Holger Reibold

Security Metrics & Audit KPIs

Informationssicherheit kennzahlenbasiert messen, steuern und auditieren

BRAIN-MEDIA.DE

Holger Reibold

Security Metrics & Audit KPIs

Informationssicherheit kennzahlenbasiert messen, steuern und auditieren

BRAIN-MEDIA.DE

ISBN: 978-3-95444-320-8

Cover: Freepik / romanbecker

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Inhaltsverzeichnis I

Vorwort 1

1 Einführung 5

1.1 Problemstellung und Relevanz 6

1.2 Begriffsdefinitionen 8

1.3 Entwicklung und Trends 11

1.4 Zielsetzung und Aufbau 13

1.5 Abgrenzung 15

1.6 Management Summary 17

2 Grundlagen der Informationssicherheit 19

2.1 Schutzziele 20

2.2 Bedrohungslandschaft 23

2.3 Frameworks 26

2.4 Governance, Risk & Compliance 29

2.5 Rolle von Audits 31

2.6 Management Summary 33

3 Klassifikation von Security Metrics 35
3.1 Arten von Metriken 36
3.2 Leading vs. Lagging Indicators 39
3.3 KPIs vs. KRIs vs. KCIs 42
3.4 Reifegradmodelle 45
3.5 Anforderungen an gute Metriken 47
3.6 Management Summary 49
4 Entwicklung und Design von KPIs 51
4.1 Ableitung aus Unternehmenszielen 52
4.2 KPI-Design-Prozess 55
4.3 Datenquellen und -qualität 58
4.4 Visualisierung und Reporting 60
4.5 Typische Fehler und Anti-Patterns 63
4.6 Management Summary 65
5 Security Metrics im operativen Einsatz 67
5.1 Incident Detection & Response KPIs 68
5.2 Vulnerability Management KPIs 71
5.3 Identity & Access Management KPIs 73
5.4 Security Awareness & Behavioral Metrics 76
5.5 DevSecOps & Cloud Security 78
5.6 Management Summary 81

6 Audit KPIs und Prüfmethodik 83
6.1 Grundlagen von Audits 84
6.2 Interne vs. externe Audits 86
6.3 Audit-Kennzahlen 89
6.4 Continuous Auditing 91
6.5 Automatisierung 95
6.6 Management Summary 97
7 Integration in Unternehmenssteuerung 99
7.1 Verknüpfung mit Business KPIs 100
7.2 Reporting an Management 102
7.3 Kommunikation kritischer Metriken 105
7.4 Benchmarking 107
7.5 Wirtschaftlichkeit und ROI 109
7.6 Management Summary 111
8 Zukunftstrends & Herausforderungen 113
8.1 Automatisierung und KI 114
8.2 Zero Trust 117
8.3 Regulatorik 119
8.4 Herausforderungen der Messbarkeit 122
8.5 Best Practices 124
8.6 Management Summary 126

Zum Schluss 129

Anhang V

KPI-Katalog „Security Metrics Master Set“ V

KPI-Design & Implementation Toolkit XI

Weitere Downloads XVI

Glossar XVII

Abkürzungsverzeichnis XXI

Literatur- und Quellenverzeichnis XXIII

Stichwortverzeichnis XXV

Mehr von Brain-Media.de XXIX

Vorwort

Sicherheit messbar machen – warum Metrics entscheidend sind

Die zunehmende Digitalisierung, die fortschreitende Vernetzung von Systemen sowie die steigende Professionalität von Cyberangriffen haben die Informationssicherheit in den vergangenen Jahren grundlegend verändert. Was früher primär als technische Disziplin verstanden wurde, ist heute ein zentraler Bestandteil unternehmerischer Steuerung und Risikokontrolle. Organisationen stehen nicht mehr nur vor der Aufgabe, Sicherheitsmaßnahmen zu implementieren, sondern müssen deren Wirksamkeit nachvollziehbar belegen, kontinuierlich überwachen und gezielt weiterentwickeln.

