Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

Fraunhofer IEM

Deutschland Digital•Sicher•BSI•

Automatisierung im Rahmen der Nachweiserbringung

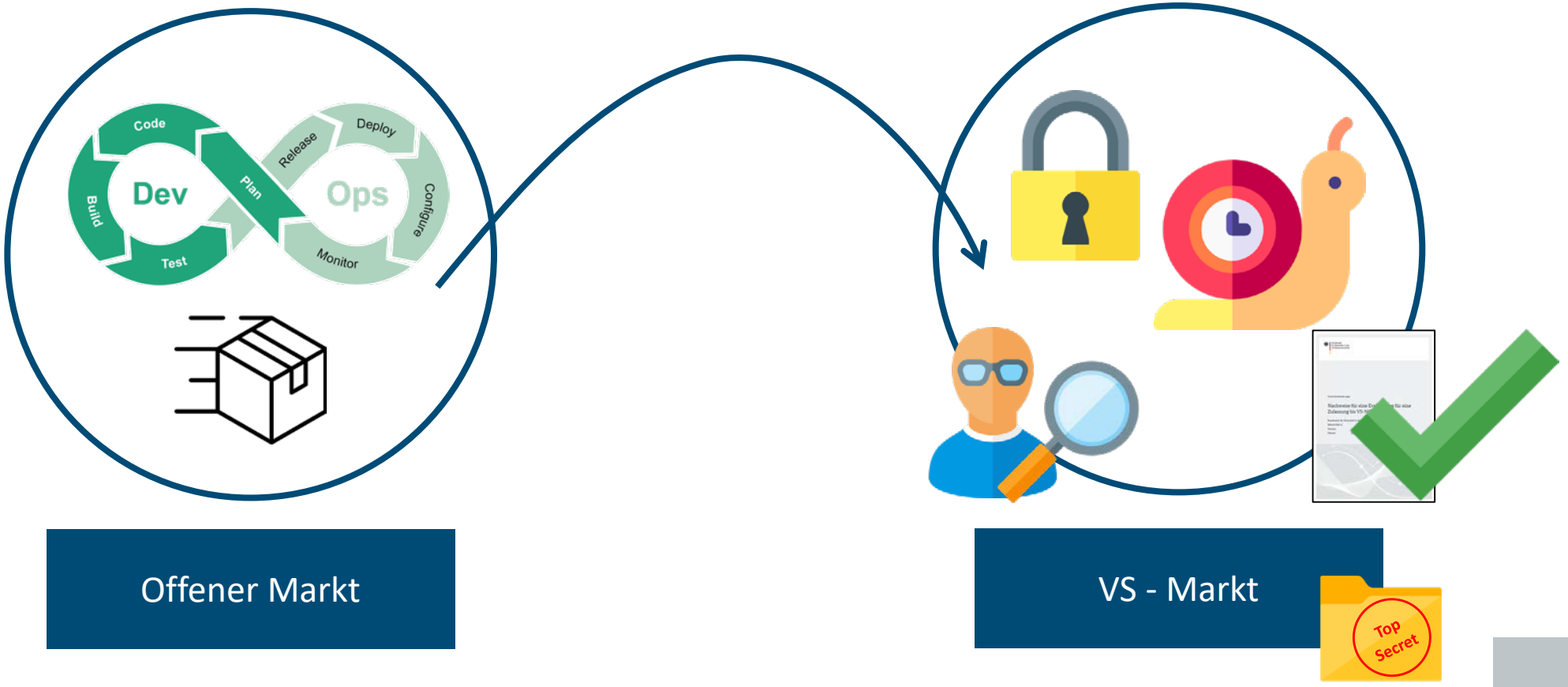
Jan Sinkewitz (BSI)
Dr. Matthias Meyer (Fraunhofer IEM)

Berlin, 24.05.2023

Interagiert mit uns via Mentimeter schon während des Talks!

