DEVISE

DatEnqualitätsmanagement zur Verbesserung der InformationsSicherhEit

UR.ifs

Sachbericht zum Verwendungsnachweis
Teil I

Verbundprojekt: Datenqualitätsmanagement zur Verbesserung der Informationssicherheit (DEVISE)

Teilvorhaben: DRIVE
Förderkennzeichen: 16KIS1347K

Oktober 2024

Universität Regensburg

1. Ursprüngliche Aufgabenstellung

Das DEVISE-Projekt hatte das Ziel, die Qualität sicherheitsrelevanter Daten aus den Bereichen Identity and Access Management (IAM) sowie Cyber Threat Intelligence (CTI) zu messen und zu verbessern. Zu diesem Zweck wurde ein umfassendes Reifegradmodell entwickelt, das Methoden zur Datenqualitätsbewertung integriert. Neben der theoretischen Entwicklung des Modells stand dessen praktische Anwendung im Fokus, um die Effektivität in realen Szenarien zu evaluieren. Durch die enge Zusammenarbeit der Projektpartner wurden die Ziele auf wissenschaftlicher und praktischer Ebene bearbeitet.

2. Anknüpfung an den wissenschaftlichen und technischen Stand

An den wissenschaftlichen und technischen Stand aus dem DEVISE Projekt kann in Zukunft angeknüpft werden. Aus dem DEVISE-Projekt sind wissenschaftliche Publikationen hervorgegangen, weitere sind in Begutachtung oder Einreichung. Diese Arbeiten fließen direkt in die Projektergebnisse und Dissertationen der beteiligten Mitarbeiter:innen ein. Auch Studierende profitieren durch Seminar- und Abschlussarbeiten in den Bereichen Reifegradmodelle und Datenqualität. Die genannten Einschränkungen des Modells bieten eine Grundlage für weitere Arbeiten in verwandten Bereichen der Informationssicherheit. Zukünftige Projekte sollten die Komplexität und den Zeitbedarf für die Messung der Datenqualität berücksichtigen.

3. Ablauf des Vorhabens

Das Projekt wurde planmäßig durchgeführt, wobei eine kostenneutrale Verlängerung von sechs Monaten notwendig war, um zusätzliche Erkenntnisse zu gewinnen und offene Arbeitspakete abzuschließen. Der Ablauf des Projekts war in sechs Arbeitspakete (AP) unterteilt:

- **AP1:** Koordination und Monitoring: Organisation und Dokumentation aller Projektaktivitäten, Bereitstellung einer Arbeitsumgebung und Kommunikation der Ergebnisse über Website und Pressearbeit.
- **AP2:** Entwicklung und Design des Reifegradmodells: Entwicklung eines Reifegradmodells mit vier Stufen basierend auf Literaturrecherchen und Zielgruppenanalysen.
- **AP3:** Instanziierung des Reifegradmodells: Anpassung des Modells an die Bereiche IAM und CTI, inklusive Berücksichtigung spezifischer Anforderungen und Validierung durch Partner.
- **AP4:** Messung der Datenqualität im Bereich IAM: Entwicklung und Validierung von Indikatoren und Qualitätsdimensionen zur Bewertung der IAM-Datenqualität.
- **AP5:** Messung der Datenqualität im Bereich CTI: Entwicklung und Evaluierung von Indikatoren zur Messung der CTI-Datenqualität mit Fokus auf Incident Response Playbooks.
- **AP6:** Implementierung und Veröffentlichung: Technische Umsetzung, iterative Tests und Veröffentlichung des Modells als Open-Source-Referenz.

4. Wesentliche Ergebnisse und Zusammenarbeit mit anderen Forschungseinrichtungen

Das DEVISE-Projekt hat eine Vielzahl von Ergebnissen hervorgebracht, die sowohl theoretische als auch praktische Fortschritte in den Bereichen Datenqualität und Informationssicherheit ermöglichen. Die enge Zusammenarbeit der Projektpartner trug wesentlich dazu bei, die angestrebten Ziele zu erreichen und die wissenschaftliche Relevanz der Ergebnisse zu sichern.

- **Reifegradmodell:** Das zentrale Ergebnis des Projekts ist ein Reifegradmodell mit hierarchischen Stufen. Diese Reifegrade ermöglichen es, die Datenqualität systematisch zu bewerten und gezielt zu verbessern. Das Modell wurde so konzipiert, dass es flexibel auf unterschiedliche Anwendungsbereiche, wie IAM und CTI, angewendet werden kann. Es bietet eine fundierte Grundlage für die Bewertung von Datenqualität und unterstützt Organisationen dabei, ihre Sicherheitsmaßnahmen schrittweise zu optimieren.
- **Datenqualitätsindikatoren:** Für IAM und CTI wurden spezifische Indikatoren (SQIs) entwickelt, die die Datenqualität messbar und vergleichbar machen. Im Bereich IAM konzentrierten sich die Indikatoren auf Dimensionen wie Vollständigkeit und Genauigkeit, während im Bereich CTI der Fokus auf der Bewertung von Daten für Incident Response Playbooks lag. Diese Indikatoren wurden in mehreren Iterationen evaluiert und in das Reifegradmodell integriert, um eine praxisnahe Anwendung zu gewährleisten.
- **Instanziierungen des Modells:** Das Reifegradmodell wurde erfolgreich in den Bereichen IAM und CTI instanziiert. Für IAM ermöglichte die Anwendung des Modells eine präzisere Bewertung der Datenqualität in Bezug auf Zugriffsrechte und -kontrollen. Im Bereich CTI wurden Incident Response Playbooks analysiert, um die Qualität und Praktikabilität sicherheitsrelevanter Daten zu verbessern. Diese Instanziierungen zeigten die Flexibilität und Anwendbarkeit des Modells in verschiedenen Domänen.

Wissenschaftliche Publikationen: Die Ergebnisse des Projekts wurden in mehreren wissenschaftlichen Publikationen veröffentlicht, die sich mit den Themen Reifegradmodelle, Datenqualität und Informationssicherheit beschäftigen. Diese Publikationen leisten einen wichtigen Beitrag zur wissenschaftlichen Diskussion und ermöglichen den Wissenstransfer in angrenzende Forschungsbereiche wie Cyber Threat Intelligence und Identity and Access Management.

DEVISE

DatEnqualitätsmanagement zur Verbesserung der InformationsSicherhEit

UR.ifs

Sachbericht zum Verwendungsnachweis
Teil II

Verbundprojekt: Datenqualitätsmanagement zur Verbesserung der Informationssicherheit (DEVISE)

Teilvorhaben: Design des Reifegradmodels und Integration Von DatenqualitätsElementen (DRIVE)
Förderkennzeichen: 16KIS1347K

Oktober 2024

UR-WI1
Universität Regensburg

1. Ausführliche Darstellung der im Rahmen des Vorhabens durchgeführten Arbeiten und Vergleich zur ursprünglichen Vorhabenbeschreibung

In diesem Abschnitt erfolgt ein SOLL-IST-Abgleich zur ursprünglichen Vorhabensbeschreibung bezüglich der Meilensteine und einzelner Arbeitspakete im Rahmen des DEVISE-DRIVE Vorhaben. Die folgende Abbildung 1 zeigt den zeitlichen Ablauf der Arbeiten des Teilvorhabens in einer Übersicht, wobei die Arbeitspakete (AP) sowie Meilensteine (M1-M5) und das ursprüngliche Projektende (E1) vor der kostenneutralen Verlängerung gekennzeichnet sind.

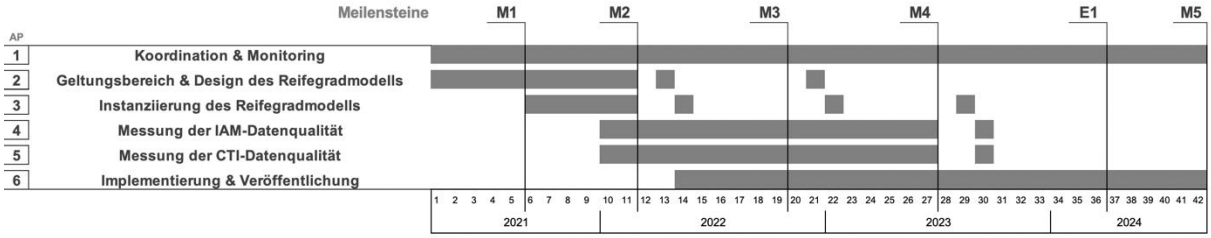

Abbildung 1: Projektablaufplan der UR-WI1 als GANTT-Diagramm

Das Ziel von DEVISE war die Messung und Verbesserung der Qualität sicherheitsrelevanter Daten aus den Bereichen Identity und Access Management sowie Cyber Threat Intelligence mittels eines umfassenden Reifegradmodells und der Anwendung von Datenqualitätsmethoden für die IT-Sicherheit.

