HOCHSCHULE DER MEDIEN
FAKULTÄT FÜR INFORMATION UND KOMMUNIKATION
WIRTSCHAFTSINFORMATIK UND DIGITALE MEDIEN

HOCHSCHULE DER MEDIEN

**BACHELORARBEIT ZUM THEMA:**

# Framework für Cybersecurity-Metriken für die Einhaltung von vorschriften

Ein ganzheitlicher Ansatz für die Messung und Verbesserung der Konformität eines Informationssystems mit Standards

## Vorgelegt von

**Tim-Oliver Habeck**
**Forststraße 129/1**
**70193 Stuttgart**
**th135@hdm-stuttgart.de**

**Matrikelnummer: 39635**
**B.Sc. Wirtschaftsinformatik und digitale Medien**
**8. Fachsemester**

**Erstprüfer: Dr. Prof. Martin Forster**
**Zweitprüfer Dr. Jesus Luna Garcia**

**Datum 14.04.2023**
**Sommersemester 2023**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952633

HOCHSCHULE DER MEDIEN

# Ehrenwörtliche Erklärung

| | | | |
|---|---|---|---|
| Name: Habeck | Habeck | Vorname: | Tim-Oliver |
| Matrikel-Nr.: | 39635 | Studiengang: | Wirtschaftsinformatik und digitale Medien |

Hiermit versichere ich, Tim-Oliver Habeck ehrenwörtlich, dass ich die vorliegende Bachelorarbeit (bzw. Masterarbeit) mit dem Titel: „Framework für Cybersecurity-Metriken für die Einhaltung von Vorschriften“ selbständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Ich habe die Bedeutung der ehrenwörtlichen Versicherung und die prüfungsrechtlichen Folgen (§ 26 Abs. 2 der Bachelor-SPO (6 Semester), § 24 Abs. 2 Bachelor-SPO (7 Semester), § 23 Abs. 2 Master-SPO (3 Semester) bzw. §19 Abs. 2 Master-SPO (4 Semester und berufsbegleitend) der HdM) einer unrichtigen oder unvollständigen ehrenwörtlichen Versicherung zur Kenntnis genommen.

Stuttgart, 14.04.2023 Habeck

..... .....

Ort, Datum Unterschrift

## Abstract

Der Einsatz von Standards ist in der Informationssicherheit essenziell, um ein ausreichendes Sicherheitslevel zu gewährleisten. Daher ist ein zentraler Aspekt die Konformität mit diesen Standards, die als Nachweis für die eigene Informationssicherheit dient und häufig gesetzlich und vertraglich gefordert ist. Um die Konformität zu überprüfen, existieren verschiedene Ansätze. Allerdings wurde noch kein umfassender Ansatz entwickelt der bekannte Metriken einsetzt, um die Konformität zu messen und zu verbessern und der dabei auf verschiedene Frameworks und Systeme anwendbar ist. Ein solcher Ansatz wurde in dieser Arbeit in Form eines Frameworks aus der Literatur abgeleitet und anhand einer Fallstudie am Beispiel der Robert Bosch GmbH validiert. Das Framework enthält Anleitungen und Werkzeuge für den gesamten Prozess der Messung, Kommunikation und Verbesserung der Konformität. Das Ergebnis ist ein ganzheitlicher Ansatz, der für verschiedene Arten von Informationssystemen oder ein Informationssicherheit-Management-System sowie eine Vielzahl verschiedener Standards angewendet werden kann.



**Schlagwörter:**

Informationssicherheit; Cybersicherheit; Metrik; Standard, Konformität


---


The use of standards is essential in information security to ensure a sufficient level of security. Therefore, a central aspect is the conformity with these standards, which serves as proof of one's own information security and is often required by law and contract. Various approaches exist to verify conformity. However, no comprehensive approach has yet been developed that uses known metrics to measure and improve compliance, and that can also be applied to different frameworks and systems. Such an approach was derived from the literature in this thesis in the form of a framework and validated by means of a case study using the example of Robert Bosch GmbH. The framework contains guidance and tools for the entire process of measuring, communicating and improving compliance The result is a holistic approach that can be applied to different types of information systems or a information security management system, as well as a variety of different standards.



**Keywords:**

Information security; Cyber security; metric, Standard, Compliance

# Inhaltsverzeichnis

## Abbildungsverzeichnis



## Tabellenverzeichnis



## Abkürzungsverzeichnis

| | |
|---|---|
| ISO: | Internationale Organisation für Normung |
| NIST: | National Institute of Standards and Technology |
| BSI: | Bundesamt für Sicherheit in der Informationstechnik |
| ISMS: | Informationssicherheit-Management-System |
| SCF: | Secure Controls Framework |
| EISA: | Enterprise IT Security Architecture |
| PaaS: | Platform as a Service |
| IaaS: | Infrastructure as a Service |

# 1 Einleitung

In dieser Arbeit soll ein Framework für die Messung und Verbesserung der Konformität von Informationssystemen mit Standards entwickelt werden. Diese Einleitung dient dazu, ein Verständnis für die Beweggründe hinter dieser Arbeit, den Zielen und den zu lösenden Problemen vermitteln. Dafür wird zuerst die Problemstellung und dann die Relevanz der Arbeit erklärt. Dann soll das Ziel definiert und daraus Fragestellungen abgeleitet werden. Schließlich sollen die dieser Arbeit zugrunde liegende Vorgehensweise beschrieben werden.

## 1.1 Problemstellung

Es existieren verschiedene Standards, um die Sicherheit von Informationssystemen zu gewährleisten. Um die eigene Informationssicherheit nicht der subjektiven Einschätzung der verantwortlichen Mitarbeiter zu überlassen und um Lücken in der Verteidigung zu vermeiden, orientieren sich Unternehmen an diesen Standards. Daher ist eine möglichst genaue Umsetzung der Standards für Unternehmen erstrebenswert und häufig auch rechtlich oder vertraglich erforderlich. In der Praxis fehlt es aber oft an Methoden, um die tatsächliche Umsetzung der Standards zu überprüfen. In dieser Arbeit soll ein allgemeines Framework aufgestellt werden, das aufzeigt, wie man bekannte Metriken einsetzen kann, um die Erfüllung der Anforderungen eines Standards und somit die Konformität mit dem Standard zu überprüfen und zu verbessern.

## 1.2 Relevanz

Ein Informationssicherheits-Managementsystem, kurz ISMS, dient dazu, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in seinem Geltungsbereich zu wahren (ISO 27004:2016, 5.1). Damit ist es die Grundlage für die systematische Wahrung und Verbesserung der eigenen Informationssicherheit. Die Umsetzung eines ISMS kann diese Ziele aber nicht garantieren. Deshalb gibt es Anforderungen, anhand denen die Erfüllung der Informationssicherheitsziele bewertet werden kann (ISO 27004:2016, 5.1). Diese Anforderungen sind in der Regel in Standards und Frameworks dokumentiert. Solche Standards können sich dabei an bestimmte Industriezweige oder Geschäftsarten richten (Hayden, 2010).

Aufgrund verschiedener gesetzlicher und vertraglicher Auflagen ist häufig der Einsatz von verschiedenen Sicherheitsstandards gefordert. Die Konformität mit solchen Standards ist aber

in der Regel ein subjektives und schwer zu definierendes Konzept. Es beinhaltet eine dynamische Mischung aus neuen und sich verändernden Vorschriften und Regeln. Darüber hinaus bedarf es der persönlichen Interaktionen einer Organisation mit Prüfern und Regulierungsbeauftragen (Hayden, 2010). Um dieser Herausforderung Herr zu werden und der Subjektivität einer Bewertung durch einen Auditor oder Prüfer eine objektive Ansicht entgegenzustellen, kann die Konformität mit Standards durch den Einsatz von Metriken gemessen und berechnet werden (Yee, 2019).

Eine Evaluation der eigenen Informationssicherheit mit Metriken kann nicht nur die Entscheidungsfindung unterstützen (Yee, 2019; ISO 27004:2016, 5.4), sondern dient auch als Nachweis für die Erfüllung von Vorschriften (ISO 27004:2016, 5.4). Ein solcher Nachweis kann Vertrauen bei Kunden und Geschäftspartnern schaffen, die oft auch ein eigenes Interesse an der Informationssicherheit einer Organisation haben. Schließlich hilft die Evaluation des eigenen ISMS auch bei der Verbesserung eben jenes ISMS und damit der Steigerung der Informationssicherheit (ISO 27004:2016, 5.4).

## 1.3 Zielsetzung und Forschungsfragen

Das Ziel der Arbeit ist es, ein Framework zu definieren, dass die nötigen Werkzeuge und Prozesse bereitstellt, um den Grad der Konformität der eigenen Systeme und Sicherheitsprogramme mit einem Sicherheitsstandard mit bekannten Metriken zu ermittelt und zu verbessern. Dafür müssen allgemeine Begrifflichkeiten sowie der Prozess der Selektion und Definition der Metriken geklärt werden. Es soll außerdem auf die Kommunikation der Ergebnisse eingegangen werden. Dadurch soll das Framework einen effizienten Ansatz bieten, um die Konformität der eigenen Systeme mit den Sicherheitsvorschriften der gewählten Standards zu ermitteln und sie schließlich zu verbessern. Das Framework soll sich dabei nicht auf einen bestimmten Standard beziehen, sondern allgemein auf die verschiedenen gängigen Standards anwendbar sein.

Um dieses Ziel zu erreichen, wird diese Forschungsfrage untersucht:

> Wie kann ein Framework entwickelt werden, um IT-Systeme unter Einsatz bekannter Cybersecurity-Metriken auf ihre Konformität mit Standards hin zu überprüfen?

Die Forschungsfrage wird, um die einzelnen Punkte der Zielsetzung besser abzubilden und eine bessere Struktur vorzugeben, in folgende Teilfragen unterteilt:

1. Wie kann relevante Metriken bestimmt werden, um IT-Systeme auf die Einhaltung von Vorschriften hin zu überprüfen?
2. Wie können die Kennzahlen der relevanten Cybersecurity-Metriken gemessen werden?
3. Wie können das entwickelte Framework in einer globalen Organisation wie der Robert Bosch GmbH eingesetzt und die Ergebnisse kommuniziert werden?
4. Wie können anhand dieser Metriken Systeme auf die Einhaltung von Vorgaben bestimmter Standards (z.B. ISO 27000) hin überprüft werden?
5. Wie kann die Effektivität des Frameworks beurteilt werden, um es in der Zukunft weiter zu verbessern?

## 1.4 Vorgehensweise

Um die Forschungsfrage zu beantworten, soll in dieser Arbeit ein Framework definiert werden. Als Vorbereitung darauf werden in Kapitel 2 zuerst die theoretischen Grundlagen untersucht. In Kapitel 2.1 Arbeitsdefinitionen von wichtigen Begriffen aufgestellt, um eventuellen Doppeldeutigkeiten oder Unklarheiten vorzubeugen. Dabei sollen die zu Grunde liegenden Konzepte im notwendigen Umfang erklärt werden.

Anschließend werden in Kapitel 2.2 einige relevante Sicherheitsstandards betrachtet, um eine Grundlage dafür zu schaffen, wie ein solcher Standard aussehen kann und worauf bei der Messung der Konformität mit einem Standard zu achten ist.

Weiter sollen in Kapitel 2.3 auch zwei existierende Ansätze für die Messung und Verbesserung der Konformität mit Standards untersucht werden. Daraus sollen eine Grundstruktur und ein allgemeines Vorgehen für das Framework abgeleitet werden.

Anschließend werden die wichtigsten Aspekte im Zusammenhang mit dem Einsatz von Metriken erarbeitet. Die dabei gewonnenen Erkenntnisse bei der Entwicklung des Frameworks eingesetzt werden.

In Kapitel 2.9 folgt eine Erklärung des PDCA-Zyklus, der die grundlegende Struktur des Frameworks bildet

In Kapitel 3 wird das Framework aus der Literatur abgeleitet. Zuerst wird die Struktur erklärt, dann werden in Kapitel 3.1.1 einige Rollen vorgeschlagen, die eingesetzt werden können, um eine klare Aufgabenverteilung zu gewährleisten. Kapitel 3.1.2 enthält Regeln, Hinweise und

Beispiele für die Analyse des gewählten Standards. Sie stellen eine Anleitung dar, um die relevanten Anforderungen zu identifizieren.

Die erste Teilfrage der Fragestellung wird in Kapitel 3.1.3 beantwortet. Dieses Kapitel enthält einen Ansatz, mit dem Metriken ausgewählt werden können, um die identifizierten Anforderungen zu überprüfen.

Im folgenden Kapitel 3.1.4 enthält eine Vorlage für die Dokumentation der gewählten Metriken. Dabei werden auch einige kleinere Schritte der Planung erklärt. Ein wichtiger Teil des Kapitels ist auch die Definition von Messungen, die als Teil der Vorlage erklärt wird. Dadurch beantwortet dieses Kapitel, zusammen mit Kapitel 3.2, die zweite Teilfrage.

Kapitel 3.2 befasst sich mit der Implementierung der Messungen und der Datenerhebung. Das folgende Kapitel 3.3 enthält eine Anleitung zur Datenauswertung und der Kommunikation der Ergebnisse. Dabei wird erklärt, wie die Metriken aggregiert und in einem Dashboard als Diagramme dargestellt werden können. Damit beantwortet dieses Kapitel einen Teil der dritten Teilfrage.

Das letzte Kapitel des Frameworks, Kapitel 3.4, behandelt die Entwicklung und Umsetzung von Korrekturmaßnahmen, um aufgedeckte Schwachstellen zu beheben. Dafür werden die Ursachen der aufgedeckten Mängel untersucht und die Korrekturmaßnahmen priorisiert.

Nach der Entwicklung des Frameworks folgt in Kapitel 4 eine Fallstudie, bei der das Framework auf Cloud-Services der Robert Bosch GmbH angewandt wird. Aufgrund der Zeitbegrenzung ist es nicht möglich, das Framework für die Allgemeinheit oder eine bestimmte Branche zu validieren. Die Fallstudie stellt aber eine Validierung am Beispiel der Robert Bosch GmbH dar. Damit wird auch die dritte Teilfrage endgültig beantwortet.

Im Anschluss an die Fallstudie werden in Kapitel 5 die Ergebnisse der Fallstudie diskutiert. Hier wird die Leistung des Frameworks anhand der Fallstudie beurteilt. Dadurch werden auch eventuelle Schwachstellen aufgedeckt. Dadurch beantwortet dieses Kapitel die fünfte Teilfrage.

Die Kapitel 3, 4 und 5 beantworten zusammen sämtliche Teilfragen und somit auch die eigentliche Forschungsfrage.

Abschließend erfolgt in Kapitel 6 eine Zusammenfassung und Diskussion der Ergebnisse. Zuletzt wird ein Ausblick über die Zukunft des Frameworks und weitere offene Forschungsfragen gegeben.

# 2 Theoretische Grundlagen

Für die Entwicklung des Frameworks soll in diesem Kapitel die theoretische Grundlage geschaffen werden. Dafür werden zuerst Arbeitsdefinitionen aufgestellt. Dann folgt eine Betrachtung einiger Frameworks und existierender Ansätze zur Messung der Konformität. Weiter wird auf die wichtigsten Aspekte im Zusammenhang mit dem Einsatz von Metriken einzeln eingegangen. Die dabei gewonnenen Erkenntnisse sollen im nächsten Kapitel wieder aufgegriffen werden, wenn das Framework entwickelt wird.

## 2.1 Definitionen

Die in diesem Kapitel untergebrachten Definitionen sollen Unklarheiten in der weiteren Arbeit vermeiden und ein einheitliches Verständnis schaffen.

**Cybersecurity**

Das National Institute of Standards and Technology, kurz NIST, definiert Cybersecurity als die Verhinderung von Schäden an sowie der Schutz und die Wiederherstellung von Computern, elektronischen Kommunikationssystemen, elektronischen Kommunikationsdiensten, kabelgebundener sowie elektronischer Kommunikation, einschließlich der darin enthaltenen Informationen, um deren Verfügbarkeit, Integrität, Authentifizierung, Vertraulichkeit und Unverfälschtheit zu gewährleisten (Michael Bartock et al., 2021).

**Framework**

Im Cambridge Dictionary wird ein Framework als die Ideen, Informationen und Grundsätze definiert, die die Struktur einer Organisation oder eines Plans bilden (Cambridge Dictionary 2023).

**Metrik**

Das Wort Metrik definiert das Oxford Advanced Learners Dictionary als eine Reihe von Zahlen oder Statistiken, die zur Messung von etwas verwendet werden, insbesondere für Ergebnisse, die zeigen, wie gut zum Beispiel ein Unternehmen, eine Schule oder ein Computerprogramm

abschneidet (Oxford University Press 2023). Weiter beschreibt Black eine Metrik als ein abstraktes, gewissermaßen subjektives Merkmal, dessen Wert annäherungsweise aus Kennzahlen ermittelt werden kann (Black et al., 2008). Im ISO-Standard 19086 wird eine Metrik stattdessen als Messstandard definiert, der Bedingungen und Regeln für die Durchführung einer Messung sowie für die Interpretation der Messergebnisse enthält (ISO 19086-2, 3.6).

Für diese Arbeit soll eine Kombination der angeführten Definitionen eingesetzt werden. Eine Metrik beschreibt ein potenziell abstraktes Merkmal dessen Wert aus einer oder mehreren Kennzahlen ermittelt werden kann. Dafür enthält sie Bedingungen und Regeln für die Messung und die Interpretation der Ergebnisse.

**Kennzahl**

Die Internationale Organisation für Normung, kurz ISO, definiert eine Kennzahl als eine Variable, der als Resultat einer Messung ein Wert zugewiesen wird (ISO 15939:2017, 3.16). Genauer ist eine Kennzahl ein konkretes, objektives Attribut, z. B. der Prozentsatz der Systeme in einer Organisation, die vollständig gepatcht sind, die Zeitspanne zwischen der Veröffentlichung eines Patches und seiner Installation auf einem System oder der Grad des Zugangs zu einem System, den eine Schwachstelle im System ermöglichen könnte (Black et al., 2008)

**Kontrolle**

Im ISO-Standard 27000 wird eine Kontrolle als eine Maßnahme definiert, die das Risiko beeinflusst (ISO 27000:2018, 3.14). Die NIST Special Publication 800-53 erklärt eine Kontrolle als eine Beschreibung der Schutzmaßnahmen und -Fähigkeiten, die für die Erreichung der besonderen Sicherheits- und Datenschutzziele der Organisation geeignet sind (NIST SP 800-53 Rev. 5, 2.1).

Für diese Arbeit soll die Definition genügen, dass eine Kontrolle eine Beschreibung einer Maßnahme ist, die die Erreichung der besonderen Sicherheits- und Datenschutzziele der Organisation zum Ziel hat.

**Anforderung**

Die ISO definiert eine Anforderung als eine Bestimmung, die zu erfüllende Kriterien enthält (ISO/IEC Guide 2:2004, 7.5).

## 2.2 Standards

Damit das in dieser Arbeit entworfene Framework in der Praxis eingesetzt werden kann, sollte vor der Entwicklung ein Überblick über die in der Praxis eingesetzten Standards geschaffen werden. Das Framework selbst soll zwar keinen Bezug zu einem oder mehreren bestimmten Standards aufweisen und stattdessen auf verschiedene Standards anwendbar sein. Dennoch kann der Blick auf einige der besonders häufig eingesetzten Standards eine Grundlage dafür schaffen, wie ein solcher Sicherheitsstandard aussehen kann und wie man die Konformität mit einem solchen Standard messen könnte.

