (im Sinne der Risikobewertungsmethode des Anbieters), stattfinden. Die Vollständigkeit der Erfassung bekannter Werte liefert den Reifegrad der Prozesse zur Erfassung und Klassifizierung der Werte.

Erwartete Werte

Die Anzahl, der unter mindestens den Aspekten Benennung und Kategorisierung, zugeordnete Verantwortlichkeiten, Klassifizierung, Schutzbedarfsfeststellung, Risikobewertung (im Sinne der Risikobewertungsmethode des Anbieters) vollständig im Sinne der zuvor genannten Informationen erfassten Werte (CA) sowie die Anzahl aller erfassten Werte (TA), wird zum Stichtag des Berichtes der Inventarliste entnommen und der Quotient (CA/TA) in Prozent gebildet. Der Quotient sollte sich über die Zeit gemessen dem Wert 100 Prozent annähern. Es können die Informationen auch in getrennten Dokumentationsmitteln vorgehalten werden, müssen aber in einer Überprüfung zueinander eindeutig in Beziehung zu setzen sein.

Ziel der Kennzahl

Durch diese Kennzahl wird nur die Vollständigkeit der Erfassung aller Attribute der bekannten Werte überprüft. Nur innerhalb eines dedizierten Audits kann die Anzahl der nicht erfassten Werte überprüft werden. Dieser Sachverhalt soll durch die hier zu ermittelnde Kennzahl jedoch nicht betrachtet werden.

2.2.6 Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management)

Um den Grad der Prozesstreue im Change Management (Änderungsverwaltung) und somit die Effizienz und Wirksamkeit der Verwaltung der IT-Systeme (Betriebssystem, Datenbank, Anwendung) zu erfassen, wird die Zahl der kurzfristig benötigten oder ungeplanten Notfalländerungen der Anzahl der geplanten und innerhalb der Wartungsintervalle vorgesehenen Änderungen gegenüber gestellt.

Erwartete Werte

Quotient (VEC=EC/C*100) in Prozent aus der Anzahl der als Notfalländerungen (EC, Emergency Changes) durchgeführten Änderungen und der Gesamtzahl der innerhalb der regulären Änderungsverwaltung durchgeführten Änderungen (C).

Ziel der Kennzahl

Ein hoher Anteil von Notfalländerungen weist auf Probleme bei der Verwaltung der Infrastruktur hin, da diese Änderungen entweder sehr kurzfristig oder nicht in den dafür vorgesehenen Zeitfenstern durchgeführt werden.

2.2.7 Kennzahl 07: Prozessablauf in der Änderungsverwaltung (Change Management)

Die Änderungen an den kritischen IT-Systemen der TI müssen über einen formalen Change-Management-Prozess beauftragt, gesteuert, getestet, freigegeben und abschließend dokumentiert werden. Damit wird erreicht, dass die Änderungen nachvollziehbar bleiben und eine systembezogene Mindestdokumentation vorliegt sowie Kontroll- und Qualitätsaspekte eingehalten werden.

Ein Change ist jede durchgeführte Änderung am IT-System, die den formalen Change-Management-Prozess durchläuft, daher auch Patches und Hotfixes, nicht nur funktionale Änderungen. Änderungsanforderungen (Change Requests) beziehen sich im Kontext immer auf die drei Ebenen Betriebssystem, Datenbank und Anwendung, sofern im Kontext des spezifischen TI-Produktes anwendbar.

Erwartete Werte

Menge aller Change Requests pro IT-System im Berichtszeitraum für die kritischen IT-Systeme der TI sowie
Durchschnittliche Bearbeitungszeit eines Change Requests in Tagen von seiner Registrierung bis zu seinem Abschluss pro IT-System für diese Change Requests.

Die Angaben sind pro IT-System bzw. pro Produkt zu liefern, sofern mehrere vom Anbieter verantwortet werden.

Ziel der Kennzahl

Anhand der Anzahl der Change Requests je IT-System kann ein Eindruck von der Stabilität bezüglich des Anforderungsverhaltens (Zunahme oder Abnahme von Anforderungen über die Zeit) von Änderungsaufträgen gewonnen werden.

Die durchschnittliche Laufzeit eines Change Requests in Tagen soll einen Eindruck vermitteln, wie schnell auf Anforderungen reagiert wird und kann in Beziehung zu der Menge der Change Requests des IT-Systems gesetzt werden.

2.2.8 Kennzahl 08: Anzahl privilegierter Benutzer

Für die IT-Systeme zur Erbringung der spezifischen Dienste der TI soll ein zentraler und dokumentierter Berechtigungsvergabeprozess für den logischen Zugang und Zugriff auf Systeme, Anwendungen und Informationen eingerichtet sein. Dieses gilt insbesondere auch für Benutzer mit privilegierten Berechtigungen, wie Administratoren.

Erwartete Werte

Anzahl der Benutzerkonten mit privilegierten Rechten (PU), die Zugang zum IT-System auf Betriebssystemebene entsprechend der umgesetzten Berechtigungsvergabe für jedes geschäftskritische IT-System des spezifischen Dienstes der TI.

Dies schließt sowohl privilegierte Benutzer wie auch technische Benutzer bzw. Dienstekonten, die grundsätzlich eine Anmeldung am System zulassen (z.B. durch einen Administrator, der Kenntnis des Passwortes des Dienstekontos besitzt), mit ein. Ausgenommen sind Systemkonten oder rollenbasierte Konten, denen eine Anmeldung systemtechnisch verweigert wird.

Berichtet wird die absolute Anzahl der privilegierten Benutzerkonten (PU) und die vom ISM der Beteiligten definierten Grenzwerte sofern vorhanden.

