Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | FB06

Bundesministerium des Innern
und für Heimat
Referat CI 3
nachrichtlich per E-Mail:
CI3Vergabe@bmi.bund.de

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker

GW 1, Raum A 2070
Universitätsallee
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Bremen 22. Dezember 2022

Konzept zur Evaluierung des IT-Sicherheitsgesetzes 2.0

I. Beschreibung des Evaluierungsrahmens und des rechtlichen Hintergrunds

Gem. Art. 6 Abs. 1 Nr. 1 IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) berichtet das Bundesministerium des Innern, für Bau und Heimat (BMI) dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele bis zum 1. Mai 2023 hinsichtlich § 2 Abs. 10, der §§ 8a, 8b, 8d und 8e sowie § 10 Abs. 1 des BSIG.

Ausweislich der Begründung zum IT-SiG 2.0 (BT-Drs. 19/26106, S. 98 f.) wären die §§ 2 Abs. 10, 8a, 8b, 8c, 8e sowie 10 Abs. 1 BSIG vier Jahre nach Inkrafttreten der BSI-KritisV zu evaluieren gewesen (siehe Art. 10 IT-SiG 1.0). Demgemäß hätte eine Evaluierung im Juni 2021 erfolgen müssen. Das BSIG hat durch das IT-SiG 2.0 zwischenzeitlich jedoch umfassende inhaltliche Anpassungen erfahren, die sich auch auf die zu evaluierenden Vorschriften beziehen. U.a. ist auch ein neuer Sektor „Siedlungsabfallentsorgung“ hinzugetreten. Soweit wie ursprünglich vorgesehen eine Evaluierung im Juni 2021 stattgefunden hätte, hätte diese mit unzureichender Erfahrungsgrundlage stattfinden müssen und sich überdies auf bereits geänderte Vorschriften bezogen. Somit hätte der ursprüngliche Evaluierungszweck einer Verbesserung der geltenden Rechtslage nicht mehr erreicht werden können. Daher wurde die in Art. 10 IT-SiG 1.0 vorgesehene Evaluierung auf einen Zeitpunkt verschoben, der zum einen gewährleistet, dass eine zur Evaluierung ausreichende Erfahrungsgrundlage zur Verfügung steht, und zum anderen bereits auf die gesetzliche Neufassung des BSIG in der Form des aktuell geltenden IT-SiG 2.0 abstellt. Ziel der Evaluierung ist ausweislich der Gesetzesbegründung die Überprüfung

„ob der mit den Vorschriften verfolgte Schutz Kritischer Infrastrukturen […] erreicht worden ist und ob die entstandenen Kosten in einem angemessenen Verhältnis zu den Ergebnissen stehen und welche Nebenwirkungen eingetreten sind“.

Die Evaluierung soll auf der Grundlage von Daten erfolgen, die vom BSI selbst, der Bundesverwaltung und Interessenverbänden der Betreiber Kritischer Infrastrukturen erhoben werden, sowie von Daten, die vom Statistischen Bundesamt zur Verfügung gestellt werden können.

Der Evaluierungsrahmen einer interdisziplinären wissenschaftlichen Untersuchung bezieht sich folglich auf den aktuellen Gesamtstand der gesetzlichen Vorgaben, wie sie im BSIG mit der Schaffung des IT-SiG 2.0 für den Schutz von Kritischen Infrastrukturen (KRITIS) enthalten sind. Im Einzelnen beinhalten die gesetzlichen Regelungen nachfolgende Vorgaben, die als Bestandteil eines Evaluierungsauftrags Berücksichtigung finden:

- § 2 Abs. 10 BSIG enthält die Legaldefinition der Kritischen Infrastrukturen hinsichtlich der Kriterien zur Qualität und Quantität ihrer Bestimmung und verweist zur näheren Konkretisierung auf die Rechtsverordnung gem. § 10 Abs. 1 BSIG, deren Rechtsgrundlage im BSIG ebenfalls Gegenstand der gutachterlichen Bewertung zur Evaluierung des IT-SiG 2.0 ist. Zu beachten ist in diesem Zusammenhang, dass der wissenschaftliche Rahmen vorliegender Beauftragung nicht die Evaluierung der BSI-KritisV selbst einbezieht. Der Rechtsrahmen zur Evaluierung der Festlegungen der kritischen Dienstleistungen und Bereiche, der Festlegung der Anlagenkategorien, die für die Erbringung der kritischen Dienstleistungen erforderlich sind, und die Bestimmung der Schwellenwerte bestimmt sich ausschließlich nach § 9 BSI-KritisV, der nicht Gegenstand der Evaluierungsvorgaben aus Art. 6 Abs. 1 Nr. 1 IT-SiG 2.0 ist.
- § 8a BSIG betrifft die Sicherheit in der Informationstechnik Kritischer Infrastrukturen und enthält zur Erreichung dieser Zielsetzung verschiedene technische und organisatorische Vorkehrungen (TOV). So müssen die Betreiber entsprechende TOV zur Erreichung der IT-Sicherheitsziele umsetzen, um die Funktionsfähigkeit der Kritischen Infrastrukturen zu gewährleisten. Hierbei soll der „Stand der Technik“ als unbestimmter Rechtsbegriff eingehalten werden. Die Vorschrift enthält überdies eine betriebswirtschaftliche Angemessenheitsbeurteilung, die Gegenstand des betrieblichen Risikomanagements zur IT-Sicherheit ist. Ab dem 01.05.2023 umfasst die Pflicht zu TOV überdies zusätzlich den Einsatz von Systemen zur Angriffserkennung (SzA), die durch das BSI in der Anwendungspraxis konkretisiert wurden. KRITIS-Betreiber können zur Realisierung der TOV branchenspezifische Sicherheitsstandards (B3S)

vorschlagen. Die getroffenen Anforderungen zur IT-Sicherheit sind von den Betreibern zweijährig gegenüber dem BSI nachzuweisen; das BSI besitzt in diesem Zusammenhang weitgehende Prüf-, Untersuchungs- und Mitentscheidungsbefugnisse unter Einbeziehung von zuständigen bereichsspezifischen Behörden.

- § 8b BSIG beschreibt die Rolle des BSI als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Hierzu hat die Behörde unterschiedliche Aufgaben der Informationssammlung, -auswertung und -verteilung im KRITIS-Kontext wahrzunehmen. Spiegelbildlich müssen die Betreiber der Kritischen Infrastrukturen eine Registrierung beim BSI vornehmen sowie eine Kontaktstelle benennen. Relevant ist hier das Melde- und Informationsportal (MIP) des BSI. In diesem Zusammenhang bestehen BSI-seitig auch Möglichkeiten zur Prüfung und Ersatzvornahme. Für die Betreiber der Kritischen Infrastrukturen besteht außerdem eine Meldepflicht über Störungsfälle über die Kontaktstelle an das BSI. Zur Bewältigung erheblicher Störungen kann das BSI notwendige Informationen/Daten herausverlangen. Zusätzlich zu der Kontaktstelle können KRITIS-Betreiber des gleichen Sektors eine gemeinsame übergeordnete Ansprechstelle benennen. Zur Beseitigung oder Vermeidung IT-sicherheitsbezogener Störungen kann das BSI die Mitwirkung des Herstellers betroffener IT-Produkte und IT-Systeme verlangen.
- § 8d BSIG regelt den Anwendungsbereich der BSIG-KRITIS-Regelungen und bestimmt in diesem Zusammenhang Bereichsausnahmen für Kleinstunternehmen sowie für solche Betreiber, die spezialgesetzlichen Anforderungen unterliegen.
- § 8e BSIG hat in der Form von Auskunftsverlangen den Zugang zu KRITIS-bezogenen Informationen durch Dritte zum Gegenstand und regelt die hierzu notwendige Interessenabwägung zwischen öffentlichen Informations- und evtl. entgegenstehenden Sicherheitsinteressen.
- § 10 Abs. 1 BSIG enthält die BMI-Ermächtigung zum Erlass der BSI-KritisV und die Anforderungen an das hierzu durchzuführende Verfahren.