Bei einer Studie im Jahr 2021 hat das Sans Institute 480 Unternehmen, aus verschiedenen Branchen, zu Cybersecurity Themen befragt (Bristow, 2021). Die Unternehmen bilden eine Mischung aus kleinen, mittleren und großen Firmen und stammen aus allen Teilen der Welt (Bristow, 2021). Unter anderem wurde danach gefragt, welche Standards die Unternehmen im Bereich Cybersecurity für ihre Kontrollsysteme einsetzten. Ein Ausschnitt der Ergebnisse ist in Abbildung 1 dargestellt:

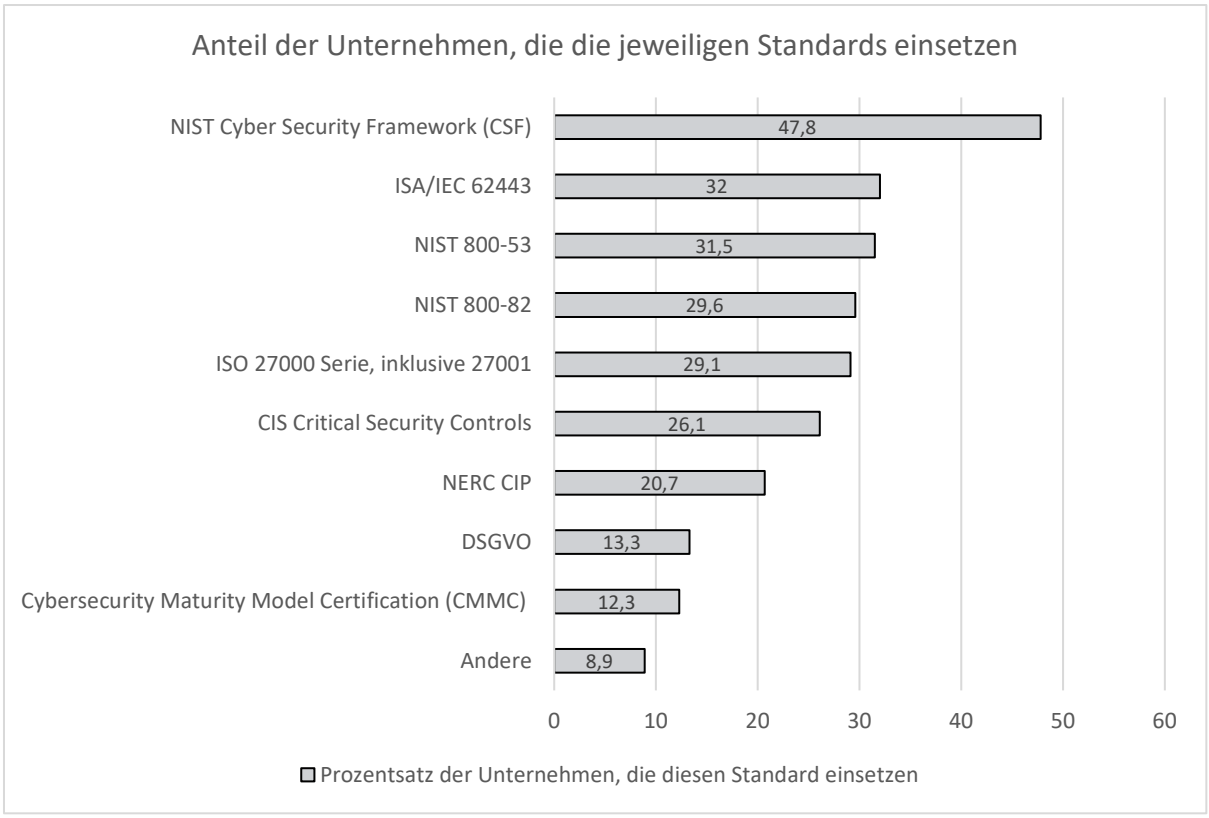


*Abbildung 1: Übersicht über die am weitesten verbreiteten Standards*

*Eigene Darstellung nach Bristow, 2021*

Die Standards des amerikanischen NIST, dem National Institute for Standards and Technologie, scheinen auch international Anwendung zu finden. Das NIST Cyber Security Framework wurde von 47,8 Prozent, die Special Publication NIST 800-53 von 31,5 Prozent und die Special Publication NIST 800-82 von immerhin 29,6 Prozent der befragten Unternehmen eingesetzt (Bristow, 2021). Alle drei sollen daher in diesem Kapitel näher betrachtet werden. Weiter sind die Standards der internationalen Organisationen ISO, IEC und ISA relevant. Die ISA/IEC 62443 Standardserie wird von 32 Prozent, also fast einem Drittel der Befragten Unternehmen eingesetzt und soll daher ebenfalls näher betrachtet werden (Bristow, 2021). Die Standards der 27000er Familie von der Internationalen Organisation für Normung, kurz ISO, wurden dabei von 29,1 Prozent der befragten Unternehmen eingesetzt (Bristow, 2021). Besonders interessant ist hier der Standard ISO 27001, auf den näher eingegangen werden soll.

Da diese Arbeit in Deutschland bei der Robert Bosch GmbH geschrieben wird und da im Rahmen dieser Arbeit das entwickelte Framework bei Systemen der Robert Bosch GmbH eingesetzt werden soll, wird außerdem auf den Standard 200-1 des deutschen Bundesamts

für Sicherheit in der Informationstechnik, sowie den Bosch eigenen Standard Enterprise IT Security Architecture, kurz EISA, eingegangen werden.

### 2.2.1 ISO 27001

Die Standards der Internationalen Organisation für Normung werden weltweit von Unternehmen und Organisationen eingesetzt. Die ISO 27000er Familie setzt dabei eine Reihe von Standards für die Informationssicherheit auf.

Das Dokument ISO 27001 in der aktuellen Fassung von 2022 stellt dabei Anforderungen auf, um ein ISMS zu erstellen, zu implementieren, zu warten und zu verbessern (ISO 27001:2022, 1). Ein solches ISMS soll die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewährleisten und damit interessierten Parteien die Gewissheit geben, dass die Risiken angemessen gehandhabt werden (ISO 27001:2022, 0.1).

Die Anforderungen sind dabei nach Themen in Kapitel aufgeteilt, die jeweils eine kurze Beschreibung und dann einige Anforderungen als Aufzählungspunkte und Unterpunkte enthalten (ISO 27001:2022). Eines der Unterkapitel befasst sich mit der Überwachung, Messung, Analyse und Evaluierung. Hier verlangt ISO 27001, dass die Organisation selbst bestimmen soll was, wann und auf welche Weise gemessen werden soll (ISO 27001:2022, 8; ISO 27001:2022, 8). Außerdem soll bestimmt werden, wer die Messungen durchführt und wer die Ergebnisse zu welchem Zeitpunkt analysieren und evaluieren soll (ISO 27001:2022, 8). Zu den Methoden der Messung wird lediglich die Anforderung aufgestellt, dass sie vergleichbare und reproduzierbare Ergebnisse produzieren (ISO 27001:2022, 9.1).

Darüber hinaus gibt es einen Anhang mit möglichen Sicherheitskontrollen, die eingesetzt werden können, um die Anforderungen zu erfüllen (ISO 27001:2022, 6.1.3). Sie sind aus dem zugehörigen Standard 27002 abgeleitet (ISO 27001:2022, Annex A), der daher auch einzeln betrachtet werden soll. Es ist ausdrücklich möglich, eigene Kontrollen hinzuzufügen falls erforderlich (ISO 27001:2022, 6.1.3).

Für alle Dokumente der 27000er Reihe gilt, das sie allgemein anwendbar sein sollen und daher einige Anpassungen auf die individuelle Situation des Unternehmens bedürfen (ISO 27004:2016, S. V). Bei ISO 27001 zeigt sich das dadurch, dass die Anforderungen sehr vage definiert sind und meist großen Freiraum für eigene Spezifikationen lassen. Darüber hinaus

verzichtet ISO 27001 darauf, in den Anforderungen numerische Ziele zu setzen, was den Einsatz von Metriken erschweren kann.

### 2.2.2 ISO 27002

Der Standard 27002 der ISO liefert eine Vorlage für die Implementierung von Kontrollen für ein ISMS, das auf dem Standard 27001 basiert (ISO 27002:2022, 0.1). Jede Kontrolle besteht unter anderem aus einem Titel, einer Beschreibung der Kontrolle, einer Zusammenfassung der Zielsetzung der Kontrolle sowie einigen Anweisungen und Hinweisen zur Implementierung der Kontrolle (ISO 27002:2022, 4.3). Die Kontrollen sind nach der Struktur von des ISO 27001 Standard in Kategorien unterteilt. Jede Kategorie enthält eine übergeordnete Zielsetzung und eine oder mehrere Kontrollen (ISO und IEC 2013). Wie im letzten Unterkapitel erwähnt, sind die Kontrollen in einer kürzeren Form auch im Anhang des Standards 27001 enthalten (ISO 27001:2022, Annex A).

### 2.2.3 NIST Cybersecurity Framework

Das Framework for Improving Critical Infrastructure Cybersecurity, oft auch nur Cybersecurity Framework oder CSF genannt, ist ein beliebter Standard von NIST im Bereich Cybersicherheit, bzw. Cybersicherheits-Risikomanagement. Das Framework wurde ursprünglich zwar für kritische Infrastruktur entworfen, kann aber von Organisationen in allen Sektoren eingesetzt werden (NIST 2018, S. V). Es kann von Organisationen als Grundlage für ein neues Informationssicherheits-Programm, oder zur Verbesserung eines bestehenden Programmes genutzt werden (NIST 2018, 3.0).

Der Kern des Frameworks ist dabei eine Auflistung von Cybersicherheits-Aktivitäten, die nach Funktionen, Kategorien und Unterkategorien gegliedert sind(NIST 2018, Appendix A). Die Kategorien und Unterkategorien beschreiben die Ergebnisse, die durch Cybersicherheits-Aktivitäten erreicht werden sollen, zunehmend genau (NIST 2018, 2.1). Zu jeder Unterkategorie sind zusätzliche einige Informative Verweise aufgeführt. Sie verweisen auf Ausschnitte anderer Standards, Richtlinien und Praktiken, die als Methoden genutzt werden können, um die gewünschten Ergebnisse der jeweiligen Unterkategorie zu erreichen (NIST 2018, 2.1).

Das NIST CSF erlaubt sehr verschiedene Einsatzmöglichkeiten und einen hohen Grad an Anpassung an die eigene Situation. Daher ist es mitunter schwierig zu definieren, wann ein

Unternehmen, bzw. ein Informationssicherheits-System oder Programm, mit dem Framework konform ist (NIST 2018, S. VI). Der Einsatz von Metriken zur Messung der Konformität wird auch hier dadurch erschwert, dass keine klaren Anforderungen definiert sind und keine numerischen Ziele gesetzt werden.

### 2.2.4 NIST Special Publication 800-53

Die NIST Special Publication 800-53 bietet einen Kontrollen-Katalog für Informationssicherheits- und Datenschutzkontrollen für einzelne Informationssysteme oder Organisationen(NIST 2020, S. II). Die Kontrollen sind auf eine Art und Weise definiert, die sie flexibel und an die jeweilige Situation anpassbar macht (NIST 2020, S. II).

Jede Kontrolle besteht aus einer Basiskontrolle, einem Diskussionsteil, einer Liste mit verwandten Kontrollen, Kontrollverbesserungen und Verweisen auf weitere Informationen (NIST 2020, 2.2). Die Basiskontrolle schreibt eine zu implementierende Sicherheits- oder Datenschutzfunktion vor (NIST 2020, 2.2). Im Diskussionsteil werden weitere Informationen zur Kontrolle geliefert (NIST 2020, 2.2). Die Kontrollverbesserungen enthalten Erklärungen zu Funktionen, mit denen die Basiskontrolle erweitert werden kann (NIST 2020, 2.2).

Die Kontrollen sind sehr systematisch definiert, dabei aber trotzdem bewusst offen formuliert. Wieder könnte das Fehlen von numerischen Zielen das Messen der Konformität mit Metriken erschweren. Außerdem muss geklärt werden, ob nur die Basiskontrolle oder auch die Verbesserungen eingehalten werden müssen.

### 2.2.5 NIST Special Publication 800-82

Die NIST Special Publication 800-2 behandelt die Sicherung von industriellen Kontrollsystemen (NIST SP 800-82, S. III). Es werden die typischen Schwachstellen und Bedrohungen der Kontrollsysteme aufgedeckt und entsprechende Sicherheitsmaßnahmen angeboten (NIST SP 800-82, S. III).

Die Special Publication besteht dabei aus mehreren Teilen. Es enthält unter anderem eine Anleitunge zur Entwicklung und Implementierung eines Cybersicherheit-Programmes für industrielle Kontrollsysteme (NIST SP 800-82, 4.0). Weiter bietet es generelle Empfehlungen, um Sicherheit in den für industrielle Kontrollsysteme typischen Netzwerkarchitekturen zu implementieren (NIST SP 800-82, 1.3). Schlussendlich greift es Kontrollen aus der Special

Publication 800-53 auf und gibt Empfehlungen dazu, wie sie für industrielle Kontrollsysteme eingesetzt werden können (NIST SP 800-82, 1.3).

Um Konformität mit diesem Standard zu messen, muss zuerst definiert werden, zu welchem Teil, bzw. welchen Teilen des Standards ein System konform sein soll. Weiter ist es dadurch erschwert, dass der Standard lediglich Empfehlungen enthält und an keinem Punkt klare Anforderungen aufstellt.

### 2.2.6 ISA/IEC 62443 Standardserie

Die ISA/IEC 62443 Standardserie spezifiziert Anforderungen an industrielle Automatisierung und Kontrollsysteme. Sie besteht aus einer Reihe verschiedener Standards und Veröffentlichungen, die in die vier Gruppen Allgemeines, Richtlinien und Verfahren, Systemanforderungen und Komponentenanforderungen unterteilt sind (ISA & IEC 06 2020).

Darüber hinaus gibt es vier verschiedene Rollen, die eine Organisation einnehmen kann, nämlich Anlageneigentümer, Wartungsdienstleister, Integrationsdienstleister und Produktlieferant. Jede dieser Rollen werden dabei bestimmte Aktivitäten zugewiesen, bei denen eine jeweils unterschiedliche Auswahl an Standards zum Einsatz kommt(ISA & IEC 06 2020).

Eine Schwierigkeit bei der Messung der Konformität mit der ISA/IEC 62443 Standardserie ist, dass vorab ermittelt werden muss, welche Standards und Anforderungen für die jeweilige Organisation, das jeweilige System oder das jeweilige Produkt relevant sind.

### 2.2.7 BSI 200-1

Der BSI 200-1 gibt Institutionen eine Anleitung für den Aufbau eines ISMS (BSI 200-1, 1.4). Dabei ist es mit dem ISO-Standard 27001 vollständig kompatibel und beinhaltet Teile er Norm ISO 27002. Der Standard dient auch dazu, die ISO-Standards besser darzustellen und in der BSI IT-Grundschutz zu integrieren, der ein ganzheitlicher Ansatz des BSI für Informationssicherheit ist (BSI 200-1, 2.1.2). Auch für eventuelle Zertifizierungen wird im Standard BSI 200-1 auf die ISO 27001 verwiesen (BSI 200-1, 9).

### 2.2.8 Bosch EISA

Die Bosch Enterprise IT Security Architecture, kurz EISA, ist ein Bosch interner Standard, der ein einheitliches Verständnis und eine konsistente Implementierung von Informationssicherheit zum Ziel hat (EISA 2022.07, 1). Darüber hinaus soll es den Grad der Einhaltung von internen und externen Vorschriften verbessern. Er basiert den Standards von ISO und BSI (EISA 2022.07, 1).

Der Standard definiert Sicherheitskontrollen, -Anforderungen und -Schemas (EISA 2022.07, 3.1), wobei ein Schema eine Zusammenstellung verschiedener Kontrollen ist, die eine gemeinsame Aufgabe erfüllen. Sie sind in die Kategorien Infrastruktur-Schemas und Dienst- und Programmschemas unterteilt (EISA Pattern Catalog 2022.07, S. 2).

Die Kontrollen sind systematisch definiert und enthalten unter anderem eine Beschreibung, eine Zielsetzung sowie ein oder mehrere Szenarien, in denen die Kontrolle Anwendung findet. Außerdem sind für alle Kontrollen die Anforderungen und Kontrollen anderer Standards angegeben, von der die Kontrolle abgeleitet wurde. Schließlich enthält jede Kontrolle eine Reihe von Implementierungsanforderungen, die eine strukturiertere und detailliertere Sicht auf die Eigenschaften der Kontrolle geben soll, die bei der Implementierung zu beachten sind (EISA 2022.07, 3.1).

### 2.2.9 Zwischenfazit

Die Analyse der Standards hat einige Schwierigkeiten aufgedeckt, die beim Aufbau eines allgemein anwendbaren Frameworks auftreten können und daher bedacht werden müssen. Wenn es darum geht, Konformität mit einem Standard nachzuweisen, muss zuerst geklärt werden, was Konformität mit dem entsprechenden Standard bedeutet. Einige Standards, wie zum Beispiel ISO 27001, stellen klare Anforderungen auf, bei denen überprüft werden kann, ob das jeweilige System oder Produkt ihnen gerecht wird oder nicht. Die Erfüllung dieser Anforderungen ist auch eine Voraussetzung für eine entsprechende Zertifizierung (ISO 27000:2018, 0.2). Andere Standards bieten allerdings Kontrollen, wie etwa bei NIST 800-53, oder auch nur Empfehlungen, wie z.B. bei NIST 800-82. In diesen Fällen sind die Empfehlungen, bzw. die Implementierung der Kontrollen als Anforderungen zu verstehen.

Weiter gibt es Standards, bei denen zuerst ermittelt oder bestimmt werden muss, welche Teile ein System oder eine Organisation tatsächlich betreffen. So zum Beispiel bei der Standardserie ISA 62443, die aus verschiedenen Standards besteht, welche nicht immer alle relevant sind.

Außerdem kann ein Standard verschiedene Reifegrade oder optionale Erweiterungen vorsehen, wie z.B. bei den Kontrollverbesserungen des NIST 800-53 Standards. Hier sollte vorher geklärt werden, welche Teile des Standards umgesetzt und auf ihre Einhaltung geprüft werden sollen.

## 2.3 Existierende Ansätze, um die Konformität mit Standards zu messen

In diesem Unterkapitel sollen existierende Ansätze für die Messung der Konformität mit Sicherheitsstandards betrachtet werden. Dabei sollen Lösungsansätze für die in Kapitel 3.1.8 herausgearbeiteten Schwierigkeiten gefunden werden. Außerdem sollen weitere Erkenntnisse aus den verschiedenen Ansätzen gesammelt werden, aus denen später das Framework abgeleitet werden soll.

### 2.3.1 ISO 27004

Mit dem Standard 27004 stellt die ISO einen Ansatz zur Verfügung, um die Effektivität eines auf der Basis des ISO 27001 Standards entstandenes ISMS zu evaluieren Der Standard bietet Konzepte und Herangehensweisen, die breit einsetzbar sein sollen, es wird aber auch darauf hingewiesen, dass es von der jeweiligen Situation und Zielsetzung abhängt, welche Metriken die jeweilige Organisation benötigt (ISO 27004:2016, S. V). An dieser Stelle muss erwähnt werden, dass in diesem Standard stets von *Measures*, also Kennzahlen, die Rede ist, die aber im Sinne der in Kapitel 2 angeführten Definition als Metriken verstanden werden können.

Wie im Kapitel 3.1.1 beschrieben, fordert ISO 27001 Organisationen auf, zu bestimmen, wer was, wann und auf welche Weise messen und wer die Ergebnisse wann und auf welche Weise analysieren und evaluieren soll. ISO 27004 greift diese Punkte im sechsten Kapitel. Es enthält Beispiele für Systeme, Prozesse oder Aktivitäten, die überwacht oder gemessen werden können (ISO 27004:2016, 6.2-3). Für die Frage nach dem Zeitpunkt der Messung und Auswertung liefert ISO 27004 einige Hinweise und Best-Practice-Regeln (ISO 27004:2016, 6). Um zu bestimmen, wer für Messung und Auswertung verantwortlich ist, stellt ISO 27004 einige Rollen bereit, die vor der Messung und Auswertung verteilt werden sollten (ISO 27004:2016, 6.5).

Schließlich enthält der ISO 27004 Standard einen Prozess für die Überwachung, Messung, Analyse und die anschließende Auswertung, der in sechs Schritten einen Kreislauf bildet (ISO 27004:2016, 8.1):

a) Informationsbedarf identifizieren
b) Metriken erstellen und pflegen
c) Verfahren für die Messung, Analyse und die Berichterstattung einführen
d) Überwachen und Messen
e) Ergebnisse analysieren
f) Informationssicherheit und ISMS-Effektivität auswerten.