- PU (pro geschäftkritischem IT-System) als absolute Anzahl
- Kurze Beschreibung des geschäftkritischen IT-Systems

Ziel der Kennzahl

Privilegierte Benutzer haben Systemrechte, die es ihnen ermöglichen, Sicherheitskontrollen außer Kraft zu setzen. Die Anzahl der privilegierten Benutzer muss daher streng kontrolliert werden.

2.2.9 Kennzahl 09: Regeltests der Notfallpläne anhand von Notfallübungen

Um die Konformität der erarbeiteten Notfallpläne mit den realen Anforderungen in Einklang zu halten und die am Notfallprozess beteiligten Mitarbeiter zu sensibilisieren und zu trainieren sowie im Bedarfsfalle Rücklagen für notfallbedingte Zusatzkosten realistisch abschätzen zu können, werden in regelmäßigen Notfallübungen die gemessene Zeitspanne zur Wiederherstellung kritischer Geschäftsprozesse gemessen und mit den geplanten Zeiten verglichen.

Erwartete Werte

Zeitspanne der durchgeführten Notfallübungen in Stunden vom Beginn der Notfallübung als der angenommene Notfallzeitpunkt bis zur Wiederherstellung der geschäftskritischen Prozesse (WP) sowie die für die Notfallübung geplante Dauer.

Die Anzahl der dabei je IT-System getesteten Notfallpläne ist dabei mit anzugeben.

Ziel der Kennzahl

Die Zeitspanne sollte den in den SLA festgelegten Werten (WS) entsprechen bzw. diese nicht überschreiten. Eine Überschreitung muss begründet werden. Es muss dazu mindestens eine Notfallübung im Erfassungszeitraum stattfinden.

2.2.10 Kennzahl 10: Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter

Das informationssicherheitsbezogene Dokumentationsrahmenwerk des Anbieters sollte in regelmäßigen Abständen und immer dann überprüft werden, wenn wesentliche Änderungen erfolgen, um die Aktualität, Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.

Erwartete Werte

Abdeckungsgrad der Regelprüfung bei einem Anbieter in Prozent als Quotient aus den im Berichtszeitraum überprüften Dokumenten und allen zum Rahmenwerk des ISM gehörenden Dokumenten.

Ziel der Kennzahl

Die Überprüfung des Regelwerks auf Aktualität signalisiert, ob der Anbieter regelmäßige Aktivitäten unternimmt, um die potentielle Differenz zwischen dokumentierten Vorgaben und gelebter Praxis in seiner Organisation möglichst gering zu halten. Ein hoher Abdeckungsgrad von angepassten im Vergleich zu nicht angepassten Dokumenten kann ein Indiz für die Funktionsfähigkeit dieser Aktivität sein. Es ist gleichwohl möglich, das es Dokumente im Rahmenwerk gibt, deren Überprüfungszyklus größer als der Abfragezyklus ist, daher wird kein vollständiger Abdeckungsgrad von 100 Prozent erwartet.

3 Anforderungen an das ISM der Anbieter

Dieses Kapitel beschreibt die Prozessschnittstellen zwischen dem koordinierenden Informationssicherheitsmanagement der TI und dem jeweiligen Informationssicherheitsmanagement der Anbieter. Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten müssen die Anforderungen dieses Kapitels umsetzen.

Die Vorgaben dieses Kapitels richten sich nicht an die Systeme der Leistungserbringer, Leistungserbringerinstitutionen und Kartenherausgeber. Sie haben gleichwohl die Vorgaben zu Informationssicherheit und Datenschutz aus den jeweils für sie geltenden allgemeinen und selbstauferlegten Vorgaben, Gesetzen und berufsspezifischen Regelungen zu erfüllen. Die derzeitigen Prozesse bei diesen Stellen werden als ausreichend angesehen, um die Interessen von Patientinnen und Patienten zu wahren und die Einhaltung der Informationssicherheit sicherzustellen.

3.1 Prozessdurchführung im Rahmen des übergreifenden Berichtsmanagements

Innerhalb des koordinierenden Informationssicherheitsmanagements (ISM) der Telematikinfrastruktur (TI) werden verschiedene Kennzahlen beschrieben, die durch den Anbieter im Rahmen des ISM der Beteiligten zu messen sind. Diesen Kennzahlen liegen Maßnahmen auf Seiten der Anbieter zugrunde, deren Implementierung und Betrieb durch diese Kennzahlen abgefragt wird. Mittels Stichproben und Vor-Ort-Audits kann die Einhaltung der abgefragten Maßnahmen bei den Anbietern und Betreibern durch den Koordinator für Informationssicherheit genauer hinterfragt und überprüft werden.

Diese spezifischen, durch Anbieter zu messenden und zu berichtenden Kennzahlen, werden durch das ISM der TI fortgeschrieben und gepflegt sowie deren Einhaltung durch den Koordinator für Informationssicherheit überwacht.

3.2 Messung der Kennzahlen für den Security Report

Im Rahmen des Informationssicherheitsmanagements der TI ist das angemessene Sicherheitsniveau aller Beteiligten an der TI zu überwachen und zu optimieren. Um dies erfolgreich durchführen zu können, müssen alle Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten im Rahmen ihres ISM die vorgegebenen Kennzahlen innerhalb für die von ihnen betriebenen Produkte der TI erheben und melden.