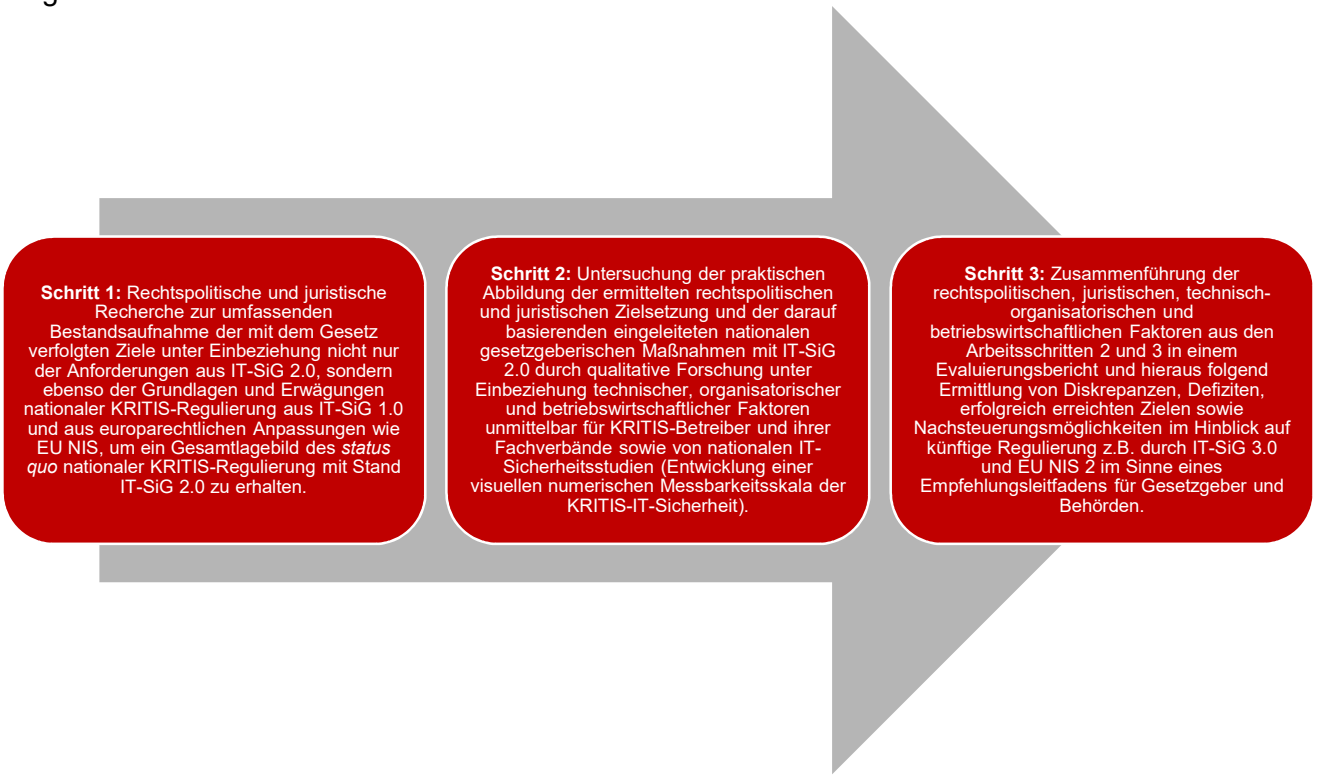
II. Beschreibung der Vorgehensweise zur Bestandsaufnahme der mit dem Gesetz verfolgten Ziele

Ausweislich der in diesem Angebot unter Punkt I. wiedergegebenen Begründung zum IT-SiG 2.0 soll die gesetzlich angeordnete Evaluierung des IT-SiG 2.0 nachfolgende drei Ziele verfolgen:

1. **Prüfung**, ob der mit den KRITIS-Vorschriften aus dem BSIG verfolgte Schutz Kritischer Infrastrukturen erreicht worden ist.
2. **Prüfung**, ob die hierfür entstandenen Kosten in einem angemessenen Verhältnis zu den Ergebnissen stehen.

3. **Prüfung**, welche Nebenwirkungen eingetreten sind ob daraus – auch im Hinblick auf ein IT-SiG 3.0 bzw. im Hinblick auf die Umsetzung der künftigen Anforderungen aus der EU NIS 2-Richtlinie – weiterer gesetzgeberischer und/oder behördlicher Handlungsbedarf abzuleiten ist, der über den bisherigen Maßnahmenkatalog des IT-SiG 2.0 hinausgeht.