### 2.3.2 NIST Special Publication 800-55

Die NIST 800-55 ist eine Anleitung für die Entwicklung, Auswahl und Implementierung von Metriken, die die Effektivität der auf ein Informationssystem oder Informationssicherheitsprogramm angewandten Kontrollen aufzeigen. Der Einsatz von Metriken wird damit begründet, dass er die Entscheidungsfindung erleichtern, die Leistung des ISMS verbessern und einen Nachweis für unternommene Sicherheitsbestrebungen liefern kann (NIST SP 800-55, S. VIII). Dabei wird allerdings nicht das Wort Metriken, sondern das Wort *Measures*, also Kennzahlen, benutzt (NIST SP 800-55, 3.1). Nach den Definitionen dieser Arbeit handelt es sich allerdings um Metriken, die weiter auch so bezeichnet werden sollen.

NIST SP 800-55 bezieht sich auf die Kontrollen aus NIST SP 800-53, die enthaltenen Prozesse können aber auch für andere Kontrollen eingesetzt werden (NIST SP 800-55, 1.1). Der Standard enthält zwei wesentliche Prozesse, nämlich den Prozess zur Entwicklung von Metriken und den Prozess zur Implementierung von Metriken (NIST SP 800-55, 1.6). Die Entwicklung von Metriken ist in zwei Aktivitäten unterteilt, die sich weiter in insgesamt sieben Schritte unterteilen lassen und einem Kreislauf folgen. Die Aktivitäten sind die Identifikation von Interessen und Definition des aktuellen Informationssicherheitsprogrammes, sowie die Entwicklung und Selektion von Metriken (NIST SP 800-55, 5). Bei der Implementierung von Metriken wird zwischen insgesamt sechs Schritten unterschieden, von denen die letzten fünf einen Kreislauf bilden. Der Prozess umfasst unter anderem die Vorbereitung und Durchführung der Datenerhebung und -Analyse, die Identifizierung von

Korrekturmaßnahmen, die Sicherungen von Mitteln und Ressourcen, sowie schließlich die Umsetzung der Korrekturmaßnahmen (NIST SP 800-55, 6).

Im Anhang A des NIST Standards befindet sich ein Katalog mit Metriken (NIST SP 800-55, 50). Sie sind allerdings nicht dazu gedacht, komplett übernommen zu werden. Stattdessen sollen sie als Beispiel dienen und an die jeweilige Situation der Organisation angepasst werden (NIST SP 800-55, Appendix A).

### 2.3.3 Zwischenfazit

Die beiden betrachteten Ansätze zeigen gewisse Gemeinsamkeiten, wie etwa die zyklische Form der Prozesse. Die einzelnen Schritte sind leicht unterschiedlich, folgen aber einem ähnlichen Konzept:

1. Die individuelle Situation wird analysiert. Daraus ergeben sich Interessen bzw. ein Informationsbedarf.
2. Metriken werden entwickelt oder selektiert.
3. Es werden Vorbereitungen für die Datenerhebung, Analyse und Berichterstattung getroffen
4. Die Daten werden gemäß den Vorbereitungen erhoben
5. Die Daten werden analysiert und ausgewertet

Während der ISO-Standard mit der Evaluierung endet (ISO 27004:2016, 8.1), fügt der Standard 800-55 von NIST noch weitere Schritte hinzu. Es sollen auf Basis der ausgewerteten Daten Korrekturmaßnahmen identifiziert und schließlich umgesetzt werden (NIST SP 800-55, 6).

## 2.4 Verschiedene Aggregationen von Metriken

Laut Black sollten Metriken auf verschiedenen Ebenen, bzw. Level, definiert werden (Black et al., 2008). Die Levels stellen dabei die Granularität und gleichzeitig meist die Nähe zur technischen Grundlage einer Metrik dar.

Ein Beispiel für eine Low-Level-Metrik ist etwa der Anteil der Computer im Unternehmensnetzwerk, die Antivirensoftware installiert haben. Diese Metriken haben meist einen klaren Bezug auf einzelne Technologien und einzelne eingesetzte Kontrollen. Dadurch sind sie in der Regel interessant für die technisch versierte Mitarbeiter und die Rollen, deren

Aufgabe die Implementierung und Überwachung der Sicherheitskontrollen ist (Black et al., 2008).

Die stärker aggregierten High-Level-Metriken lassen sich aus Kennzahlen und außerdem aus Low-Level-Metriken berechnen (Black et al., 2008). Diese Art von Metrik wird auch Komposit-Metrik genannt (NIST SP 500-307. 5.2.6). Sie adressieren auch weniger technisch versierte Mitarbeiter und eignen sich für die Kommunikation der Ergebnisse an das Management (Black et al., 2008). Ein Beispiel für eine High-Level-Metrik ist der Schutz vor Hacking-Angriffen. Zur Berechnung könnte der Anteil der Computer mit installiertem Virenschutz dienen, aber auch andere Größen wie etwa die Umsetzung von Richtlinien zur Passwortstärke.

Zusammenfassend schreibt Black, dass Low-Level-Metriken für taktische und High-Level-Metriken für strategische Entscheidungen geeignet sind (Black et al., 2008). Die Überprüfung einzelner Kontrollen ist dabei eher eine taktische und die Überprüfung der gesamten Konformität eine strategische Angelegenheit.

## 2.5 Eigenschaften einer guten Metriken

Es gibt einige Eigenschaften, die eine gute Metriken haben sollte und auf die bei der Selektion zu achten ist. Schon bei der Selektion der Metriken ist darauf zu achten, dass die notwendigen Daten tatsächlich verfügbar sind (Yee, 2013). Dadurch wird vermieden, dass Arbeit in die Definition und Vorbereitung von Metriken fließt, die im Endeffekt nicht zum Einsatz kommen können, da die Messung mit verhältnismäßigem Aufwand nicht möglich ist. Weiter empfiehlt es sich, Gelegenheiten zu suchen, um bereits existierende Datenquellen zu nutzen. Dadurch werden die zusätzlichen Kosten für den Aufbau neuer Datenquellen und die Implementierung der Datenerhebung vermieden (Black et al., 2008).

Außerdem sollen Metriken objektiv (Yee, 2019) und in ihrer Messung konsistent sein (Jaquith, 2007). So schreibt Jaquith, dass eine Metrik, wenn sie von zwei verschiedenen Personen gemessen wird, trotzdem das gleiche Ergebnis haben muss. Weiter schreibt er, dass eine Metrik nicht auf subjektiven Einschätzungen basieren darf. In diesem Fall sei es keine Metrik, sondern lediglich eine Bewertung (Jaquith, 2007). Yee fügt hinzu, dass die Reproduzierbarkeit von Ergebnissen eine wichtige Anforderung für die Wissenschaftlichkeit der Metriken ist (Yee, 2013). Ob der Aspekt der Wissenschaftlichkeit für die jeweilige Organisation relevant ist, ist nicht allgemein festzustellen.

Um die konsistente Messung sicherzustellen, muss sie klar definiert werden, worauf im nächsten Unterkapitel eingegangen werden soll. Allerdings sind sich die betrachteten Quellen einig, dass die Messung falls möglich automatisiert werden soll, da eine automatisierte Messung in der Regel konsistentere und genauere Ergebnisse hervorbringt, menschliche Fehler vermieden werden und nach der anfänglichen Implementierung sogar Kosten und Aufwand gespart werden (Jaquith, 2007; Black et al., 2008; ISO 27004:2016, 7.1). Es ist also sinnvoll bei der Auswahl von Metriken solche vorzuziehen, die in der Organisation automatisiert messbar sind.

Jaquith empfiehlt, Metriken als Zahl oder Prozentsatz anzugeben, wobei im Fall von absoluten Zahlen ordinale Skalen, wie zum Beispiel Levels, vermieden werden sollen, da diese subjektiven Bewertungen zugrunde liegen (Jaquith, 2007). In der NIST SP 800-55 ist außerdem festgehalten, dass die Quantifizierbarkeit für die Vergleichbarkeit der Metriken relevant ist (NIST SP 800-55, 3.1). Hayden spricht sich stattdessen für den Einsatz von qualitativen Metriken, wie etwa ordinale Level, aus, da nicht der numerische Wert, sondern die Interpretation der Werte den eigentlichen Mehrwert für die Organisation schafft (Hayden, 2010). Dagegen lässt sich einwenden, dass für die Interpretation mit quantitativen Metriken eine bessere und genauere Datengrundlage geschaffen wird (Yee, 2019). Schließlich dienen Metriken nicht nur dazu, den aktuellen Stand abzubilden, sondern auch dazu Trends und die Veränderung über einen längeren Zeitraum hinweg aufzuzeigen (Yee, 2013), wofür eine Ordinal-Skala womöglich nicht genau genug wäre.

Weiter schreibt Hayden, dass qualitative Metriken zwar ungenau, quantitative Metrik aber oft unvollständig sein (Hayden, 2010). Daher ist es wichtig, sicherzustellen, dass die gewählten Metriken ausreichen, um den jeweiligen Informationsbedarf zu decken (Yee, 2019). Dafür schlägt Yee (2019) vor, sich drei Fragen zu stellen, die frei übersetz lauten wie folgt:

1. Bedeutet ein Anstieg des gemessenen Wertes auch einen konsistenten Anstieg, bzw. eine Konsistente Verringerung des Sicherheitslevels?
2. Hat die gemessene Kennzahl einen direkten Einfluss auf das Sicherheitslevel?
3. Gibt es Aspekte, die bei der Definition der Kennzahl fehlen, die aber notwendig wären, damit die Metrik ein effektives Maß für den betrachteten Teil der Informationssicherheit wäre?

Darüber hinaus schreibt Yee, eine Metrik solle progressiv sein. Das bedeutet, dass sie nach den durch Sicherheitsmaßnahmen erreichten Fortschritt abbilden und nach gegebener Zeit ein akzeptables Level erreichen können muss (Yee, 2019). Dieses akzeptable Level soll dabei bereits bei der Definition der Metrik als Richtwert festgelegt werden.

Zusammenfassend lässt sich sagen, dass bei der Auswahl der Metriken auf einige Aspekte geachtet werden soll. Die Daten für die Berechnung der Metrik müssen im Kontext der jeweiligen Organisation verfügbar und mit verhältnismäßigem Aufwand messbar sein. Dafür empfiehlt es sich auch bestehende Datenquellen mit- bzw. umzunutzen. Weiter soll eine Metrik in ihrer Messung konsistent sein, d.h. sie soll reproduzierbare Ergebnisse liefern. Automatisierte Messungen sollten daher manuellen Messungen vorgezogen werden. Eine Metrik sollte objektiv sein, weshalb ordinale Skalen zu vermeiden sind. Gute Metriken müssen außerdem progressiv sein, d.h. sie müssen eine Veränderung der Sicherheitslage durch eine konsistente Veränderung ihres Wertes abbilden, und sie sollen einen Zielwert enthalten, ab dem das Ziel als zu genüge erfüllt gilt. Weiter muss bei der Wahl darauf geachtet werden, dass die gewählten Metriken für den jeweiligen Zweck ausreichend sind.

## 2.6 Genauigkeit der Messungen

Nachdem im letzten Kapitel wichtige Aspekte für die Selektion von Kennzahlen herausgearbeitet wurden, soll in diesem Kapitel darauf eingegangen werden, worauf bei der Definition der gefundenen Metriken zu achten ist.

Wie im Kapitel 3.4 festgestellt, ist die Konsistenz der gemessenen Kennzahlen ein wichtiger Aspekt bei der Auswahl und Definition von Metriken. Die Genauigkeit einer Metrik hängt per Definition von der Genauigkeit der Kennzahlen ab, aus der sie sich zusammensetzt (Black et al. 2008). Es ist also wichtig, bei der Definition der Metrik auch die Messung der Kennzahl genau zu definieren. Ein Beispiel hierfür ist der Anteil der Systeme, die vollständig aktuell sind. Um diese Größe zu messen, müsste erst geklärt werden, ob mit *System* nur das Betriebssystem oder auch alle anderen installierten Dienste und Programme gemeint sind (Black et al. 2008). Weiter könnte unklar sein, ob ein System schon als aktuell gilt, sobald ein Patch installiert ist oder erst nachdem das System neugestartet wurde, wodurch die Änderungen wirksam werden.

Auch Fachbegriffe können Unklarheiten enthalten, die beachtet werden müssen. Wenn man zum Beispiel misst, wie viele Port-Scans pro Monat durchgeführt werden, muss die Bedeutung eines Port-Scans im aktuellen Kontext definiert werden. Wenn z.B. ein Angreifer 100 Ports scannt, könnte das als ein einzelner oder 100 verschiedene Port-Scans gewertet werden (Black et al. 2008). Bei automatischen Messmethoden, wie etwa einem Virenschutzprogramm oder im Fall des Port-Scan-Beispiels, einem Intrusion Detection System, muss bedacht werden, dass unterschiedliche Programme bzw. Systeme dieselben Kennzahlen eventuell anders messen. Auch können durch veränderte Einstellungen die Ergebnisse beeinflusst werden (Black et al., 2008). Es sollte also bei der Definition der Metrik die Messung so genau wie praktisch möglich definiert werden, wobei speziell Unklarheiten bei vermeintlich eindeutigen Begrifflichkeiten bedacht werden müssen. Als eine alternative Möglichkeit, um mit Doppeldeutigkeiten bei der Messung umzugehen, führt Black die Idee an, beide oder mehrere Messmethoden als jeweils eigenständige Kennzahl zu definieren und zu einer Metrik zu verrechnen (Black et al., 2008).

## 2.7 Einheitliches Format für die Dokumentation von Metriken

Für die Dokumentation der Metriken wird in der NIST SP 800-55 ein standardisiertes Format empfohlen, um die Wiederholbarkeit der Entwicklungs-, Anpassungs-, Analyse- und Berichterstattungsprozesse von Metriken zu gewährleisten. Dafür wird im Standard eine Vorlage zur Verfügung gestellt, die elf Felder in einer Tabelle enthält (NIST SP 800-55, 5.6). Im Standard ISO 27004 findet sich eine ähnliche Vorlage, die bis auf das Feld *Typ*, dieselben Felder enthält (ISO 27004:2016, 8.3.3). Anstelle des *Zieles* enthält es allerdings ein Feld namens *Informationsbedarf.* Im Folgenden sollen die Felder genauer betrachtet werden, wobei Erklärungen aus beiden Standards genutzt werden.

Die **ID** ist dabei eine einzigartige Identifizierung, die der Nachverfolgung und der Ordnung dient (NIST SP 800-55, 5.6).

Das Feld ***Ziel*** aus dem NIST Standard beschreibt ein strategisches Ziel oder ein Ziel in der Informationssicherheit, das mit der Metrik überprüft werden soll. Eine Kombination aus beidem ist auch möglich. Für Metriken, die sich auf einzelne Kontrollen beziehen, ist das Ziel auch eine Anleitung für die Implementierung der Kontrolle (NIST SP 800-55, 5.6). Der ***Informationsbedarf*** aus dem ISO Standard wird als der übergreifende Informationsbedarf beschrieben, zu dem die Metrik beiträgt (ISO 27004:2016, 8.3.3). Der Sinn beider Felder scheint zu sein, zusätzliche Informationen über die Hintergründe der Metrik zu liefern.

Das Feld ***Metrik*** enthält eine Erklärung zur Messung, die einen Begriff wie etwa Prozentsatz, Anzahl, Frequenz oder Durchschnitt enthalten soll (ISO 27004:2016, 8.3.3).

Die ***Formel*** gibt an, wie die Metrik berechnet wird. Die einzelnen Größen, die zum Ergebnis der Metrik verrechnet werden, werden im Feld *Implementierungsnachweis* beschrieben (NIST SP 800-55, 5.6).

Der ***Zielwert*** stellt einen Grenzwert dar, ab dem die Anforderung als ausreichend umgesetzt oder die Kontrolle als ausreichend erfolgreich gilt (NIST SP 800-55, 5.6). Es kann trotzdem notwendig sein, die Metrik weiter zu verfolgen, nachdem sie erstmals den Zielwert erreicht hat, um sicherzustellen, dass er auch weiterhin erreicht wird (ISO 27004:2016, 8.3.3). Für Metriken, die die Implementierung einer Kontrolle messen, soll der Zielwert immer bei 100 Prozent liegen (NIST SP 800-55, 5.5.3).

Das Feld ***Implementierungsnachweis*** dient dazu, eine oder mehrere Messungen zu beschreiben, die für die jeweilige Metrik relevant sind. Bei einer manuellen Messung sollen Fragen und Daten, bei einer automatisierten Messung nur Daten, definiert werden, die für die Berechnung gebraucht werden. Außerdem können Fragen für die Validierung der Metrik formuliert werden (NIST SP 800-55, 5.6).

Die ***Frequenz*** gibt an, wie oft die für jeweilige Metrik erforderlichen Daten erhoben und wie oft die Berichterstattung für die Ergebnisse stattfindet (ISO 27004:2016, 8.3.3). Im NIST Standard wird empfohlen, die Frequenz der Datenerhebung von der Änderungsrate der jeweiligen Sicherheitskontrolle abhängig zu machen, während die Häufigkeit der Berichterstattung von externen Anforderungen oder internen Präferenzen abhängig gemacht werden sollte (NIST SP 800-55, 5.6).

Die ***verantwortlichen Parteien***, die genannt werden sollen, sind der Eigentümer der Informationen, der Messbeauftragte und der Interessent, der die Ergebnisse der Analyse erhält. Weiter wird von NIST empfohlen, dass der Eigentümer der Informationen und der Messbeauftragte idealerweise nicht dieselbe Person bzw. Partei sein soll, um einen Interessenkonflikt zu vermeiden (NIST SP 800-55, 5.6).

Die ***Datenquelle*** könnte eine Datenbank, ein Programm, eine Organisation oder eine Person, bzw. Rolle sein, die die jeweiligen Informationen enthält oder liefern kann (ISO 27004:2016, 8.3.3).

Das ***Berichterstattungsformat*** gibt Auskunft darüber, wie die Ergebnisse der Metrik kommuniziert werden sollen. ISO nennt beispielhaft die Formate Text, Zahl oder verschiedene Graphen, die als Dashboard oder anderweitig präsentiert werden können (ISO 27004:2016, 8.3.3).

Es empfiehlt sich also, Metriken in einem standardisierten Format zu dokumentiert. Dafür wurden Vorlagen aus zwei bekannten Standards betrachtet, die als Ausgangspunkt für die Entwicklung einer eigenen Vorlage dienen können.

## 2.8 Kommunikation von Ergebnissen

Wenn durch die Messung und Berechnung von Metriken Erkenntnisse gewonnen werden, müssen diese natürlich noch eingesetzt werden. Der erste Schritt dabei ist, die interessierten Parteien über die Ergebnisse zu informieren.

Der ISO Standard 27001 enthält dafür unter anderem die Anforderung, dass eine Organisation bestimmen muss, wem sie was, wann und auf welche Weise kommunizieren muss (ISO 27001:2022, 7.4). Um diese Anforderung zu erfüllen, soll laut ISO 27004 bestimmt werden, welche Metriken intern und extern kommuniziert werden sollen. Weiter sollen Auflistungen mit relevanten Metriken für die einzelnen interessierten Parteien erstellt werden (ISO 27004:2016, 8.9). Aber auch wer nicht selbst den ISO-Standard einsetzt, tut gut daran, schon frühzeitig und am besten schon bei der Definition der Metriken die Kommunikation der Ergebnisse zu planen.

Mögliche Formen der Berichterstattung, die im ISO 27004 vorgeschlagen werden, sind als Text, Zahlenwert oder grafisch, etwa in Form eines Diagrammes als Teil eines Dashboards (ISO 27004:2016, 8.3.3). Gerade Dashboards sind dabei eine sehr beliebte Form der Berichterstattung. Bereits 2009 hatte eine Studie des Data Warehousing Institute bei einer Befragung von 495 Unternehmen festgestellt, dass 72 Prozent der Unternehmen bereits Dashboards einsetzten, was im Vergleich zu 2004 einen Anstieg von 21 Prozent bedeutete. Weitere 13 Prozent gaben an, dass sie daran arbeiten, Dashboards im Unternehmen einzusetzen (Eckerson, 2011).