3.3 Dokumentationsvorgaben des Informationssicherheits-Managements

Im Rahmen des Aufbaus und der Pflege eines ISM müssen durch Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten Maßnahmen umgesetzt werden, um das erforderliche Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Maßnahmen für den Aufbau und die Aufrechterhaltung des ISMS können etablierten Standards wie der ISO 27001 oder dem IT-Grundschutz des BSI entnommen werden. Der Anbieter muss aus den in den Standards vorgeschriebenen Maßnahmen diejenigen auswählen, umsetzen, pflegen, mindestens jährlich überprüfen und dokumentieren, die für seine Einsatzumgebung anwendbar und somit relevant sind. Die Dokumentation des ISM muss dem koordinierenden ISM insbesondere bei einem Informationssicherheits-Audit zur Verfügung gestellt werden.

⌦ **GS-A_4503 Dokumentation des ISM**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die Umsetzung ihres Informationssicherheitsmanagements mit seinen Maßnahmen derart dokumentieren, dass es von sachverständigen Dritten mit angemessenem Aufwand nachvollzogen und geprüft werden kann.⌫

⌦ **GS-A_4504 Bereitstellung der Dokumentation des ISM bei Audits**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die dokumentierten Maßnahmen ihres Informationssicherheitsmanagements bei einem durch die gematik veranlassten Informationssicherheits-Audit zur Verfügung stellen.⌫

⌦ **GS-A_4505 Jährliche Prüfung der Dokumentation des ISM**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die dokumentierten Maßnahmen ihres Informationssicherheitsmanagements mindestens jährlich überprüfen und ggf. anpassen. ⌫

3.4 Reports an das koordinierende ISM der TI

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten müssen dem koordinierenden ISM in regelmäßigen Reports über die Einhaltung der Vorgaben zum Informationssicherheitsmanagement bzgl. der von ihnen betriebenen Produkte der TI berichten (Security Report).

Die in diesem Dokument festgelegten Pflichten für Anbieter sind Bestandteil der verbindlichen Vergabebedingungen. Werden die festgelegten Pflichten, insbesondere die termingerechte und vollständige Lieferung der Security Reports mit den Kennzahlen, verletzt, so greifen die Sanktionsmechanismen der Vergabe bzw. der Zulassung.

Anbieter müssen zur Übermittlung von Security Reports die von der gematik bereitgestellten Prozesse gemäß den Übergreifenden Richtlinien zum Betrieb der TI [gemRL_Betr_TI] nutzen.

⌦ **GS-A_4506 Übermittlung von Security Reports**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN Security Reports gemäß den Regelungen zum Reporting aus den übergreifenden Richtlinien zum Betrieb der TI übermitteln. ⌫

Es wird zwischen quartalsweisem Report im Rahmen der Erprobung und jährlichen Reports im Produktivbetrieb unterschieden.

3.5 Berichtszeiträume der Security Reports

Der Security Report wird in der Erprobung quartalsweise über alle Kennzahlen geliefert, um die damit verbundenen Prozesse zu testen und für den Produktivbetrieb weiterzuentwickeln.

⌦ **GS-A_4507 Bereitstellung des Security Reports in der Erprobung**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN während der Erprobung den Security Report an das koordinierende ISM quartalsweise versenden. Die Quartale umfassen dabei als jeweiligen Erfassungszeitraum den 1.1.-31.3. (Q1), 1.4.-30.6. (Q2), 1.7.-30.9. (Q3) sowie den 1.10.-31.12. (Q4) eines Kalenderjahres.⌫

Der Security Report wird im Produktivbetrieb über alle Kennzahlen jährlich an den Koordinator für Informationssicherheit in standardisierter Form berichtet.

⌦ **GS-A_4508 Bereitstellung des Security Reports im Produktivbetrieb**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Produktivbetrieb den Security Report an das koordinierende ISM jährlich versenden. Jährliche Security Reports MÜSSEN bis zum Ende des zweiten Kalendermonats (Februar) versendet werden. Das Jahr ist dabei definiert vom 1.1.-31.12. eines Kalenderjahres.⌫

3.5.1 Format zur Bereitstellung des Security Reports

⌦ **GS-A_4509 Dateiformat und -struktur des Security Reports**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN den Security Report als CSV-Datei (Comma-Separated Values) [RFC4180] an das koordinierende ISM versenden. Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN innerhalb der CSV-Dateien als Trennzeichen ein Semikolon (;) benutzen.⌫

⌦ **GS-A_4510 Dateinamenskonvention des Security Reports**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN den an das koordinierende ISM der TI zu übermittelnden Security Report eineindeutig mit folgenden Dateinameninhalten benennen:

- Jahr und dem Monat der Zulieferung (JJJJMM)
- der fortlaufenden Versionsnummer (VNR) (Hochzählung der Versionsnummer ab dem ersten Regel-Report mit 001 beginnen, 002 für den nächstfolgenden usw. Regel-Report)
- Teilnehmer-ID des Anbieters (TID)
- Produktbezeichnung (P)
- Interne Bezeichnung (IB) zur Unterscheidung

und nach dem Schema „JJJJMM-VNR-TID-P-IB-RF.CSV“ erstellen. (Beispiel: 201209-08-001-1234-VSDM-SAP_R3-CSV). ⌫

Die Teilnehmer-ID identifiziert die Teilnehmer im Betrieb der TI eineindeutig. Sie ist vom Typ „String [5]“ und wird von der gematik vergeben. Ist eine AnbieterID gemäß [gemSpec_OM] vorhanden, wird sie verwendet.

3.6 Kennzahlen und technische Struktur des Security Reports

Die Struktur des Security Reports muss einem einheitlichen Schema folgen. Dazu ist eine feste Reihenfolge der Datenfelder einzuhalten und der Datentyp der Felder, wie spezifiziert, durch den Anbieter umzusetzen. Es wird pro TI-Produkt eine CSV-Datei mit allen Kennzahlen und der dazugehörigen spezifizierten Dateinamenskonvention erwartet. Ggf. auftretende Nachkommastellen werden abgeschnitten.

