Bundesamt
für Sicherheit in der
Informationstechnik

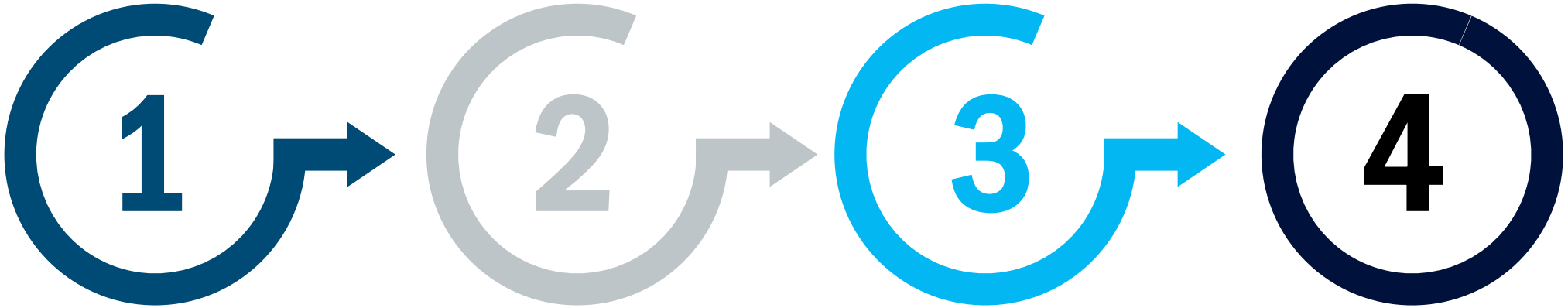
Deutschland
Digital•Sicher•BSI•

Qualifizierung (für die Zertifizierung) von Personen zur Prüfkompetenz nach §8a Abs. 3 BSIG

Michael Rauh (BSI-WG15), Lutz Naake (EY)

12.03.2024

Agenda



Projektüberblick

Projektzeitplan

Überblick Schulungsinhalte

Fragen

1 Projektüberblick

Ausgangslage und Handlungsbedarf

Verbesserung der Nachweisqualität

- Erfahrungen aus der Nachweisprüfung zeigen Schwankungen in der Qualität von Prüfungen und Nachweisen
- BSI konfrontiert mit Herausforderungen bei der Einschätzung der Nachweise, was zu häufigen Rückfragen führt

Drei Kerninitiativen:

- Formulierung übergreifender Anforderungen im Nachweisprozess
- Konkretisierung des technischen Standards für ausgewählte KRITIS-Branchen
- Förderung der KRITIS-spezifischen Qualifikation für Prüfer

Bedeutung der Prüferqualifikation:

- Die Qualifikation der prüfenden Stellen und Prüfer ist entscheidend für die Qualität der Nachweise
- Notwendigkeit eines umfangreichen Verständnisses abstrakter gesetzlicher Anforderungen sowie einer Prüfungsmethodik

Zielsetzung:

- Weiterentwicklung der § 8a Abs. 3 BSIG-Prüfverfahrenskompetenz
- Einheitliche Vermittlung der notwendigen Inhalte zur Steigerung der Nachweisqualität