Um die Information grafisch anschaulich darzustellen, sei es als Teil eines Dashboards oder in einer anderen Form, gibt es einige Regeln und Best-Practices. So zum Beispiel die SUCCESS Regeln, die in den International Business Communication Standards definiert sind und Regeln

für das Design von Diagrammen und Tabellen in Berichten, Präsentationen und Dashboards sind (IBCS Association, 2023). Das Wort Success ist dabei ein Akronym für die Wörter Say, Unify, Condense, Check, Express, Simplify und Structure, die die einzelnen Regeln darstellen (Rosenfelder & Terbuch, 2018). Im Folgenden soll eine kurze Zusammenfassung der wichtigsten Regeln für das Design von Dashboards und Grafiken erbracht werden.

Noch vor der Gestaltung des Diagramms oder Graphen ist es aber wichtig zu entscheiden, welcher Diagrammtyp für welche Daten eingesetzt werden soll. Hierfür haben Costa und Aparicio einen Entscheidungsbaum aufgestellt, der eingesetzt werden kann, um den richtigen Typ zu finden (Costa & Aparicio, 2019). Er ist in Abbildung 2 leicht vereinfacht dargestellt. Um den Entscheidungsbaum zu nutzen, muss zuerst der Sinn des Graphen in eine von vier Gruppen eingeteilt werden, nämlich Vergleich, Verteilung, Zusammensetzung oder Beziehung. Weiter wird nach Anzahl Kategorien und betrachteter Objekte unterschieden werden. Bei zeitlich verteilten Daten ist die Anzahl der einzelnen Zeitpunkte und die Natur des zeitlichen Verlaufs ausschlaggebend (Costa & Aparicio 2019).

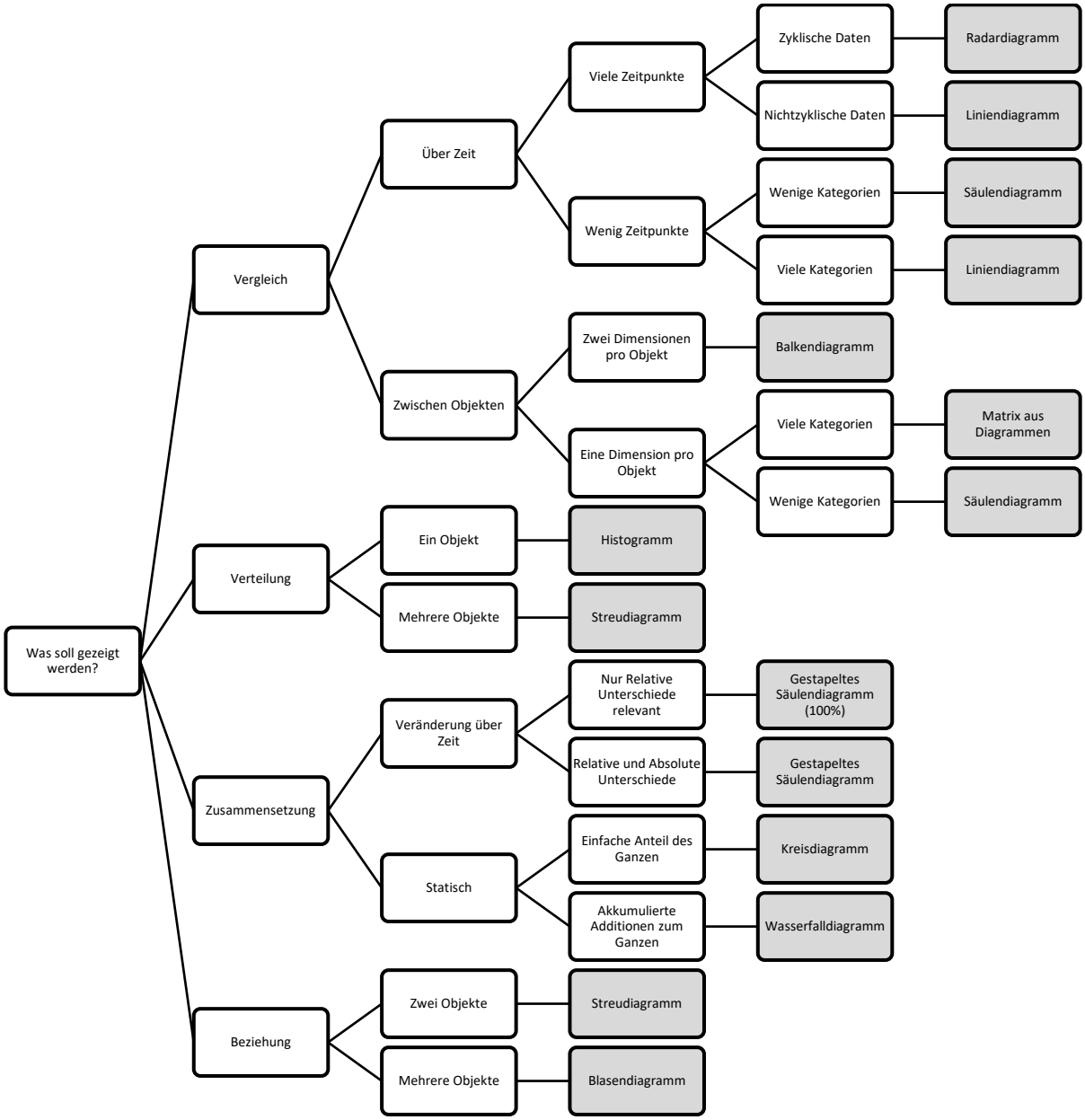


*Abbildung 2: Entscheidungsbaum für die Auswahl eines Diagrammtypen*

*In Anlehnung an Costa & Aparicio, 2013, S.13*

Nach der Auswahl eines Diagrammtypen muss über die Gestaltung des Diagramms nachgedacht werden. Dabei soll das Hauptaugenmerk der Gestaltung einer Grafik auf der zu vermittelnden Information liegen. Im besten Fall soll ein Betrachter keinen Grund haben, um über das Design selbst nachzudenken (Jaquith 2007). Weiter besagt die erste der SUCCESS Regeln, Say, dass eine Grafik nicht nur Daten, sondern auch eine Botschaft vermitteln soll (Rosenfelder & Terbuch, 2018). Die Gestaltung der Grafik sollte also nie im Vordergrund stehen und nur dazu beitragen die Informationen und insbesondere die Kernaussage der Grafik zu präsentieren.

Daher ist es sinnvoll, alle überflüssigen gestalterischen Elemente zu entfernen(Jaquith, 2007; Rosenfelder & Terbuch, 2018). Überflüssig ist ein Element dann, wenn es nicht zur Vermittlung der dargestellten Informationen beiträgt. Beispielhaft nennt Jaquith die Rahmen des Diagramms oder die Rahmen der einzelnen Säulen eines Säulendiagramms (Jaquith, 2007). Beides enthält keine Information und trägt auch nicht zur Vermittlung der Information bei. Anders ist es etwa bei Gitterlinien, die dem Betrachter erlauben die Höhe der Säulen besser einzuschätzen und die daher der Informationsvermittlung zuträglich sind. Dennoch fordert Jaquith (2007), dass sie mit schwacher Farbe oder nur als gepunktete Linie dargestellt werden, um nicht von den Kerninformationen abzulenken.

Auch die Farben, die benutzt werden, sollten der Vermittlung der Information dienen und daher eine Bedeutung haben. Ein möglicher sinnvoller Ansatz ist, gute Informationen grün und schlechte Informationen rot darzustellen. Dabei sollten bestenfalls nur 3-5 verschiedene Farben genutzt werden, da Menschen Schwierigkeiten hat mehr als fünf Farben auf einmal zu unterscheiden (Costa und Aparicio, 2019). Weiter können Farben eingesetzt werden, um Zusammengehörigkeit erkenntlich zu machen. Wenn etwa in einem Diagramm daten aus verschiedenen Quellen oder Kategorien verglichen werden, ist es sinnvoll, den einzelnen Kategorien jeweils eine Farbe zuzuweisen (Rosenfelder & Terbuch, 2018).

Damit ein Betrachter verstehen kann, worum es bei einer Grafik geht, muss sie entsprechend beschriftet sein. Im Titel sollte knapp der Kern der dargestellten Daten zu beschreiben werden. Bei mehreren betrachteten Dimensionen soll die Abhängigkeit mit einem Wort wie von, nach oder pro beschrieben werden (Jaquith 2007). Beispiele dafür sind die Durchschnittliche Anzahl an Softwarefehler pro Programm oder die akkumulierte Downtime nach System. Weiter sollen die Achsen knapp die Dimension und Einheit der Daten beschreiben (Jaquith 2007). Die Beschriftung der Y-Achse könnte beispielsweise lauten: Akkumulierte Downtime in Stunden.

## 2.9 PDCA-Zyklus

Das zu entwickelnde Framework soll dem PDCA-Zyklus folgen. Dieses Kapitel soll zeigen, was die Vorteile des Zyklus sind und warum er sich für dieses Framework eignet.

Der PDCA-Zyklus kommt aus dem Qualitätsmanagement und beinhaltet eine Reihe von Aktivitäten zur kontinuierlichen Verbesserung. Er ist eine ursprünglich japanische Abwandlung des Deming-Kreises (Imai, 1986).

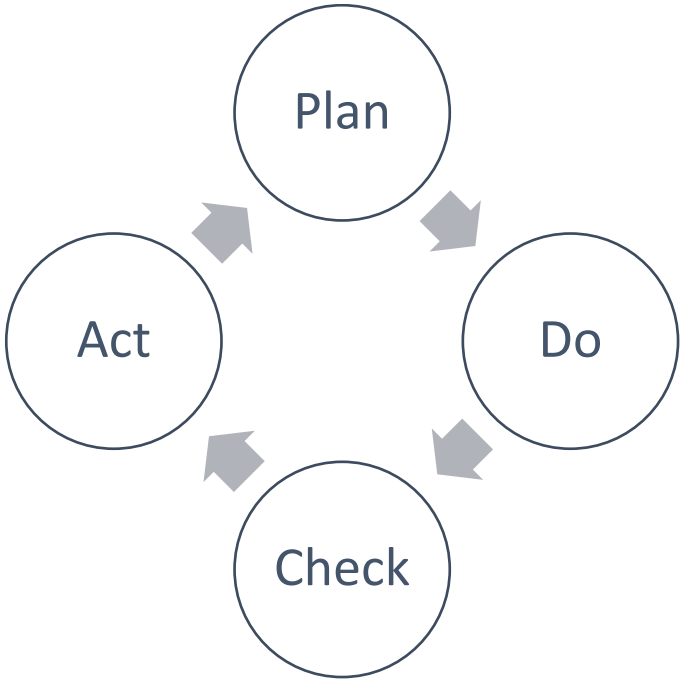


*Abbildung 3: Die vier Phasen des PDCA-Zyklus*
*Eigene Darstellung nach Imai, 1986*

Der Zyklus besteht aus den vier Phasen Plan, Do, Check und Act. Die erste Phase, Plan beschreibt die Entwicklung eines Produktes. In der zweiten Phase, Do, wird das Produkt dann hergestellt, bzw. eingesetzt. Bei Check geht es darum, den Erfolg des Produktes zu überwachen, zum Beispiel indem Verkaufszahlen betrachtet werden. Am Ende sollen, abhängig vom dritten Schritt, Konsequenzen gezogen werden. Der Schritt Act, der teilweise auch Action genannt wird, beschreibt dabei die Korrekturen am Produkt und die Vorbereitungen für die weitere Entwicklung (Imai, 1986).

Der PDCA-Zyklus findet auch im Themenbereich Informationssicherheit häufig Anwendungen. Externe Rahmenbedingungen, wie gesetzliche Vorgaben oder die Bedrohungslandschaft, aber auch die interne Situation, wie etwa die eingesetzte Technik oder die Prozesse, können sich ständig verändern. Daher muss ein Sicherheitskonzept aktiv verwaltet und überarbeitet werden, um die Sicherheit weiter zu gewährleisten und kontinuierlich zu verbessern (BSI 200-1, 3.2.1). Der BSI-Standards 200-1 zum Beispiel, setzt den PDCA-Zyklus für den Aufbau und die Wartung eines ISMS ein (BSI 200-1, 3.2.2). Die aktuelle Version des ISO 27001 Standards verlangt zwar eine kontinuierliche Verbesserung der Eignung, Angemessenheit und Wirksamkeit des ISMS (ISO 27001:2022, 10.1), geht dabei aber nicht auf einen spezifischen Zyklus ein, der eingehalten werden muss. Allerdings lassen sich die vier Phasen des PDCA-Zyklus im Kapitel 6, Planning, dem Kapitel 8, Operations, dem Kaptiel 9, Performance

Evaluation und dem Kapitel 10, Improvement, wiederfinden (ISO 27001:2022, S. III), weshalb der Zyklus auch hier gut anwendbar ist. Dazu sei gesagt, dass der ISO 27001 Standard den PDCA-Zyklus in seiner ersten Version von 2005 noch namentlich erwähnt und eingesetzt hat (ISO 27001:2005, S. V–VI).

Das sind nur zwei Beispiele für Einsatzmöglichkeiten des PDCA-Zyklus im Bereich der Informationssicherheit, bzw. zwei Beispiele für die Anwendung auf Standards, die ein ISMS definieren. Aufgrund der Beliebtheit und der Vorzüge des bewährten Ansatzes, wird es auch in diesem Framework zum Einsatz kommen. Die folgenden Kapitel entsprechen dabei den vier Phasen des Zyklus.

# 3 Entwicklung des Frameworks

In diesem Kapitel soll ein Framework zur Bestimmung der Konformität mit Sicherheitsstandards durch den Einsatz von Metriken definiert werden. Dafür sollen die in den vorigen Kapiteln gesammelten Erkenntnisse aufgegriffen und eingesetzt werden.

Die Struktur des folgenden Kapitels ist an den PDCA-Zyklus angepasst, der in Kapitel 3.8 beschrieben ist. Die Abbildung 4 zeigt dabei die einzelnen Unterpunkte jeder einzelnen Phase. Die einzelnen Punkte sind dabei von den in Kapitel 3.2.3 identifizierten Schritten aus den Standards ISO 27004 und NIST 800-55 abgeleitet. In den folgenden Kapiteln soll auf die einzelnen Phasen eingegangen werden. Dabei werden die einzelnen Unteraufgaben erklärt.

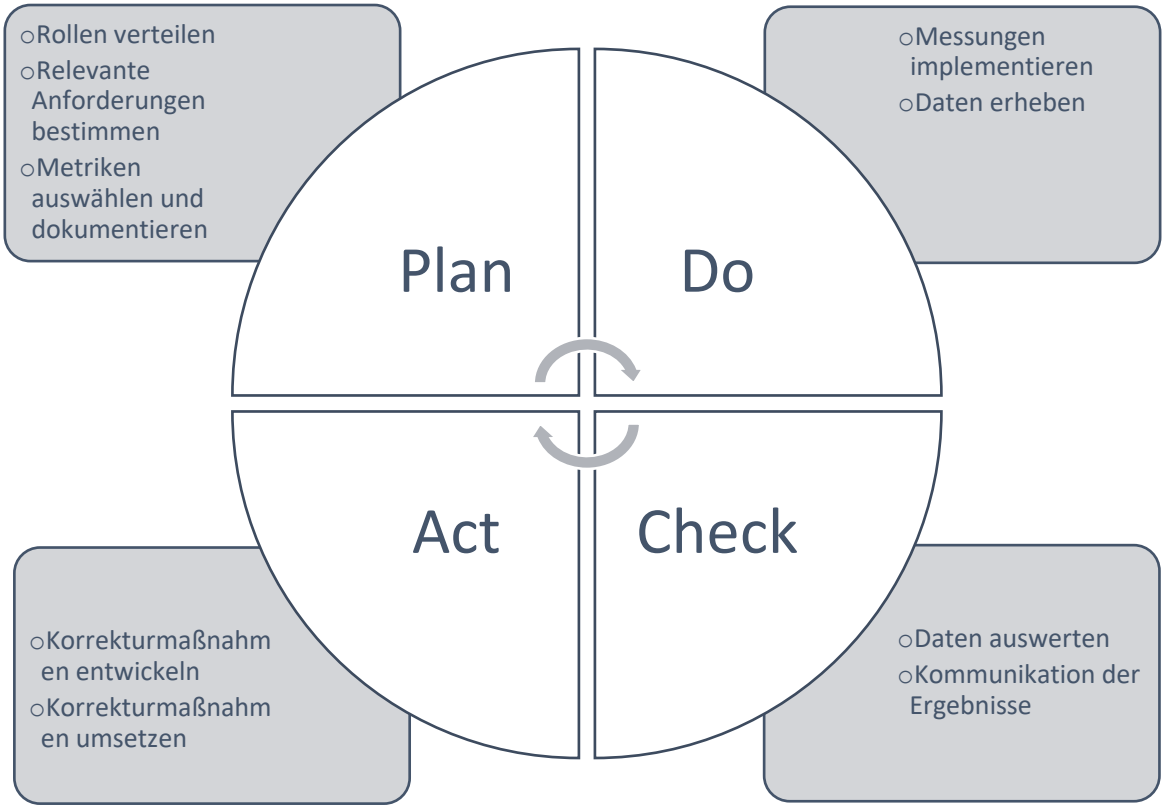


*Abbildung 4: Der PDCA-Zyklus mit den einzelnen Schritten*

*Eigene Darstellung*

## 3.1 Phase 1 - Plan

In dieser ersten Phase des Zyklus sollen die planerischen Vorbereitungen für die Messung der Konformität mit dem gewählten Standard getroffen werden. Dafür müssen zuerst Rollen verteilt werden. Danach sollen die relevanten Anforderungen aus dem gewählten Standard identifiziert werden. Schließlich müssen passende Metriken gefunden und systematisch definiert sowie dokumentiert, werden.

### 3.1.1 Rollen verteilen

Um eine klare Aufgabenverteilung zu gewährleisten ist es wichtig ganz zu Beginn des Prozesses Rollen zu verteilen. Einige Standards haben eine Rollenverteilung auch als Anforderung definiert, wie etwa ISO 27001, der von der Organisation verlangt festzulegen, wer für die Überwachung und Messung und wer für die Analyse und Auswertung der Daten zuständig ist (ISO 27001:2022, 9.1).

Die genaue Rollenverteilung hängt von der individuellen Situation des Unternehmens und gegebenenfalls auch vom gewählten Standard ab. Die folgenden Rollen, die von ISO 27004 abgeleitet und für dieses Framework leicht angepasst sind (ISO 27004:2016, 6.5), können aber als Beispiel dienen:

- **Messauftraggeber**: Die Partei, die die Informationen anfordert oder benötigt.
- **Messungsplaner**: Die Person oder Organisationseinheit, die für die Planung der Messung, inklusive der Auswahl und Definition von Metriken und Kennzahlen, verantwortlich ist.
- **Prüfer der Messung**: Die Person oder Organisationseinheit, die überprüft, ob die Metriken und Kennzahlen geeignet sind, um wirksam die Konformität mit den Anforderungen des jeweiligen Standards zu überprüfen.
- **Informationseigentümer**: Die Person oder Organisationseinheit, die Eigentümer der Informationen ist, die in die Messungen einfließen und für die Bereitstellung der Daten verantwortlich ist.
- **Informationssammler**: Die Person oder Organisationseinheit, die für die Sammlung, Aufzeichnung und Speicherung der Daten verantwortlich ist.
- **Informationsanalytiker**: Die Person oder Organisationseinheit, die für die Analyse und Auswertung der Daten verantwortlich ist.
- **Informationsvermittler**: Die Person oder Organisationseinheit, die für die Kommunikation der Analyseergebnisse verantwortlich ist.

### 3.1.2 Standard analysieren und relevante Anforderungen extrahieren

Wenn die Rollen verteilt sind, kann mit der Planung der Metriken und Messungen begonnen werden. Zuerst muss dabei geklärt werden, was gemessen werden soll. Wie es sich bei der

Beispielhaften Betrachtung einiger Standards in Kapitel 3.1 gezeigt hat, ist es oft notwendig zu ermitteln, welche Teile eines Standards für die jeweilige Situation relevant sind. Es könnte Standards bzw. Standardserien geben, die sich aus mehreren Publikationen zusammensetzen, wie die ISA/IEC 62443 Standardserie. Hier müssten die relevanten Standards oder die relevanten Teile des Standards ausgewählt werden.