⌦ **GS-A_4511 Aufschlüsselung pro TI-Produkt**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN für jedes der von ihnen betriebenen TI-Produkte die Angaben zu ISM-Kennzahlen liefern.⌫

⌦ **GS-A_4512 Dateistruktur der Informationen in den Security Reports**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die allgemeinen Informationen gemäß des Schemas in Tabelle Tab_Kennzahlen_AllgTeil als CSV (die Reihenfolge ist verbindlich) für den Security Report aufbereiten.

Tabelle 1: Tab_Kennzahlen_AllgTeil, Allgemeine Informationen in den Security Reports

#	Spaltenname	Beschreibung	Wertebereich
1	Teilnehmer-ID	ID des Anbieters	[String]
2	Produkt	Produkt des Reportgegenstandes	[String]
3	Produktversion	Produktversion des Reportgegenstandes	[String]

#	Spaltenname	Beschreibung	Wertebereich
4	Interne Bezeichnung	Interne Bezeichnung, als Unterscheidungsmerkmal wenn Beteiligte mehrere Reports zu einer Kennzahl z.B. für unterschiedliche IT-Systeme melden	[String]
5	Berichtszeitraum	Auswahlfeld: Quartal [3] Halbjährlich [6] Jährlich [12]	[Integer] Auswahl: 3, 6, 12
6	Startdatum	Zeitpunkt, ab dem die Messung für den Wert im Berichtszeitraum gestartet worden ist	[Datum]
7	Enddatum	Zeitpunkt, ab dem die Messung für den Wert im Berichtszeitraum beendet worden ist	[Datum]
8	Kennzahlen ID	ID der Kennzahl nach Vorgabe	[String]

⌫

3.6.1 Kennzahl 01: Budgetierung der Informationssicherheit

⌦ **GS-A_4513 Kennzahl 01: Budgetierung der Informationssicherheit**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN dem koordinierenden ISM der TI Angaben zum Verhältniswert vom Budget der Informationssicherheit betreffender Investitionen im Vergleich zum gesamten IT-Budget gemäß dem Schema in Tabelle Tab_Kennzahlen_BudgetIS übermitteln (die Reihenfolge ist verbindlich).

Tabelle 2: Tab_Kennzahlen_BudgetIS, Budgetierung der Informationssicherheit

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]

#	Spaltenname	Beschreibung	Wertebereich
9	IS Budget pro IT Budget	Verhältniswert Budget der Informationssicherheit betreffenden Investitionen im Vergleich zum gesamten IT-Budget. (Prozentwert)	Integer: 0-100

⌫

3.6.2 Kennzahl 02 Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter

⌦ **GS-A_4514 Kennzahl 02: Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur durchschnittlichen Anzahl der Schulungen und der durchschnittlichen Dauer der Informationssicherheitsschulungstage der mit der TI befassten Mitarbeiter im Berichtszeitraum gemäß des Schemas in Tabelle Tab_Kennzahlen_SchulungstageIS übermitteln (die Reihenfolge ist verbindlich).

Tabelle 3: Tab_Kennzahlen_SchulungstageIS, Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Durchschnittliche Anzahl Schulungen pro mit der TI befassten TI Mitarbeiter	Durchschnittliche Anzahl der Schulungen bzgl. der mit der TI befassten Mitarbeiter im Berichtszeitraum. Personenbezogene Daten sind dabei nicht zu übermitteln.	Integer: 0-65535
10	Durchschnittliche Dauer Informationssicherheits-Schulungstage pro mit der TI befassten Mitarbeiter	Durchschnittliche Dauer der Informationssicherheitsschulungstage bzgl. der mit der TI befassten Mitarbeiter im Berichtszeitraum in Tagen. Personenbezogene Daten sind dabei nicht zu übermitteln.	Integer: 0-65535

⌫

Anhand der Kennzahlen lässt sich eine Aussage treffen, ob Mitarbeiter im Rahmen ihrer Tätigkeit ausreichend zum Thema Informationssicherheit sensibilisiert und weitergebildet

werden, um auf Veränderungen mit Bezug zur Informationssicherheit (z.B. technischen Fortschritt und rechtliche Änderungen) angemessen reagieren zu können.

3.6.3 Kennzahl 03 Anzahl der externen und internen Informationssicherheits-Audits

⌦ **GS-A_4515 Kennzahl 03: Anzahl der externen und internen Informations-sicherheits-Audits**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur Anzahl der durchgeführten Audits im Rahmen des Betriebs seines ISM und die Anzahl aller gefundenen Schwachstellen im Berichtszeitraum gemäß dem Schema in Tabelle Tab_Kennzahlen_ISAudits übermitteln (die Reihenfolge ist verbindlich). Falls Anbieter Betreiber beauftragen, MÜSSEN die Anbieter die Angaben zusätzlich auch für die beauftragten Betreiber mit Bezug zum spezifischen Dienst der TI angeben.

Tabelle 4: Tab_Kennzahlen_ISAudits, Anzahl der externen und internen Informationssicherheits-Audits

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Anzahl interne IS Audits	Anzahl der durchgeführten internen Audits im Rahmen des Betriebs des ISM des Anbieters.	Integer: 0-65535
10	Anzahl externe IS Audits	Anzahl der durchgeführten externen Audits im Rahmen des Betriebs des ISM des Anbieters.	Integer: 0-65535
11	Anzahl gefundene Schwachstellen	Anzahl aller gefundenen Schwachstellen	Integer: 0-65535

⌫

Die Anbieter müssen hierbei beachten, dass die Auditberichte zumindest gefundene Schwachstellen, eine Risikobewertung und eine Maßnahme zur Mitigation enthalten. Auch externe Berichte über z.B. durchgeführte Penetration Testings zählen hierzu.