Projektüberblick

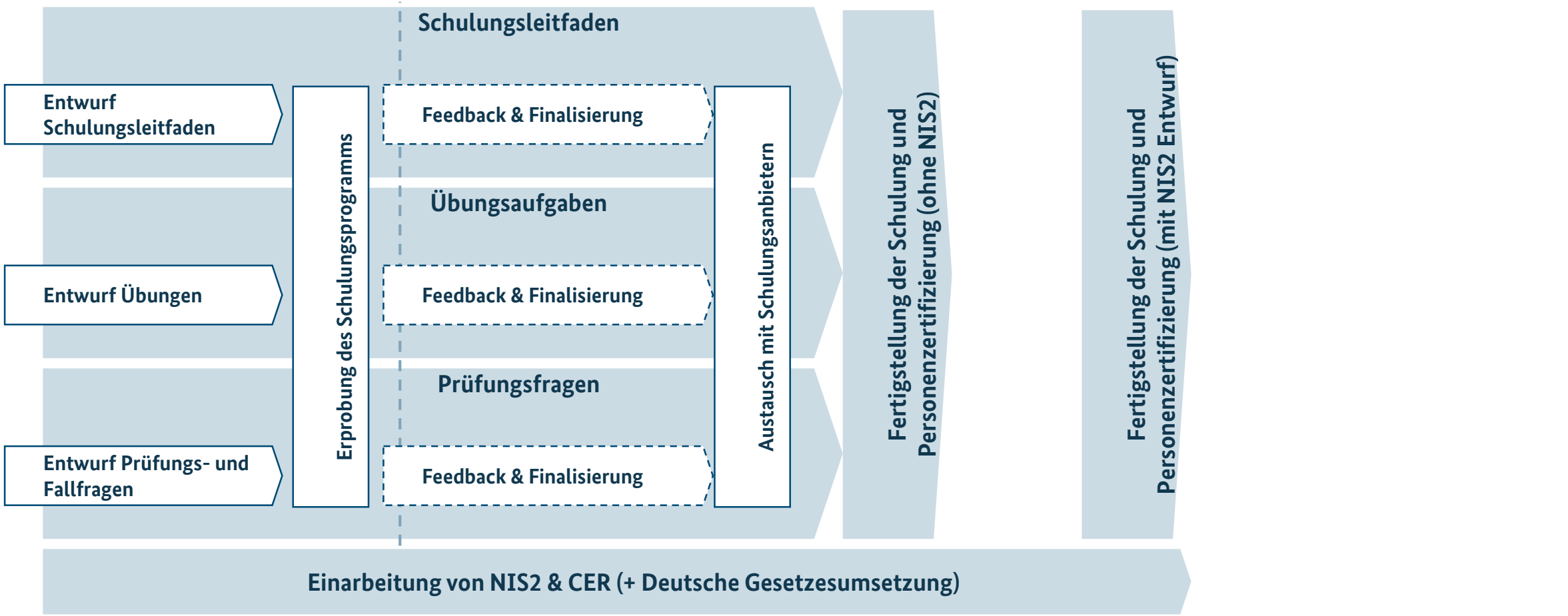
Ziel des Projekts ist die Entwicklung eines modular aufgebauten Schulungsprogramms zur Vermittlung der notwendigen Kompetenzen um geeignete KRITIS-Prüfungen und damit geeignete Nachweise zur Erfüllung der gesetzlichen Anforderungen erbringen zu können.

Das Schulungsprogramm soll sich aus den folgenden Bausteinen zusammensetzen:

1. • Modular aufgebautes Curriculum der Schulung
2. • Schulungsleitfaden zur Konkretisierung der im Curriculum festgelegten Schulungsinhalte
3. • Begleitender Foliensatz zum Schulungsleitfaden
4. • Übungspaket mit Praxisbeispielen zum Schulungsleitfaden
5. • Fragepool aus Wissensfragen und Fallbeispielen zur Kompetenzfeststellung und Personenzertifizierung auf Grundlage des Schulungsleitfadens

2 Projektzeitplan

Projektzeitplan



3 Überblick Schulungsinhalte

Überblick über das Schulungsprogramm

ENTWURF!!

Modul 1

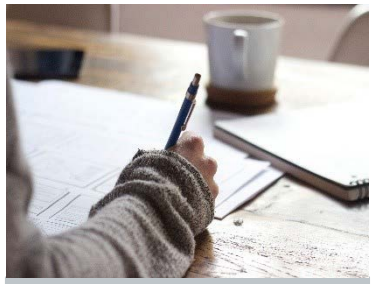
Kritische Infrastrukturen und das IT-Sicherheitsgesetz

- Einführung in den Schutz kritischer Infrastrukturen
- Hintergrund und Motivation
- Gesetzliche Grundlagen

Modul 2

Umsetzung der Anforderungen

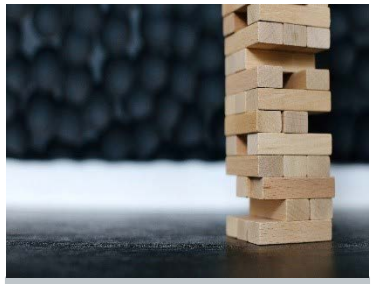
- Identifizieren als KRITIS-Betreiber
- Konsequenzen für KRITIS-Betreiber
- Hilfestellungen für KRITIS-Betreiber