In diesem Kontext gewinnen Security Metrics und Audit KPIs eine entscheidende Bedeutung. Sie schaffen die Grundlage dafür, Sicherheitsniveaus messbar zu machen, Risiken transparent darzustellen und Entscheidungen auf einer belastbaren Datenbasis zu treffen. Insbesondere auf Management- und C-Level-Ebene werden Kennzahlen zunehmend zur zentralen Kommunikations- und Steuerungsgröße. Gleichzeitig steigt durch regulatorische Anforderungen und etablierte Frameworks der Druck, Sicherheitsmaßnahmen nicht nur umzusetzen, sondern auch auditierbar und revisionssicher zu dokumentieren.

Die Praxis zeigt jedoch, dass viele Unternehmen Schwierigkeiten haben, diesen Anforderungen gerecht zu werden. Häufig existieren zwar zahlreiche Datenquellen, Tools und Reports, doch fehlt es an einer klaren Struktur, konsistenten Definitionen und einer zielgerichteten Nutzung der gewonnenen Informationen. Kennzahlen werden isoliert betrachtet, sind nicht auf strategische Ziele ausgerichtet oder liefern keine echten Entscheidungsgrundlagen. In anderen Fällen scheitert die Umsetzung bereits an mangelnder Datenqualität oder unzureichender Integration in bestehende Prozesse und Systeme.

Dieses Buch setzt genau an dieser Stelle an. Es verfolgt das Ziel, einen strukturierten und praxisnahen Ansatz zur Entwicklung, Implementierung und Nutzung von Security Metrics und Audit KPIs zu vermitteln. Dabei steht nicht die isolierte Betrachtung einzelner Kennzahlen im Vordergrund, sondern deren Einbettung in ein ganzheitliches Steuerungsmodell, das technische, organisatorische und strategische Aspekte miteinander verbindet. Der Leser erhält ein fundiertes Verständnis dafür, wie Kennzahlen aus Unternehmenszielen abgeleitet, sinnvoll klassifiziert und in konkrete Steuerungsmechanismen überführt werden können.

Ein besonderer Fokus liegt auf der praktischen Anwendbarkeit. Neben konzeptionellen Grundlagen werden typische Herausforderungen, häufige Fehler sowie bewährte Lösungsansätze aus der Praxis dargestellt. Ziel ist es, nicht nur Wissen zu vermitteln, sondern konkrete Orientierung für die Umsetzung im eigenen Unternehmen zu geben. Dabei richtet sich das Buch gleichermaßen an Fach- und

Führungskräfte aus den Bereichen Informationssicherheit, IT, Governance, Risk und Compliance sowie an Auditoren und Berater, die sich mit der Bewertung und Weiterentwicklung von Sicherheitsstrukturen befassen.

Methodisch basiert der Inhalt auf einer Kombination aus etablierten Standards, theoretischen Modellen und praktischen Erfahrungen aus realen Projekten und Audits. Die dargestellten Konzepte folgen einem strukturierten, aber zugleich flexiblen Ansatz, der es ermöglicht, unterschiedliche Organisationsgrößen und Reifegrade zu berücksichtigen. Security Metrics werden dabei nicht als statisches Konstrukt verstanden, sondern als kontinuierlicher Verbesserungsprozess, der sich an veränderte Bedrohungslagen, technologische Entwicklungen und geschäftliche Anforderungen anpassen muss.

Das vorliegende Werk versteht sich als Leitfaden für ein modernes, kennzahlenbasiertes Security-Management. Es bietet sowohl einen fundierten Einstieg in das Thema als auch vertiefende Impulse für die Weiterentwicklung bestehender Ansätze. Damit bildet es die Grundlage für die folgenden Kapitel, in denen zentrale Begriffe geklärt, theoretische Grundlagen geschaffen und konkrete Methoden sowie Anwendungsbeispiele detailliert ausgearbeitet werden.