3.6.4 Kennzahl 04 Behebungszeit von in internen oder externen Audits festgestellten Abweichungen

⌦ **GS-A_4516 Kennzahl 04: Behebungszeit von in internen oder externen Audits festgestellten Abweichungen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur mittleren Zeitspanne

(MC) zwischen dem Zeitpunkt der Identifikation der Abweichung (FIA) und dem Zeitpunkt der Behebung der Abweichung (FIB) in Kalendertagen von innerhalb von Audits festgestellten und behobenen Abweichungen (FI) gemäß des Schemas in Tabelle Tab_Kennzahlen_BehebungszeitISAudits übermitteln.

Tabelle 5: Tab_Kennzahlen_BehebungszeitISAudits, Anzahl der externen und internen Informationssicherheits-Audits

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Mittlere Zeitspanne Behebung Maßnahmen	Mittlere Zeitspanne MC zwischen Identifikation und Behebung von Abweichungen im Berichtzeitraum in Tagen $MC = \frac{\sum_{i=1}^{Anzahl(FI)} (FIB_i - FIA_i)}{Anzahl(FI)}$	Integer: 0-65535

⌫

3.6.5 Kennzahl 05 Vollständigkeit der Erfassung organisationseigener Werte (Assets)

⌦ **GS-A_4517 Kennzahl 05: Vollständigkeit der Erfassung organisationseigener Werte (Assets)**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur (1) Anzahl der mindestens unter den Aspekten Benennung und Kategorisierung, zugeordnete Verantwortlichkeiten, Klassifizierung, Schutzbedarfsfeststellung, Risikobewertung erfassten Werten (CA), (2) zur Anzahl aller Werte (TA) am Stichtag aus der Inventarliste entnehmen und (3) als Quotient (CA/TA) gemäß des Schemas in Tabelle Tab_Kennzahlen_AssetErfassung übermitteln.

Tabelle 6: Tab_Kennzahlen_AssetErfassung, Vollständigkeit der Erfassung organisationseigener Werte (Assets)

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]

#	Spaltenname	Beschreibung	Wertebereich
9	Quotient Vollständigkeit Erfassung Assets	Vollständigkeit der Erfassung organisationseigener Werte (Assets) in Prozent. Quotient (CA/TA) aus: CA: Anzahl der mindestens unter den Aspekten Benennung und Kategorisierung, zugeordnete Verantwortlichkeiten, Klassifizierung, Schutzbedarfsfeststellung, Risikobewertung erfassten Werte und TA: alle Werte $\frac{CA}{TA} * 100 \leq 100$ [%]	Integer: 0-100

⌫

3.6.6 Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management)

⌦ **GS-A_4518 Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management)**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zum Verhältniswert der als Notfalländerungen (emergency changes, EC) durchgeführten Änderungen zu allen durchgeführten Änderungen (C) gemäß dem Schema in Tabelle Tab_Kennzahlen_ProzesstreueChangeMgmt übermitteln (die Reihenfolge ist verbindlich).

Tabelle 7: Tab_Kennzahlen_ProzesstreueChangeMgmt, Prozesstreue in der Änderungsverwaltung (Change Management)

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	C	Anzahl C aller durchgeführten Änderungen	Integer: 0-65535
10	EC	Anzahl der als Notfalländerungen (emergency changes, EC) durchgeführten Änderungen	Integer: 0-65535
11	VEC	$VEC = \frac{EC}{C} * 100 \approx 0$ [%]	Integer: 0-100

⌫

3.6.7 Kennzahl 07: Prozessablauf in der Änderungsverwaltung (Change Management)

GS-A_4519 Kennzahl 07: Prozessablauf in der Änderungsverwaltung (Change Management)

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur Anzahl der Changes und deren durchschnittlichen Laufzeit je verantwortetem Produkt der TI gemäß dem Schema in Tabelle Tab_Kennzahlen_ProzessablaufChangeMgmt übermitteln (die Reihenfolge ist verbindlich). Die Laufzeit eines Change Requests (kurz Change oder CR) ermittelt sich dabei aus der Differenz vom Zeitpunkt des Abschlusses eines Changes (CRE) und seinem Startdatum (CRA) in Kalendertagen. Changes MÜSSEN sich im Kontext immer auf die drei Ebenen Betriebssystem, Datenbank und Anwendung, sofern im Kontext des IT-Systems anwendbar, beziehen.

Tabelle 8: Tab_Kennzahlen_ProzessablaufChangeMgmt, Prozessablauf in der Änderungsverwaltung (Change Management)

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Anzahl der Changes	Anzahl der Changes des IT-Systems	Integer: 0-65535
10	Durchschnittliche Laufzeit der Changes	Durchschnittliche Laufzeit der Changes des IT-Systems $DCR = \frac{\sum_{i=1}^{Anzahl(CR)} (CRE_i - CRA_i)}{Anzahl(CR)}$ in Tagen	Integer: 0-65535

3.6.8 Kennzahl 08: Anzahl privilegierter Benutzer

GS-A_4520 Kennzahl 08: Anzahl privilegierter Benutzer

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur Anzahl des privilegierten Benutzers für jedes IT-System eines TI-Produktes gemäß dem Schema in Tabelle Tab_Kennzahlen_PrivilegierterBenutzer übermitteln (die Reihenfolge ist verbindlich).

