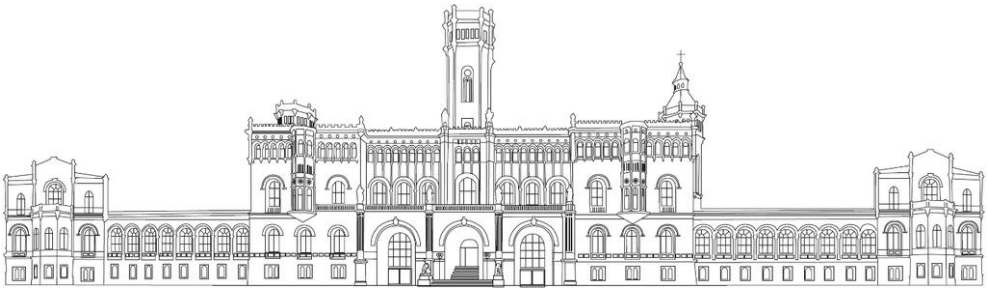

LEIBNIZ UNIVERSITÄT HANNOVER
WIRTSCHAFTSWISSENSCHAFTLICHE FAKULTÄT
INSTITUT FÜR WIRTSCHAFTSINFORMATIK

Integration gesetzlicher Anforderungen in IT-Prozesse der Cyber Sicherheit

Masterarbeit

Zur Erlangung des akademischen Grades „Master of Science (M. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von:

Name: Roufflair Vorname: Cathérine Louise

geb. am: in:

Prüfer/in: Prof. Dr. Michael H. Breitner
Betreuer/in: Kathrin Bouba (TUIfly)

Hannover, den 14.11.2023

Inhaltsverzeichnis

1 Einleitung und Motivation

In dem Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) vom 27.12.2022 werden verschiedene Maßnahmen definiert, die die Mitgliedsstaaten der Europäischen Union für ein gemeinsames Sicherheitsniveau von Netz- und Informationssystemen umsetzten müssen. Das Bundesamt für Sicherheit der Informationstechnik (BSI) ist in Deutschland für die Umsetzung der europäischen Richtlinie in nationales Recht verantwortlich. Im Rahmen der Umsetzung wurde das IT-Sicherheitsgesetz entwickelt, um einen einheitlichen Rechtsrahmen für Betreiber kritischer Infrastrukturen (KRITIS) zu schaffen. Als KRITIS werden „[...] Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." definiert (BSI, 2023). KRITIS-Betreiber müssen daher im Sinne des IT-Sicherheitsgesetztes handeln und verschiedene Pflichten erfüllen.

Der in dieser Arbeit verwendete Design Science Research (DSR) Ansatz basiert auf der Lösung eines realen Problems mit dem Ziel, eine in der Praxis anwendbare Lösung zu entwickeln. KRITIS-Betreiber stehen vor den Herausforderungen, neue Anforderungen in bestehende Maßnahmen für die Cyber Sicherheit zu integrieren. Für die Entwicklung eines Artefakts und beispielhafte Anwendung in der Praxis wurde die TUIfly ausgewählt. Die TUIfly ist eine deutsches Luftfahrtunternehmen und unterliegt der Zugehörigkeit einer der KRITIS-Sektoren. Bei der TUIfly existieren bereits eine Vielzahl von Maßnahmen der Cyber Sicherheit, die durch einen konzernweiten IT-Dienstleister der TUI Group IT ausgeführt werden. Das BSIG und Vorgaben anderer Institutionen, die auf nationalen, internationalen und branchenspezifischen Anforderungen basieren, führen dazu, dass die TUIfly existierende Maßnahmen und Prozesse beim IT-Dienstleister in Hinblick auf gesetzliche Vorgaben prüfen muss, um rechtliche Konformität zu gewährleisten und Rechenschaftspflichten nachzukommen. Eine Herausforderung dabei ist, dass nationale Gesetzesgrundlagen von einem international agierenden IT-Dienstleister ausgeführt werden müssen. Interne Strukturen erfordern somit diverse beteiligte Akteure und Ressourcen. Die vorliegende Arbeit verfolgt das Ziel, einen Prozess zur Integration gesetzlicher Anforderungen in IT-Prozesse der Cyber Sicherheit zu modellieren.[1] In der Praxis soll der Prozess zusätzlich eine schnelle und effiziente Kommunikation zu IT-Dienstleistungen zwischen der TUIfly und dem IT-Dienstleister ermöglichen. Der Fokus der theoretischen Komponente liegt in dieser Arbeit auf dem Best-Practice-Leitfaden Information Technology Infrastructure Library (ITIL) 4, da Schlüsselaktivitäten im Wertschöpfungsprozess repräsentiert werden, die für die Prozessmodellierung als Grundlage genutzt werden können und ITIL 4 eine intensive Kommunikation zwischen IT-Dienstleister und Kunden unterstützt, wodurch das Ziel der

[1] Im weiteren Verlauf dieser Arbeit wird die Kurzform Prozess zur Integration gesetzlicher Anforderungen genutzt.

schnellen und effizienten Kommunikation berücksichtigt wird. Andere Rahmenwerke bleiben aus diesen Gründen unberücksichtigt. Eine Literaturrecherche konnte keinen Prozess identifizieren, welcher das vorliegende Problem lösen kann, wodurch die folgende Forschungsfrage abgeleitet wird:

Wie kann ein Prozess zur Integration gesetzlicher Anforderungen in IT-Prozesse der Cyber Sicherheit durch einen IT-Dienstleister gestaltet werden?