Die Bearbeitung der drei vorgenannten Prüfungspunkte erfordert insgesamt ein interdisziplinäres Vorgehen unter Einbeziehung juristischen, technisch-organisatorischen und betriebswirtschaftlichen Sachverstands. Die Interdisziplinarität kommt dabei vor allem bei der Konzeption zur Wirkungsanalyse zur Geltung:



Da die aktuell gesetzlich bestehenden inhaltlichen Anforderungen und Vorgaben für Kritische Infrastrukturen aus dem IT-SiG 2.0 rechtspolitisch und juristisch in erheblichen Teilen auch auf dem IT-SiG 1.0 aus dem Jahr 2015 basieren, müssen in die Erstellung eines Evaluierungsberichts dessen Ziele, Erwägungen und Maßnahmen ebenso einfließen. Ebenso werden die nationalen rechtlichen Vorgaben zum KRITIS-Schutz bereits seit Jahren auch europarechtlich überformt, so beispielsweise durch die EU Netz- und Informationssicherheitsrichtlinie (NIS) aus dem Jahr 2016. Zur effektiven Evaluierung des IT-SiG 2.0 muss deshalb ein holistischer Rahmen gezogen werden, der einerseits als Schwerpunkt auf die nationale Rechtsetzung nach IT-SiG 2.0 fokussiert, andererseits aber auch das europäische Recht nicht völlig außer Acht lässt, da sich dessen Vorgaben und rechtspolitische Erwägungen infolge der Implementierung in das nationale

Recht auch für KRITIS-Betreiber als relevant erweisen und ggf. das Potenzial für einen EU-basierten, transnationalen Vergleich des *status quo* in der IT-Sicherheitsgesetzgebung für Kritische Infrastrukturen eröffnen. Inhaltlich soll in der Evaluierung jedoch eine deutliche Trennlinie in der Abgrenzung von IT-SiG 2.0, IT-SiG 1.0 und europarechtlichen Vorgaben gezogen werden, damit die unterschiedlichen Regelungsinhalte und Regelungsintentionen klar erkennbar sind. Mit der Bestandsaufnahme nach Schritt 1 wird in der durch das BMI geforderten Berichtstruktur der Punkt „Verfolgte Ziele des IT-Sicherheitsgesetz 2.0 gemäß Art. 6 Abs. 1 Nr. 1 2. ITSiG“ bearbeitet.

Hieraus leitet sich zur Durchführung einer Bestandsaufnahme der mit dem Gesetz verfolgten Ziele folgendes Vorgehen ab (Schritt 1):

- Umfassende Analyse der unter I. beschriebenen Rechtsvorschriften für die Regulierung von Kritischen Infrastrukturen nach IT-SiG 2.0: Auswertung der Gesetzesmaterialien, der Stellungnahmen von Verbänden, Wissenschaft, Unternehmen und von weiteren beteiligten Stakeholdern, Sichtung und Analyse der seither im Themenkontext publizierten rechtswissenschaftlichen Literatur.
- Darauf aufbauend: Zusätzlich Einbeziehung und Kenntlichmachung der durch IT-SiG 1.0 und Europarecht (insb. EU NIS) eingeführten Maßnahmen und Ziele zur IT-Sicherheit für Kritische Infrastrukturen, ebenso Literaturrecherche und Sichtung von Auslegungsmaterial, Ableitung entsprechender Ziele und Schlussfolgerungen.
- Erarbeitung einer Bestandsaufnahme und Gegenüberstellung der mit dem IT-SiG 2.0 verfolgten Ziele als tabellarische Übersicht von gesetzgeberischen Maßnahmen, verfolgten Regelungszielen, inhaltlicher Diskussion sowie öffentlicher Kritik und Würdigung der mit dem IT-SiG 2.0 ursprünglich verfolgten gesetzgeberischen Regelungsziele. Darstellung der Überschneidungen/Schnittmengen und Diskrepanzen der Anforderungen aus IT-SiG 2.0 mit IT-SiG 1.0 und insb. EU NIS, um eine bessere Vergleichbarkeit der Regelungsintentionen der KRITIS-Regulierung im chronologischen Verlauf sowie im transnationalen Rahmen zu erhalten.