- Stellen Sie Fragen **jederzeit in Mentimeter**
  - Fragen werden nach dem Vortrag in der Q&A diskutiert
- Stimmen Sie für bereits gestellte Fragen ab (Daumen hoch!)
  - Hilft uns die interessantesten Fragen zu priorisieren
- Weitere Interaktionspunkte während des Vortrags bei Erscheinen des Logos

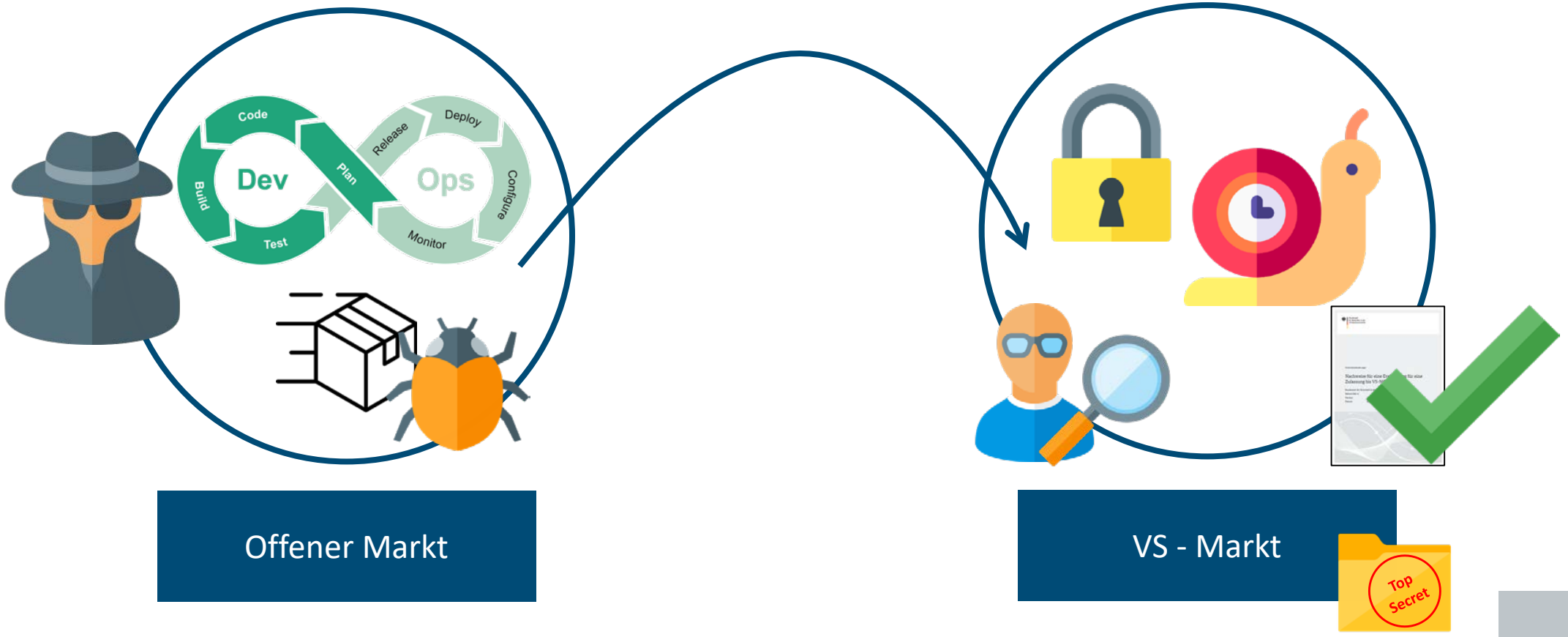
Motivation



Offener Markt

VS - Markt