Das Teilvorhaben DEVISE-DRIVE widmete sich vor allem dem Design, der Implementierung sowie der iterativen Verbesserung des zu entwickelnden Reifegradmodells zur Feststellung und Verbesserung der Qualität sicherheitsrelevanter Daten. Von zentraler Bedeutung ist in diesem Zusammenhang auch die Anwendung des Modells in den berücksichtigten Geltungsbereichen. Im Teilvorhaben DEVISE-DRIVE wurde zudem das Gesamtvorhaben DEVISE koordiniert. Neben den genannten Schwerpunkten war UR-WI1 zudem verantwortlich für die Integration der Arbeitsergebnisse aus allen Teilprojekten, um eine zielgerichtete Erstellung eines umfassenden Reifegradmodells zu überwachen und sicherzustellen.

AP1: Koordination und Monitoring (SOLL)
In AP1 werden die globalen Arbeiten des Projektes durch den Partner UR-WI1 koordiniert. Die **6 PM** von UR-WI1 werden auf die folgenden Aufgaben aufgeteilt.
Aufgaben und Problemlösungsstrategie von UR-WI1: - **Interne Projektkommunikation und Dokumentation (1 PM)** Für das DEVISE-Projekt wird im Rahmen dieses APs von UR-WI1 die interne Projektkommunikation und Dokumentation durchgeführt. Dabei werden die erzielten Ergebnisse aufbereitet und für das weitere Projektvorgehen zusammengefasst. Weiter koordiniert UR-WI1 die Dokumentation bezüglich der einzelnen Projektergebnisse der Projektpartnern. - **Projektmonitoring und -steuerung (1 PM)** Im Rahmen des Projektmonitoring wird der Fortschritt der Arbeiten überwacht und ggf. steuernd eingegriffen, um die langfristigen Projektziele zu erreichen. - **Pressearbeit und Webseite (1 PM)** Um die Reichweite des Projektes zu erhöhen wird UR-WI1 mit regelmäßigen Pressemitteilungen für eine Sichtbarkeit des Projektes nach außen sorgen. Daneben wird eine Webseite erstellt, die Ziele und Inhalte des DEVISE-Projekts darstellt. - **Organisation und Durchführung der Projekttreffen (2 PM)** UR-WI1 organisiert die internen Projekttreffen und führt diese durch. - **Virtuelle Arbeitsumgebung (1 PM)** Zur Zusammenarbeit dient ein internes Source-Code Repository für die

Referenzimplementierungen sowie eine Plattform zur kollaborativen Bearbeitung von Dokumenten. Mögliche Optionen werden von UR-WI1 evaluiert. Die am besten geeignete Option wird von UR-WI1 für das Projektvorhaben vorbereitet und falls notwendig, bereitgestellt.
Beitrag zu den Meilensteinen von UR-WI1: - **M1:** Gemeinsame virtuelle Arbeitsumgebung

AP1: Koordination und Monitoring (IST)

Im Rahmen der Projektkoordination und des Monitorings der Projektfortschritte wurden die Projektfortschritte dokumentiert und aufbereitet, sowie die Projektkommunikation über unterschiedliche Kanäle (Teams, Zoom, Cloud) verwaltet.

Damit die langfristigen Projektziele erreicht werden konnten wurden diese in regelmäßigen Abständen in den Arbeitstreffen sowie bei den Projekttreffen überprüft und falls notwendig gesteuert.

Um das Projekt nach außen hin zu bewerben und die Sichtbarkeit zu erhöhen, hat UR-WI1 eine Website erstellt, auf der die aktuellen Entwicklungen und Publikationen kommuniziert werden. Des Weiteren wurden Publikationen, die im Rahmen des Projektes entstanden auf LinkedIn und ResearchGate veröffentlicht.

Über den gesamten Projektverlauf hinweg wurden globale Projekttreffen (in 6-monatigen Abständen) sowie dedizierte Projektreffen zu spezifischen Meilensteinen durchgeführt. Zur Optimierung der Abstimmung zwischen den Projektpartnern, fanden zusätzlich im 4-wöchigen Turnus Onlinekonferenzen statt. Die Organisation der Projekttreffen wird zwischen den Projektpartnern rotiert und die jeweiligen Themen an den Fortschritt angepasst. UR-WI 1 achtet auf die Durchführung der Projekttreffen sowie die Kommunikation des Projektfortschrittes.

Meilenstein M1: Gemeinsame virtuelle Arbeitsumgebung

- Eine gemeinsame virtuelle Arbeitsumgebung wurde erstellt und setzt sich aus nachfolgenden Tools zusammen:
    - Nextcloud (Speicherung gemeinsamer Inhalte)
    - Gitlab (Speicherung und gemeinsame Bearbeitung von Code)
    - Teams (schnelle und einfache Kommunikation und Dokumentbearbeitung)
    - E-Mail-Verteiler (einfache Erreichbarkeit aller Projektpartner)
    - Zoom (einfache Erstellung und Nutzung von Onlinekonferenzen)

AP2: Geltungsbereich & Design des Reifegradmodells (SOLL)
In AP2 wird die zielgruppengerechte Erhebung des Geltungsbereiches und das Design des allgemeinen Reifegradmodells verfolgt. Zur Bewerkstelligung des AP2 sind seitens UR-WI1 **12 PM** geplant.
Aufgaben und Problemlösungsstrategie von UR-WI1: - **Literaturübersicht (2 PM)** UR-WI1 erstellt eine Übersicht der akademischen Literatur sowie praxisnaher Dokumentation zu Reifegradmodellen mit einer ausführlichen Analyse bestehender Ansätze, Einordnung dieser und Herausarbeitung von Weiterentwicklungspotentialen. Der Schulterschluss zum Datenqualitätsmanagement ist in diesem Zusammenhang eine weitere relevante Aufgabe. - **Bestimmung des Geltungsbereichs (3 PM)** UR-WI1 bestimmt den Geltungsbereich aus einer akademischen Perspektive. Zudem koordiniert und konsolidiert UR-WI1 die Definition des Geltungsbereichs (u.a. Zielgruppe, Anwendungsbereich, Anwendungszweck, etc.), welcher sich aus den ermittelten organisatorischen Anforderungen bei den Projektpartnern und assoziierten Partnern zusammensetzt.

- **Entwurf des Reifegradmodells (4 PM)** Entsprechend des Geltungsbereichs definiert UR-WI1 das Design der Architektur für das Reifegradmodell und bündelt dabei die Bedürfnisse der Zielgruppen. In diesem Zusammenhang werden auch die assoziierten Partner mit einbezogen und eine fundierte Analyse der für die Anwendung des Modells erforderlichen Daten und Datenformate wird durchgeführt. - **Definition der Reifegrade (3 PM)** Basierend auf dem Entwurf und den funktionalen sowie nicht-funktionalen Anforderungen der Partner bestimmt UR-WI1 iterativ die Reifegrade (SQMs) des Modells. Dabei werden neugewonnene Erkenntnisse aus der Wissenschaft und Erfahrungen aus der Anwendung des Reifegradmodells berücksichtigt.
Beitrag zu den Meilensteinen von UR-WI1: - **M1:** Wissenschaftliche Literaturübersicht zu bestehenden Reifegradmodellen und Datenqualitätsmanagementansätzen - **M1:** Definition der Ausrichtung und des Umfangs des DEVISE-Reifegradmodells - **M2:** Design des Reifegradmodells durch Einbezug der Anforderungen und Modellaufbau - **M2:** Initiale Definition der Reifegrade (SQMs) - **M4:** Finale Version der SQMs

AP2: Geltungsbereich & Design des Reifegradmodells (IST)

Meilenstein M1: Wissenschaftliche Literaturübersicht zu bestehenden Reifegradmodellen und Datenqualitätsmanagementansätzen

- Eine wissenschaftliche Literaturübersicht zu bestehenden Reifegradmodellen bildet einen wesentlichen Bestandteil der CTI-SOC2M2 Publikation. Im Detail werden dabei Reifegradmodelle zu CTI und verwandten Anwendungsgebieten (z.B. Incident Response, Information Security Management, oder Security Operations) diskutiert. Es lässt sich dabei feststellen, dass Reifegradmodelle für verschiedene Anwendungsgebiete existieren (z.B. Security Operations Center), jedoch CTI und Datenqualität zusammen nicht näher betrachtet werden. Ein zunehmender Einsatz von Reifegradmodellen im Kontext der Informationssicherheit ist auszumachen.
- An dieser Stelle sei zudem auf den kollaborativen Ansatz des DEVISE-Projekts hingewiesen. So konnten durch die Expertise von UR-WI2 wesentliche Publikationen zu Datenqualitätsmanagementansätzen zusammengetragen werden. Hier hat UR-WI2 im Rahmen der regelmäßigen Arbeitstreffen relevante Publikationen vorgestellt. UR-WI1 hat sich daraufhin mit diesen auseinandergesetzt und Herausforderungen und wesentliche Elemente (z.B. DQ-Prozessschritte und Herangehensweisen von DQ-Frameworks) identifiziert. Die Prozessschritte spielen bei dem Design des Reifegradmodells eine Rolle.