Aber auch bei weniger fragmentierten Standards müssen jene Anforderungen selektiert werden, die im aktuellen Kontext Anwendung finden. Die betrachteten Standards in Kapitel 3.1 bezogen sich meist auf die unternehmensweite Cybersicherheit. Wenn die Messung der Konformität sich aber nur auf ein System, eine Gruppe an Systemen, ein bestimmtes Netzwerk oder einen anderen Teilbereich beziehen, ist es durchaus möglich, dass einige der Anforderungen des gewählten Standards, nicht anwendbar sind. Genauso könnten bestimmte Anforderungen aufgrund der Zielsetzung der Messung nicht relevant sein. So widmet etwa die NIST Special Publication 800-53 ein Kapitel den Maßnahmen zum Schutz vor physischen und Umgebungsschutz (NIST SP 800-53 Rev. 5, 3.11). Sollte die Messung der Konformität zum Zweck einer besseren Softwaresicherheit durchgeführt werden, werden viele der in diesem Kapitel aufgeführten Kontrollen nicht relevant sein, auch wenn sie die ausgewählten Systeme betreffen können. Darüber hinaus kann es aufgrund der individuellen Lage der Organisation immer zu weiteren Unstimmigkeiten kommen.

### 3.1.3 Metriken für die relevanten Anforderungen auswählen

Wie in Kapitel 3.3 dargestellt, kann man bei Metriken zwischen verschiedenen Leveln der Granularität unterscheiden. Um die Konformität mit einer Anforderung zu prüfen, müssen häufig mehrere Metriken zu einer Komposit-Metrik zusammengesetzt werden. Die Herausforderung ist es, zu bestimmen, welche Metriken für die jeweilige Anforderung relevant sind und wie sie möglichst sinnvoll zu einer Komposit-Metrik verrechnet werden können.

Die Metriken können aus verschiedenen Quellen stammen. So gibt es einige bekannte Kataloge mit Metriken, zum Beispiel vom *Center for Internet Security*, kurz CIS (CIS, 2019) oder dem *Europäischen Institut für Telekommunikationsnormen*, kurz ETSI (ETSI, 2016). Außerdem gibt es einige Kataloge, die sich bereits auf bestimmte Standards beziehen und somit bereits eine Zuordnung zu den einzelnen Anforderungen mitbringen. Beispiele hierfür sind die

Metriken in den Anhängen der des ISO 27004 (ISO 27004:2016) oder des NIST 800-55 (NIST SP 800-55) Standards befinden. Allerdings haben beide Kataloge nicht den Anspruch, die Anforderungen des jeweiligen Standards voll abzudecken.

Nach einer umfassenden Suche mit verschiedenen Suchmaschinen wie Google Scholar und MetaGer konnte in der Literatur kein Ansatz für die Zuordnung von Metriken auf Anforderungen gefunden werden. Um die eigenständige Zuordnung zu vermeiden, könnten aber vorhandene Zuordnungen genutzt werden. Viele Quellen für Metriken bringen bereits eine Zuordnung zu den Anforderungen eines oder mehrere Standards mit sich, wie zuvor erwähnt. Interessant dafür sind die CIS Critical Security Controls (CIS, 2019), für die das CIS Zuordnungen zu einer Vielzahl anderer Standards bereitstellt. Diese können eingesetzt werden, um die Metriken, die bei den CIS Controls als *Measure* bezeichnet werden (CIS, 2019), auch für andere Standards einzusetzen.

Bei weniger verbreiteten Standards ist es allerdings nicht unwahrscheinlich, dass keine direkten Zuordnungen zwischen den Anforderungen und den Metriken eines anderen Standards oder Kataloges zur Verfügung stehen. Hier kann ein anderer Standard als Bindeglied eingesetzt werden, falls von ihm aus Zuordnungen zu den Metriken und Anforderungen bestehen.

Zum besseren Verständnis soll ein Beispiel gemacht werden. Dafür sollen passende Metriken aus den CIS Controls gesucht werden, um Kontrollen des EISA-Standards zu überprüfen. Der der EISA-Standard von Bosch entwickelt und eingesetzt und ist außerhalb des Unternehmens nicht weit verbreitet. Daher gibt es vonseiten des CIS keine Zuordnungstabelle der für den EISA-Standard. Allerdings enthalten die Kontrollen des EISA-Standards eine Zuordnung zum Standard ISO 27001, wie in Kapitel 3.1.8 herausgefunden. Für den ISO-Standard ist eine Zuordnungstabelle des CIS verfügbar. Er kann also als Bindeglied eingesetzt werden. Eine beispielhafte Zuordnung für zwei zufällige EISA-Kontrollen ist in Abbildung 5 dargestellt. Die Kontrolle EISA-ACC-201 ist von zwei ISO 27001 Anforderungen, nämlich die 9.2.1 und 9.4.2 abgeleitet (Wernke et al. 2022b, 22). In der vom CIS herausgegebenen Zuordnungstabelle lassen sich insgesamt vier Kontrollen finden, die zu diesen beiden Anforderungen passen, wie in Abbildung 5 zu sehen.

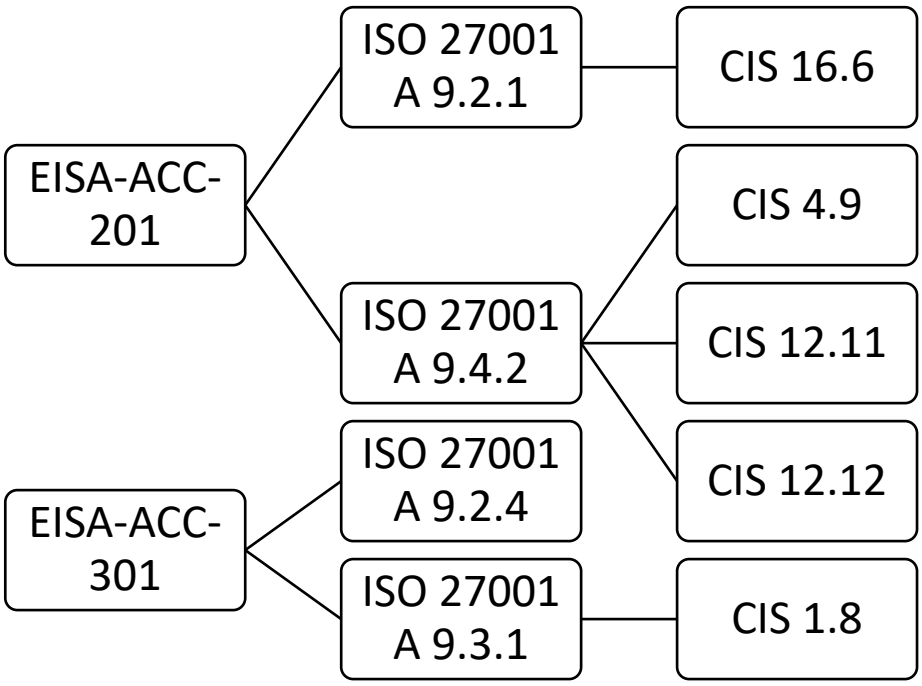


*Abbildung 5: Beispielhafte Zuordnung von EISA-Kontrollen zu CIS Metriken*

*Eigene Darstellung*

Ein besonders vielseitiges Bindeglied ist das Secure Controls Framework, kurz SCF. Das SCF ist ein umfassender Katalog von über 1000 Kontrollen (Secure Controls Framework Council, 2022), mit Zuordnungen zu über 100 Frameworks und Standards (Secure Controls Framework Council, 2022). Dieser Katalog könnte eingesetzt werden, um solche die Kontrollen und Anforderungen verschiedener Standards zu verbinden.

Unabhängig davon, ob die Metriken selbstständig gewählt oder über vorhandene Zuordnungen gefunden wurden, ist eine gewisse Kontrolle der Ergebnisse notwendig. Die verantwortlichen Experten sollten die gefundenen Metriken sowohl auf ihre Qualität und insbesondere beim Einsatz von vorhandenen Zuordnungen, auch auf ihre tatsächliche Eignung für die jeweilige Anforderung hin überprüfen.

Wie in Kapitel 3.4 erarbeitet, sollte für jede Metrik überprüft werden, wie die erforderlichen Daten erhoben werden können. Dafür sollten folgende Fragen beantwortet werden:

1. Ist es möglich, die Daten mit einem verhältnismäßigen Aufwand zu erheben?
2. Gibt es bereits existierende Datenquellen, die für diese Metrik eingesetzt werden können?
3. Ist es möglich, die Datenerhebung für diese Metrik zu automatisieren?

Die erste Frage soll bereits klären, ob sich die Metrik in der jeweiligen Organisation einsetzen lässt. Wird sie mit nein beantwortet, muss nach anderen Metriken für die jeweilige Anforderung gesucht werden. Wenn es möglich ist, die Daten für die Metrik zu erheben, bleibt noch zu klären, auf welche Weise die Daten erhoben werden sollen. Bei der zweiten Frage gilt es herauszufinden, ob die Daten bereits für einen anderen Zweck erhoben werden. In diesem Fall können sie für die Berechnung dieser Metrik übernommen werden, um Aufwand und Kosten zu sparen. Da eine automatisierte Messung zu einer höheren Genauigkeit und Konsistenz führen kann, sollte zuletzt noch überprüft, ob die Messung auch automatisch erfolgen kann. Stehen verschiedene Metriken zur Auswahl, könnte die Art der Messung als Argument für oder gegen eine bestimmte Metrik genommen werden.

Weiter müssen die gefundenen Metriken nach einigen qualitativen Aspekten bewertet werden, die ebenfalls in Kapitel 3.4 erarbeitet wurden. Dafür können wieder einige Fragen beantwortet werden:

1. Ist das Ergebnis rein objektiv?
2. Ist das Ergebnis quantifizierbar? Bzw. lässt sich das Ergebnis als Zahl oder Prozentsatz ausdrücken, die nicht eine ordinale Skala darstellen?

Die erste Frage soll subjektiven Faktoren vorbeugen, die einen Einfluss auf das Ergebnis der Metrik haben. Die Messungen dürfen also nicht die Meinungen von Mitarbeitern oder anderen Personen erfassen, sondern nur nachweisbare Fakten. Weiter könnten unklare Formulierungen raum für verschiedene Auslegungen einer Frage oder einer Messung lassen. Darauf soll im nächsten Kapitel genauer eingegangen werden. Die zweite Frage zielt darauf ab, qualitative Metriken auszuschließen. Wie in Kapitel 3.4 herausgefunden, können diese zwar auch einen Mehrwert liefern, quantitative Metriken sind aber dennoch vorzuziehen, da sie eine höhere Genauigkeit haben und somit eine bessere Ausgangslage für Interpretationen darstellen.

Zuletzt muss überprüft werden, inwiefern die jeweilige Metrik oder die gefundene Auswahl an Metriken, das Ziel der Messung erfüllen können. Dafür können Fragen aus den in Kapitel 3.4 betrachteten Fragen von Yee abgeleitet werden, indem sie für die Bewertung von Metriken für die Konformität mit Standards angepasst werden (Yee 2019):

1. Bedeutet eine konsistente Veränderung des Ergebnisses jeder einzelnen Metrik eine konsistente Veränderung des Grades der Erfüllung der jeweiligen Anforderung?
2. Gibt es Aspekte der jeweiligen Anforderung, die von den gewählten Metriken nicht abgedeckt werden?

Die erste Frage soll für jede einzelne Metrik, die für eine Anforderung gewählt wurde, herausfinden, ob sie zur Bestimmung der Erfüllung der Anforderung beiträgt. Wird diese Frage mit Nein beantwortet, sollte überprüft werden, ob die jeweilige Metrik notwendig ist und ob sie gegebenenfalls weggelassen werden kann. Die zweite Anforderung überprüft umgekehrt, ob die Summe der gewählten Metriken ausreicht, um die entsprechende Anforderung vollständig zu überwachen. Wird sie mit nein beantwortet, müssen eventuell weitere Metriken gesucht werden.

### 3.1.4 Metriken dokumentieren

Wie in Kapitel 3.6 herausgefunden, ist ein standardisiertes Format für Metriken von Vorteil. Daher sollen die betrachteten Vorlagen aus den Standards NIST SP 800-55 und ISO 27004, die ebenfalls in Kapitel 3.6 erklärt wurden, übernommen und für diese Arbeit angepasst werden (ISO 27004:2016, 8.3.3; NIST SP 800-55, 5.6):

| **Feldnamen** | **Inhalt** |
|---|---|
| **ID der Metrik** | Einzigartige Identifikation z.B. in Form einer Nummer oder nach einer bestimmten Nomenklatur |
| **Ziel** | Die Anforderung oder Kontrolle auf die die Metrik sich bezieht. |
| **Metrik** | Eine knappe Beschreibung der Metrik. Sie sollte einen Begriff wie Anteil, Prozentsatz oder Anzahl enthalten, der Aufschluss über die Messgröße gibt. |
| **Formel** | Die Formel nach der die Metrik berechnet wird. Sie enthält gemessene Werte, kann aber auch statische Zahlen enthalten. |
| **Zielwert** | Ein Grenzwert, ab dem die Anforderung als zu genüge erfüllt, bzw. die Kontrolle als zu genüge umgesetzt |

| | |
|---|---|
| | einzuschätzen ist. Wie in Kapitel 3.6 herausgefunden, soll das Ziel einer Metrik, die die Implementierung einer Kontrolle misst, immer bei 100 Prozent liegen. |
| **Messungen** | Anweisungen für eine oder Mehrere Messungen, zum Beispiel als Frage formuliert. Jede hier spezifizierte Messung liefert einen Wert für die Berechnung der Metrik. Die Messungen sollen so genau wie möglich spezifiziert und Unklarheiten ausgeräumt werden, wie in Kapitel 3.5 begründet. |
| **Frequenz** | Die Frequenz, zu der die Messungen stattfinden, und die Frequenz, in der die Daten analysiert, ausgewertet und den interessierten Parteien kommuniziert werden. Daten können z.B. monatlich, pro Quartal, Kalenderjahr oder Geschäftsjahr oder auch kontinuierlich erhoben, ausgewertet und kommuniziert werden. |
| **Verantwortliche und Interessierte Parteien** | Die Personen, Rollen oder Geschäftsbereiche, die eine Verantwortung in Bezug auf die Metrik oder ein Interesse am Ergebnisse haben. Für die Rollen können die in Kapitel 4.1.1 spezifizierten Rollen zum Einsatz kommen. |
| **Datenquelle** | Die Quelle aus der die zu messenden Informationen stammen. Das kann z.B. eine Datenbank, ein Programm oder eine Person sein. |
| **Berichterstattungsformat** | Die Art und Weise, auf die die Ergebnisse der Metrik kommuniziert werden sollen, wie z.B. als schriftlicher Bericht oder als Graph in einem Dashboard. |

*Tabelle 1: Vorlage für die Dokumentation von Metriken*

Für jede gefundene Metrik soll eine Tabelle ausgefüllt werden. Anpassungen der Struktur sind je nach der individuellen Situation möglich. Für das Ausfüllen der Tabelle ist eine gewisse Planung notwendig. Die einzelnen Schritte finden sich in den Feldern der Vorlage.

## 3.2 Phase 2 – Do

Nach abgeschlossener Planung müssen die Pläne nun umgesetzt werden. Dazu gehört die Implementierung von Messungen als Vorbereitung auf die Datenerhebung. Dabei sollten die in der Phase *Plan* identifizierten notwendigen Messungen als Anleitung verstanden werden. Mehr Daten als notwendig zu messen ist kostspielig und kontraproduktiv, da bei zu vielen Daten die wichtigen Aspekte der Masse an Information untergehen können (ISO 27004:2016, 6.1). Wie in Kapitel 3.5 herausgearbeitet und in Kapitel 4.1.3 festgehalten, muss bei der Planung von Metriken auch die Messung genau geplant werden, um eine ausreichende Genauigkeit zu gewährleisten und konsistente und damit auch vergleichbare Ergebnisse erhalten. Daher ist es bei der Implementierung der Messungen sehr wichtig, die zuvor spezifizierten Messungen so akkurat wie möglich umzusetzen. Weiter könnten in dieser Phase weitere Unklarheiten und Spielräume identifiziert werden. In diesem Fall sollen die festgehaltenen Anweisungen zur Messung angepasst und für weitere Iterationen dokumentiert werden.

Die Implementierung von Messungen kann verschiedene Formen annehmen. Teilweise müssen Systeme angepasst oder neue Programme angeschafft werden, wenn automatisch Daten gesammelt werden sollen. Bei einer Befragung eines Mitarbeiters oder Partners reicht es entsprechende Fragebögen zu formulieren. In jedem Fall muss nach der Implementierung die Datenerhebung losgetreten oder durchgeführt werden. Bei automatischen Datenquellen muss lediglich der Prozess der Datenerhebung gestartet werden. Bei manuellen Datenquellen müssen Messungen händisch durchgeführt, Fragebögen verschickt oder Interviews geführt werden.

## 3.3 Check – Daten auswerten und Ergebnisse kommunizieren

Nachdem in der zweiten Phase Daten erhoben wurden, müssen diese nun analysiert und ausgewertet werden. Die Berechnung der Metriken erfolgt dabei gemäß der zuvor als Teil der Metrik definierten Formel, wie in Kapitel 4.1.4 beschrieben. Die Berechnung kann dabei manuell oder automatisch, etwa als Teil eines ETL-Prozesses, stattfinden. Weiter müssen die berechneten Ergebnisse kommuniziert und eventuell Konsequenzen gezogen werden.

Die Kommunikation der Ergebnisse bedarf schon einiger Planung in der ersten Phase *Plan.* Diese wurde, wie in Kapitel 4.1.4 in als Teil der Metriken festgehalten. Zum einen sollten die

interessierten Parteien bestimmt werden, denen nun die Ergebnisse kommuniziert werden müssen. Dabei entspricht der Adressat der Ergebnisse in der Regel der Rolle des Messauftraggebers. Zum anderen kann schon bei der Planung der Metrik ein Berichterstattungsformat spezifiziert werden. Darauf aufbauend soll nun die tatsächliche Berichterstattung stattfinden.

Um die Berichterstattung an den Adressaten anzupassen, ist es wichtig, dass jeweilige Interesse des Adressaten zu verstehen. Wie in Kapitel 3.3 herausgefunden, richten sich Low-Level-Metriken eher an technisches Personal, während High-level-Metriken besser für die Berichterstattung an Managementpositionen geeignet sind. Je nach Adressaten und Zielsetzung sollten die einzelnen Metriken also unterschiedlich weit aggregiert werden, wie in Abbildung 5 beispielhaft dargestellt. Eine Aufschlüsselung nach Anforderungen ist denkbar, wenn es darum geht, gezielte Verbesserungen in der Informationssicherheit vorzunehmen. Eine Aufschlüsselung nach einer übergeordneten Kategorie, wie zum Beispiel einer Kategorie aus einem Standard oder aber einem bestimmten System, könnte zum Einsatz kommen, wenn es darum geht, dass Management zu informieren und Verhandlungen über Budgets einzuleiten. Wie weit die Ergebnisse aggregiert werden, hängt stark von der jeweiligen individuellen Situation und insbesondere von der Zielsetzung ab.