Modul 3

Die Prüfungsvorbereitung

- Prüfgrundlage
- Stand der Technik
- Prüfende Stelle und Prüfer
- Prüfungsmethodik im Phasenmodell



Modul 4

Grundlagenprüfung

- Eignung des Geltungsbereichs
- Eignung des KRITIS-Risikomanagements
- Erstellung eines Prüfplans
- Mehrjahresplanung

Modul 5

Angemessenheits- und Wirksamkeitsprüfung

- Einführung in die KRITIS-Schwerpunktthemen
- Durchführung einer Angemessenheits- und Wirksamkeitsprüfung
- Exemplarische Beispiele für die Angemessenheits- und Wirksamkeitsprüfung

Modul 6

Prüfbericht und Nachweise

- Formulierung und Bewertung von Mängeln und Ergebnissen
- Prüfbericht & Prüfungsurteil
- Nachweisverfahren und Nachweisdokumente

Die KRITIS-Prüfung im Phasenmodell

ENTWURF!!

Grundlagenprüfung		Angemessenheitsprüfung		Wirksamkeitsprüfung		Ergebnis
Leitfragen: • Eignung KRITIS-Geltungsbereich • Eignung Risiko Management	Validiert	Leitfragen: 1. Sind geeignete Maßnahmen geregelt? 2. a) Sind die Maßnahmen konform zum Stand der Technik? 2. b) Sind die Maßnahmen zu einem Stichtag umgesetzt?	Angemessen	Leitfragen: 3. Wurden die Maßnahmen über einen Zeitraum umgesetzt? 4. Wurden die Maßnahmen regelmäßig auf Effektivität überprüft? 5. Wurden die Maßnahmen regelmäßig verbessert?	Wirksam	• Prüfungsurteil • Berichterstattung • Nachweisformulare

Reifegrade 1-2

Reifegrade 3-5

Mängelfeststellung

Beispielhafter Zeitplan und Aktivitäten

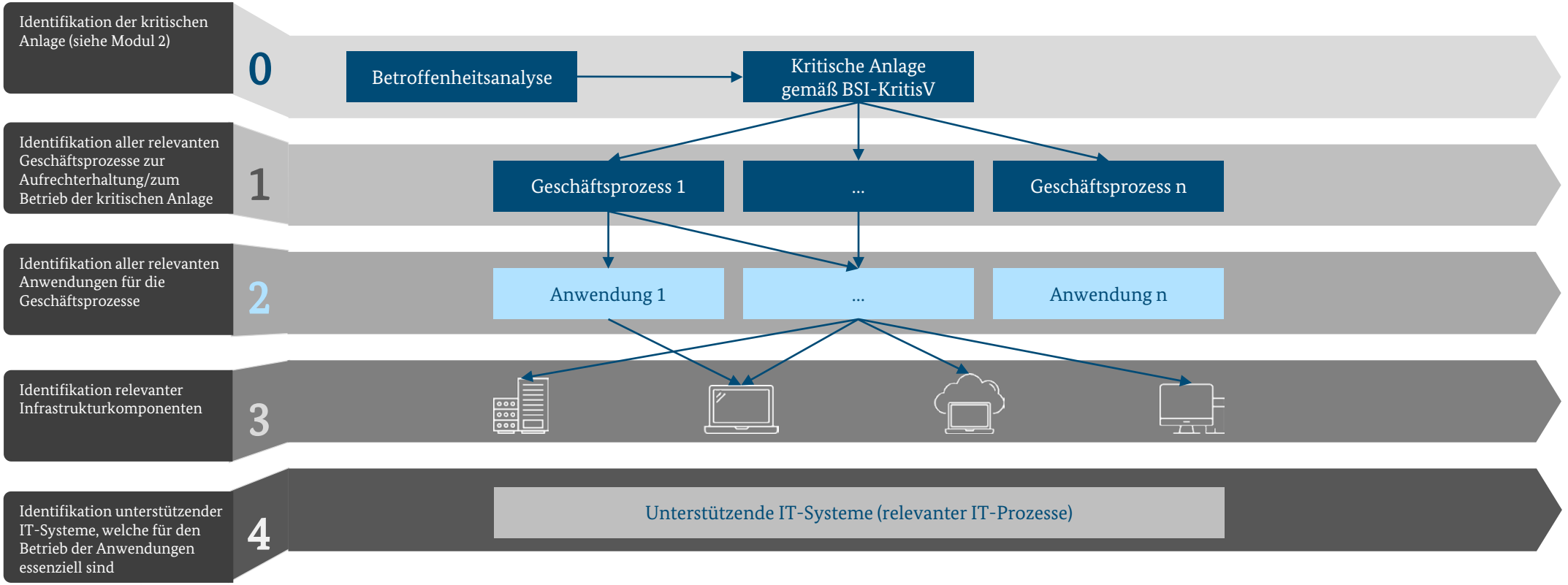
ENTWURF!!