III. Konzeption der Wirkungsanalyse, Beschreibung der Methodik

Die in Schritt 1 ermittelten Ergebnisse aus der holistischen Bestandsaufnahme der mit dem IT-SiG 2.0 verfolgten Ziele unter Berücksichtigung des Regulierungsrahmens aus IT-SiG 1.0 und EU NIS werden im Rahmen der interdisziplinären Wirkungsanalyse einer technischen, organisatorischen und betriebswirtschaftlichen wissenschaftlichen Untersuchung unterzogen. Zu diesem Zweck wird die Expertise der von Staat und Wirtschaft unabhängigen „Arbeitsgruppe Kritische Infrastrukturen“ (AG KRITIS) im Rahmen einer Unterbeauftragung einzelner Experten aus der Arbeitsgruppe herangezogen. Überdies ist geplant,

durch bestehende Kontakte zum Bundesamt für Sicherheit in der Informationstechnik (BSI) ergänzende Experteninterviews zu ermittelten Schwerpunktthemen/Problemen/Diskrepanzen oder strittigen Anforderungen in Einzelfällen flankierend durchzuführen (z.B. Referat BL 23 „IT-Sicherheit und Recht“) zur Auslegung bestimmter Vorgaben aus dem IT-SiG 2.0. Für sämtliche wissenschaftlichen Maßnahmen im Rahmen der interdisziplinären Wirkungsanalyse wird die „Konzeption zur Evaluierung neuer Regelungsvorhaben gem. Arbeitsprogramm bessere Rechtsetzung der BReg vom 28. März 2012, Ziffer II. 3.“ in der vom St. Ausschuss Bürokratieabbau vom 23.01.2013 beschlossenen Fassung zugrunde gelegt. Mit den Ergebnissen aus der Wirkungsanalyse wird in der durch das BMI geforderten Berichtstruktur der Punkt „Wirksamkeit der im Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele gemäß Art. 6 Abs. 1 Nr. 1 2. ITSiG“ bearbeitet.

Folgende inhaltliche Maßnahmen werden als Bestandteil der Wirkungsanalyse unter Berücksichtigung nachfolgender Methodik durchgeführt (Schritt 2):

- Entwicklung einer visuellen Skala zur numerischen Messbarmachung der unter Schritt 1 ermittelten einzelnen Ziele und Maßnahmen des IT-SiG 2.0 anhand von konkreten Prüfkriterien, beispielsweise gemessen an ihrer Praktikabilität, Umsetzbarkeit, Prozesswertigkeit, Bedeutung und betriebswirtschaftlichen Aufwänden, die zur Umsetzung erforderlich sind. In die Erstellung der Skala ebenso einbezogen werden positive/negative Nebenfolgen des IT-SiG 2.0, die Akzeptanz der Regelungen seitens KRITIS-Betreibern und Fragen des wirtschaftlichen Kosten-/Nutzen-Verhältnisses.
- Durchführung von ergänzenden qualitativen Forschungsmethoden durch die unabhängige AG KRITIS im Unterauftrag zur Bestimmung des Stands der Umsetzung der vordefinierten Wertungsskala zum IT-SiG 2.0. Dies kann anhand von Indikatoren wie einer Erhebung von quantitativen Daten zu KRITIS-Vorfällen, der aktuellen Bedrohungslage unter Einbeziehung der Entwicklungen in der Corona-Pandemie und dem Russland-Ukraine-Krieg geschehen. Darüber hinaus wird eine umfassende Befragung von im KRITIS-Kontext relevanten Funktionsträgern in einzelfallbezogenen Interviews durchgeführt, einbezogen werden beispielsweise:
  - IT-Sicherheitsbeauftragte (SiBe) in Kritischen Infrastrukturen
  - Geschäftsleitung in Kritischen Infrastrukturen
  - KRITIS-Prüfer und prüfende Stellen wie z.B. KPMG Deutschland, DQS Holding GmbH, TÜV Rheinland Cert GmbH und HiSolutions AG
  - entsprechende IT-Sicherheitsberater und Verbände wie z.B. TeleTrusT