Herzlichst

Holger Reibold

1 Einführung

Security Metrics verstehen: Grundlagen, Begriffe, Trends

Die Steuerung von Informationssicherheit erfordert heute mehr als den Einsatz technischer Schutzmaßnahmen. Unternehmen stehen vor der Herausforderung, Sicherheitsniveaus messbar zu machen, Risiken transparent zu bewerten und Fortschritte nachvollziehbar zu dokumentieren. Security Metrics und Audit KPIs bilden hierfür die zentrale Grundlage. Sie ermöglichen es, komplexe Sicherheitszustände in quantifizierbare Kennzahlen zu überführen und als Entscheidungsbasis für operative und strategische Maßnahmen zu nutzen.

Gleichzeitig zeigt sich in der Praxis, dass die Definition geeigneter Kennzahlen häufig unscharf bleibt und deren Aussagekraft begrenzt ist. Unterschiedliche Begriffsverständnisse, fehlende Standardisierung sowie eine unzureichende Verknüpfung mit Unternehmenszielen erschweren eine wirksame Anwendung. Parallel dazu entwickeln sich Methoden, Technologien und regulatorische Anforderungen dynamisch weiter, wodurch sich auch die Anforderungen an Security Metrics kontinuierlich verändern.

Dieses Kapitel führt in die grundlegenden Konzepte von Security Metrics und Audit KPIs ein, schafft begriffliche Klarheit, beleuchtet

aktuelle Entwicklungen und definiert den Rahmen sowie die Zielsetzung des weiteren Buchaufbaus.

1.1 Problemstellung und Relevanz

Die Informationssicherheit steht vor einem grundlegenden Dilemma: Während Investitionen in Technologien, Prozesse und Personal kontinuierlich steigen, bleibt die Frage nach deren tatsächlicher Wirksamkeit häufig unbeantwortet. Unternehmen implementieren Firewalls, SIEM-Systeme, Awareness-Programme und komplexe Governance-Strukturen – doch ohne belastbare Messgrößen lässt sich weder beurteilen, ob diese Maßnahmen greifen, noch ob sie im Verhältnis zum Risiko und zu den Kosten angemessen sind.

Ein zentrales Problem besteht darin, dass Sicherheit per se schwer messbar ist. Anders als in klassischen betriebswirtschaftlichen Disziplinen existieren keine universellen Kennzahlen, die unmittelbar Aufschluss über den „Zustand" der Sicherheit geben. Stattdessen bewegen sich Organisationen in einem Spannungsfeld aus Bedrohungsszenarien, Wahrscheinlichkeiten und potenziellen Schadensausmaßen. Ohne geeignete Metriken bleibt die Steuerung daher oft reaktiv, erfahrungsbasiert oder von subjektiven Einschätzungen geprägt.

Hinzu kommt eine zunehmende Komplexität der IT-Landschaften. Cloud-Umgebungen, hybride Infrastrukturen, mobile Arbeitsmodelle und vernetzte Lieferketten erweitern die Angriffsfläche erheblich.

Gleichzeitig steigen die Anforderungen durch regulatorische Vorgaben und Standards, die eine nachvollziehbare und auditierbare Bewertung der Sicherheitslage verlangen. Organisationen müssen nicht nur sicher sein, sondern ihre Sicherheit auch nachweisen können.

In der Praxis zeigt sich jedoch häufig ein fragmentiertes Bild: Daten liegen in unterschiedlichen Systemen vor, Kennzahlen sind nicht konsistent definiert und Reports liefern zwar Informationen, aber keine echten Entscheidungsgrundlagen. Oft werden lediglich leicht verfügbare Daten gemessen, anstatt relevante. Dies führt zu einer verzerrten Wahrnehmung der Sicherheitslage und kann falsche Prioritäten setzen.