Meilenstein M1: Definition der Ausrichtung und des Umfangs des DEVISE-Reifegradmodells

- **Ausrichtung:** Das DEVISE-Reifegradmodell hat einen klaren Bezug zur Informationssicherheit und ist auf die Messung der Datenqualität ausgerichtet. Es erfolgt eine Abgrenzung vom Management der Datenqualität (DQ-Management). DQ-Management ist implizit durch den stufenweisen Aufbau des Reifegradmodells gegeben. Im Rahmen von DEVISE entstehen einzelne elementare Komponenten eines übergeordneten Reifegradmodells. Diese Komponenten sind explizit auf einzelne Aspekte zur Messung der Datenqualität ausgerichtet, bilden aber kein vollumfängliches Reifegradmodell.
- **Umfang:** Der Geltungsbereich wird über vorliegende sicherheits-relevante Daten und modulare Komponenten definiert. Das DEVISE-Reifgradmodell wird in seiner Definition allgemein gehalten (angelehnt an CMMI, Reifegrade, Fähigkeitsgrade und Indikatoren), damit

es sowohl IAM als auch CTI abdeckt. Es erfolgt daher keine Einschränkung auf Ebene des Reifegradmodells, sondern ausschließlich auf Ebene der Instanziierung in verschiedenen Anwendungsgebieten. Konkret bedeutet dies, dass mit dem DEVISE-Reifegradmodell stets eine Aggregation von Ergebnissen der DQ-Metriken von den Indikatoren aufwärts möglich ist. Der Umfang des DEVISE-Reifegradmodells wird über die bereitgestellten Verfahren und Methoden präzisiert. Verfahren und Methoden sind Teil der Instanziierung.

Meilenstein M2: Design des Reifegradmodells durch Einbezug der Anforderungen und Modellaufbau

- Die DEVISE-Projektpartner haben gemeinsam das Design des DEVISE-Reifegradmodells festgelegt. Dabei wurde eine Struktur angelehnt an das CMMI-Reifegradmodell verwendet. Das DEVISE-Reifegradmodell ist im Rahmen der Instanziierung flexibel auf einzelne Anforderungen, Zielgruppen und Anwendungsbereiche anwendbar.
- Nach einer kleinen Verzögerung beim Design des DEVISE-Reifegradmodells aufgrund der doch sehr unterschiedlichen Anwendungsbereiche innerhalb der IT-Sicherheit konnte dies fertig gestellt werden.

Meilenstein M2: Initiale Definition der Reifegrade (SQMs)

- Die initiale Definition der Reifegrade ist erfolgt. Dabei wurde ein aggregierter Ansatz für CTI und IAM mit den Reifegraden: 0) Initial, 1) Reaktiv, 2) Proaktiv, und 3) Kollaborativ gewählt. Diese werden nun dementsprechend von den Projektpartnern angewandt und instanziiert.

Meilenstein M4: Finale Version der SQMs

- Diese Reifegrade leiten sich aus dem Kontext der IT-Sicherheit ab und umschreiben damit in ihrer hierarchisch aufsteigenden Art (von SQM-0 hin zu SQM-3) die zunehmende Nutzbarkeit der Daten in der jeweiligen Qualität für umfassendere Sicherheitsmaßnahmen. Die finalen Reifegrade wurden wie folgt definiert.
- SQM-0: Initial: Das Datenqualitätsmanagement der sicherheitsrelevanten Daten ist nicht bis kaum vorhanden. Die entsprechenden Daten werden nur teilweise und bruchstückhaft gesammelt und hinsichtlich ihrer Qualität bewertet. Eine kontinuierliche Verbesserung der Datenqualität für die IT-Sicherheit ist nicht etabliert.
- SQM-1: Reaktiv: Es liegt eine umfassende Datensammlung für die IT-Sicherheit vor. Die Datenqualität dieser Sammlung ist auf einem Niveau, welches vor allem reaktive Sicherheitsmaßnahmen ermöglicht. Es finden erste Initiativen zur Verbesserung der Datenqualität statt.
- SQM-2: Proaktiv: Die Sammlung sicherheitsrelevanter Daten ist auf den gesamten Geltungsbereich ausgeweitet und neue Datenquellen werden erschlossen. Die Qualität der Daten und Datenquellen ist auf einem hohen Niveau, welches neben reaktiven auch umfassende proaktive Sicherheitsmaßnahmen unterstützen kann. Die iterative Verbesserung des Datenqualitätsmanagements wird weiter forciert.
- SQM-3: Kollaborativ: Alle Maßnahmen der vorhergehenden Reifegrade werden weiter verbessert. Jedoch findet vor allem im Hinblick auf die Verbesserung der Datenqualität eine Öffnung statt und entsprechende Aktivitäten werden von mehreren Akteuren aus möglicherweise unterschiedlichen adressierten Personenkreisen kollaborativ und kontinuierlich vorangetrieben.
- Bei der Instanziierung des DEVISE-Reifegradmodells in unterschiedlichen Geltungs- und Anwendungsbereichen sowie damit verbunden für verschiedene Zielgruppen kann es notwendig sein, dass die Reifegrade in ihrer Grundform zwar erhalten bleiben, aber in ihrer Reihenfolge angepasst werden. Beispielsweise kann es notwendig sein, dass die

Reifegrade „Reaktiv“ und „Proaktiv“ vertauscht werden. Zudem kann auch ihre Beschreibung im Hinblick auf den jeweiligen Anwendungsbereich erweitert und konkretisiert werden. Entsprechende Maßnahmen im Rahmen einer Instanziierung bleiben explizit möglich.

AP3: Instanziierung des Reifegradmodells (SOLL)
Das AP3 zielt auf die Instanziierung des Reifegradmodells ab. Für das AP3 sind insgesamt **8 PM** für die Arbeiten von UR-WI1 veranschlagt.
Aufgaben und Problemlösungsstrategie von UR-WI1: - **Identifizierung der Fähigkeitsgrade (2 PM)** UR-WI1 liefert einen wissenschaftlichen Beitrag zur Ausgestaltung der Fähigkeitsgrade (SQCs) nach unternehmensweiten Bestimmungsbereichen in Kooperation mit den Projektpartnern. - **Instanziierung des Reifegradmodells (4 PM)** Der Abgleich der Fähigkeitsgrade hinsichtlich Exklusivität und Vollständigkeit wird von UR-WI1 durchgeführt. Daneben erfolgt die Erstellung einer Zuordnung der Fähigkeitsgrade zu den in AP2 erarbeiteten Reifegraden in Zusammenarbeit mit den weiteren am AP beteiligten Partnern. Durch die Gewichtung der SQCs für die Bestimmung der Reifegrade wird ein weiterer Aspekt zur Instanziierung des Reifegradmodells bearbeitet. - **Aufbereitung des Reifegradmodells (2 PM)** Das Reifegradmodell wird von UR-WI1 unter Berücksichtigung unterschiedlicher Detailierungsebenen zur bedarfsgerechten Kommunikation innerhalb und außerhalb des Projektes aufbereitet.
Beitrag zu den Meilensteinen von UR-WI1: - **M2:** Zuordnung und Gewichtung exklusiver und vollständiger SQCs zu den SQMs - **M3:** Vorarbeit zur ersten Version der Referenzimplementierung durch eine erste Aufbereitung der bereits erarbeiteten Bestandteile

AP3: Instanziierung des Reifegradmodells (IST)

Meilenstein M2: Zuordnung und Gewichtung exklusiver und vollständiger SQCs zu den SQMs

- Eine spezifische Zuordnung und Gewichtung der Bestandteile erfolgt weiterhin wie im DEVISE-Rahmenkonstrukt beschrieben auf individueller Ebene. Hierbei liegt der Fokus auf der Messung der Datenqualität.
- Eine explizite Zuordnung und Gewichtung der Bestandteile hat wie im DEVISE-Rahmenkonstrukt beschrieben auf individueller Ebene bei der Instanziierung zu erfolgen. Es wurde dabei auf eine Fokussierung der Messung der Datenqualität abgestellt, die jedoch auch Datenverfügbarkeit und Verbesserung umfasst. Das Zusammensetzen einzelner Komponenten kann erst nach deren Entwicklung erfolgen, weshalb zum jetzigen Zeitpunkt die Gewichtung über eine Beschreibung des Vorgehens abgedeckt wird.

