SRQ - Specification Related Question

SRQ-ID: 1174

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Anpassungen Risikomanagement
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	8.6.13, 8.7.1.3, 8.9, 8.10

Stichwort: Anpassungen Risikomanagement

Frage:

Welche Änderungen ergeben sich durch die Einführung eines Risikomanagement-prozesses durch die gematik?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Die Tabellen in Kapitel 8.6.13 wurden entsprechend der Regelungen im Risikomanagementprozess angepasst und die Liste der erforderlichen Maßnahmen vervollständigt. Ferner wurde das Kapitel 8.9 in „informativ“ geändert.

8.6.13 Erstellung einer Restrisikoabschätzung

[…]

Hierzu MUSS der Dienstanbieter die Restrisiken aufzählen und eine Einstufung dieser Restrisiken in die ~~Risikoklassen~~ Risikobereiche vornehmen [A_02412].

~~**Tabelle 26: Risikoklassen**~~

Tabelle 26: Risikobereiche

Risikobereich	Beschreibung
Risikobereich inakzeptabler Risiken („roter Bereich“)	Die im roten Bereich liegenden Risiken können zu sehr beträchtlichen negativen Situationen für den betroffenen Akteur führen. Eine Risikoreduktion durch spezifische Sicherheitsmaßnahmen ist zwingend erforderlich. Die dort liegenden Risiken gelten aufgrund der hohen Schadensschwere und/oder der großen Eintrittshäufigkeit als inakzeptabel.
ALARP (As Low As Reasonably Practicable) Bereich („gelber Bereich“)	Die im gelben Bereich liegenden Risiken können zu einer beträchtlichen negativen Situation für den betroffenen Akteur führen. Eine Risikoreduktion durch spezifische Sicherheitsmaßnahmen ist unter Berücksichtigung der Verhältnismäßigkeit erforderlich. Gelbe Risiken können akzeptiert werden, wenn risikoreduzierende Maßnahmen unverhältnismäßig sind (Kosten-/Nutzenabwägung).
Risikobereich akzeptabler Risiken („grüner Bereich“)	Bei Risiken im grünen Bereich erscheint es auf Grund der geringen Schadensschwere oder niedrigen Eintrittshäufigkeit als ausgeschlossen, dass eine beträchtliche negative Situation für den Betroffenen eintritt. Eine Risikoreduktion durch spezifische Sicherheitsmaßnahmen wird zwar empfohlen, ist aber nicht vorgeschrieben. Risiken des grünen Bereichs gelten als akzeptabel, auch wenn keine risikoreduzierenden Maßnahmen umgesetzt wurden.
Neutraler Bereich („blauer Bereich“)	In diesen Bereich fallen Risiken, die entweder keinen Schaden verursachen oder die nicht eintreten können. Diese Kategorie ist für Risiken vorbehalten, die bei der Erfassung für nicht relevant befunden wurden aber eventuell zu einem späteren Zeitpunkt relevant werden können, z. B. durch eine Änderung der Gesetzeslage oder eine Änderung der Rahmenbedingungen, z. B. durch Einführung zusätzlicher Funktionalitäten. Es ist kein Handlungsbedarf gegeben. Falls bekannt, ist das Ereignis oder der Termin anzugeben, welches/r dieses Risiko zu einem relevanten Risiko machen würde.

Ferner ist für jedes Restrisiko eine ~~Eintrittswahrscheinlichkeit~~ Eintrittshäufigkeit abzuschätzen und zu begründen [A_02413].

~~Tabelle 27: Eintrittswahrscheinlichkeiten für Restrisiken~~

Tabelle 27: Eintrittshäufigkeiten für Restrisiken

Eintrittshäufig-keit (EHK)	Beschreibung	EHK-Klasse
Sehr Selten	Der Eintritt eines Schadereignisses wird **einmal alle 100 Jahre** erwartet.	1
Selten	Der Eintritt eines Schadereignisses wird **einmal alle 10 Jahre** erwartet.	2
Gelegentlich	Der Eintritt eines Schadereignisses wird **einmal pro Jahr** erwartet.	3
Häufig	Der Eintritt eines Schadereignisses wird **einmal pro Monat** erwartet.	4
Sehr häufig	Der Eintritt eines Schadereignisses wird **einmal pro Woche** erwartet.	5

~~**Interpretation 1:** Wird verwendet, wenn ein Ereignis aus einer vergleichsweise kleinen Grundmenge in einem Jahr eintreten kann, z. B. der Ausfall eines Rechenzentrums aus einer Grundmenge von 5 Rechenzentren. Die Semantik dieser Interpretation ist „tritt x-Mal pro Jahr" ein.~~