Die Relevanz von Security Metrics und Audit KPIs liegt daher in ihrer Fähigkeit, Transparenz zu schaffen und Komplexität zu reduzieren. Sie ermöglichen eine strukturierte Bewertung von Risiken, die Identifikation von Schwachstellen sowie die gezielte Steuerung von Maßnahmen. Richtig eingesetzt, bilden sie die Brücke zwischen operativer Sicherheit und strategischer Unternehmensführung.

Darüber hinaus sind sie ein wesentliches Instrument für Kommunikation und Governance. Sie unterstützen dabei, Sicherheitszustände verständlich darzustellen, Fortschritte zu belegen und Entscheidungen gegenüber Stakeholdern zu legitimieren. Insbesondere im Kontext von Audits und regulatorischen Prüfungen stellen sie sicher, dass Sicherheitsmaßnahmen nicht nur implementiert, sondern auch wirksam und nachvollziehbar sind.

Vor diesem Hintergrund wird deutlich: Ohne ein durchdachtes, konsistentes Kennzahlensystem bleibt Informationssicherheit in vielen Organisationen eine Blackbox. Security Metrics und Audit KPIs sind daher kein optionales Reporting-Instrument, sondern ein zentraler Bestandteil moderner Sicherheitssteuerung.

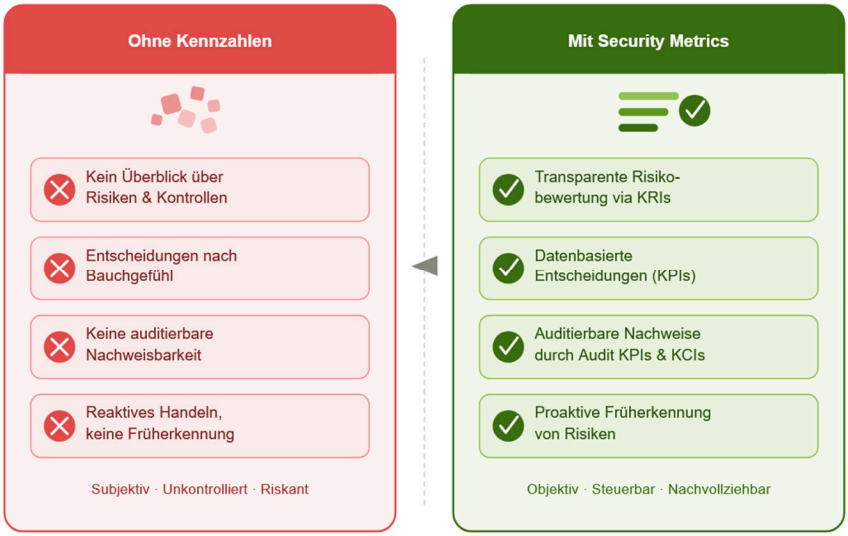


Abbildung 1: Die Gegenüberstellung zeigt den Unterschied zwischen einer subjektiven Sicherheitsbewertung ohne Kennzahlen und einer datenbasierten Steuerung mit klar definierten Metrics und KPIs.

1.2 Begriffsdefinitionen

Eine klare und konsistente Verwendung von Begriffen ist eine zentrale Voraussetzung für den erfolgreichen Einsatz von Security

Metrics und Audit KPIs. In der Praxis zeigt sich jedoch häufig, dass unterschiedliche Definitionen parallel existieren oder Begriffe unscharf verwendet werden. Dies führt zu Missverständnissen, inkonsistenten Auswertungen und letztlich zu einer eingeschränkten Aussagekraft von Kennzahlen.

Unter Security Metrics werden allgemein messbare Größen verstanden, die den Zustand, die Leistung oder die Wirksamkeit von Maßnahmen der Informationssicherheit quantifizieren. Sie dienen dazu, komplexe Sachverhalte zu objektivieren und Entwicklungen über die Zeit hinweg vergleichbar zu machen. Security Metrics können sowohl technische Aspekte (z. B. Anzahl erkannter Angriffe, Patch-Status) als auch organisatorische oder prozessuale Dimensionen (z. B. Schulungsquote, Reaktionszeiten) abbilden.