Meilenstein M3: Vorarbeit zur ersten Version der Referenzimplementierung durch eine erste Aufbereitung der bereits erarbeiteten Bestandteile

- Die bereits entwickelten Komponenten sind in flexibel anpassbare Ansätze gegliedert, die mit Unterstützung einzelner Metriken von den DEVISE-Projektpartnern umgesetzt werden. Dies spiegelt sich in einem Auswahlleitfaden für die DQ-Dimensionen wider, denn es soll ein fester Ansatz, der sich global durch das Projekt zieht, vermieden werden, um Flexibilität in der Integration und Interaktion der einzelnen Komponenten zu gewährleisten. Dabei beanspruchte die Umsetzung der Referenzimplementierung zusätzliche Arbeiten, die nun durch die kostenneutrale Verlängerung abgefangen werden können.

AP4: Messung der IAM-Datenqualität (SOLL)
In AP4 werden die Indikatoren (SQIs) zur Bestimmung der Fähigkeitsgrade im Bereich des IAM erhoben und mit bereits bestehenden generischen IAM-Indikatoren abgeglichen. Im AP4 sind **14 PM** für die Arbeiten von UR-WI1 geplant.
Aufgaben und Problemlösungsstrategie von UR-WI1: - **Entwicklung der Indikatoren zur Messung von IAM-Datenqualität (5 PM)** Für die Entwicklung der Indikatoren (SQIs) bestimmt UR-WI1 zusammen mit dem Projektpartner NEX zunächst die wesentlichen Einflussfaktoren für die DQ im Kontext des IAM. Ein Vergleich generischer IAM-Indikatoren mit den erhobenen Einflussfaktoren wird durchgeführt. Die Indikatoren von UR-WI1 und NEX werden durch Zuordnung zu Untergebieten des IAM konkretisiert. UR-WI1 fasst die Indikatoren mit den erarbeiteten Qualitätsdimensionen, Metriken und Verfahren in einem übersichtlichen Katalog zusammen, um eine Implementierung im Rahmen des Referenzmodells (AP6) zu ermöglichen. - **Quantitative Analysen der Datenqualität in IAM (5 PM)** UR-WI1 koordiniert die Ableitung von Qualitätsdimensionen für die Indikatoren. Hierfür erhebt UR-WI1 zusammen mit UR-WI2 vorrangig Dimensionen aus der Wissenschaft. Zudem werden weitere, praxisnahe Dimensionen des Partners NEX berücksichtigt. Im Rahmen der quantitativen Analysen führt UR-WI1 Qualitätsdimensionen, Metriken und Messverfahren der am AP beteiligten Partner zusammen und konsolidiert diese. - **Evaluation der IAM-bezogenen Qualitätsdimensionen, Metriken und Verfahren (4 PM)** Mit der Ausarbeitung unterschiedlicher Evaluationsszenarien für die entwickelten Qualitätsdimensionen, Metriken und Verfahren wirkt UR-WI1 an der Evaluation mit. Die Kommunikation und Analyse der Evaluationsszenarien hinsichtlich Relevanz und Praktikabilität mit den Projektpartnern gehört zusätzlich zu den Aufgaben von UR-WI1. Die Ergebnisse der Evaluation dienen als Input für iterative Anpassungen in AP2 und AP3.
Beitrag zu den Meilensteinen von UR-WI1: - **M3:** Erarbeitung von SQIs und SQDs im Bereich IAM - **M5:** Finale Version der SQIs und SQDs

AP4: Messung der IAM-Datenqualität (IST)

Meilenstein M3: Erarbeitung von SQIs und SQDs im Bereich IAM

- Im Bereich IAM wurden in Kooperation mit dem Projektpartner NEX Datenqualitätsdimensionen erörtert. Mit Hilfe einer Auswahlhilfe werden im aktuellen Verlauf Ansätze zur Messung der IAM-Datenqualität in enger Kooperation mit NEX geprüft und umgesetzt. Einblicke in praxisrelevante IAM-Daten sind hier entscheidend.

Meilenstein M5: Finale Version der SQIs und SQDs

- Die geforderten Fähigkeiten innerhalb der einzelnen Reifegrade des DEVISE-Modells leiten sich aus den drei zentralen Phasen des Datenqualitätsmanagements ab:
- ***SQC-1*: State Reconstruction:** In dieser Phase werden die (sicherheits-)relevanten Daten sowie Kontextinformationen aus Prozessen, Services, Datensammlungen, (Management-) Vorgaben, bereits bekannte Qualitätsprobleme, Kosten, etc. zusammengetragen.
- ***SQC-2*: Assessment:** In dieser Phase wird die konkrete Qualität der gesammelten sicherheitsrelevanten Daten gemessen und bewertet. Eine zentrale Rolle spielen dabei die unterschiedlichen Qualitätsdimensionen anhand derer die Daten gemessen werden müssen.
- ***SQC-3*: Improvement:** Diese letzte Phase des Datenqualitätsmanagement betrifft die konkreten Schritte, Strategien und Techniken, welche zur Erfüllung weiterführender Ziele hinsichtlich der Datenqualität verfolgt werden müssen.