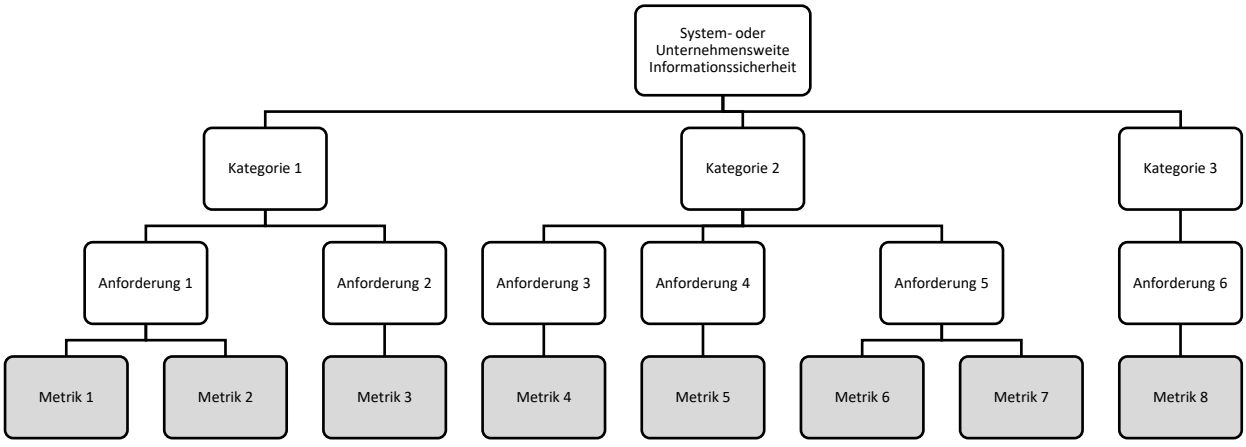


*Abbildung 6: Beispielhafte Darstellung eines Aggregationsschemas*

*Eigene Darstellung*

Neben der Aggregation der Ergebnisse kann aber auch die Art der Präsentation eine Herausforderung darstellen. Wie in Kapitel 3.7 erarbeitet, sind verschiedene Arten der Kommunikation möglich. Dashboards sind dabei eine besonders beliebte Methode.

Um die Ergebnisse als Teil eines Dashboards darzustellen, muss für jede Metrik oder jedes aggregierte Ergebnis eine Darstellungsweise gewählt und die Darstellung gestaltet werden.

Um den richtigen Diagrammtypen zu wählen, kann der in Abbildung 2 dargestellte Entscheidungsbaum genutzt werden. Er wurde von Costa und Aparicio entworfen (Costa & Aparicio, 2019) und liefert einen guten Ansatz für die Auswahl.

Für die Gestaltung eines Diagramms wurden in Kapitel 3.6 einige Regeln herausgearbeitet. Allgemein dient das Design eines Diagramms nur der Informationsvermittlung und gestalterische Elemente, die nicht die Vermittlung der Kernaussage unterstützen können, weggelassen oder entfernt werden.

Weiter soll ein Diagramm auch immer eine Botschaft vermitteln. Es ist also bei der Gestaltung darauf zu achten, dass die Information hinter den Daten durch das Diagramm ersichtlich wird.

Farben sollen entweder einer sinnvollen Skala folgen, also etwa rot bis grün, um schlechte und gute Daten darzustellen, oder aber Zugehörigkeiten darstellen. In beiden Fällen sollte darauf geachtet werden, die Gesamtanzahl der eingesetzten Farben auf etwa drei bis fünf Farben zu beschränken, da eine Unterscheidung zwischen mehr Farben auf den ersten Blick den meisten Menschen schwerfällt.

Zuletzt braucht ein Diagramm einen knappen, treffenden und ausdrucksstarken Titel. Dieser soll die einzelnen Dimensionen und ihre Beziehung darstellen. Weiter sollen die Achsen eine knapp beschriftet werden, wobei die jeweilige Dimension und die Einheiten der Daten genannt werden müssen.

## 3.4 Phase 4 – Act

Als letzter Schritt des Zyklus müssen die Ergebnisse eingesetzt werden, um eine Verbesserung der Konformität zu erreichen. Bei der Auswertung und Kommunikation wird erkenntlich, wo die offenen Schwachstellen liegen. Nun müssen Maßnahmen entwickelt werden, um den Problemen gezielt entgegenzuwirken und die Schwachstellen zu schließen. Dafür sollte bestenfalls ermittelt werden, was die verfehlten Ziele verursacht. Das könnte zum Beispiel ein

Mangel an Ressourcen oder unzureichendes Training sein. Den identifizierten Ursachen müssen dann mit Korrekturmaßnahmen entgegengewirkt werden. Beispiele für solche Maßnahmen könnten mehr Training für Mitarbeiter, mehr Budget an den richtigen Stellen oder etwa die Anschaffung neuer Programme und Werkzeuge sein (NIST SP 800-55, 6.3).

Die entwickelten Korrekturmaßnahmen sollten nachfolgend noch priorisiert werden. Dabei muss das Risiko, dass durch den jeweiligen Mangel verursacht wird, beurteilt werden. Außerdem müssen die Kosten und der Aufwand, die die Korrekturmaßnahmen mit sich bringen, verglichen werden. Schließlich sollen die Maßnahmen priorisiert werden, die den größten Nutzen zu akzeptablen Kosten erzeugen (NIST SP 800-55, 6.3).

# 4 Durchführung des Praxisbeispiels

Um das entwickelte Framework zu erproben, soll es im Rahmen einer kurzen Fallstudie bei der Robert Bosch GmbH eingesetzt werden. Dabei soll die Konformität der vorhandenen Microsoft Azure Subscriptions mit dem EISA-Standard zu messen. Eine Subscription entspricht einem Vertrag mit Microsoft über die Nutzung von Cloud-Ressourcen. Unter Azure-Subscriptions fallen entweder Infrastructure-as-a-Service, IaaS, oder Platform-as-a-Service, PaaS, Ressourcen (Microsoft, 2023).

## 4.1 Rollen:

Der Zyklus beginnt mit der Planungsphase. Hier sollen zuerst Rollen bestimmt werden, wie in Kapitel 4.1.1 festgehalten. Da das Praxisbeispiel nur von einer Person durchgeführt wird, sind einige Rollen doppelt besetzt:

- **Messauftraggeber**: Management und IT (Fiktiv)
- **Messungsplaner**: Der Autor
- **Prüfer der Messung**: Der Autor
- **Informationseigentümer**: Mitarbeiter aus dem Bereich Security Governance
- **Informationssammler**: Der Autor
- **Informationsanalytiker**: Der Autor
- **Informationsvermittler**: Der Autor

Die Rolle des Messauftraggebers wird doppelt besetzt, um bei der Kommunikation auf die verschiedenen Berichterstattungen für Marketingpositionen und Rollen in der IT bzw. Cybersicherheit durchführen zu können.

## 4.2 Anforderungen bestimmen

Weiter sieht das Framework vor, dass die relevanten Anforderungen bestimmt werden. Wie in Kapitel 4.1.2 beschrieben, kann es notwendig sein, die Anforderungen auszuwählen, die auf das Objekt der Messung Anwendung finden. Bei dieser Fallstudie ist das Objekt der Messung eine Reihe von Azure Subscriptions. Um dafür Relevanten Anforderungen zu ermitteln, können die im EISA-Standard enthaltenen Schemas genutzt werden. Diese Schemas enthalten jeweils eine Reihe von Kontrollen, die sich auf eine Art von System, Programm oder Infrastruktur anwenden lassen, wie in Kapitel 3.1.8 herausgearbeitet. Die Azure-Subscriptions

fallen dabei in das Schema *EISA-PIS-101 Cloud Platform* (EISA Pattern Catalog 2022.07, 3). Es enthält insgesamt 17 verschiedene Kontrollen aus verschiedenen Kategorien des Standards, die allesamt bei Azure-Subscriptions Anwendung finden können.

Da diese Fallstudie sich auf einige beispielhafte Metriken beschränken soll und da die Möglichkeiten der Datenerhebung stark beschränkt sind, können nicht alle Kontrollen betrachtet werden. Der weitere Verlauf der Fallstudie beschränkt sich daher auf die Kontrollen *EISA-OPS-201* und *EISA-INC-101*.

Die Kontrolle EISA-OPS-201 soll einen Schutz gegen Malware sicherstellen. Dafür enthält sie die folgenden neun Implementierungs-Anforderungen (EISA Control Catalog 2022.07, 12.2):

- 201.1: Einsatz von Malware-Schutz
    - Es muss ein Malware-Schutz eingesetzt werden, falls einer verfügbar ist und das System mit Malware infiziert werden kann.
- 201.2: Genehmigter Malware-Schutz
    - Der Malware-Schutz muss vom Bosch Central Malware Protection Team genehmigt sein.
- 201.3: Zentrales Management
    - Der Malware-Schutz muss zentral gemanagt sein
- 201.4: Zentrales loggen von Sicherheitsvorfällen
    - Sicherheitsvorfälle müssen an eine zentrale Stelle geloggt werden
- 201.5: Automatische Updates
    - Der Malware-Schutz muss automatisch aktualisiert werden
- 201.6: Scan Methoden
    - Es müssen regelmäßig (mindestens monatlich) Scans durchgeführt werden
    - Außerdem muss Echtzeitüberwachung eingesetzt werden
- 201.7: Scan-Ausnahmen
    - Scan-Ausnahmen dürfen nicht gleichzeitig für Echtzeitscans und regelmäßige Scans gelten
    - Scan-Ausnahmen dürfen nicht ganze Festplatten betreffen
- 201.8: Umgang mit Malware-Vorfällen
    - Entdeckte Malware muss geblockt oder in Quarantäne verschoben werden
- 201.9: Sicherheitsfunktionen für übertragene E-Mails

- Regeln für den Umgang mit gefährlichen Anhängen sollen aufgestellt und regelmäßig aktualisiert werden

Die Anforderung 201.9, die sich auf den Umgang mit E-Mails bezieht, ist für Azure-Subscriptions nicht relevant, da sie sich auf persönlich genutzte Systeme bezieht, von denen aus Mails empfangen werden. Die Anforderung 201.7 ist deshalb nicht relevant, weil Scan-Ausnahmen für im Rahmen von Azure-Subscriptions Bosch-intern allgemein verboten sind. Somit bleiben sieben Anforderungen, deren Einhaltung gemessen werden soll.

Die Kontrolle EISA-INC-101 bezieht sich auf die Vorbereitung von Sicherheitsvorfällen. Dafür enthält sie vier Implementierungs-Anforderungen, von denen im Rahmen dieser Fallstudie allerdings nur eine überprüft werden kann. Daher soll bei dieser Kontrolle nur die eine Anforderung betrachtet werden. Somit wird anhand von EISA-OPS-201 gezeigt, wie mit dem entwickelten Framework eine Kontrolle auf ihre Umsetzung überprüft werden kann und EISA-INC-101 wird danach herangezogen, um zu zeigen, wie Metriken aggregiert werden können, um auch über eine Kontrolle hinaus die Konformität des betrachteten Systems aufzuzeigen. Die Anforderung, die betrachtet werden soll, hat die Nummer 101.3, die verlangt, dass ein Verantwortlicher als Kontakt für Sicherheitsvorfälle dokumentiert werden muss.

## 4.3 Metriken finden

Nachdem nun die relevanten Anforderungen bestimmt wurden, müssen Metriken gefunden werden, die nachweisen, dass die Anforderungen erfüllt werden. Kapitel 4.1.3 enthält dafür einige Regeln und Ansätze. Zuerst sollte überprüft werden, ob bereits Metriken existieren, die den gewählten Anforderungen oder Kontrollen bereits direkt oder indirekt zugeordnet wurden. Da der EISA-Standard sich stark am ISO-Standard 27001 orientiert, wie in Kapitel 3.1.8 herausgefunden, könnten die in ISO 27004 enthaltenen Metriken auch beim EISA Standard Anwendung finden. Die zugehörigen Anforderungen des ISO Standards sind bei jeder EISA Kontrolle ausgeschrieben (EISA Control Catalog 2022.07, 12.2 & 16.1). Im ISO 27004 Standard lassen sich dann die zugehörigen Metriken ermitteln (ISO 27004:2016, Annex B) Daraus ergibt sich, dass zur Kontrolle EISA-OPS-201 die ISO Metriken B.23-26, und zur Kontrolle EISA-INC-101 die Metriken B.32/33 passen könnten. Um diese Auswahl zu überprüfen, müssen die Metriken einzeln betrachtet und ihre Eignung beurteilt werden.

- B.23 misst den das Verhältnis von geblockten zu nicht geblockten Cyberattacken, um die Performance der Malware-Schutzes zu beurteilen
- B.24 misst den Anteil der mit Malware infizierten Systeme, deren Malware-Schutz nicht aktuell ist
- B.25 vergleicht die Ausfallzeit mit der maximal erlaubten Ausfallzeit
- B.26 misst die Anzahl der nicht genutzten Firewall regeln

Die ausgewählten Metriken eigenen sich kaum, um Konformität mit der EISA-Kontrolle zu messen. B.23 hat misst die Leistung des Malware-Schutzes, die aber kein Teil der Kontrolle ist. B.24 behandelt Aktualisierungen des Malware-Schutzes, genau wie die Anforderung 201.5 der Kontrolle. Allerdings verlangt die Anforderung spezifisch nach automatischen Updates. Weiter wird bezieht sich die Anforderung nicht speziell auf infizierte Systeme. Die Metriken B.25 und B.26 behandeln beide Themen, die in der Kontrolle nicht vorkommen. Dasselbe gilt für die Metriken B.32 und B.33, die für die Kontrolle EISA-INC-101 ausgewählt wurden.

- B.32 misst den Anteil der relevanten Sicherheitsanforderungen, die in Vereinbarungen mit Dritten behandelt werden.
- B.33 misst die Anzahl an Sicherheitsvorfällen, die nicht im Ziel-Zeitraum behandelt wurden.

Beide Metriken behandeln Themen, die in der gewählten Anforderung EISA-INC-101.3 nicht vorkommen. Es muss also nach anderen Quellen für Metriken gesucht werden. Dafür kann der Kontrollen-Katalog des CIS herangezogen werden, der bereits in Kapitel 4.1.3 erwähnt wurde. CIS stellt Zuordnungstabellen für den Katalog und verschiedene Standards bereit. Damit ist es möglich die EISA-Kontrollen über den ISO 27001 Standard den Kontrollen und Metriken des CIS-Katalogs zuzuordnen.

Der Kontrolle EISA-OPS-201 lassen sich so die CIS-Kontrollen 7.7, 7.10, 8.1, 8.2 und 8.4-6 zuordnen. Der Kontrolle EISA-INC-101 wiederum lässt sich nur die CIS-Kontrolle 19.1 zuordnen. Die CIS-Kontrollen 7.7 und 7.10 betreffen die Themen DNS und E-Mail, die in den gewählten EISA-Anforderungen nicht vorkommen. Dasselbe gilt für die Kontrollen 8.4 und 8.5, die sich beide auf Wechseldatenträger beziehen. Die CIS-Kontrolle 8.1 verlangt die Implementierung eines zentral gemanagten Malware-Schutzes und zeigt somit Übereinstimmung mit den Anforderungen 201.1 und 201.3 der Kontrolle EISA-OPS-201. Die

dazugehörige Metrik misst den Anteil der Server und Systeme, die keinen zentral gemanagten Malware-Schutz haben. Die CIS-Kontrolle 8.2 verlangt, dass der eingesetzte Malware-Schutz stets aktuell ist. Die zugehörige Metrik misst den Anteil der Systeme, die keinen kürzlich aktualisierten und zentral gemanagten Malware-Schutz haben. Hier ist eine Überschneidung zur Anforderung EISA-OPS-201.5, allerdings werden nicht automatische Aktualisierungen, sondern kürzlich erfolgte Aktualisierungen gemessen. Die Metrik könnte dennoch in angepasster Form eingesetzt werden. Bei der CIS-Kontrolle 8.6 geht es um zentrales Logging von Sicherheitsvorfällen. Es ist also ein starker Zusammenhang zur Kontrolle EISA-OPS-201.4. Allerdings ist die Metrik, die CIS für diese Kontrolle angedacht hat, dieselbe wir für die Kontrolle 8.1. Sie hat also keinen Bezug auf das zentrale Logging und ist somit auch nicht für die Anforderung 201.4 geeignet. Zuletzt gilt es die Kontrolle 19.1 zu betrachten. Sie gibt vor, dass Pläne zur Reaktion auf Sicherheitsvorfälle existieren, in denen Rollen verteilt und Phasen für den Umgang mit Sicherheitsvorfällen beschrieben werden. Die Metrik misst mit einem Ja/Nein – Frage, ob die Organisation sichergestellt hat, dass eben solche Pläne existieren. Es ist eine gewisse Überschneidung mit der Anforderung EISA-INC-101.3 vorhanden, allerdings enthält die CIS-Metrik auch einige Aspekte, die in der EISA-Kontrolle nicht vorkommen. Die Metrik ist also nur bedingt brauchbar.

Es wurden also lediglich zwei Metriken gefunden, die für die Messung der Umsetzung mit den gewählten Kontrollen eingesetzt werden können:

- CIS 8.1 für EISA-OPS-201.1/3
- CIS 8.2 (mit Änderungen) für EISA-OPS-201.5

Um die restlichen Anforderungen auch überprüfen zu können, müssen also eigene Metriken entworfen werden. Dafür sollen aus den Anforderungen Fragen abgeleitet werden, die vom Informationseigentümer beantwortet werden. In Kapitel 3.4 wurde zwar herausgefunden, dass quantitative Metriken qualitativen Metriken vorgezogen werden sollen, es ist aber im Rahmen dieser Fallstudie keine aufwändigere Messung möglich. Aus der Anforderung 201.2 ließe sich so etwa folgende Frage ableiten:

*Ist der Malware-Schutz durch das Bosch Central Malware Protection Team genehmigt?*

Dieselbe Vorgehensweise wird auf alle Anforderungen der Kontrolle EISA-OPS-201 angewandt, hier aufgrund der Redundanz der Aufgabe aber nicht weiter erklärt. Die Metriken finden sich gesammelt im Anhang A.

Für die gewählte Anforderung der Kontrolle EISA-INC-101 sind bereits Messdaten vorhanden, weshalb hier auch eine quantitative Metrik möglich ist. Die Metrik misst daher den Prozentsatz der Azure-Subscriptions, für die keine Kontaktinformationen vorhanden sind.

## 4.4 Metriken dokumentieren

Nachdem nun Metriken für alle Anforderungen bestimmt wurden, müssen sie einheitlich dokumentiert werden. In Kapitel 4.1.4 wird dafür ein Format vorgeschlagen, in das die ermittelten Metriken eingetragen werden. Im Folgenden soll für jedes Feld das Vorgehen bei den gewählten Metriken erklärt werden. Die Erklärung ist wegen der hohen Redundanz der Aufgabe aber allgemein gehalten. Die einzelnen Metriken sind im Anhang A in vollem Umfang dokumentiert.

Als **ID** wird für die Metriken aus dem CIS-Katalog die Nummer der Kontrolle genutzt, aus der sie stammen. Die selbst definierten Metriken werden durchnummeriert.

Im Feld **Ziel** werden die Kontrollen und Anforderungen eingetragen, auf die sich die Metrik bezieht.

Die **Formel** bei den aus dem CIS-Katalog entnommenen Metriken und der Metrik, die für die Kontrolle EISA-INC.101 formuliert wurde, berechnet jeweils den Anteil als Prozentzahl aus der Gesamtanzahl und der Zahl der Subscriptions, die die Anforderung erfüllen. Bei den Metriken, die zusätzlich zu den quantitativen Metriken auch Metriken in Form einer Frage enthalten, wird das Ergebnis als Eins oder Null formatiert und mit dem Anteil multipliziert. Die Eins steht für die Antwort ja, die Null für die Antwort nein. Dadurch gelten die berechneten Anteile nur, wenn die ganze Anforderung erfüllt ist. Bei den Metriken, die nur eine Frage als Messung enthalten, wird das als Eins oder Null codierte Ergebnis mit 100 multipliziert, um eine Prozentzahl zu erhalten.

In Kapitel 3.6 wurde erarbeitet, dass bei Metriken, die eine Implementierung messen, der **Zielwert** immer 100 Prozent ist. Das trifft auf sämtliche definierte Metriken zu.