Zur Beantwortung der Forschungsfrage werden zunächst die Begrifflichkeiten IT Service Management (ITSM), Cyber Sicherheit und IT-Prozess näher erläutert. Diese Arbeit baut auf der Forschungsmethode des DSR-Ansatzes auf, welcher anschließend erläutert wird. Ebenso werden die Methoden zur Literaturrecherche, den Experteninterviews, der Prozessmodellierung sowie der Fokusgruppendiskussion beschrieben. Im Anschluss werden die Ergebnisse der Literaturrecherche und der Experteninterviews präsentiert, um anhand dessen einen Prozessentwurf mittels der erweiterten Ereignisgesteuerten Prozesskette (eEPK) zu modellieren. Der Prozessentwurf wird mittels mehrerer Fokusgruppendiskussion diskutiert und evaluiert, woraufhin der finale Prozess modelliert wird. Zusätzlich wird der finale Prozess mit externen Experten diskutiert, um Gemeinsamkeiten und Unterschiede zu anderen unternehmensspezifischen Prozessen herauszuarbeiten. Im Anschluss erfolgt eine Diskussion der Ergebnisse und die Limitationen werden aufgezeigt. Abschließend wird das Fazit und einen Ausblick zu künftigen Forschungsfragen dargestellt.

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im Verlauf dieser Arbeit auf das Gendern verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

7 Fazit und Ausblick

Ziel dieser Arbeit war es, einen Prozess zur Integration gesetzlicher Anforderungen in IT-Prozesse der Cyber Sicherheit zu modellieren, welcher einen Überblick über die grundlegenden Aktivitäten und Prozessbeteiligten bietet. Dafür wurden zunächst relevante Begrifflichkeiten sowie die Methodik erläutert. Die Methodik umfasst die Erläuterung des DSR-Ansatzes, die Vorgehensweise der Literaturrecherche, Experteninterviews, Prozessmodellierung sowie Fokusgruppendiskussion und Evaluation mit externen Experten. Anschließend wurden die Ergebnisse präsentiert. Hierfür wurde zunächst ITIL 4 als ganzheitlicher Ansatz für das ITSM erläutert sowie die Analyse der Experteninterviews vorgenommen. Die Ergebnisse der Literaturrecherche und Experteninterviews wurden kombiniert und ein erster Entwurf des Prozesses angefertigt. Mit Hilfe der Fokusgruppendiskussionen und Evaluation mit externen Experten wurde der Prozessentwurf evaluiert, woraufhin dieser überarbeitet und finalisiert wurde. Es folgte eine Diskussion der Ergebnisse, bei dem der Prozess in das ITIL 4 Umfeld eingeordnet sowie Herausforderungen und die Allgemeingültigkeit des Prozesses diskutiert wurden. Dabei konnte die Forschungsfrage, wie ein Prozess für die Integration gesetzlicher Anforderungen in IT-Prozesse der Cyber Sicherheit durch einen IT-Dienstleister gestaltet werden kann, beantwortet werden. Darüber hinaus wurde gezeigt, welche Organisationseinheiten für die einzelnen Aktivitäten bei der TUIfly und dem IT-Dienstleister am Prozess zuständig sind und welche Herausforderungen existieren, die den Prozess begleiten.

Der Prozess zur Integration gesetzlicher Anforderungen in IT-Prozesse der Cyber Sicherheit adressiert eine Vielzahl von Organisationen, die bereits KRITIS sind oder werden. Die vorliegende Arbeit bietet Unternehmen einen strukturierten Überblick über die Entwicklung eines solchen Prozesses. Gleichzeitig wird eine Grundstruktur des Prozesses dargestellt und umfasst die wichtigsten Aktivitäten, welche Unternehmen zukünftig bei der Entwicklung eines entsprechenden unternehmensspezifischen Prozesses unterstützen kann. Diese Arbeit verschafft KRITIS-Betreibern somit eine Grundlage, wie der Prozess zur Integration gesetzlicher Anforderungen aussehen kann. Durch diese Arbeit wurde eine Forschungslücke identifiziert und gleichzeitig auch ein Lösungsansatz dargestellt. Diese Arbeit konnte zudem Herausforderungen bei der Integration gesetzlicher Anforderungen aufdecken, die weiteren Forschungsarbeiten aufgreifen, weitere Herausforderungen in einer repräsentativen Stichprobe identifizieren und Handlungsempfehlungen im Umgang damit ableiten können. Eine weitere Möglichkeit für zukünftige Forschungsarbeiten ist die Modellierung des Prozesses zur Integration gesetzlicher Anforderungen bei KRITIS-Betreibern verschiedener Sektoren, um die Prozesse sektorenspezifisch zu gestalten. Dabei könnten auch alle relevanten Compliance Anforderungen erfasst werden, um die Anforderungen und Prozesse zwischen den Sektoren zu vergleichen sowie Gemeinsamkeiten und Unterschiede zu identifizieren.