- Für jede dieser Phasen muss in den einzelnen SQMs ein bestimmter Zielerreichungsgrad nachgewiesen werden. Die jeweiligen notwendigen Voraussetzungen sowie ihr Aufbau sind im Rahmen des Prozesses der Instanziierung festzulegen.
- **SQI:** Die Indikatoren dienen der Bestimmung der Zielerreichung innerhalb der SQCs erfolgt durch die Definition konkreter Zielgrößen. Innerhalb des DEVISE-Projektes liegt hierbei ein starker Fokus auf der Sammlung, Strukturierung und Interpretation von Datenqualitätsdimensionen, welche innerhalb des Reifegradmodells die zentralen Indikatoren für SQC-2 (Assessment) darstellen. Die Qualität von sicherheitsrelevanten Daten lässt sich anhand einer Vielzahl unterschiedlicher Dimensionen bestimmen, welche stark abhängig vom jeweiligen Geltungsbereich, der Ausrichtung, sowie des adressierten Personenkreises sind. Entsprechend erarbeiten die Projektpartner:innen ein ergänzendes Dokument zur Sammlung relevanter Dimensionen als Auswahlhilfe für SQIs die Fähigkeit SQC-2 betreffen. Jedem Indikator muss ein konkretes Verfahren zur transparenten und möglichst objektiven Messung sowie eine Interpretation verschiedener Ergebnisse der Messung zugeordnet werden.
- **Auswahl und Gewichtung der SQI:** Im nächsten Schritt der Instanziierung sind für die Domäne relevante Indikatoren (SQI) für die übergeordneten Fähigkeiten (SQC) zu bestimmen. Im Hinblick auf das DQ-Management als Grundlage des DEVISE-Reifegradmodells spielen hier vor allem unterschiedliche, für die Domäne relevante DQ-Dimensionen eine zentrale Rolle. Dies ist der Fall, da in den verschiedenen Geltungsbereichen äußerst unterschiedliche DQ-Dimensionen von unterschiedlicher Bedeutung sein können. Neben der Abhängigkeit vom konkreten Geltungsbereich sind diese Dimensionen auch im Hinblick auf den adressierten Personenkreis und dessen Erwartungen bzw. Vorstellungen unterschiedlich zu bewerten. An dieser Stelle der Instanziierung kann das in diesem Dokument beschriebene, übergeordnete Modell nur noch wenige Anhaltspunkte liefern, sondern es muss vielmehr ein möglichst komplettes Bild des Geltungsbereichs mit unterschiedlichen SQIs ermöglicht werden. Das übergeordnete Modell gibt hierfür keine konkreten Vorgaben mehr.
- Eine weitere Notwendigkeit in diesem Zusammenhang ist die Interpretation der SQIs im Geltungsbereich. So kann die Datenqualitätsdimension der Genauigkeit (als ein Beispiel für einen Indikator für SQC-2) in unterschiedlichen Anwendungsbereichen unterschiedliche Bedeutungen haben. Insbesondere gilt dies für die Interpretation des Grades der Erfüllung des SQI. Es gilt hier also beispielsweise zu beantworten was eine „Genauigkeit von 80% der zugrundliegenden Daten“ in einer Domäne bedeutet.
- Neben der Bestimmung und Interpretation der SQIs selbst müssen diese auch den Fähigkeiten zugeordnet werden. Zudem ist es notwendig, dass die Schwellwerte der SQCs für die SQMs innerhalb des Geltungsbereichs festgeschrieben werden. Die Erreichung der Schwellwerte muss transparent, nachvollziehbar und möglichst objektiv über die SQIs bestimmbar sein.
- **Entwurf der Messverfahren für die SQI:** Um die Bestimmbarkeit der Zielerreichung innerhalb der SQCs zu ermöglich, müssen konkrete Messverfahren i.S.v. Metriken für die SQIs definiert werden. Die Metriken sind nach einer initialen, abstrakten Definition zudem für die zur Verfügung stehenden sicherheitsbezogenen Informationen, für die sie im Geltungsbereich angewendet werden sollen zu konkretisieren.
- Mit dem Durchlaufen dieser Aktivitäten kann das abstrakten DEVISE-Reifegradmodell zum DQ-Management für sicherheitsrelevante Daten in ein spezifisches, auf einen bestimmten Geltungsbereich zugeschnittenes Modell überführt werden. Dieses spezifische Modell enthält daraufhin zudem die konkreten Messverfahren zur möglichst transparenten und objektiven Bewertung der Reifegrade. Das entsprechende Vorgehen wird im DEVISE-Projekt selbst für die zwei oben aufgeführten Geltungsbereich durchgeführt.

AP5: Messung der CTI-Datenqualität (SOLL)

In AP5 werden die Indikatoren zur Bestimmung der Fähigkeitsgrade im Bereich CTI erhoben. Im AP5 sind **12 PM** für die Arbeiten von UR-WI1 eingeplant.
Aufgaben und Problemlösungsstrategie von UR-WI1: - **Wissenschaftliches Vorgehen zur Erhebung der CTI-Datenqualität (5 PM)** Für die Entwicklung der Indikatoren zur Messung von CTI Datenqualität wird von UR-WI1 zusammen mit den akademischen Partnern in diesem AP ein Vorgehen ausgewählt und für die Anwendung vorbereitet. Die so entwickelten Indikatoren werden von UR-WI1 mit den erarbeiteten Qualitätsdimensionen, Metriken und Verfahren in einem übersichtlichen Katalog zusammengefasst, damit diese in die Implementierung des Referenzmodells (AP6) einfließen können. - **Qualitative Analysen der Datenqualität in CTI (4 PM)** UR-WI1 wirkt über die Identifizierung CTI-spezifischer Eigenschaften bei der Entwicklung der Qualitätsdimensionen für die Indikatoren im Bereich CTI mit. UR-WI1 wendet für die qualitativen Analysen die zuvor konzipierten Indikatoren zusammen mit den Partnern auf CTI-Daten an. - **Evaluation der CTI-bezogenen Qualitätsdimensionen, Metriken und Verfahren (3 PM)** Die Analyse der Evaluationsszenarien hinsichtlich Relevanz und Praktikabilität mit den Projektpartnern bildet einen von UR-WI1 gelieferten Baustein zur Evaluation. Darüber hinaus stellt UR-WI1 innerhalb geeigneter Evaluationsszenarien die Vorgehensweise der Evaluation zusammen. Die Ergebnisse der Evaluation dienen als Input für die iterative Anpassungen in AP2 und AP3.
Beitrag zu den Meilensteinen von UR-WI1: - **M3:** Erarbeitung des Vorgehens zur Entwicklung der SQIs und Evaluationsszenarien für SQDs im Bereich CTI

AP5: Messung der CTI-Datenqualität (IST)

Meilenstein M3: Erarbeitung des Vorgehens zur Entwicklung der SQIs und Evaluationsszenarien für SQDs im Bereich CTI

- Auf dem Gebiet der CTI und der Entwicklung von SQIs und SQDs sind zunächst durch eine wissenschaftliche Recherche interessante Datentypen und deren Datenqualität extrahiert worden. Die Komplexität innerhalb des Forschungsfeldes der CTI selbst macht jedoch eine Fokussierung auf einzelne CTI-Typen notwendig. Im Hinblick auf die Erreichung des Meilensteins stehen somit Incident Response Playbooks im Fokus.

AP6: Implementierung & Diskussion (SOLL)
In AP6 wird die Implementierung des Reifegradmodells und die Veröffentlichung der Projektergebnisse durchgeführt. Im AP6 sind **12 PM** für die Arbeiten von UR-WI1 vorgesehen.
Aufgaben und Problemlösungsstrategie von UR-WI1: - **Bereitstellung von Persistierungsmöglichkeiten (3 PM)** Für die Bereitstellung von Persistierungsmöglichkeiten erarbeitet UR-WI1 zuerst ein geeignetes Datenmodell. Die Evaluation möglicher Persistierungsvarianten und die Auswahl einer konkreten Option bildet eine Basis für die technische Implementierung des Reifegradmodells. Mit der Inbetriebnahme einer geeigneten Lösung schließt UR-WI1 die Bereitstellung ab. - **Implementierung der Reifegrade (4 PM)** Bei der Implementierung der Reifegrade besteht für UR-WI1 die Aufgabe der Umsetzung von Anforderungen und Design. Zusätzlich wird eine Schnittstelle zu den in AP3 entwickelten Fähigkeiten realisiert. Die Implementierung adressiert die funktionalen und nicht-funktionalen Anforderungen und bringt diese beiden Aspekte in Einklang.

- **Periodisches Testen (2 PM)** Für die Implementierung führt UR-WI1 in einem zuvor festgelegten Testintervall periodische Funktions- und Plausibilitätstests durch. - **Wissenschaftliche Diskussion (3 PM)** Die erzielten Teilergebnisse des DEVISE-Projekts werden im Rahmen von Konferenzen und Fachjournalen zur Diskussion gestellt. Das daraus resultierende Feedback und die Diskussion in unterschiedlichen Communities dient der Verifizierung von Entscheidungen, der Ausrichtung sowie Validierung des weiteren Vorgehens und wird in das Projekt integriert.
Beitrag zu den Meilensteinen von UR-WI1: - **M3**: Erarbeitung eines ersten Datenmodell und Auswahl der Speichermöglichkeit - **M4**: Fertigstellung des Datenmodells und Bereitstellung der Speichermöglichkeit und erste Version der Reifegradimplementierung - **M5**: Finale und evaluierte Version der Implementierung der Reifegrade

AP6: Implementierung & Diskussion (IST)

Meilenstein M3: Erarbeitung eines Datenmodells und Auswahl der Speichermöglichkeit

- In Zusammenarbeit mit allen Projektpartnern ist eine dezentrale Vorgehensweise und Umsetzung in Symbiose mit den einzelnen Teilbereichen vorgesehen. Dies bietet mehr Flexibilität und basiert auf dem gegebenen DEVISE-Reifegradmodell als übergeordnetes Rahmenkonstrukt. Grundsätzlich kann festgehalten werden, dass die Analyseergebnisse das Datenmodells tendenziell in Richtung key-value führen. Die Umsetzung eines dokumentenorientierten Ansatzes mit JSON und der Open-Source-Datenbank MongoDB steht in Diskussion und wäre eine Möglichkeit.