Die qualitativen Metriken, aber auch die aus CIS-entnommenen Metriken enthalten jeweils eine als Frage formulierte Messung. Hier muss also die Frage in das Feld **Messungen** eingetragen werden. Wie in Kapitel 3.5 festgestellt, ist es wichtig hierbei Unklarheiten zu vermeiden, um ein objektives Ergebnis zu erhalten. Weiter werden in diesem Feld Antwortmöglichkeiten und eine Codierung der Antworten angegeben. Bei den **Messungen**, die sich auf die vorhandenen Messdaten stützen, muss spezifiziert werden, was jeweils gemessen wird. Ein Beispiel kann anhand der Metrik CIS 8.1 gemacht werden. Sie misst den Prozentsatz der Subscriptions, die einen zentral gemanagten Malware-Schutz einsetzten. Es wird nur eine Malware-Schutz Lösung eingesetzt. Es muss also nur gemessen, wie viele Subscription den Malware-Schutz einsetzen, wie viele Subscriptions insgesamt vorhanden sind und ob der Malware-Schutz zentral gemanagt ist. Die ersten beiden **Messungen** stützen sich auf die vorhandenen Messdaten. Sie können wie folgt festgehalten werden:

1. Anzahl vorhandener Azure-Subscriptions
2. Anzahl Azure-Subscriptions, die den verfügbaren Malware-Schutz einsetzten.

Die **Frequenz** muss für jede einzelne Messung und die Berichterstattung angegeben werden. Die Frequenz der quantitativen Messungen ist monatlich, da die vorhandenen Messdaten diese Frequenz aufweisen. Die **Frequenz**, in die der die Fragen beantwortet werden sollen, ist einmalig. Es wäre unter normalen Umständen sinnvoll, die Befragung regelmäßig durchzuführen, um Veränderungen aufzuzeigen. Aufgrund der Limitationen dieser Fallstudie soll die Befragung für nur einen Zeitpunkt durchgeführt werden. Dabei herrscht die Annahme, dass sich die Eigenschaften der Malware-Schutz-Lösung nicht verändern. Die Berichterstattung erfolgt für alle Metriken kontinuierlich, da Power-Bi eingesetzt werden soll.

Im Feld **Verantwortliche und Interessierte Parteien** werden die in Kapitel 5.1 festgelegten Rollen notiert. Sie gelten für alle Metriken.

Bei den qualitativen Metriken gibt es nur eine **Datenquelle**, nämlich den Informationseigentümer, der befragt werden soll. Die quantitativen Metriken nutzen außerdem zweite **Datenquelle**, nämlich die vorhandenen Messdaten, die als Excel-Datei vorliegen.

Für das **Berichterstattungsformat** soll ein Diagrammtyp unter Zuhilfenahme des Entscheidungsbaums in Abbildung 2 ausgewählt werden.

## 4.5 Messungen implementieren

In der zweiten Phase des Zyklus, der Do-Phase, sollen Messungen implementiert und Daten erhoben werden. Dafür müssen die dokumentierten Messungen durchgeführt werden. Insgesamt wurden zwei Arten von Messungen geplant. Zum einen gibt es quantitative Messdaten, die allerdings bereits vorhanden sind und nur noch ausgewertet werden müssen. Zum anderen soll eine Befragung durchgeführt werden. Die Fragen sind bereits als Messungen in den Metriken ausformuliert. Insgesamt wurden sieben Fragen formuliert:

1. Wird der für Azure eingesetzte Malware-Schutz zentral gemanagt?
2. Ist der für Azure eingesetzte Malware-Schutz vom Bosch Central Malware Protection Team genehmigt?
3. Wird der für Azure eingesetzte Malware-Schutz automatisch aktualisiert?
4. Loggt der für Azure eingesetzte Malware-Schutz Sicherheitsvorfälle an eine zentrale Stelle?
5. Führt der für Azure eingesetzte Malware-Schutz regelmäßig (mindestens monatlich) Scans durch?
6. Bietet der für Azure eingesetzte Malware-Schutz Echtzeitüberwachung?
7. Wird die vom für Azure eingesetzte Malware-Schutz detektierte Malware entweder geblockt oder in Quarantäne verschoben?

Die Fragen wurden per E-Mail an den Informationseigentümer übermittelt. Frage 4 wurde mit *Nein* beantwortet. Der Rest der Fragen wurde mit *Ja* beantwortet.

## 4.6 Ergebnisse auswerten und kommunizieren

Die Kommunikation der Ergebnisse wird als Power BI-Dashboard umgesetzt. Die Datenauswertung kann ebenfalls in Power BI umgesetzt werden. Dadurch kann das Dashboard jederzeit mit neuen Daten aktualisiert werden, ohne dass eine händische Berechnung der Metriken notwendig ist. Als Messauftraggeber wurden in Kapitel 5.1 zwei fiktive Personen bzw. Rollen festgehalten. Die Ergebnisse sollen also einmal für IT-Mitarbeiter und einmal für das Management kommuniziert werden.

Für die Berichterstattung an die Rollen im IT soll genau gezeigt werden, an welcher Stelle Verbesserungspotenzial besteht. Dafür werden die Metriken auf die Ebene der einzelnen Implementierungsanforderungen aggregiert. Da für EISA-INC-101 nur eine Anforderung

gemessen werden konnte, wird die Berichterstattung hier nur für EISA-OPS-201 durchgeführt. Von den sieben ausgewählten Anforderungen sind fünf mit jeweils einer Metrik belegt. Allerdings werden die Anforderungen 201.1 und 201.3 beide mit der Metrik CIS 8.1 überprüft. Es müssen also beide Anforderungen zusammen visualisiert werden. Bei dieser Metrik kann der zeitliche Verlauf der Daten dargestellt werden, da hier die vorhandenen Messdaten zum Einsatz kommen. Um den richtigen Diagrammtyp zu wählen, kann Abbildung 2 herangezogen werden. Es soll ein Vergleich der verschiedenen Stände über Zeit hinweg gezeigt werden. Es handelt sich hier um viele Zeitpunkte und nicht zyklische Daten. Der vorgeschlagene Diagrammtyp ist daher ein Liniendiagramm. Die für die Anforderung 201.5 gefundene Metrik wird aus der Antwort einer Frage und den vorhandenen Daten berechnet. Da hier dieselben Daten quantitativen Daten wie bei der ersten CIS-Metrik genutzt wurden, würde die Darstellung dieser Daten keine neuen Erkenntnisse bringen. Daher beschränkt die Visualisierung sich auf die Ergebnisse der Befragung. Für diese und die übrigen vier Anforderungen wird die Tachometer Darstellung in Power BI gewählt.

Um einen Gesamtüberblick über die Konformität der Azure-Subscriptions mit der Kontrolle zu erhalten, müssen die einzelnen Anforderungen aggregiert werden. Dafür werden zuerst alle qualitativen Ergebnisse zusammengerechnet. Es ergibt sich ein Prozentsatz, der darstellt, wie groß der Anteil der eingehaltenen Anforderungen ist. Diese Prozentzahl wird nun mit dem quantitativen Ergebnis der CIS-Metrik 8.1 multipliziert. Auf diese Weise ergibt sich eine Zahl, die den Anteil der Subscriptions mit Malware-Schutz und die Konformität des Malware-Schutzes mit den Anforderungen der Kontrolle widerspiegelt. Sie kann nur dann 100 Prozent erreichen, wenn sämtliche Subscriptions einen Malware-Schutz einsetzen und alle zusätzlichen Anforderungen erfüllt sind. Das Dashboard für die Berichterstattung an IT-Mitarbeiter ist in Abbildung 5 dargestellt.

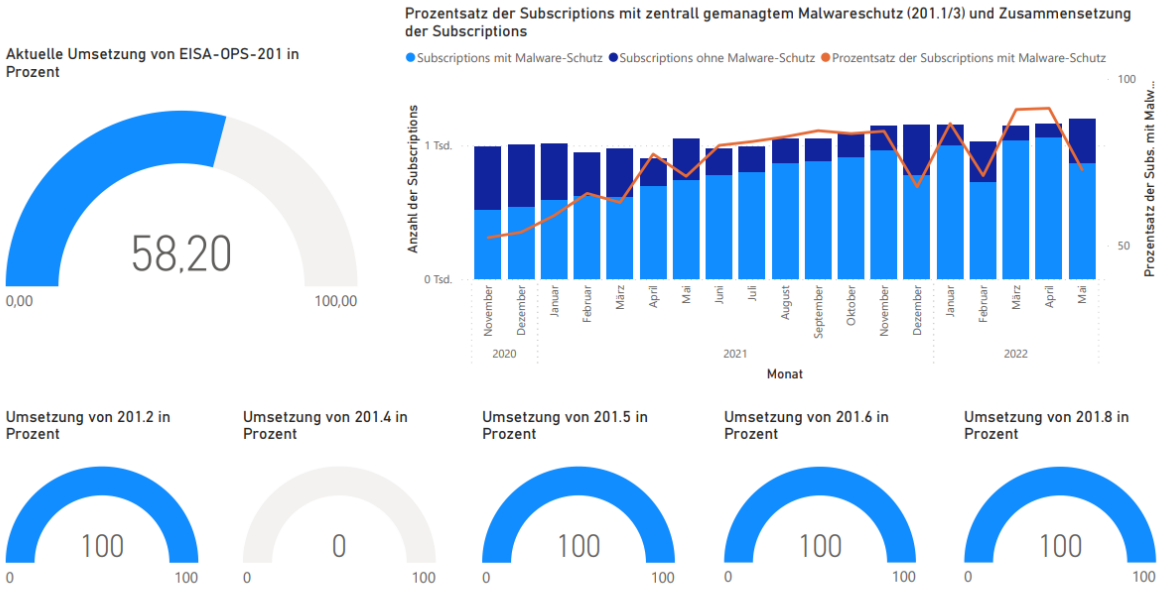


*Abbildung 7: Power BI Dashboard für die Berichterstattung an IT-Mitarbeiter*

*Eigene Darstellung*

Für das Management sind stärker aggregierte Ansichten zu empfehlen wie in Kapitel 4.3.1 festgehalten. Es wird daher die gesamte Konformität der Azure-Subscriptions mit den gewählten Kontrollen dargestellt. Diese ergibt sich aus dem Durchschnitt beider Kontrollen. Das Ergebnis der Aggregation, sowie die Gesamtergebnisse der beiden Kontrollen, können auf verschiedene Arten dargestellt werden. Für alle drei werden die aktuellen Ergebnisse als Tachometer dargestellt. Der zeitliche Verlauf soll als Liniendiagramm abgebildet werden. Die drei Linien können in einem Diagramm dargestellt werden, wodurch die Zahlen besser vergleichbar sind. Das Dashboard ist in Abbildung 6 dargestellt

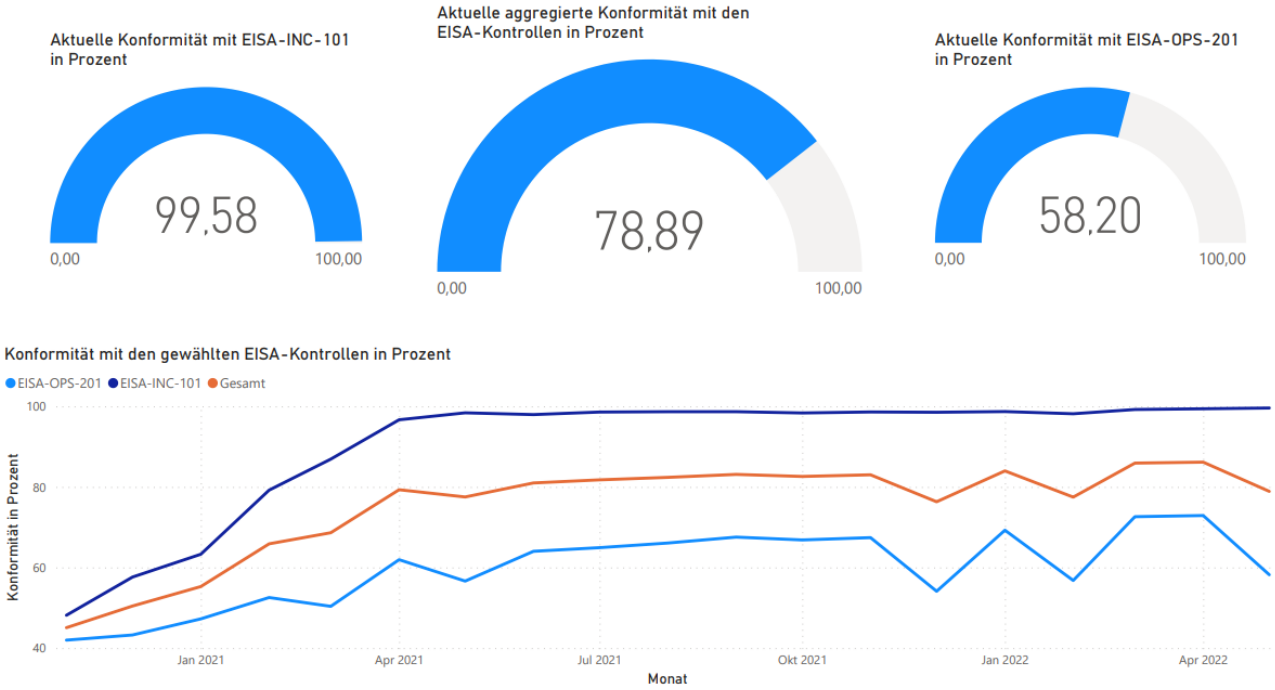


*Abbildung 8: Power BI Dashboard für die Berichterstattung an Management Positionen*
*Eigene Darstellung*

## 4.7 Korrekturmaßnahmen festlegen

Als letzter Schritt des Zyklus müssen in der Phase *Act* Korrekturmaßnahmen beschlossen werden. Wie in Kapitel 4.4 festgehalten, beginnt dieser Prozess damit, die Schwachstellen des betrachteten Systems zu untersuchen.

Die geringe Abweichung der Kontrolle EISA-INC-101 ist auf einige Subscriptions ohne hinterlegten Sicherheitskontakt zurückzuführen. Die insgesamt 41.8 Prozent Abweichung bei der Kontrolle EISA-OPS-201 sind größtenteils darauf zurückzuführen, dass für etwa 27% der Azure-Subscriptions im Mai 2022 kein Malware-Schutz aktiviert war. Interessant ist auch, dass der Anteil der Subscriptions mit Malware-Schutz im Mai im Vergleich zum April um fast 18,4 Prozent zurückgegangen ist. Das lässt sich auch an der abfallenden Kurve am rechten Ende des Liniendiagramms in Abbildung 5 erkennen. Das Balkendiagramm zeigt, dass die absolute Anzahl Subscriptions mit aktiviertem Malware-Schutz sinkt, während die gesamte Anzahl leicht steigt. Es hat den Anschein, als wäre der Malware-Schutz für einige Subscriptions deaktiviert worden. Zuletzt wird noch die Anforderung EISA-OPS-201.4 nicht erfüllt, weil kein zentrales Logging von Sicherheitsvorfällen stattfindet.

Für die identifizierten Schwachstellen müssen nun Korrekturmaßnahmen entwickelt werden. Um 100 Prozent Übereinstimmung mit der Kontrolle EISA-INC-101 zu erreichen, müssten Sicherheitskontakte für die letzten Azure-Subscriptions dokumentiert werden. Für die EISA-OPS-201 Metrik müsste der Malware-Schutz auf den verbleibenden Subscriptions aktiviert werden. Hier sollte zuerst festgestellt werden, warum dies bisher nicht geschehen ist. Sollten die Kosten der Grund sein, müssen entsprechende Mittel bereitgestellt werden. Falls der Malware-Schutz für diese Systeme als nicht notwendig sein herausstellt, kann darüber nachgedacht werden, eine Ausnahme in der Kontrolle hinzuzufügen. Zuletzt sollte versucht werden, ein zentrales Logging von Sicherheitsvorfällen zu erreichen. Da es sich um eine externe Malware-Schutz-Lösung handelt, könnte es unter Umständen nicht oder nur schwer möglich sein, diese Funktion hinzuzufügen. Es sollte geprüft werden, ob die Option besteht. Unter Umständen muss Kontakt zum Entwickler des Malware-Schutzes aufgenommen werden.

Schließlich sollen die entwickelten Korrekturmaßnahmen priorisiert werden. Die wichtigste Maßnahme ist die Aktivierung des Malware-Schutzes auf allen Subscriptions. Ausschlaggebend dafür ist die Schwere der Verfehlung und das damit verbundene hohe Risiko. Außerdem ist der Aufwand überschaubar, da bereits für die meisten Subscriptions der Malware-Schutz aktiviert ist und somit keine neuen Prozesse erstellt werden müssen. An zweiter Stelle sollte geprüft werden, wie und ob zentrales Logging von Sicherheitsvorfällen umzusetzen ist. Falls der Aufwand akzeptabel ist, soll das schließlich umgesetzt werden. Zuletzt müssen Sicherheitskontakte für die verbleibenden Subscriptions angelegt werden. Das Risiko ist hier überschaubar, da der Anteil von Subscriptions ohne Sicherheitskontakt bereits sehr gering ist. Es könnte aber schon früher geprüft werden, ob unter den Subscriptions solche sind, die für kritische oder anderweitig wichtige Aufgaben eingesetzt werden. In diesem Fall könnte sich das Risiko erhöhen.

Die Korrekturmaßnahmen sollten jetzt nach ihrer Priorisierung abgearbeitet werden. Währenddessen und danach können neue Planungen angestellt und weitere Daten erhoben werden, um die nächste Iteration des Zyklus vorzubereiten.

# 5 Ergebnisse der Fallstudie

Das Praxisbeispiel hat anschaulich dargestellt, wie das zuvor entwickelte Framework in einem Unternehmen wie der Robert Bosch GmbH eingesetzt werden kann. Daraus können verschiedene Erkenntnisse abgeleitet werden.

Insgesamt wurden in der Fallstudie gute Ergebnisse erzielt. Obwohl die Möglichkeiten zur Datenerhebung sehr beschränkt waren, konnte der Prozess für eine gesamte Kontrolle und zumindest einen Teil einer weiteren Kontrolle durchgeführt werden. Im Rahmen des Prozesses wurden zuerst die relevanten Kontrollen und Anforderungen ausgewählt. Das stellte ein gutes Beispiel diesen Teil des Prozesses dar. Bei der Selektion der Anforderungen der Kontrolle EISA-OPS-201 wurde gezeigt, wie die Beschränkung auf Teile einer Kontrolle oder Anforderung im Einzelfall aussehen kann. Gerade dafür war die Fallstudie gut geeignet, da es ein Prozess ist der stark von dem gewählten Standard und System abhängt.

Die Metriken wurden einheitlich dokumentiert, wobei auf die Besonderheiten der einzelnen Attribute der Metriken eingegangen werden konnte. Dadurch wurde die in Kapitel 4.1.4 entwickelte Vorlage eingesetzt, was ihren praktischen Nutzen untermauert hat. Bei der Datenerhebung konnte trotz der bestehenden Limitationen eine Messung in Form einer Befragung durchgeführt werden. Die in Kapitel 3.5 erarbeiteten Regeln für Messungen konnten eingesetzt werden, um eindeutige Fragen zu formulieren und Unklarheiten zu vermeiden.

Bei der Datenauswertung wurden Schwachstellen und Probleme aufgedeckt, was den Mehrwert des Prozesses für reale Organisationen aufzeigt. Die Visualisierung in Power BI hat anschaulich dargestellt, wie ansprechende und Informative Dashboards für die Kommunikation der Ergebnisse erstellt werden können. Dafür konnten die in Kapitel 4.3.1 festgehaltenen Regeln und Hinweise für die Erstellungen von Diagrammen und Dashboards eingesetzt werden. Die Visualisierung hat auch den Mehrwert von verschiedenen Aggregationen und Darstellungen für verschiedene Rollen und Positionen deutlich gemacht.

Zuletzt wurden für die identifizierten Schwachstellen Korrekturmaßnahmen vorgeschlagen. Dabei konnte der damit verbundene Prozess dargestellt werden. Schließich wurden die Maßnahmen priorisiert und das weitere Vorgehen angesprochen.

Im Verlauf der Fallstudie gab es neben den positiven Ergebnissen aber auch ein paar Probleme. Sie lassen sich teilweise auf die Limitationen der Fallstudie, aber teilweise auch auf das entwickelte Framework selbst zurückführen. Bei der Verteilung der Rollen hätten idealerweise mehr verschiedene Rollen verteilt werden müssen, um die Bedeutung der einzelnen Rollen hervorzuheben. Das war aufgrund der Limitationen der Fallstudie allerdings nicht möglich.