Motivation

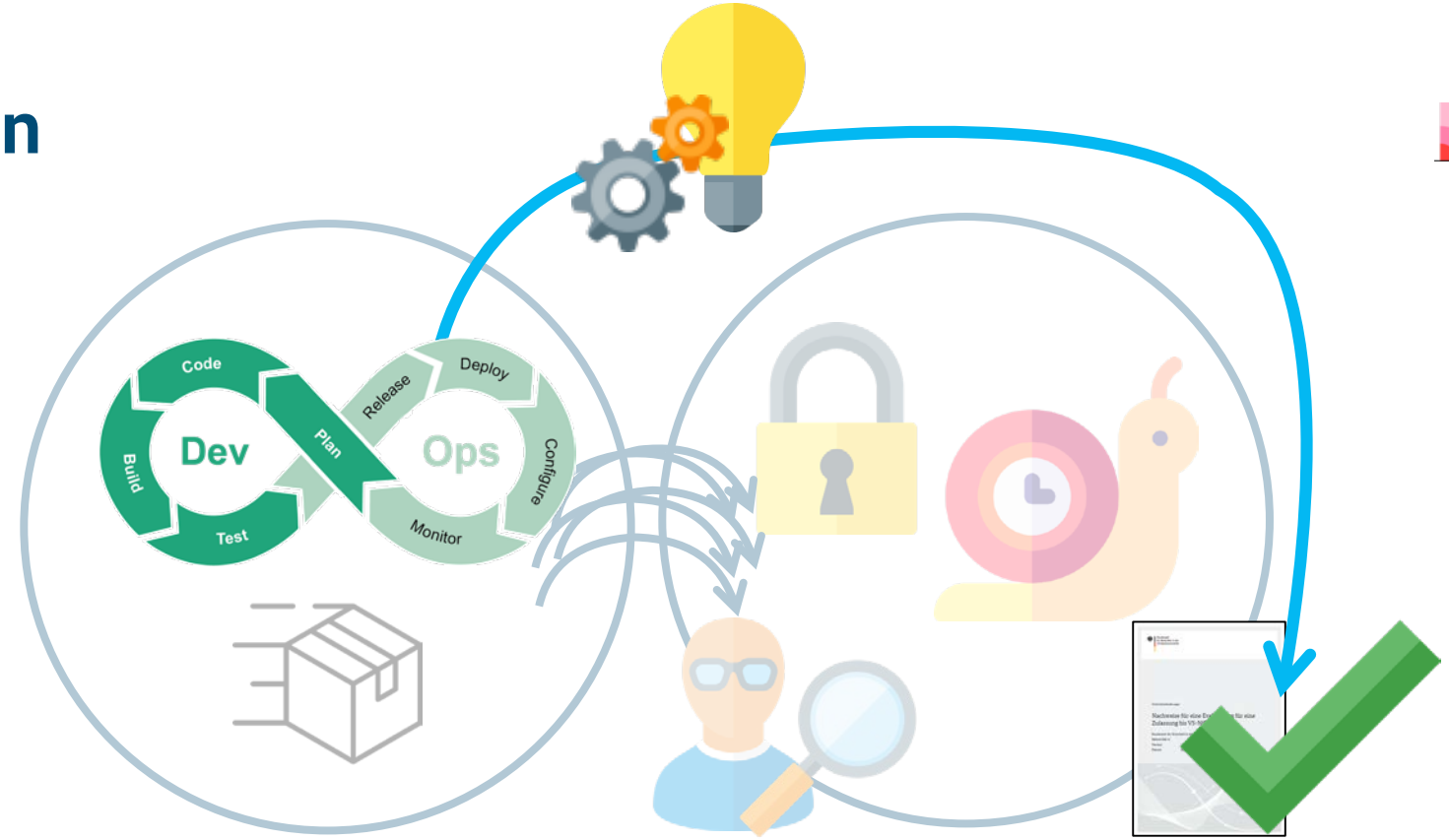


Offener Markt

VS - Markt

Motivation

Mentimeter



Offener Markt

VS - Markt

Top Secret

Projekt 552 - DUST

- Voller Titel: **D**ie a**U**tomati**S**che digi**T**ale Nachweisführung zur Evaluierung von VS-IT
- Projektlaufzeit: 11/22 – 04/24
- Ziel
  - Erhöhung des Automatisierungsgrades im VS-IT Evaluierungsprozess
- Partner