Key Performance Indicators (KPIs) sind eine spezifische Untergruppe von Metriken, die sich unmittelbar auf die Leistung und Zielerreichung beziehen. Im Kontext der Informationssicherheit messen sie, inwieweit definierte Sicherheitsziele erreicht werden, beispielsweise die Effizienz von Incident-Response-Prozessen oder die Reduktion von Schwachstellen über einen bestimmten Zeitraum. KPIs sind typischerweise eng an strategische oder operative Ziele gekoppelt.

Demgegenüber stehen Key Risk Indicators (KRIs), die darauf abzielen, potenzielle Risiken frühzeitig sichtbar zu machen. Sie liefern Hinweise auf Entwicklungen, die zu Sicherheitsvorfällen führen könnten, etwa steigende Fehlkonfigurationen, zunehmende Phishing-Erfolgsquoten oder wachsende Angriffsversuche. KRIs haben somit eine

präventive Funktion und unterstützen ein proaktives Risikomanagement.

Ergänzend dazu werden häufig Key Control Indicators (KCIs) eingesetzt. Diese messen die Wirksamkeit und den Reifegrad implementierter Kontrollen, beispielsweise die Abdeckung von Zugriffskontrollen, die Qualität von Logging-Mechanismen oder die Einhaltung definierter Richtlinien. KCIs stellen sicher, dass definierte Sicherheitsmaßnahmen nicht nur existieren, sondern auch wie vorgesehen funktionieren.

Im Kontext von Audits spielen zudem Audit KPIs eine wichtige Rolle. Diese fokussieren sich auf die Messbarkeit von Prüfprozessen und deren Ergebnissen. Typische Beispiele sind die Anzahl festgestellter Abweichungen, die Dauer bis zur Behebung von Findings oder die Wiederholungsrate identischer Mängel. Sie ermöglichen eine Bewertung der Auditqualität sowie der nachhaltigen Wirksamkeit von Korrekturmaßnahmen.

Ein weiterer zentraler Begriff ist der der Messgröße selbst. Eine Metrik besteht in der Regel aus einer klar definierten Berechnungslogik, einer Datenquelle sowie einem Bezugsrahmen (z. B. Zeitraum oder Organisationseinheit). Erst durch diese Struktur wird sichergestellt, dass Kennzahlen reproduzierbar, vergleichbar und interpretierbar sind.

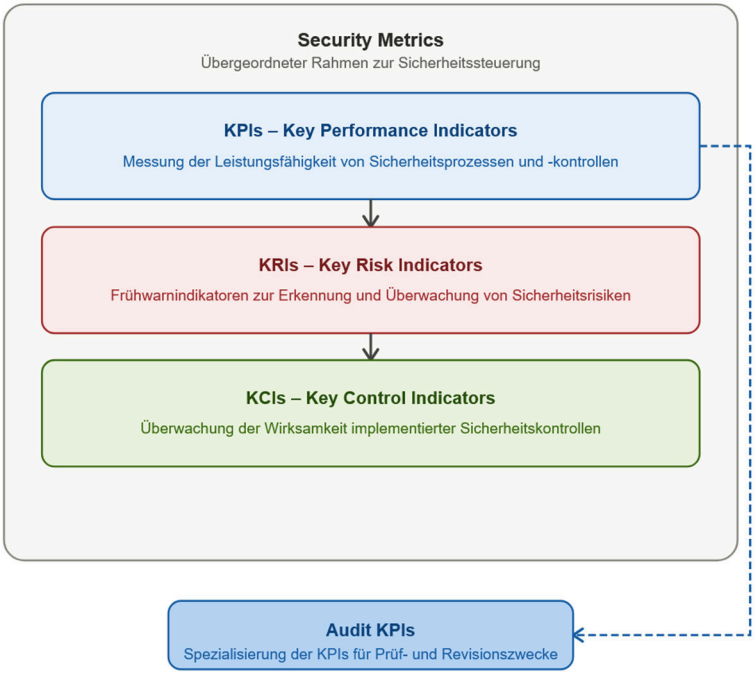
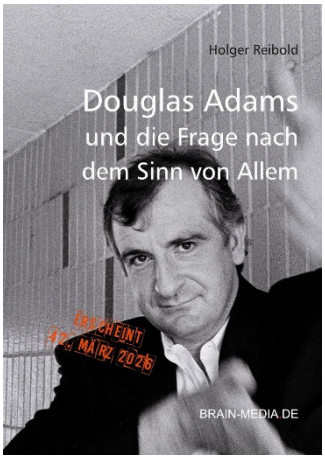