Tabelle 9: Tab_Kennzahlen_PrivilegierterBenutzer, Anzahl privilegierter Benutzer

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Anzahl Privilegierter Benutzer	Absolute Anzahl der privilegierten Benutzerkonten (PU)	Integer: 0-65535
10	Grenzwert Privilegierter Benutzer	Der vom ISM der Beteiligten definierte Grenzwert (sofern vorhanden) Falls kein Grenzwert vorhanden ist hier ein Wert von 0 einzutragen.	Integer: 0-65535
11	Systembeschreibung	Kurze Beschreibung des geschäftkritischen IT-Systems	String

⌫

3.6.9 Kennzahl 09: Regeltests der Notfallpläne anhand von Notfallübungen

⌦ **GS-A_4521 Kennzahl 09: Regeltests der Notfallpläne anhand von Notfall-übungen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zur Anzahl der durchgeführten Notfallübungen und der Zeitspanne von Regeltests der Notfallpläne je IT-System der TI-Produkte gemäß des Schemas in Tabelle Tab_Kennzahlen_Notfallübungen übermitteln (die Reihenfolge ist verbindlich).

Tabelle 10: Tab_Kennzahlen_Notfallübungen, Regeltests der Notfallpläne anhand von Notfallübungen

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Geplante Zeitspanne	Für die Notfallübung geplante Zeitspanne zur Wiederherstellung in Stunden	Integer: 0-65535

#	Spaltenname	Beschreibung	Wertebereich
10	Getestete Zeitspanne	Die Zeitspanne vom Beginn der Notfallübung als der angenommene Notfallzeitpunkt bis zur Wiederherstellung der geschäftskritischen Prozesse in Stunden	Integer: 0-65535
11	Anzahl der Notfallpläne	Anzahl der getesteten Notfallpläne	Integer: 0-65535

⌫

3.6.10 Kennzahl 10 Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter

⌦ **GS-A_4522 Kennzahl 10: Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Angaben zum Abdeckungsgrad der Regelprüfung (Quotient aus den im Berichtszeitraum überprüften Dokumenten und allen zum Rahmenwerk des ISM gehörenden Dokumenten bei einem Anbieter) in Prozent gemäß des Schemas in Tabelle Tab_Kennzahlen_RegelpruefungISRahmen übermitteln (die Reihenfolge ist verbindlich).

Tabelle 11: Tab_Kennzahlen_RegelpruefungISRahmen, Regelprüfung des Dokumentationsrahmenwerks des ISM

#	Spaltenname	Beschreibung	Wertebereich
1-8	Allgemeiner Teil	Allgemeine Informationen zu den Kennzahlen in den Informationssicherheitsberichten nach Tabelle [Tab_Kennzahlen_AllgTeil]	vgl. [Tab_Kennzahlen_AllgTeil]
9	Abdeckungsgrad Regelprüfung	UD: Im Berichtszeitraum überprüfte Dokumente und AD: Alle zum Rahmenwerk des ISM gehörenden Dokumente bei einem Anbieter Abdeckungsgrad AR der Regelprüfung. $AR = \frac{UD}{AD} * 100 \leq 100$ [%]	Integer: 0-100

⌫

3.7 Meldung von Kontaktinformationen zum übergreifenden ISM

Anbieter müssen ihre Kontaktinformationen zum Informationssicherheitsmanagement an die gematik übermitteln. Änderungen an diesen Informationen sind dem koordinierenden ISM der TI umgehend mitzuteilen.

⌦ **GS-A_4523 Bereitstellung Kommunikationsschnittstelle für Informationssicherheit**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen des Informationssicherheitsmanagements dem Koordinator für Informationssicherheit eine Kommunikationsschnittstelle mitteilen (übliche Kontaktinformationen, wie Name Ansprechpartner, Emailadresse, Telefon, Fax, Anschrift, …).⌫

⌦ **GS-A_4524 Meldung von Kontaktinformationen zum Informationssicherheitsmanagement**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Änderungen an den Kontaktinformationen ihres lokalen ISM umgehend an das übergreifende ISM melden. ⌫

3.8 Audit des Informationssicherheitsmanagements

Der Koordinator für Informationssicherheit der TI wird im Rahmen seiner Aufgaben auch Audits bei den Anbietern von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten durchführen. Diese können zum einen durch telefonische Interviews und Sichtung von angeforderten Nachweisdokumenten erfolgen als auch ein Audit bei Anbietern vor Ort umfassen. Für beide Wege sind die Anbieter zur unterstützenden Mitarbeit verpflichtet. Die Mitarbeit umfasst dabei zum Beispiel die Bereitstellung von Unterlagen zum ISM (Regelungsdokumente und Nachweisdokumente zur Einhaltung von Vorgaben und im Rahmen der Security Reports gemachten Angaben) der Anbieter, die Bereitstellung von relevanten Interviewpartnern, Zugang zu den ISM-unterstützenden Rechenzentren und weitere mit dem Koordinator für Informationssicherheit der TI im Vorfeld eines Audits abzustimmenden Themenbereiche.