Zur Befragung ergänzend und abgleichend herangezogen werden öffentlich publizierte IT-Sicherheitsberichte und Stellungnahmen von Sachverständigen und Verbänden aus den Gesetzgebungsverfahren zu IT-SiG 2.0 und IT-SiG 1.0. Darüber hinaus soll eine Abgrenzung zu hybriden Bedrohungslagen für KRITIS erfolgen. Ergänzend wird wie vorgenannt einzelfallbezogen der Kontakt zum BSI hergestellt und Dokumente wie nationale IT-Sicherheitsstudien werden aktiv einbezogen. Um KRITIS-Vorfälle zahlenmäßig besser erfassen und beleuchten zu können, werden KRITIS-Vorfälle vom BSI MIP und den BSI-Lageberichten zur IT-Sicherheit berücksichtigt. Überdies werden vom Auftraggeber zur Verfügung gestellte Datensätze wie z.B. vom Statistischen Bundesamt ebenso in die Erstellung und Auswertung der IT-SiG 2.0-Regelungsskala einbezogen. Die von der Allianz für Cybersicherheit mit TLP GREEN zur Verfügung gestellten Monatsberichte werden analysiert, um KRITIS-Vorfälle detailliert zu beschreiben und strukturiert auszuwerten.

- Erstellung einer grafischen Matrix zur Wirkungsanalyse von Zielen und Maßnahmen nach IT-SiG 2.0 zur visuellen Verdeutlichung erreichter Ziele und ggf. noch bestehender Diskrepanzen, Umsetzungsdefizite und zukünftiger gesetzgeberischer Nachsteuerungsbedarfe. Die konkrete Form der Visualisierung wird in Abstimmung mit dem Auftraggeber festgelegt. Zusätzlich verschriftlichte und systematisierte Wiedergabe der Kernaspekte aus der Hinzuziehung externen Expertenwissens, z.B. der im Rahmen von qualitativen Befragungen erlangten Datensets.

IV. Beschreibung der Vorgehensweise zur Erstellung des Evaluierungsberichts

Der Evaluierungsbericht verfolgt das Ziel, die wesentlichen Ergebnisse des Untersuchungsgegenstands IT-SiG 2.0, die zugrundeliegenden Daten und Annahmen sowie die relevanten unter Schritt 1 festgestellten und im Rahmen von Schritt 2 erhobenen und ausgewerteten Prüfkriterien in anschaulicher Form darzustellen, um darauf basierend in wissenschaftlich-fundierter Aussage objektive Folgemaßnahmen abzuleiten sowie gesetzgeberische und behördliche Handlungsempfehlungen und Best Practices an die Hand zu geben. Hierdurch wird in der durch das BMI geforderten Berichtstruktur der Punkt „Diskussion und Empfehlungen“ bearbeitet. Mit dem Evaluierungsbericht werden somit gleichsam auch politische Empfehlungen für etwaige Verbesserungsmöglichkeiten an die Hand gegeben, so beispielsweise im Hinblick auf ein mögliches IT-SiG 3.0 und/oder die national durch EU NIS 2 erforderlichen rechtlichen Implementierungen.

Der Bericht zur Evaluierung des IT-Sicherheitsgesetzes 2.0 untergliedert sich in zwei Abschnitte (Schritt 3):

- Detailliertes interdisziplinäres Vollgutachten, das alle Rahmenbedingungen, Anforderungen, Maßnahmen, Prüfkriterien, Studienergebnisse und darauf basierende Folgerungen, Diskussionen und Ableitungen aus den Arbeitsschritten 1 und 2 enthält. Überdies wird die Prüfmethodik nachvollziehbar dargestellt. Im Hinblick auf die rechtswissenschaftlichen Quellen enthält der Evaluierungsbericht ein umfassendes Literaturverzeichnis und kann insoweit zusätzlich als chronologisches Kompendium des aktuellen juristischen, fachlichen und politischen Diskussionsstandes zum IT-SiG 2.0 und mit ihm korrespondierender Regelungen wie IT-SiG 1.0 und z.B. EU NIS fungieren. Der Anhang zum Evaluierungsbericht enthält die Rohdaten insb. der qualitativen Forschungsmethoden, soweit dies sachdienlich ist.
- Executive Summary, das aus den unterschiedlichen Bearbeitungsschritten der Evaluation nur die Kernaussagen enthält und diese anschaulich, laienverständlich und komplexitätsreduzierend auf ca. einer Seite aufbereitet. Die Ergebnisse werden dabei auch – soweit sachdienlich – grafisch aufbereitet bzw. dargestellt, z.B. in der Form von Diagrammen. Im Executive Summary wird besonderer Wert auf die abzuleitenden Schlussfolgerungen gelegt, sodass das Executive Summary als separates Dokument mit Verweis auf die jeweils einzelnen Passagen der Volleevaluierung unmittelbar in den weiteren Prozess politischer Willensbildung eingebracht werden kann.