~~**Interpretation 2:** Wird verwendet, wenn die Eintrittswahrscheinlichkeit für ein Ereignis aus einer vergleichsweise großen Grundmenge (z. B. die Menge aller eGKs) geschätzt wird. Die Semantik dieser Interpretation ist „x% aller Elemente sind in einem Jahr von diesem Ereignis betroffen" (z. B. 10-15% aller ausgegebenen eGKs werden in einem Jahr gestohlen).~~

~~Allgemein ist die Wahl zwischen Interpretation 1 und 2 von der Anzahl der Elemente der betrachteten Grundmenge abhängig. Beispielsweise könnte man die Interpretation 2 ab einer Grundmenge von deutlich mehr als 100 Elementen wählen. Dies ist jedoch abhängig vom Dienst bzw. Netz und somit nicht allgemein gültig. Der Dienstanbieter MUSS deshalb die Grenze für Interpretation 1 oder Interpretation 2 für den jeweiligen Dienst bzw. das jeweilige Netz selbst festlegen und begründen.~~

~~Die Bewertung der Restrisiken erfolgt dann in der üblichen Weise durch gleichzeitige Betrachtung der Risikoklasse und der Eintrittswahrscheinlichkeit.~~

[…]

8.7.1.3 Prüfung der Maßnahmen auf Übereinstimmung mit der Sicherheitspolicy

Security Compliance Checks müssen sowohl im Rahmen der Implementierung der Maßnahmen als auch als wiederholte Aktivität zur Gewährleistung der Sicherheit im laufenden Betrieb durchgeführt werden [A_02420, A_02417].

Dabei muss geprüft werden:

- die Übereinstimmung der Maßnahmen mit der Sicherheitspolicy

- die Vollständigkeit der Maßnahmen
- die vollständige und korrekte Umsetzung der Sicherheitsmaßnahmen
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen
- die Einhaltung der organisatorischen Sicherheitsmaßnahmen im täglichen Betrieb.

8.9 Zulassungsverfahren (informativ) ~~- und Akkreditierungsprozesse~~

[…]

8.10 Zusammenstellung der Ausgangsanforderungen

Afo-ID	Art	Titel	Beschreibung	Rel.	Quelle
A_02412	S	Restrisikoabschätzung: Der Dienstanbieter muss eine Restrisikoabschätzung vornehmen	Der Dienstanbieter muss eine Restrisikoabschätzung vornehmen. Darin MUSS der Dienstanbieter die verbleibenden Risiken darstellen und bewerten. Insbesondere MUSS er begründen, warum die verbleibenden Risiken akzeptabel sind. Hierzu MUSS der Dienstanbieter die Restrisiken aufzählen und eine Einstufung dieser Restrisiken in die ~~Risikoklassen~~ Risikobereiche vornehmen.		Kap. 8
A_02413	S	Restrisikoabschätzung_ ~~Eintrittswahrscheinlichkeit~~ Eintrittshäufigkeit: Für jedes Restrisiko ist eine ~~Eintrittswahrscheinlichkeit~~ Eintrittshäufigkeit abzuschätzen und zu begründen	Ferner MUSS für jedes Restrisiko eine ~~Eintrittswahrscheinlichkeit~~ Eintrittshäufigkeit abgeschätzt und begründet werden.		Kap. 8
A_02417	S	Umsetzung_spezifisches_ Siko: Vor der Umsetzung des Sicherheitskonzeptes sind die zu implementierenden Maßnahmen auf ihre Übereinstimmung mit der	Vor der Umsetzung des Sicherheitskonzeptes sind die zu implementierenden Maßnahmen auf ihre Übereinstimmung mit der Sicherheitspolicy zu überprüfen (Security Compliance Checking). Ferner sind sie auf Vollständigkeit zu prüfen und zu testen. Vor der Aufnahme der Produktion erfolgt eine Abnahme durch die gematik.		Kap. 8

		Sicherheitspolicy zu überprüfen.			
A_02420	S	Prüfung_Maßnahmen_spezifisches_Siko: Security Compliance Checks sind zur Umsetzjngskontrolle erforderlich.	Security Compliance Checks müssen sowohl im Rahmen der Implementierung der Maßnahmen als auch als wiederholte Aktivität zur Gewährleistung der Sicherheit im laufenden Betrieb durchgeführt werden. Dabei muss geprüft werden: • die Übereinstimmung der Maßnahmen mit der Sicherheitspolicy • die Vollständigkeit der Maßnahmen • die vollständige und korrekte Umsetzung der Sicherheitsmaßnahmen • der korrekte Einsatz der implementierten Sicherheitsmaßnahmen • die Einhaltung der organisatorischen Sicherheitsmaßnahmen im täglichen Betrieb.		Kap. 8