⌦ **GS-A_4525 Audit-Unterstützung des Koordinators für Informationssicherheit**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN die Auditaktivitäten des Koordinators für Informationssicherheit in der Planung und Durchführung aktiv unterstützen**.** Dies umfasst mindestens die Bereitstellung eines zentralen Ansprechpartners für die Koordination des Audits, Interviewmöglichkeiten relevanter Mitarbeiter beim Anbieter, Einsicht in relevante Dokumente und Möglichkeiten zur Ziehung von Stichproben. ⌫

⌦ **GS-A_4526 Aufbewahrungsvorgaben an die Nachweise zu den im Security Report gemachten Angaben**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN geeignete Nachweise zu den im Security Report zur Verfügung gestellten Angaben mindestens ein (1) Jahr

vorhalten, um bei einem Informationssicherheitsaudit die Richtigkeit der gemachten Angaben belegen zu können.⌫

⌦ **GS-A_4527 Audit-Kennzahlen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN die Nachvollziehbarkeit der mittels der Kennzahlen als Selbstauskunft bereitgestellten Informationen in einem Audit oder bei der Zusendung von prüfbaren Unterlagen im Rahmen von Stichproben gewährleisten. Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN nachvollziehbar machen, wie sie die angegebenen Werte ermittelt haben.⌫

3.9 Behandlung von gravierenden Informationssicherheitsvorfällen

Im ISM der TI werden Sicherheitsvorfälle folgendermaßen klassifiziert:

- Lokaler Sicherheitsvorfall (entspricht lokalem als sicherheitsrelevant eingestuftem Incident nach [gemRL_Betr_TI])

  Die Bearbeitung eines lokalen Sicherheitsvorfalles erfolgt innerhalb der etablierten Prozesse des ISM des zuständigen Anbieters. Informationen zu lokalen Sicherheitsvorfällen werden, abhängig von der festgestellten Priorität, an das koordinierende ISM berichtet.

- Schwerwiegender Sicherheitsvorfall und -notfall (entspricht übergreifendem als sicherheitsrelevant eingestuftem Incident nach [gemRL_Betr_TI])

  Ein *schwerwiegender Sicherheitsvorfall und -notfall* betrifft kritische Produkte der TI oder hat Auswirkungen, die über den direkt betroffenen Anbieter hinausgehen. Schwerwiegende Sicherheitsvorfälle und Sicherheitsnotfälle werden umgehend über das Incident Management dem koordinierenden ISM gemeldet.

Das Berichtsformat und der Übertragungsweg für Sicherheitsvorfälle erfolgt analog zu der in [gemRL_Betr_TI] beschriebenen Vorgehensweise.

⌦ **GS-A_4528 Meldung von lokalen Sicherheitsvorfällen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Meldungen von lokalen Sicherheitsvorfällen, die sich auf die vom Anbieter verantworteten Systeme der TI beziehen, quartalsweise gesammelt an das koordinierende ISM der TI übermitteln. ⌫

⌦ **GS-A_4529 Meldung von schwerwiegenden Sicherheitsvorfällen und -notfällen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Meldungen von schwerwiegenden Sicherheitsvorfällen oder Sicherheitsnotfällen gemäß den Regelungen zum übergreifenden Incident Management aus den übergreifenden Richtlinien zum Betrieb der TI mit der Priorität 1 klassifizieren und übermitteln. ⌫

⌦ **GS-A_4530 Maßnahmen zur Behebung von schwerwiegenden Sicherheitsvorfällen und -notfällen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN bei schwerwiegenden Sicherheitsvorfällen und -notfällen, von denen sie betroffen sind, bei der Behebung der Ursachen des Verstoßes mitwirken und in Abstimmung mit dem koordinierenden ISM der TI umgehend Maßnahmen umsetzen.⌫

⌦ **GS-A_4531 Umgehende Umsetzung von Maßnahmen bei schwerwiegenden Sicherheitsvorfällen und -notfällen**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN bei schwerwiegenden Sicherheitsvorfällen und -notfällen die mit dem koordinierenden ISM der TI abgestimmten Maßnahmen umgehend umsetzen und den erfolgreichen Abschluss an das koordinierende ISM der TI melden.⌫

⌦ **GS-A_4532 Kontrolle der Umsetzung von Maßnahmen in Folge eines schwerwiegenden Sicherheitsvorfalls oder -notfalls**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN der gematik zusichern, dass die gematik die Umsetzung der Maßnahmen, die sich aufgrund eines schwerwiegenden Sicherheitsvorfalls oder -notfalls beim Anbieter ergaben und mit dem koordinierenden ISM der TI abgestimmt wurden, beim Anbieter kontrollieren kann.⌫

Eine Kontrolle der erfolgreichen Umsetzung kann je nach Maßnahme unterschiedlich aussehen. Der Nachweis kann z.B. in Form von zur Verfügung gestellten Dokumentationen, neuen Regelungen oder Prozessen sowie anhand von Konfigurationsauszügen erfolgen. Alternativ kann die Kontrolle auch durch ein anlassbezogenes Audit erfolgen.

3.10 Berücksichtigung von Informationen des koordinierenden ISM

Das koordinierende ISM informiert Anbieter der TI

- über wesentliche Änderungen im Bereich der Informationssicherheit und wesentliche Ergebnisse des technischen Fortschritts, sofern diese Auswirkungen auf die Einhaltung der Vorschriften zum Schutz personenbezogener Daten der vom Anbieter betriebenen Produkte der TI haben,
- über Änderungen von Sicherheitsanforderungen der TI, sofern diese Auswirkungen auf die vom Anbieter betriebenen Produkte haben,
- bei schwerwiegenden Sicherheitsvorfällen und -notfällen in der TI, die mehrere Beteiligte der TI und insbesondere mehrere Anbieter betreffen.

Eigene gesetzliche oder vertragliche Pflichten der Anbieter bleiben durch die Information des koordinierenden ISM der TI unberührt.