V. Projektablaufplan, Meilensteinplan, Konzeption der Zusammenarbeit

Die Ausschreibung zu dem Auftrag der Evaluierung des IT-SiG 2.0 sieht eine Bindefrist bis Freitag, den 27.01.2023 vor. Eine aussagekräftige Version des Berichts muss bis zum 15.03.2023 vorliegen, der finale Bericht soll bis spätestens Freitag, den 14.04.2023 vorliegen. Dabei wird ein konkreter und verbindlicher Terminplan nach Beauftragung zwischen den Parteien abgestimmt.

Unter Zugrundelegung dieser wesentlichen Annahmen kann folgender vorläufiger Vorschlag eines Projektablaufplans inklusive nachfolgender Meilensteine gemacht werden:

- **Meilenstein 1 anvisiert für 10.02.2023:** Abschluss der rechtspolitischen und juristischen Recherche zur Bestandsaufnahme der mit dem IT-SiG 2.0 verfolgten Ziele unter Einbeziehung auch von IT-SiG 1.0 und europarechtlichen Regelungen wie insb. EU NIS.
- **Meilenstein 2 anvisiert für 01.03.2023:** Spätester Termin für den Abschluss der Stakeholder-Interviews unter Zugrundelegung der im Rahmen der entwickelten Messbarkeitsskala zur IT-Sicherheit ermittelten relevanten Kriterien zur zahlenmäßig belastbaren Nachverfolgbarkeit der festgestellten Ziele nach IT-SiG 2.0.

- **Meilenstein 3 am 15.03.2023 gem. Ausschreibungsdokument:** Erste präfinale vollständige Berichtsversion zur elektronischen Übersendung an den Auftraggeber zur gemeinsamen Abstimmung der finalen Fassung der Evaluierung des IT-SiG 2.0.

Durch die Festlegung eines einzelnen Meilensteins für jeden der drei Arbeitsschritte der Evaluierung des IT-SiG 2.0 wird durch den Auftragnehmer sichergestellt, dass eine laufend abschnitts- und erfolgsabhängige Zwischenspiegelung der Ergebnisse an das BMI als Auftraggeber gewährleistet wird. Hierdurch erhält der Auftraggeber die Möglichkeit, den Entstehungsprozess der Evaluierung aktiv zu steuern und eventuelles Feedback sowie Input einzubringen. Hierdurch wird ein struktureller Rahmen zur konzeptionierten Zusammenarbeit, Planung sowie durchgehenden Erfolgskontrolle des Vorhabens gewährleistet.

Durch die regelmäßige Abstimmung und den Austausch und der Kommunikation der Meilensteine zwischen Auftraggeber und Auftragnehmer erfolgt nicht nur ein adäquater inhaltlicher Austausch, sondern es wird dadurch ebenfalls die fristgerechte Erstellung des Evaluierungsberichts zum IT-SiG 2.0 im Sinne der durch den Auftraggeber beschriebenen und vorausgesetzten Zielsetzung gesichert.

VI. Übersicht der Preiskalkulation

Die Projektstruktur zur Evaluierung des IT-SiG 2.0 sieht eine Projektleitung, mehrere Projektmitarbeiter und eine Unterbeauftragung vor:

- **Projektleiter:** Prof. Dr. jur. Dennis-Kenji Kipker
- **Projektmitarbeiter (voraussichtlich):** XXX
- **Unterauftrag:** AG KRITIS

Die für dieses Angebot veranschlagte Gesamtkalkulation beträgt EUR XXX und beinhaltet alle darin beschriebenen Leistungen.

Hiervon entfallen EUR XXX auf Personalkosten von Projektleiter und Projektmitarbeitern zur Erstellung der Evaluierung des IT-SiG 2.0 inkl. Vollgutachten und Executive Summary sowie der mit dem Auftraggeber notwendigen Abstimmungsarbeiten und EUR XXX auf die Unterbeauftragung von AG KRITIS zur fachlichen Unterstützung bei der Durchführung der Wirkungsanalyse des IT-SiG 2.0 in Arbeitsschritt 2.