Fraunhofer AISEC

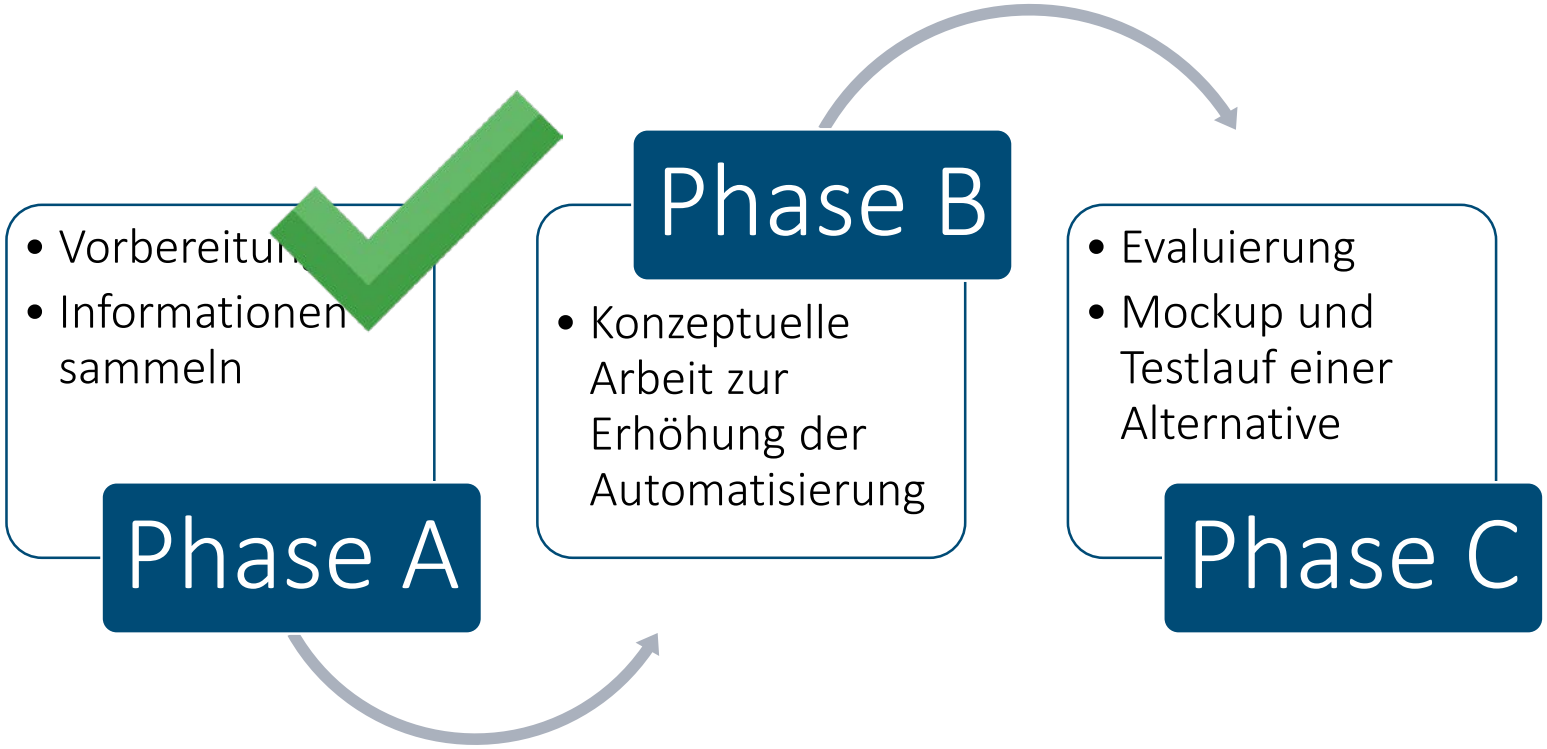
Fraunhofer IEM

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

Fraunhofer IEM

Projektplan



Phase A - Vorbereitung

Analyse der aktuellen Nachweise und des Prozesses zur Nachweiserbringung

Recherche und Evaluierung von marktrelevanten Tools

Analyse der Methoden Fuzzing, statische, dynamische & instrumentierte Analyse, inkl. Betrachtung welche Nachweise diese erbringen können

Phase B – Konzeptuelle Arbeit

Automatisierung der aktuellen Nachweise

Erhöhung des Automatisierungsgrads durch kleine Änderungen an den aktuellen Nachweisen

Redesign des Nachweiskatalogs zur Maximierung des Automatisierungspotentials

Phase B – Konzeptuelle Arbeit

Automatisierung der aktuellen Nachweise

ATE_FUN.NfD.4C

Die tatsächlichen Testergebnisse müssen mit den erwarteten Testergebnissen übereinstimmen.

boost C++ LIBRARIES

JUnit 5

pytest

Phase B – Konzeptuelle Arbeit

Automatisierung der aktuellen Nachweise

ASE_OBJ.NfD.4C

Das Security Objectives Rationale muss nachweisen, dass die Sicherheitsziele (TOE und operationelle Einsatzumgebung) alle Bedrohungen abwehren.

Phase B – Konzeptuelle Arbeit

Automatisierung der aktuellen Nachweise

Erhöhung des Automatisierungsgrads durch kleine Änderungen an den aktuellen Nachweisen

Redesign des Nachweiskatalogs zur Maximierung des Automatisierungspotentials

Phase B – Konzeptuelle Arbeit

Erhöhung des Automatisierungsgrads durch kleine Änderungen an den aktuellen Nachweisen

ATE_IND.NfD.2E

Der Evaluator muss eine Stichprobe der Tests aus der Testdokumentation durchführen, um die Ergebnisse der Herstellertests zu verifizieren.

*ATE_IND.NfD.2E**

Die Tests aus der Testdokumentation müssen stichprobenartig durchgeführt werden, um die Ergebnisse der Herstellertests zu verifizieren.