Bei der Bestimmung der Anforderungen musste sich auf die Anforderungen beschränkt werden, die mit den vorhandenen Daten belegt werden können. Das hat zwar auch aufgezeigt, wie mit Limitationen in realen Unternehmen umgegangen werden könnte, mehr Kontrollen und Anforderungen hätten in den anderen Schritten aber ein kompletteres und anschaulicheres Bild des Frameworks aufzeigen können.

Bei der Entwicklung von Korrekturmaßnahmen sollten unter normalen Umständen Untersuchungen bezüglich der Ursache der Probleme und der Risiken und Kosten der verschiedenen Maßnahmen angestellt werden. Diese konnten im Rahmen dieser Fallstudie nur sehr eingeschränkt durchgeführt werden. In einem ausführlicheren Anwendungsbeispiel mit mehr Möglichkeiten könnte hier der Prozess besser dargestellt werden.

Die größten Probleme gab es aber bei der Selektion von Metriken. Hier hat der im Framework vorgeschlagenen Ansatz nicht die gewünschten Ergebnisse hervorgebracht. Es konnten zwar zwei Metriken gefunden werden, eine davon musste für den Einsatz in der Fallstudie aber leicht angepasst werden. Ein Großteil der Anforderungen konnte nicht mit bereits bekannten Metriken überprüft werden. Stattdessen mussten eigene Metriken definiert werden. Dafür könnte es verschiedene Erklärungen geben. Es ist denkbar, dass ein anderer Ansatz für die Zuordnung von Metriken und Anforderungen bessere Ergebnisse erzielt hätte. Dazu muss aber gesagt werden, dass der der Ansatz, existierende Zuordnungen zu nutzen, größtenteils zu Metriken geführt hat, die einen sehr ähnlichen Themenbereich abdecken. Allerdings scheint es, als wären Metriken aus anderen Standards, die für andere Kontrollen entworfen wurden, oft zu verschieden, um für die Kontrollen des EISA-Standards eingesetzt zu werden. Das wirft die Frage auf, ob der Ansatz, bereits existierende Metriken zu nutzen, anstatt von vornherein eigenen Metriken zu entwerfen, sinnvoll ist. Diese Frage kann in dieser Arbeit aufgrund von zeitlichen Limitationen und aufgrund der Zielsetzung leider nicht weiter untersucht werden.

Auch dort wo die Metriken aus dem CIS-Katalog eingesetzt werden konnten, ist es fragwürdig, ob sie tatsächlich einen Vorteil gegenüber selbst entworfenen Metriken haben. So hat die CIS-Metrik 8.1 sich etwa auf zwei Kontrollen gleichzeitig bezogen. Dadurch konnte der Informationsbedarf zwar gedeckt werden, die Visualisierung konnte aber nicht für jede Anforderung einzeln durchgeführt werden. Dadurch könnten wichtige Informationen potenziell nicht ersichtlich werden, auch wenn die Auswirkungen in der Fallstudie nicht bedeutend waren.

# 6 Fazit und Ausblick

## 6.1 Ergebnisse

In dieser Arbeit wurde ein Framework entwickelt, mit dem es möglich ist, ein Informationssystem, eine Gruppe von Informationssystemen oder eine ganze Organisation auf ihre Konformität mit einem Standard hin zu überprüfen und zu verbessern. Dabei werden bereits existierende Metriken eingesetzt, falls möglich. Dafür wird ein zyklisches Vorgehen auf der Grundlage des PDCA-Zyklus vorgeschlagen. Zuerst soll sowohl die individuelle Situation, was Natur der jeweiligen Systeme miteinschließt, als auch der gewählte Standard analysiert werden. Dadurch können die Teile des Standards gewählt werden, die für die betrachteten Systeme relevant sind.

Weiter sollen Metriken gefunden werden, um die Erfüllung der Anforderungen zu messen. Dieser Teil der Arbeit, in Kapitel 4.1.3, beantwortet die erste Teilfrage der Forschungsfrage. Die Metriken, die zur Messung genutzt werden sollen, können aus verschiedenen Standards, Katalogen oder anderen Ansammlungen stammen. Die manuelle Zuordnung der Metriken zu den Anforderungen ist aufwendig und höchst subjektiv. Der in dieser Arbeit vorgeschlagene Ansatz sieht daher vor, dass vorhandene Zuordnungen von Metriken und Anforderungen genutzt werden. Solche Zuordnungen sind häufig zwischen mehreren Standards oder zwischen Standards und Metrik-Katalogen vorhanden. Wenn keine direkte Zuordnung zwischen dem gewählten Standard und existierenden Metriken besteht, kann auch ein anderer Standard als Bindeglied eingesetzt werden. Um die auf diese Weise gefundenen Metriken auf ihre Eignung zu überprüfen, wurden außerdem einige Regeln für gute Metriken herausgearbeitet.

Um die zweite Teilfrage zu beantworten, wurde in den Kapiteln 4.1.4 und 4.2.1 zuerst wichtige Regeln für die Definition einer Messung aufgestellt. Damit sollten eine hohe Genauigkeit und Vergleichbarkeit der Ergebnisse erreicht werden. Weiter wurde hier eine einheitliche Vorlage für die Dokumentation der Metriken aus der Literatur abgeleitet. Die Vorlage enthält unter anderem auch eine Formel für die Berechnung der Metrik.

Diese Berechnung findet im Rahmen der Datenauswertung statt, wie in Kapitel 4.3 beschrieben. Die bei dieser Datenauswertung ermittelten Ergebnisse sollen nun an die interessierten Parteien kommuniziert werden. Für diese Kommunikation wurden in Kapitel 4.3.1 einige Regeln, Richtlinien und Hinweise festgehalten, die einen Teil dritten Forschungsfrage beantworten. Sie helfen dabei, die Ergebnisse in einer für den jeweiligen Adressaten geeigneten Form zu aggregieren und darzustellen. Für die grafische Darstellung gibt wurde ein Leitfaden zur Wahl des richtigen Diagrammtyps aus der Literatur übernommen. Weiter wurden einige Regeln für die Gestaltung von Diagrammen festgehalten. Die zweite und dritte Phase des Zyklus, die die Datenerhebung, die Auswertung und die Kommunikation enthalten, können dabei als Antwort auf die vierte Teilfrage verstanden werden.

Schließlich wurde, in Kapitel 4.4, ein Ansatz für die Entwicklung und Priorisierung von Korrekturmaßnahmen bereitgestellt. Er sieht vor das die Ursachen für die Missstände aufgedeckt und gezielt behandelt werden.

Um das Framework zu validieren und die dritte Forschungsfrage vollständig zu beantworten wurde das entwickelte Framework in einer Fallstudie bei der Robert Bosch GmbH eingesetzt. Im Rahmen der Fallstudie wurden die im Framework definierten Schritte auf die Azure-Dienste des Unternehmens angewandt. Trotz der Limitationen konnten dabei überzeugende Ergebnisse erzielt werden. Es wurden Missstände bei der Konformität mit dem Bosch-eigenen EISA-Standard aufgedeckt und Korrekturmaßnahmen entwickelt. Die Fallstudie hat aber auch eine Schwäche des Frameworks aufgedeckt, nämlich den Ansatz zur Selektion von Metriken. Es konnte nur ein kleiner Teil der Anforderungen erfolgreich mit bereits existierenden Metriken überprüft werden. Diese Ergebnisse sind in Kapitel 6 festgehalten und beantworten die fünfte Teilfrage. Um das Framework zu verbessern, müsste entweder ein besserer Ansatz zur Selektion von existierenden Metriken gefunden werden oder es müssten von vornherein neue Metriken für die Anforderungen entwickelt werden.

## 6.2 Diskussion

Das behandelte Thema, also der Einsatz von bekannten Metriken zur systematischen Messung und Verbesserung der Konformität mit einem Sicherheitsstandard, stellt einen kleinen und spezifischen Teil der Forschung auf diesem Gebiet dar. Es gibt eine große Literaturvielfalt bezüglich des Einsatzes von Metriken zur Verbesserung der Informationssicherheit. Auch existieren einige Ansätze, um die Konformität bestimmter Systeme mit einem Sicherheitsstandard zu messen. Der hier behandelte Ansatz ist aber insofern einzigartig, dass bereits existierende Metriken zur Messung der Konformität mit einem Standard, auf den sie in der Regel nicht angepasst sind, umgenutzt werden sollen. Weiterhin konnte kein bestehender Ansatz gefunden werden, der die Konformität mit einem Standard mit Metriken misst und dabei nicht auf einen bestimmten Standard zugeschnitten ist.

Die Ergebnisse der Fallstudie legen nahe, dass der vorgeschlagene Ansatz zur Zuordnung der von Metriken und Anforderungen, keine zufriedenstellenden Ergebnisse erzeugt. Wie bereits in Kapitel 6 erwähnt gibt es dafür verschiedene Erklärungen. Es ist durchaus nicht unwahrscheinlich, dass ein anderer Ansatz bessere Ergebnisse erzeugen könnte. Leider konnte in der Literatur kein existierender Ansatz gefunden werden, um Metriken und Anforderungen zu verbinden. Wo Metriken für die Messung der Konformität eingesetzt werden, sind sie in der Regel bereits den Kontrollen oder Anforderungen eines bestimmten Standards zugeordnet.

Weiter waren die Ergebnisse der Fallstudie zufriedenstellend. Allerdings wären die Ergebnisse insgesamt aussagekräftiger, wenn die Fallstudie in einem größeren Umfang ausgeführt worden wäre. Mehr verschiedene Kontrollen, verschiedene Standards, verschiedene Systeme und weitere verschiedene Arten der Datenerhebung wären für die Fallstudie erstrebenswert gewesen. Aufgrund von zeitlichen Limitationen und begrenzten Möglichkeiten der Datenerhebung ist der Umfang aber beschränkt.

## 6.3 Ausblick

Wie bereits im letzten Kapitel erwähnt, gibt es momentan keine bedeutende Forschung zum Thema der Zuordnung von Metriken und Anforderungen. Auch unabhängig vom Einsatz in diesem Framework könnte, das ein interessantes Thema für weitere Forschungen darstellen. Wenn Metriken zuverlässig und objektiv mit Anforderungen aus verschiedenen Standards

verbunden werden können, wäre es möglich dieselben Metriken für eine Vielzahl von Standards einzusetzen. Dadurch könnte sich der Aufwand, der mit der Einhaltung der gesetzlich und vertraglich auferlegten Vorschriften einhergeht, stark reduziert werden.

Außerdem könnte durch weitere Forschung das hier definierte Framework auch für weitere Unternehmen, eine Branche oder sogar den allgemeinen Einsatz in Unternehmen und Organisationen aller Art validiert werden. Dafür wäre die Erprobung in weiteren Fallstudien und die eventuell anschließend eine Anpassung des Frameworks notwendig.

# Literaturverzeichnis

200-1. BSI-Standard 200-1, 2007.

Black, Paul E./Scarfone, Karen/Souppaya, Murugiah (2008). Cyber Security Metrics and Measures. NIST. https://doi.org/10.1002/9780470087923.hhs440.

Cambridge Dictionary (2023). FRAMEWORK | English meaning. Cambridge Dictionary.

CIS (2019). CIS Controls Measures and Metrics for Version 7.

Costa, C. J./Aparicio, M. (2019). Supporting the decision on dashboard design charts 2019. Online verfügbar unter https://www.researchgate.net/publication/336680372_SUPPORTING_THE_DECISION_ON_DASHBOARD_DESIGN_CHARTS.

Eckerson, Wayne W. (2011). Performance dashboards. Measuring, monitoring, and managing your business. 2. Aufl. New York, Wiley.

EISA. Bosch EISA, 01.08.2022.

EISA Control Catalogue, 01.08.2022.

EISA Pattern Catalogue, 01.08.2022.

ETSI (2016). TR 103 305-2. Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing.

Hayden, Lance (2010). IT security metrics. A practical framework for measuring security & protecting data. New York, McGraw Hill.

IBCS Association (2023). International Business Communication Standards. IBCS Version 1.2.

ISA/IEC (06 2020). Quick Start Guide: An Overview of ISA/IEC 62443 Standards. Security of Industrial Automation and Control Systems.

ISO 19086-2. ISO/IEC 19086-2:2018.

ISO 27000:2018. ISO/IEC 27000:2018.

ISO 27001:2005. ISO/IEC 27001:2005.

ISO 27001:2022. ISO/IEC 27001:2022.

ISO 27002:2022. ISO/IEC 27002:2022.

ISO 27004:2016. ISO/IEC 27004:2016.

ISO/IEC (2004). ISO/IEC Guide 2:2004.

ISO/IEC (2013). ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls.

ISO/IEC (2017). ISO/IEC/IEEE 15939:2017.

Jaquith, Andrew (2007). Security Metrics_ Replacing Fear, Uncertainty, and Doubt. Addison-Wesley.

Mark Bristow (2021). A SANS 2021 Survey: OT/ICS Cybersecurity. Sans Institute.

Masaaki Imai (1986). Kaizen, the key to Japan's competitive success.

Michael Bartock/Joseph Brule/Ya-Shian Li-Baboud/Suzanne Lightman/James McCarthy/Karen Reczek/Doug Northrip/Arthur Scholz/Theresa Suloway (2021). NISTIR 8323. Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. NIST.

Microsoft (2023). Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings. Microsoft.

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD, National Institute of Standards and Technology.

Rosenfelder, Mario/Terbuch, Thomas (2018). International Business Communication Standards.

Secure Controls Framework Council (2022). Secure Controls Framework Overview & Instructions.

SP 500-307. NIST Special Publication 500-307, 2018. Gaithersburg, MD.

SP 800-53. NIST Special Publication 800-53, 2020.

SP 800-55. NIST Special Publication 800-55 Revision 1, 2022. Gaithersburg, MD.

SP 800-82. NIST SP 800-82, 2015.

Yee, George O. M. (2019). Designing Good Security Metrics. In: 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15.07.2019 - 19.07.2019. IEEE, 580–585.

Yee, George O.M. (2013). Security Metrics. An Introduction and Literatur Review. In: Computer and Information Security Handbook. Elsevier, 553–566.

# Anhang A: Die Metriken der Fallstudie

| **Feldnamen** | **Inhalt** |
|---|---|
| **ID der Metrik** | CIS 8.1 |
| **Ziel** | 201.1: Usage of Malware Protection Solutions<br>201.3: Central Management |
| **Metrik** | Prozentsatz der Azure-Subscriptions, die einen zentral verwalteten Malware-Schutz, zur kontinuierlichen Überwachung einsetzen. |
| **Formel** | (Messung 2 / Messung 1) * Messung 3 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 1. Wie viele Azure Subscriptions sind vorhanden?<br>2. Wie viele Azure Subscriptions haben den Malware-Schutz aktiviert?<br>3. Ist der Malware-Schutz zentral organisiert?<br>o Ja = > 1<br>o Nein => 0 |
| **Frequenz** | Messungen 1 und 2: Monatlich<br>Messung 3: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>• **Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1 und 2: Vorhandene Messdaten (Excel)<br>Messung 3: Informationseigentümer |
| **Berichterstattungsformat** | Liniendiagramm (Über Zeit)<br>Oder<br>Kreisdiagramm (Einzelner Zeitpunkt) |

| Feldnamen | Inhalt |
|---|---|
| **ID der Metrik** | CIS 8.2 |
| **Ziel** | 201.5: Automatic Updates and Update Deployment |
| **Metrik** | Prozentsatz der Azure-Subsriptions, bei denen ein automatisch aktualisierter Malware-Schutz zur kontinuierlichen Überwachung und Abwehr eingesetzt wird |
| **Formel** | (Messung 2 / Messung 1) * Messung 3 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 1. Wie viele Azure Subscriptions sind vorhanden?<br>2. Wie viele Azure Subscriptions haben den Malware-Schutz aktiviert?<br>3. Wird die Security automatisch aktualisiert?<br>o Ja = > 1<br>o Nein => 0 |
| **Frequenz** | Messungen 1 und 2: Monatlich<br>Messung 3: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>a) **Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1 und 2: Vorhandene Messdaten (Excel)<br>Messung 3: Informationseigentümer |
| **Berichterstattungsformat** | Liniendiagramm (Über Zeit)<br>Oder<br>Kreisdiagramm (Einzelner Zeitpunkt) |

| Feldnamen | Inhalt |
|---|---|
| **ID der Metrik** | Eigene Metrik 1 |
| **Ziel** | 201.4: Centralize Anti-malware Logging |
| **Metrik** | Zentrales Logging von Security Events der Azure-Subscriptions |
| **Formel** | Messung 1 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 1. Setzt die für Azure eingesetzte Security-Lösung zentrales Logging ein?<br>o Ja => 1<br>o Nein => 2 |
| **Frequenz** | Messung 1: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>**Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1: Informationseigentümer |
| **Berichterstattungsformat** | Als Karte (Ja / Nein)<br>➔ Visualisierung am besten zusammengesetzt mit anderen Metriken |

| Feldnamen | Inhalt |
|---|---|
| **ID der Metrik** | Eigene Metrik 2 |
| **Ziel** | 201.4: Approved Malware Protection Solutions |
| **Metrik** | Genehmigung der Malware-Lösung |
| **Formel** | Messung 1 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 2. Ist die für Azure eingesetzte Security-Lösung vom Bosch Central Malware Protection Team genehmigt?<br>o Ja => 1<br>o Nein => 2 |
| **Frequenz** | Messung 1: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>**Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1: Informationseigentümer |
| **Berichterstattungsformat** | Als Karte (Ja / Nein)<br>➔ Visualisierung am besten zusammengesetzt mit anderen Metriken |

| Feldnamen | Inhalt |
|---|---|
| **ID der Metrik** | Eigene Metrik 3 |
| **Ziel** | 201.6: Scan Method |
| **Metrik** | Regelmäßige (mindestens monatliche) Scans von Azure-Supscritions |
| **Formel** | Messung 1 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 1. Führt die für Azure eingesetzte Security-Lösung regelmäßig und mindestens monatlich automatische Scans durch?<br>○ Ja => 1<br>○ Nein => 2 |
| **Frequenz** | Messung 1: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>**Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1: Informationseigentümer |
| **Berichterstattungsformat** | Als Karte (Ja / Nein)<br>➔ Visualisierung am besten zusammengesetzt mit anderen Metriken |

| Feldnamen | Inhalt |
|---|---|
| **ID der Metrik** | Eigene Metrik 4 |
| **Ziel** | 201.6: Scan Method |
| **Metrik** | Echtzeit-Überwachung von Azure-Supscriptions |
| **Formel** | Messung 1 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 1. Bietet die für Azure eingesetzte Security-Lösung Echtzeitüberwachung?<br>o Ja => 1<br>o Nein => 2 |
| **Frequenz** | Messung 1: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>**Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1: Informationseigentümer |
| **Berichterstattungsformat** | Als Karte (Ja / Nein)<br>➔ Visualisierung am besten zusammengesetzt mit anderen Metriken |

| Feldnamen | Inhalt |
|---|---|
| **ID der Metrik** | Eigene Metrik 5 |
| **Ziel** | 201.8: Malware Incident Handling |
| **Metrik** | Block oder Quarantäne bei Malware auf Azure-Subscriptions |
| **Formel** | Messung 1 * 100 |
| **Zielwert** | 100% |
| **Messungen** | 1. Wird Malware von der für Azure eingesetzte Security-Lösung entweder geblockt oder in Quarantäne verschoben?<br>o Ja => 1<br>o Nein => 2 |
| **Frequenz** | Messung 1: Einmalig (Unter der Annahme, dass sich dieser Wert nicht verändert)<br>Berichterstattung: kontinuierlich (Power BI Dashboard) |
| **Verantwortliche und Interessierte Parteien** | • **Messauftraggeber**: Management und IT (Fiktiv)<br>• **Messungsplaner**: Der Autor<br>• **Prüfer der Messung**: Der Autor<br>• **Informationseigentümer:** Mitarbeiter aus dem Bereich Security Governance<br>• **Informationssammler**: Der Autor<br>• **Informationsanalytiker**: Der Autor<br>**Informationsvermittler**: Der Autor |
| **Datenquelle** | Messung 1: Informationseigentümer |
| **Berichterstattungsformat** | Als Karte (Ja / Nein)<br>➔ Visualisierung am besten zusammengesetzt mit anderen Metriken |