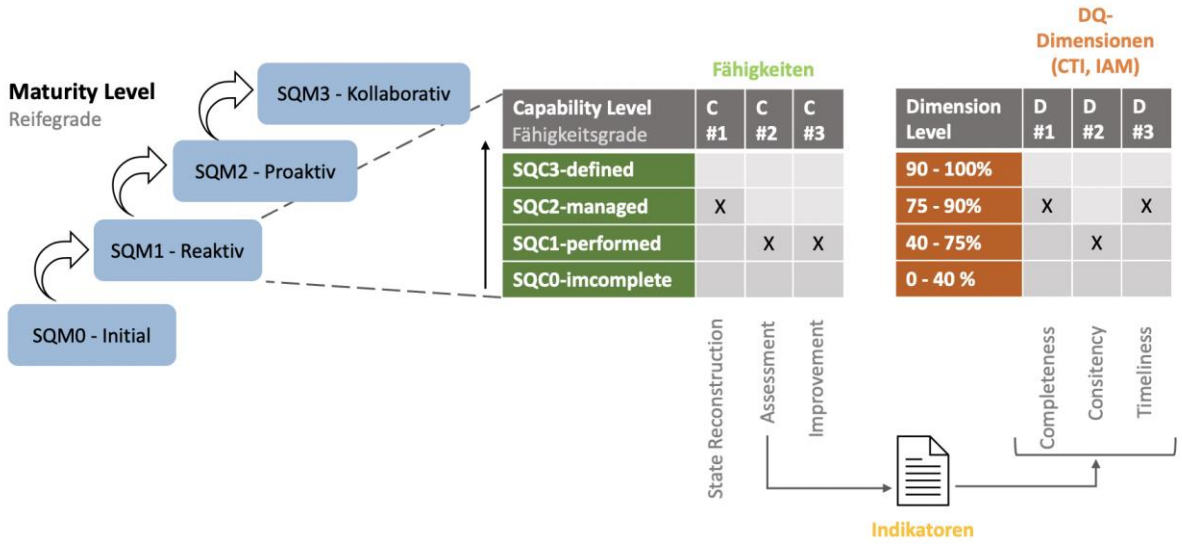

Abbildung 2: Entwickeltes DEVISE Reifegradmodell

2. Die wichtigsten Positionen des zahlenmäßigen Nachweises

Der Finanzierungsplan für das Teilvorhaben DEVISE-DRIVE umfasste im Wesentlichen drei Teilbereiche, für die finanzielle Mittel zur Bereitstellung von Ressourcen notwendig waren. Dabei handelte es sich zum einen um Personalkosten für die Durchführung der Aufgaben von UR-WI1 und zum anderen um Reisekosten und Sachkosten, welche in direktem Zusammenhang mit dem Teilvorhaben standen. Die tatsächlichen Kosten sind sehr ähnlich dem ursprünglich erstellten Finanzierungsplan und es gab keine größeren Abweichungen davon.

3. Notwendigkeit und Angemessenheit der geleisteten Projektarbeit

Die im Rahmen dieses Teilprojektes geplante Forschung barg große Risiken, die eine Zuwendung notwendig machten. Die spezielle Forschung im Bereich der Entwicklung eines Reifegradmodells zur Verbesserung der Qualität sicherheitsrelevanter Daten sowie die umfassende Messung der Datenqualität in den Bereichen IAM und CTI war durch die vielen offenen Fragen unter Umständen nur teilweise erfolgreich. Dies konnte dazu führen, dass einige Schritte des DEVISE-Prozesses nur teilweise oder gar nicht in der geplanten Form umsetzbar waren. Als Gegenmaßnahme wirkte UR-WI1 darauf hin, dass die Grundlagenforschung im Teilvorhaben DEVISE-DRIVE entsprechend aufbereitet wurde, um für weitere Forschung zur Verfügung zu stehen. Auftretende Probleme hinsichtlich der Umsetzbarkeit von Teilschritten wurden frühzeitig durch alternative Lösungsansätze sowie eine enge und iterative Abstimmung mit den Verbundpartnern adressiert.

Konkret gab es bislang kaum belastbare Erfahrungen zur Entwicklung und dem Einsatz eines Reifegradmodells zur zielgerichteten Beurteilung der Datenqualität, insbesondere in Bezug auf die IT-Sicherheit und die Auswirkungen auf diesen Bereich. Der Einsatz von Reifegradmodellen an sich war zwar etabliert, allerdings bestanden nur sehr eingeschränkte Erkenntnisse darüber, wie sich solche Modelle zur tatsächlichen Verbesserung der IT-Sicherheit nutzen ließen. Aus diesem Grund barg die noch nicht abschätzbare Komplexität zur Erstellung eines umfassenden und vollständigen Reifegradmodells für die Qualität sicherheitsrelevanter Daten sowie dessen Anwendung in exemplarischen Gebieten der IT-Sicherheit erhebliche Risiken, die bei ihrem Eintreten den Erfolg des Gesamtvorhabens deutlich schmälerten. Als Gegenmaßnahme zur Risikoreduzierung sah UR-WI1 die vorliegende Expertise im Bereich der Reifegradmodelle und der IT-Sicherheit vor und konnte die Komplexität frühzeitig in Teilen abschätzen. Dadurch konnten gezielt bestimmte Herausforderungen herauskristallisiert und priorisiert werden.

Auch die Erfassung und Verbesserung der Datenqualität im IAM und der CTI barg ein hohes Risiko. Durch verwandte Forschungsarbeiten von UR-WI1 im Bereich der IAM-Datenqualität und der Erfassung von CTI-Datenqualität hatte sich die Erkenntnis bestätigt, dass eine entsprechende Messung nur mithilfe von geeigneten automatisierten Techniken, aber auch unter Einbeziehung von Experten erfolgreich sein konnte. Inwiefern die Qualität hier allerdings möglichst umfassend und effizient erfasst werden konnte und wie die Verbesserung der Qualität auch die IT-Sicherheit verbessern konnte, dazu existierten bislang keine bekannten Erfahrungen. Als Gegenmaßnahme brachte UR-WI1 im Teilvorhaben Anforderungen und Möglichkeiten der Umsetzung zusammen. Der Zusammenhang von IT-Sicherheit und Datenqualität ließ sich gegebenenfalls auch mit einem begrenzten und nur in Teilen optimierten Ansatz belegen.

Die Erarbeitung möglicher, praxisnaher Umsetzungen und Implementierungen des Reifegradmodells war darüber hinaus ebenfalls mit einem hohen Risiko verbunden. Da vor allem die Erfassung der Datenqualität sowohl für das IAM als auch die CTI bisher nur wenig praktische Umsetzung erfahren hatte, galt dies als nicht-triviales Unterfangen. Eine breite Palette unterschiedlichster, moderner Techniken und Technologien war höchstwahrscheinlich zu kombinieren, um die notwendigen Datenqualitätsmetriken möglichst automatisiert und effizient zu erfassen. Des Weiteren ließ sich sehr wahrscheinlich keine komplett automatisiert arbeitende Komponente gestalten, sondern es war auch die subjektive Einschätzung von Domänenexperten zu berücksichtigen. Somit war zum damaligen Zeitpunkt noch nicht abzusehen, inwieweit eine Implementierung des angestrebten Reifegradmodells mit all seinen Bestandteilen realistisch war. Als Gegenmaßnahme forcierte UR-WI1 durch die iterative Gestaltung des Reifegradmodells kontinuierlich eine realistische Gestaltung und Anpassung der erarbeiteten Komponenten. Sofern sich subjektive Einschätzungen nicht in Gänze ausschließen ließen, wurden diese

eindeutig kenntlich gemacht und konsequent berücksichtigt. Insgesamt besaß ein Reifegradmodell einen dynamischen Charakter und musste für zukünftige Veränderungen Anpassungsmöglichkeiten bereithalten. Dabei konnte der Grad subjektiver Einflussfaktoren adjustiert werden, ohne dass das Modell über den Zeitverlauf seine Gültigkeit verlor.

4. Voraussichtlicher Nutzen und Verwertbarkeit der Ergebnisse

In diesem Abschnitt wird die Aktualisierung des Verwertungsplans im Bereich der wissenschaftlichen Erfolgsaussichten und im Bereich der wissenschaftlichen und wirtschaftlichen Anschlussfähigkeit erläutert.