Grundlagenprüfung	→ Validiert →	Angemessenheitsprüfung	→ Angemessen →	Wirksamkeitsprüfung	→ Wirksam →	Ergebnis
Leitfragen: • Eignung KRITIS-Geltungsbereich • Eignung Risiko Management		Leitfragen: 1. Sind geeignete Maßnahmen geregelt? 2. a) Sind die Maßnahmen konform zum Stand der Technik? 2. b) Sind die Maßnahmen zu einem Stichtag umgesetzt?		Leitfragen: 3. Wurden die Maßnahmen über einen Zeitraum umgesetzt? 4. Wurden die Maßnahmen regelmäßig auf Effektivität überprüft? 5. Wurden die Maßnahmen regelmäßig verbessert?		• Prüfungsurteil • Berichterstattung • Nachweisformulare
Phase I: Januar 2024		Phase II/III: Februar 2024				Phase IV: März 2024
Aktivitäten • Kickoff • Validierung Geltungsbereich & Risikoanalyse • Erstellung Prüfplan und Mehrjahresplan (risikobasiert)		Aktivitäten • Einsicht Richtlinien und Prozessdokumentation • Durchführung Interview mit Prozess- und Systemverantwortlichen • Abnahme exemplarischer Beispiele zum Stichtag („Test of One“)		Aktivitäten • Validierung Grundgesamtheiten • Stichprobenauswahl zur Überprüfung der Umsetzung (~10% Grundgesamtheit) • Auswertung der Stichprobennachweise • Prüfung der Effektivität und Verbesserung		Aktivitäten • Dokumentation und Bewertung der Ergebnisse • Erstellung Prüfbericht • Ableitung Formular P aus Prüfbericht

Regelmäßige Kommunikation von Prüfungsfortschritt, vorläufigen Ergebnissen und Projektrisiken

Phase I - Validierung Geltungsbereich

ENTWURF!!



Phase II/III – Beispiel Angemessenheit vs. Wirksamkeit

ENTWURF!!

Beispielhafte Maßnahme

Der administrative Zugriff auf ein hochkritisches IT-Systeme erfolgt nur nach schriftlicher Genehmigung durch den Systemverantwortlichen.

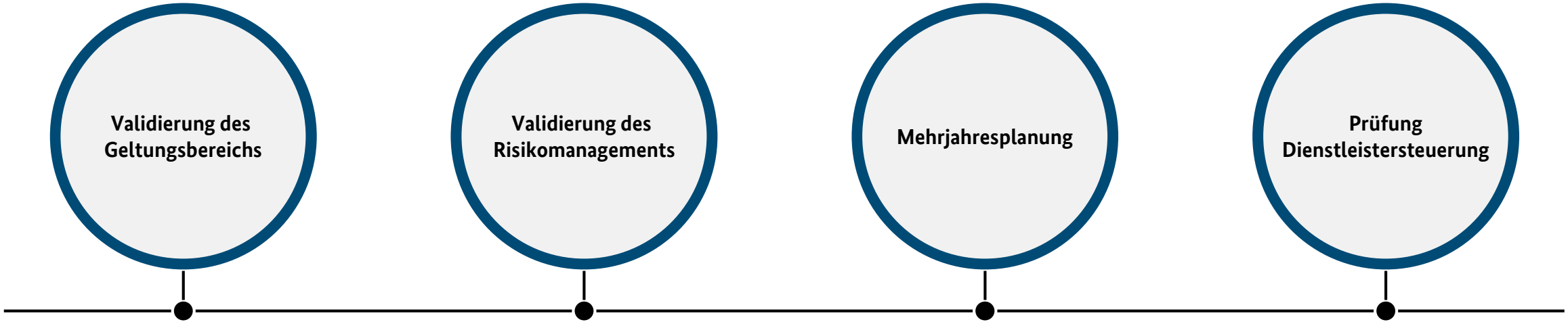
Angemessenheitsprüfung (Reifegrad 1-2)