Phase B – Konzeptuelle Arbeit

Automatisierung der aktuellen Nachweise

Erhöhung des Automatisierungsgrads durch kleine Änderungen an den aktuellen Nachweisen

Redesign des Nachweiskatalogs zur Maximierung des Automatisierungspotentials

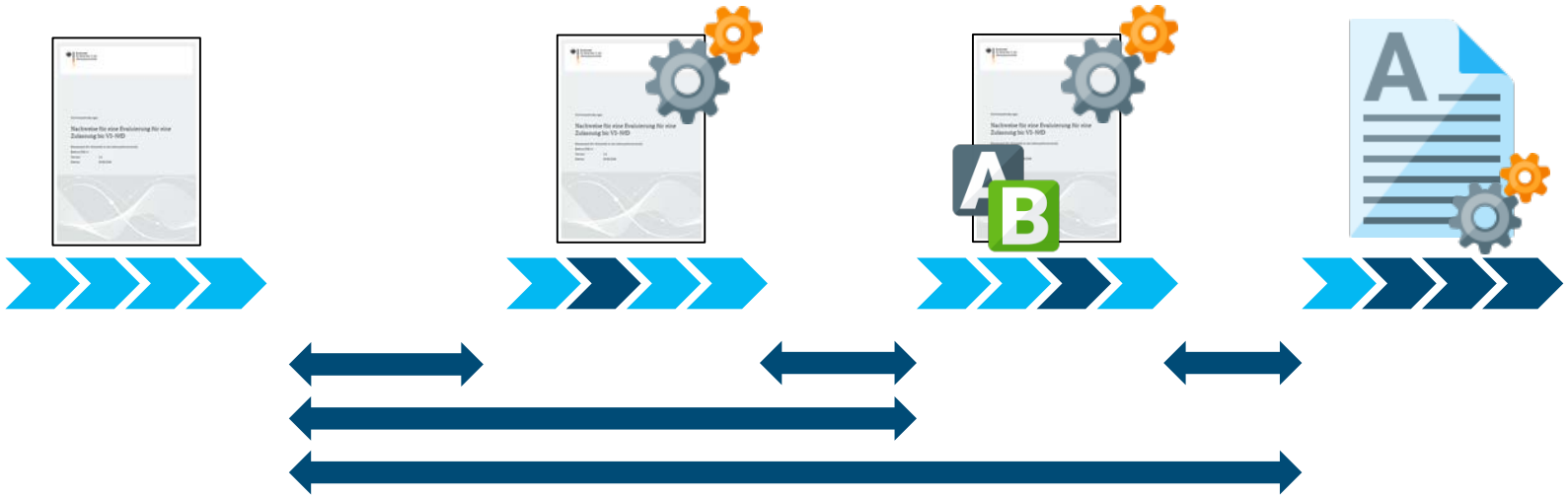
Phase B – Konzeptuelle Arbeit

Redesign des Nachweiskatalogs zur Maximierung des Automatisierungspotentials

NIST OSCAL

Codeanalyse

Phase C - Evaluierung



Analyse und Vergleich der Änderungen im Evaluierungsprozess

Mockup und Testlauf für eine Alternative

Vergleich der Ergebnisse und Empfehlungen

Ausblick

- Was bedeutet das für Sie?
  - In Zukunft: Weniger repetitive manuelle Tätigkeiten
  - Diskussion in nationalen und internationalen Communities
  - Einsatz von Tools (CI/CD-Pipeline)
  - Standardisierung von Tools und Schnittstellen

Welche Tools verwenden Sie in Ihrer CI/CD-Pipeline?

gp-dust@bsi.bund.de

Kontakt

Deutschland
Digital•Sicher•BSI•

Jan Sinkewitz, BSI

Sachbearbeiter
Referat KM 26 – Sichere stationäre VS-IT
Jan.sinkewitz@bsi.bund.de
Tel. +49 228 99 9582 5638

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de / www.bsi-fuer-buerger.de

Dr. Matthias Meyer, Fraunhofer IEM

Abteilungsleiter
Sichere IoT-Systeme
matthias.meyer@iem.fraunhofer.de
Tel. +49 5251 5465 122

Fraunhofer IEM
Zukunftsmeile 1
33102 Paderborn
www.iem.fraunhofer.de

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

Fraunhofer IEM

Offene Diskussion

Mentimeter

- Welche Tools benutzen Sie bereits in Ihren Build Pipelines?
  - Unterstützen diese den Evaluierungsprozess?
  - Verwenden Sie statische oder dynamische Analysetools?

- Sehen Sie Risiken in der weiteren Automatisierung des Evaluierungsprozesses?
  - Wie könnten diese entschärft werden?