Durch die wissenschaftlich fundierte Entwicklung des DEVISE Reifegradmodells für Datenqualität in der IT-Sicherheit wird eine aktuelle Problemstellung mit einem zukunftsfähigen Ansatz adressiert. UR-WI1 wirkt hierbei insbesondere bei der Ausgestaltung des Reifegradmodells mit und baut auf etablierte Vorgehensmodelle aus der Forschung auf. Die konkrete Anwendung der Modellentwicklung auf den Bereich der Datenqualität in der IT-Sicherheit leistet einen wissenschaftlichen Mehrwert hinsichtlich etablierter Methoden. Insbesondere entstehen bei der Entwicklung des DEVISE-Reifegradmodells voraussichtlich weiterführende Forschungsfragen. Dabei können innerhalb der Projektlaufzeit von drei Jahren mehrere Publikationen für die Wirtschaftsinformatik und auch für die managementorientierte Betriebswirtschaftslehre entstehen. UR-WI1 kann somit Teilbeiträge aber auch weiterführende Aspekte aus dem Projekt herausgreifen und in die Wissenschaft einbringen. Da auch in angrenzenden Bereichen wie der *künstlichen Intelligenz* große Herausforderung hinsichtlich schlechter Datenqualität herrschen, können Teilergebnisse ebenfalls in diese Bereiche durch wissenschaftliche Veröffentlichung hineinwirken. Daher geht UR-WI1 von einer sehr hohen wissenschaftlichen Erfolgsaussicht hinsichtlich der Entwicklung wirkungsvoller Publikationen während des Projekts aus. Nach Projektende kann das Reifegradmodell für weitere Einsatzbereiche in der Forschung herangezogen werden.

Die Komplexität der Modellentwicklung kann durch das erfahrene Projektkonsortiums über den Projektverlauf beherrschbar gehandhabt werden. UR-WI1 wirkt u.a. bei der Implementierung des Referenzmodells mit und bearbeitet funktionale sowie nicht-funktionale Anforderungen. Durch agile Entwicklungsmethoden kann dabei von einer sehr hohen Erfolgsaussicht auf eine optimale Umsetzung ausgegangen werden. Es wird eine Bereitstellung des Referenzmodells über eine öffentliche Open-Source-Plattform angestrebt und somit auch eine praktische Anwendung des Modells über den Projektverlauf hinaus sichergestellt.

Das angestrebte Reifegradmodell bildet sowohl für die IT-Sicherheit als auch die betriebswirtschaftliche Wissenschaftsdomäne einen adaptionsfähigen Ansatz mit wissenschaftlicher Anschlussfähigkeit. Durch die Mitwirkung von UR-WI1 werden hinreichend generische Definitionen der Reifegrade und Fähigkeitsgrade im Rahmen von DEVISE-DRIVE erstellt. Nach dem Projekt kann das Referenzmodell durch Ausgestaltung auf weitere Anwendungsbereiche und zur Auswertung von Daten aus der industriellen Fertigung erweitert werden. Dadurch können auf den DEVISE-Ergebnissen aufbauende nationale und internationale Forschungsprojekte angestrebt werden.

Die Zusammenstellung des Projektkonsortiums bündelt die für DEVISE notwendigen Kompetenzen. UR-WI1 verfolgt durch die Koordination und das Monitoring in AP1 eine bestmögliche Durchführung des Projektes. Nichtdestotrotz besteht das Risiko verzögerter Projektfortschritte und niedriger Qualität einzelner Teilergebnisse. Durch eine adäquate Ausführung der Managementfunktion wird UR-WI1 bei einem solchen Vorkommnis die definierten Arbeitspakete und die dazugehörigen Tasks hinsichtlich einer möglichen zeitlichen Umplanung sowie einer Umverteilung oder Integration weiterer Partner im Rahmen einer Lösungsstrategie untersuchen. Als weiteres Risiko für die erfolgreiche Durchführung des Projektes erwägt UR-WI1 den fehlenden oder nicht ausreichenden Austausch zwischen den Bearbeitern der unterschiedlichen Arbeitspakte und Tasks. Bei Bekanntwerden eines solchen Umstands werden situationsbedingt adäquate Kommunikationskanäle bereitgestellt. Zudem wird als weiteres Managementelement der kontinuierliche Austausch der Betroffenen durch regelmäßige

Projekttreffen, -telefonkonferenzen, etc. forciert. Hinsichtlich der inhaltlichen Ausgestaltung des Reifegradmodells werden seitens UR-WI1 mögliche Unstimmigkeiten bei der Bestimmung des Geltungsbereiches (AP2) als geringes Risiko eingeordnet. Da im Projektvorhaben unterschiedliche Blickwinkel und Erwartungshaltungen aus Wissenschaft und Praxis auf die Modellentwicklung einwirken, können eventuelle Diskrepanzen aufgedeckt werden. Als Lösungsstrategie für dieses Risiko wird eine Konsensbildung durch eine Arbeitspaket-übergreifende Interaktion verfolgt.

In diesem Abschnitt wird die Aktualisierung des Verwertungsplans im Bereich der wissenschaftlichen Erfolgsaussichten und der wirtschaftlichen Anschlussfähigkeit des DEVISE-Reifegradmodells für Datenqualität in der IT-Sicherheit beschrieben. UR-WI1 spielte eine zentrale Rolle bei der Entwicklung und Anwendung dieses Modells und konnte dadurch neue Forschungsfragen und Publikationen in der Wirtschaftsinformatik und Betriebswirtschaftslehre generieren.

Das Projektkonsortium nutzte agile Methoden zur erfolgreichen Umsetzung und stellte das Modell als Open-Source-Plattform zur Verfügung. Das Reifegradmodell kann sowohl für IT-Sicherheit als auch für betriebswirtschaftliche Anwendungen angepasst und nach Projektende in weiteren Forschungsbereichen genutzt werden.

UR-WI1 übernahm die Koordination und das Monitoring des Projekts und begegnet möglichen Risiken wie Kommunikationsproblemen durch entsprechende Managementstrategien und regelmäßigen Austausch. Unstimmigkeiten im Geltungsbereich des Modells wurden durch interdisziplinäre Konsensbildung gelöst.

a. Erfindungen/Schutzrechtsanmeldungen und erteilte Schutzrechte

Dies trifft auf das DEVISE-Projekt nicht zu.

b. Wirtschaftliche Erfolgsaussichten nach Projektende

Dies trifft auf das DEVISE-Projekt nicht zu.

c. Wissenschaftliche Erfolgsaussichten nach Projektende

Die wissenschaftlichen Erfolgsaussichten des Projekts sind weiterhin ohne weitreichende Einschränkungen gegeben. Lediglich das im Rahmen des UR-WI1-Projekts zu entwickelnde Reifegradmodell als Grundlage für alle weiteren Projektarbeiten wird derzeit in seiner allgemeinen Form als schwer publizierbar angesehen. Alle Projektpartner arbeiten an der Fertigstellung Ihrer Aufgaben und wissenschaftlichen Veröffentlichungen in ihren jeweiligen Fachgebieten. Auf globaler Ebene wurde ein Rahmenwerk definiert, das nur als bedingt publizierbar eingeschätzt wird. Alle weiteren Arbeiten von UR-WI1 und vor allem die Forschungsergebnisse hinsichtlich der Instanziierung des Modells in den Bereichen CTI und IAM bieten weiterhin vielversprechende Erfolgsaussichten, die sich auch im dritten Berichtsjahr bestätigt haben. Aus wissenschaftlicher Sicht sind einzelne ineinandergreifende Komponenten und kein vollumfänglicher Demonstrator zu erwarten.

d. Wissenschaftliche und wirtschaftliche Anschlussfähigkeit für eine mögliche notwendige nächste Phase bzw. die nächsten innovatorischen Schritte zur erfolgreichen Umsetzung der Ergebnisse.

Aus DEVISE sind wissenschaftliche Publikationen entstanden, weitere befinden sich derzeit unter Begutachtung oder werden demnächst eingereicht. Diese Publikationen und insbesondere die Begutachtung der Arbeiten fließen direkt in die Projektergebnisse und die Dissertationsvorhaben der beteiligten Mitarbeiter:innen ein. Eines der Dissertationsvorhaben wurde zum Ende von 2023 abgeschlossen, ein weiteres steht vor dem unmittelbaren Abschluss, sodass DEVISE auch im Hinblick auf die Förderung der wissenschaftlichen Mitarbeitenden einen Projekterfolg darstellt. Darüber hinaus sind in den Bereichen Reifegradmodelle und Datenqualität von CTI, IAM, sowie Digitaler Forensik

weitere Seminar- und Abschlussarbeiten entstanden, sodass auch die Studierenden von dem Projekt profitieren.