- Aufnahme des Prozesses mit Prozessverantwortlichen und Sichtung der Prozessdokumentation zur Genehmigung von administrativen Zugriffen auf kritische IT-Systeme
- Beispielhafte Sichtung der dokumentierten Genehmigung für einen durchgeführten, administrativen Zugriff eines Administrators

Wirksamkeitsprüfung (Reifegrad 3-5)

- Auf Basis einer Grundgesamtheit von administrativen Zugriffen in den letzten 6 Monaten (beispielhafter Betrachtungszeitraum) auf das kritische IT-System wird stichprobenweise die dokumentierte Genehmigung durch den Systemverantwortlichen angefordert und eingesehen (Prozesseffektivität)
- Einsichtnahme in den Prozess zur kontinuierlichen Verbesserung der Maßnahme und die Umsetzung der identifizierten Verbesserungspotenziale (Ergebniseffektivität)

Übungsaufgaben - Auszug



Worauf ist beim Geltungsbereich zu achten?

Welche Anforderungen stellen sich an eine Geltungsbereichsdokumentation?

Welche Besonderheiten stellen sich beim KRITIS-Risikomanagement?

Wie sollte eine Risikoanalyse umgesetzt sein?

Was ist eine Mehrjahresplanung?

Wie könnte eine Mehrjahresplanung aufgebaut werden und wie funktioniert diese?

Worauf ist bei der Durchführung einer Angemessenheits- und Wirksamkeitsprüfung zu achten?

Welche konkreten Handlungen ergeben sich bei einem Fallbeispiel?

Übungsaufgaben - Beispiel

Szenario:

Sie sind Teil des Prüfungsteams, das für die Prüfung des kritischen Tanklagers der SPRIT GmbH verantwortlich ist. Ihre Aufgabe ist es gemeinsam mit dem Branchenexperten den Geltungsbereich der SPRIT GmbH nachzuvollziehen und insbesondere zu validieren, inwieweit der dokumentierte Geltungsbereich den geltenden Anforderungen entspricht. Die SPRIT GmbH stellt Ihnen hierzu den dokumentierten Geltungsbereichs bereit

Scope der Kritischen Infrastruktur

SPRIT GmbH

Tanklager und Tankstellennetz

Versionskontrolle:

Datum	Version	Inhaltliche Änderungen	Verfasser
10.03.2023	0.1	Initialentwurf	Max Mustermann (Risikomanager Sprit GmbH)
24.03.2023	1.0	Review und Freiabe	John Doe (CISO Sprit GmbH)

Personenzertifzierung – Beispiel Prüfungsfragen

Qualifizierung (für die Zertifizierung) von Personen zur
Prüfkompetenz nach §8a (3) BSIG (KRITIS_PQ_8a3)

Prüfung zur Personenzertifizierung

Entwurf

Auswertungsbereich

Datum: _____

Vorname, Name des Prüflings: _____

Datum der Auswertung: _____

Vorname, Name des Auswertenden: _____

Prüfungsinhalte und Lehrziele:
Zur Personenzertifizierung muss der Prüfer eine Prüfung ablegen. Die Prüfungsfragen orientieren sich an den Modulen des Schulungsleitfaden und setzen sich aus Multiple-Choice-Fragen und Praxisaufgaben zusammen in verschiedenen Schwierigkeits- und Komplexitätsgraden.