GS-A_4533 Berücksichtigung von Änderungen im Umfeld der Informationssicherheit und Ergebnissen des technischen Fortschritts

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN die vom koordinierenden ISM der TI bereitgestellten Informationen zu Änderungen in den Anforderungen zur Informationssicherheit und zu Ergebnissen des technischen Fortschrittes in ihrem lokalen ISM berücksichtigen.

GS-A_4534 Berücksichtigung von Änderungen der Informationssicherheitsanforderungen der TI

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Änderungen der Sicherheitsanforderungen der TI in ihrem lokalen ISM berücksichtigen.

GS-A_4535 Kontrolle der Umsetzung von Maßnahmen durch die gematik

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN der gematik zusichern, dass die gematik die Umsetzung der Maßnahmen, die sich aus Änderungen der Sicherheitsanforderungen der TI ergaben, beim Anbieter kontrollieren kann.

3.11 Meldung von Informationssicherheitsrisiken

Anbieter müssen Informationssicherheitsrisiken an das koordinierende ISM melden. Die Meldung der Risiken erfolgt anhand der Risikodokumentationen. Diese Dokumentationen enthalten sowohl Anfangsrisiken (vor Umsetzung von Maßnahmen, kurz: Risiken) als auch Restrisiken (verbleibende Risiken nach Umsetzung von Maßnahmen).

GS-A_4537 Meldung von Informationssicherheitsrisiken

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN die bei ihnen erkannten Informationssicherheitsrisiken, die sich auf TI-Produkte beziehen, umgehend an das koordinierende ISM melden.

GS-A_4538 Nutzen des Risikobewertungstemplate

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN die bei ihnen erkannten Informationssicherheitsrisiken, die sich auf TI-Produkte beziehen, in dem von der gematik bereitgestellten Risikobewertungstemplate [gemMeth_Risk] an das koordinierende ISM der TI melden.

GS-A_4539 Meldung von angepassten Risikoleveln

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Veränderungen des Risikolevels von gemeldeten Informationssicherheitsrisiken umgehend durch Anpassung des Risikobewertungstemplate [gemMeth_Risk] an das koordinierende ISM melden.

⌦ **GS-A_4540 Risikoreporting**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN für gemeldete Risiken mit geplanter Maßnahmenumsetzung durch den Anbieter quartalsweise den Umsetzungsstatus der Maßnahmen gesammelt an das koordinierende ISM melden. ⌫

3.12 Gesamtübersicht Anbieterreporting für das koordinierende ISM

In der nachfolgenden Übersicht sind alle Berichte mit der dazugehörigen Frequenz und dem jeweiligen Bezug zum Dokument mit den dazugehörigen Anforderungen übersichtlich aufgelistet.

Tabelle 12 Gesamtübersicht ISM Berichte

Berichtsart	Frequenz	Bezug
Kennzahlenbericht	Vergabeverfahren: Quartalsweise Wirkbetrieb: Jährlich	[gemSpec_ISM]
Risikostatusbericht	Quartalsweise	[gemRL_RiPo_TI]
Auditbericht	Anlassbezogen	[gemAud_Strat]
Bericht über sicherheitsrelevante Incidents	Quartalsweise	[gemSpec_ISM] [gemRL_Betr_TI]

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AK DIS	Arbeitskreis Datenschutz und Informationssicherheit
BDSG	Bundesdatenschutzgesetz
DSM	Datenschutzmanagement
ISM	Informationssicherheitsmanagement
SGB	Sozialgesetzbuch

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

A3 – Tabellenverzeichnis

Tabelle 1: Tab_Kennzahlen_AllgTeil, Allgemeine Informationen in den Security Reports 17

Tabelle 2: Tab_Kennzahlen_BudgetIS, Budgetierung der Informationssicherheit 18

Tabelle 3: Tab_Kennzahlen_SchulungstageIS, Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter 19

Tabelle 4: Tab_Kennzahlen_ISAudits, Anzahl der externen und internen Informationssicherheits-Audits 20

Tabelle 5: Tab_Kennzahlen_BehebungszeitISAudits, Anzahl der externen und internen Informationssicherheits-Audits 21

Tabelle 6: Tab_Kennzahlen_AssetErfassung, Vollständigkeit der Erfassung organisationseigener Werte (Assets) 21

Tabelle 7: Tab_Kennzahlen_ProzesstreueChangeMgmt, Prozesstreue in der Änderungsverwaltung (Change Management) 22

Tabelle 8: Tab_Kennzahlen_ProzessablaufChangeMgmt, Prozessablauf in der Änderungsverwaltung (Change Management) 23

Tabelle 9: Tab_Kennzahlen_PrivilegierterBenutzer, Anzahl privilegierter Benutzer 24

Tabelle 10: Tab_Kennzahlen_Notfallübungen, Regeltests der Notfallpläne anhand von Notfallübungen 24

Tabelle 11: Tab_Kennzahlen_RegelpruefungISRahmen, Regelprüfung des Dokumentationsrahmenwerks des ISM 25

Tabelle 12 Gesamtübersicht ISM Berichte 30

A4 – Referenzierte Dokumente

A4.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemAud_Strat]	gematik: Auditstrategie
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_RiPo_TI]	gematik: Risikopolicy für Informationssicherheitsrisiken in der Telematikinfrastruktur
[gemMeth_Risk]	gematik: Risikoanalyse der Sicherheitskonzeption in der TI
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance

A4.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO/IEC27001]	ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements
[ISO/IEC27002]	ISO/IEC 27002:2005 Code of Practice for Information Security Management ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[Jelen00]	Jelen, George. “SSE-CMM Security Metrics.” NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC4180]	RfC 4180: Common Format and MIME Type for Comma-Separated Values (CSV) Files http://tools.ietf.org/html/rfc4180