Die in den vorangegangenen Abschnitten genannten Einschränkungen hinsichtlich des Umfangs des DEVISE-Reifegradmodells und seiner Instanziierung stellen notwendige wissenschaftliche Ausgangspunkte für weitere Arbeiten in verwandten Bereichen dar. Eine weitere Detaillierung und Anwendung in anderen Bereichen der Informationssicherheit erscheint sinnvoll. Die Berücksichtigung der Komplexität des Themas und des Zeitbedarfs hinsichtlich der Daten und der Messung der Datenqualität, insbesondere in der Informationssicherheit, sollte bei zukünftigen Projekten und Forschungsaktivitäten betont werden.

5. Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen während der Durchführung des Vorhabens

In diesem Abschnitt wird die Relevanz von FE-Ergebnissen von Dritten diskutiert. Im Laufe des Projekts wurden verschiedene Literaturrecherchen zu aktuellen Ergebnissen in Forschungsbereichen durchgeführt, die mit UR-WI1 in Verbindung stehen. Diese haben sowohl auf theoretischer als auch auf praktischer Seite gezeigt, dass nur sehr wenige Ergebnisse Dritter bekannt sind, die für die Durchführung des Projekts relevant sind. Sie zeigen lediglich, dass das Thema erforscht wird (siehe Literatur unten), was aber keinen Einfluss auf die Durchführung des DEVISE-Projekts hat. Aus wissenschaftlicher Sicht ist jedoch eine stärkere Fokussierung und die damit verbundene Einarbeitung in Daten und Themenbereiche sinnvoll.

- H. D. Pambudhi and R. F. Aji, "Evaluation of Cyber Threat Intelligence Maturity Models: A Comparison Based on Maturity Model Design Principles," 2022 2nd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Bandung, Indonesia, 2022, pp. 105-110, doi: 10.1109/ICICyTA57421.2022.10038112.
- Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: a review and research agenda for practice. *Computers & Security*.
- Tokerud, S., Jansen, J. N., Niemimaa, M., & Järveläinen, J. (2023). Designing Extended Zero Trust Maturity Model–From Technical to Socio-Technical.

6. Erfolgte und geplante Veröffentlichungen der Ergebnisse

In diesem Abschnitt werden die veröffentlichten Projektergebnisse des DEVISE-DRIVE Vorhabens dargelegt. Es handelt sich dabei maßgeblich um wissenschaftliche Publikationen.

Schlette, D., Vielberth, M., & Pernul, G. (2021). CTI-SOC2M2–The quest for mature, intelligence-driven security operations and incident response capabilities. Computers & Security, 111, 102482.

- Diese Publikation beschreibt ein Reifegradmodel mit Fokus auf Cyber Threat Intelligence (CTI) Datenformaten und Anwendungsgebieten innerhalb eines Security Operations Center (SOC). Ein Vergleich bestehender Reifegradmodelle sowie die Berücksichtigung von Datenqualität stellen einen direkten Bezug zum DEVISE-Projekt dar.

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525-2556.

- Diese Publikation beschreibt verschiedene Datenformate im Bereich der Cyber Threat Intelligence (CTI) mit Relevanz für die Incident Response. Die Publikation nimmt Bezug auf das DEVISE-Projekt und betont die Notwendigkeit der strukturierten Darstellung von sicherheits-relevanten Informationen.

Böhm, F., Englbrecht, L., Friedl, S., & Pernul, G. (2021). Visual Decision-Support for Live Digital Forensics. In 2021 IEEE Symposium on Visualization for Cyber Security (VizSec) (pp. 58-67). IEEE.

- Diese Publikation beschreibt ein visuelles Entscheidungsunterstützungssystem im Kontext der echtzeit-basierten Digitalen Forensik. Der dabei verfolgte Ansatz kann für eine ganzheitliche Methode zur Akquisition und Analyse von sicherheitsrelevanten Daten im Rahmen der State Reconstruction im Qualitätsmanagement genutzt werden.

Empl, P., Schlette, D., Zupfer, D., & Pernul, G. (2022). SOAR4IoT: Securing IoT Assets with Digital Twins. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES 2022). ACM.

- Diese Publikation beschreibt Fragestellungen im Kontext der Nutzung von CTI mittels Digital Twins und Security Orchestration, Automation, and Response (SOAR) Plattform. Auf Basis von CTI werden Incident Response Playbooks zur Bewältigung von Sicherheitsvorfällen im Internet of Things (IoT) erstellt. Diese Incident Response Playbooks stellen einen neuen Ansatz innerhalb CTI dar und sind hinsichtlich ihrer Datenqualität von Interesse für die Forschung, Praxis und das DEVISE-Projekt.

Friedl, S., Englbrecht, L., Böhm, F. and Pernul, G. (2022). Support Tool Selection in Digital Forensics Training. International Journal of Cyber Forensics and Advanced Threat Investigations (UBISEC22).

- Diese Publikation beschreibt ein Konzept, das zum Training einer geeigneten Tool-Auswahl für forensische Ermittler dient und auf Basis einer Analytic Hierarchy Process (AHP)-Anwendung eine objektive Tool-Auswahl auf Grundlage der vom Ermittler gewünschten Tool-Eigenschaften ermöglicht. Ein indirekter Bezug zum Projekt DEVISE entsteht, durch die Anwendung der AHP-Methodik, die eine Gewichtung unterschiedlicher Faktoren erlaubt und somit auf Qualitätsmerkmale angewandt werden kann.

Friedl, S., Glas, M., Englbrecht, L., Böhm, F. und Pernul, G. (2022). ForCyRange: An educational IoT Cyber Range for Live Digital Forensics. In Proceedings of the 15th World Conference on Information Security Education (WISE15).

- Diese Publikation beschreibt ein Konzept, dass angehende Forensiker mit Fähigkeiten und Kenntnissen im IoT-Cyber-Bereich für Live Digital Forensics (LDF) ausstatten soll. Um eine realistische Lernerfahrung zu kreieren, wird ein einfaches IoT-System simuliert. Integriert in eine Cyber Range kann damit eine IoTF-Untersuchung durchgeführt werden. Die angewandte Methodik zeigt einen Ansatz, um ein sicherheitsrelevantes Vorgehen Personen näher zu bringen, die lediglich Grundwissen besitzen und ist im Bezug zum DEVISE-Projekt hinsichtlich des CTI-Wissenstransfers von Interesse.

Schlette, D., Empl, P., Caselli, M., Schreck, T., & Pernul, G. (2023, October). Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 60-60). IEEE Computer Society.

- Diese Publikation untersucht Playbooks für die Reaktion auf Vorfälle und verschiedene Faktoren, die ihre gemeinsame Nutzung, Pflege und Verwendung beeinflussen und prägen. Handlungsrelevante Erkenntnisse über Datenqualität, gemeinsame Sprachelemente und technologische Unterstützung dokumentieren notwendige Überlegungen für Playbooks. Die Ergebnisse deuten darauf hin, dass Technologie und Sicherheitsteam(s) entscheidende Faktoren bei der Gestaltung von Playbooks für die Reaktion auf Vorfälle darstellen. Die untersuchten Incident Response Playbooks stellen

einen neuen Ansatz innerhalb CTI dar und sind hinsichtlich ihrer Datenqualität von Interesse für die Forschung, Praxis und das DEVISE-Projekt.

Empl, P., Schlette, D., Stöger, L., & Pernul, G. (2023). Generating ICS vulnerability playbooks with open standards. International Journal of Information Security, 1-16.

- Diese Publikation beschreibt ein Prozessmodell zur Erfassung und Umwandlung von Sicherheitshinweisen im CSAF-Format (Common Security Advisory Framework) und zur Erstellung von CACAO-Playbooks (Collaborative Automated Course of Action Operations) auf deren Grundlage der Maßnahmen entwickelt wurden. Mit einem Proof of Concept wird gezeigt, dass strukturierte CSAF-Dokumente nahtlos in CACAO-Playbooks umgewandelt werden können. CSAF und CACAO bilden zwei offene Standards für den Umgang mit Schwachstellen. Da auch in diesem Zusammenhang die zugrundeliegende Datenqualität sowie CTI sehr wichtig und einflussreich sind, ist diese Publikation Teil des DEVISE-Vorhabens.