Auswertung:
Jede **Multiple-Choice-Frage** hat vier Antwortmöglichkeiten:
- alle Aussagen sind richtig oder
- genau eine Aussage ist richtig oder
- mehrere Aussagen sind richtig oder
- alle Aussagen sind falsch.

Jede **Single-Choice-Frage** hat vier Antwortmöglicheiten, es ist aber nur genau eine Antwort richtig.

Die **Praxisaufgaben** müssen in eigenen Worten beantwortet werden. Bewertet werden die Vollständigkeit der Inhalte, die Argumentationslogik und die verständliche Darstellung des Sachverhalts.

Bewertung:
- Alle Antwortmöglichkeiten sind gleich gewichtet. Für jede richtig beantwortete Frage gibt es einen Punkt, es gibt keine Punktabzüge.
- Eine Frage gilt als richtig beantwortet, wenn alle Antworten richtig angekreuzt sind. Ist eine Antwort falsch, gilt die gesamte Frage als nicht beantwortet).
es gibt keine Punktabzüge.
- Nicht alle Fragen sind gleich gewichtet: Die Multiple-Choice-Fragen werden einfach gewertet, die Single-Choice-Fragen mit 5 Punkten und die Praxisaufgaben mit 10 Punkten.

Fragen zu Modul 1

ID	Multiple-Choice-Fragen	Bitte kreuzen Sie die korrekten Antworten an:	Lösung	Mögliche Punkte	Erreichte Punkte	Kommentar
1.1	Welche KRITIS-Sektoren werden derzeit nicht durch das BSIG und KRITISV reguliert?	◻ a) Gesundheit ◻ b) Staat und Verwaltung ◻ c) Medien und Kultur ◻ d) Wasser	b) c)	1		
...				1		

Personenzertifzierung – Erste Überlegungen für den Ablauf

ENTWURF!!

Anmeldung Schulungsprogramm

- Schulungsanbieter die BSI Anforderungen erfüllen können Schulungsprogramm anbieten
- Teilnehmende könne sich für Schulung anmelden (keine Teilnahmevoraussetzungen)

Teilnahme Schulungsprogramm

- Durchführung der Schulung nach BSI Vorgaben (Remote / Präsenz)
- Teilnahme am Schulungsprogramm verpflichtend für Personenzertifizierung

Teilnahme Prüfung

- Deutsch & Multiple Choice
- 45 Prüfungsfragen
- Basis, Experten und Verständnisfragen

Ausstellung Bestätigung

- Schulungsanbieter oder BSI stellt Bestätigung über bestandene Prüfung aus
- Teilnehmende reichen diese bei der verantwortlichen BSI-Stelle ein

Ausstellung Zertifizierung

- Validierung der eingereichten Unterlagen durch BSI
- Ggf. Veröffentlichung der zertifizierten KRITIS-Prüfer

Möglichkeit der Aberkennung der Zertifizierung

Rezertifizierung

- Festgelegte Gültigkeit der Personenzertifizierung
- „Verlängerung“ durch Nachweis von durchgeführten KRITIS-Prüfungen (Teil des Prüfteams) + Auffrischungsschulung (falls veröffentlicht)

Und: Was bedeutet das in der Praxis ab 2024?

- Derzeit gilt: Die „alte“ Zertifizierung ist noch gültig
- Es wird eine angemessen Übergangsphase geben innerhalb der die derzeitigen Zertifizierung Anerkennung finden
- Unser Plan sieht vor, diese aktualisierten Materialien baldmöglichst einem breiteren Publikum zur Verfügung zu stellen
- Einführung des Phasenmodells in der Breite (verstärkter Fokus auf Geltungsbereich und Risikomanagement)
- Verstärkt KRITIS-Prüfungen mit risikobasierter Prüfung der Wirksamkeit der umgesetzten Maßnahmen
- Ziel der Prüfmethodik: Kenne deine Risiken und habe einen Umsetzungsplan. Du musst nicht Mängelfrei sein

4

Fragen?

Kontakt

Michael Rauh
Referent WG 15 - Kritische Infrastrukturen-Prüfungen
michael.rauh@bsi.bund.de

Lutz Naake
Partner EY Technology Risk
lutz.naake@de.ey.com

Vielen Dank für Ihre Aufmerksamkeit!

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.