Abbildung 2: Die Abbildung zeigt die systematische Einordnung von Security Metrics und deren Unterkategorien. Sie verdeutlicht die unterschiedlichen Rollen von KPIs, KRIs und KCIs im Kontext der Sicherheitssteuerung.

1.3 Entwicklung und Trends

Die Entwicklung von Security Metrics und Audit KPIs ist eng mit der zunehmenden Reife der Informationssicherheit als Managementdisziplin verbunden. Während Sicherheitsmaßnahmen früher primär technisch geprägt und reaktiv ausgerichtet waren, hat sich in den letzten Jahren ein deutlicher Wandel hin zu einer systematischen, kennzahlenbasierten Steuerung vollzogen. Treiber dieser Entwicklung

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.
Umfang: 140 Seiten
Preis: 14,99 EUR
Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.
100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.

Compliance-Matrix – NIS-2, DORA, CRA & EU AI Act integriert umsetzen

So bauen Sie ein effizientes, auditfähiges Compliance-System ohne Doppelarbeit und mit klarem Management-Fokus auf.
Preis: 29,99 EUR
Umfang: 295 Seiten

NIS-2 Survival Kit – Der Praxisleitfaden mit Sofort-Maßnahmen, Checklisten und Vorlagen zur rechtssicheren Umsetzung

Dieses Buch schafft Klarheit, welche Anforderungen nicht gestellt werden – und wo der tatsächliche Fokus liegt.
Preis: 29,99 EUR
Umfang: 180 Seiten

Knowledge as a Service (KaaS)

Compliance als operativer Vorteil

NIS-2, DORA, EU AI Act, CRA – der regulatorische Druck wird zum Geschäftsrisiko. KaaS (Knowledge as a Service) macht Ihr Unternehmen sicher und audit-ready – schnell, strukturiert und ohne externe Beratungsabhängigkeit. Statt fragmentierter Anforderungen und schwer umsetzbarer Vorgaben erhalten Sie ein System, das Compliance in operative Umsetzung überführt:

- klare, priorisierte Anforderungen
- direkt umsetzbare Templates
- auditfähige Dokumentation
- kontinuierlich aktualisierte Inhalte

Von Unsicherheit und Einzelmaßnahmen zu strukturierter, prüfbarer Umsetzung. KaaS reduziert Ihre Risiken, beschleunigt die Umsetzung und schafft Transparenz auf allen Unternehmensebenen.

Vier Varianten – für jeden Bedarf die passende Lösung

KaaS ist in vier Tarifen verfügbar: von Personal für Einzelpersonen und IT-Leiter über Team (empfohlen) für Compliance-Abteilungen und Berater bis zu Business für Mittelstand und IT-Dienstleister – und Enterprise für größere Unternehmen und KRITIS-Betreiber mit unbegrenzter Nutzerzahl. Ihren Fragen beantwortet unsere FAQ. Für Kunden steht eine 20seitige Einleitung zur Nutzung von KaaS bereit.

Individuelle Anforderungen

Kein Unternehmen ist wie das andere – Branche, Größe, Reifegrad und regulatorisches Umfeld unterscheiden sich signifikant. Sie haben individuelle Anforderungen? Wir setzen diese gerne um.