ISACA®

Germany Chapter

Praxisleitfaden für ein zielorientiertes IS-Kennzahlensystem nach ISO/IEC 27004:2016

Bewertung der Leistung eines ISMS durch Schlüsselindikatoren

Dirk Meissner, ISACA Fachgruppe Informationssicherheit, IT-GRC Kongress Dezember 2020

ISACA® Germany Chapter

Vorstellung Dirk Meissner, Allevio AG

Seit 1996 fokussiert auf Informationssicherheit und IT-GRC

Was ich gerade so mache….

- Security Manager AWS Public Cloud Automotive Konzern
- Datenschutzbeauftragter einer Collaboration Plattform
- Aufbau eines ISMS nach ISO 27001 im Healthcare Umfeld
- Aufbau eines CERT für Unternehmung mit über 100 Standorten

ISACA Germany Chapter

ISACA Germany Chapter (Mission statement)

Experten - nur ein Steinwurf entfernt

ISACA Germany Chapter e.V.

Deutscher Berufsverband der IT-Revisoren, IT-Sicherheitsmanager
sowie der IT-Governance-Experten mit mehr als 2.500 Mitgliedern.

Das deutsche Chapter ist das siebtgrößte ISACA Chapter weltweit.

Ziel des Vereines ist die Durchführung von Aus- und Weiterbildung der Mitglieder [..] aufgrund spezifischer deutscher Bedürfnisse. Zusammen mit Partnern kooperieren wir bei Seminaren, Konferenzen und Tagungen in Deutschland und International.

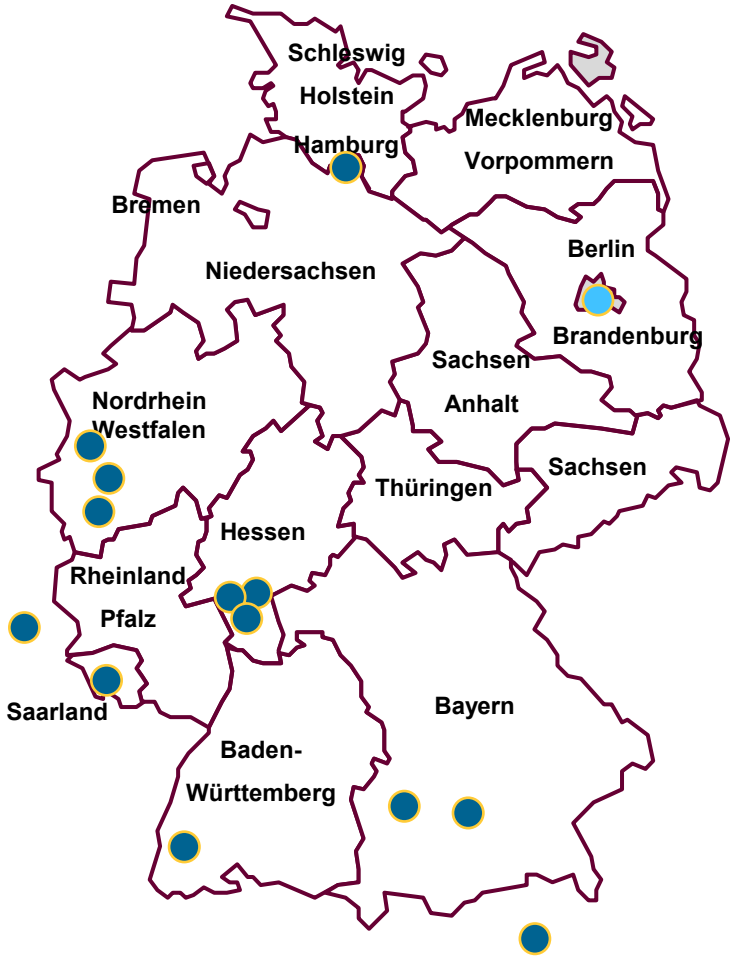
Förderung von Publikationen von Mitgliedern sowohl durch

: **Fachartikel in unserer Zeitschrift IT-Governance**
oder
: **eigenen Publikationen um ihre Arbeit an eine breitere Öffentlichkeit** heranzutragen.

Überblick über die Fachgruppen innerhalb des ISACA Germany Chapter

ISACA EXPERTS TOGETHER Germany Chapter

1. **Akademische Aus- und Weiterbildung** - Dr. Ulrich Hahn, Frankfurt
2. **COBIT & Rechnungslegung** - Heiko Jacob, Düsseldorf
3. **Cloud Computing** - Edgar Röder, Saarbrücken
4. **Cyber Security** - Andreas Teuscher, Freiburg
5. **Datenanalyse** - Henning Lieder, Hamburg
6. **GxP** - Rainer Voglmaier, Verona
7. **IT-Compliance – Grundlagen** - Ioannis Karamitros, Köln
8. **IT Compliance – Finanz/Versicherungsw.** - C. Reffgen, Bonn
9. **I&T Governance** - Alexander Riemer, Dreieich
10. **IT-Revision** - Torsten Enk, Köln
11. **IT-Risikomanagement** - Jürgen Kempter, Offenburg
12. **Informationssicherheit** – Angelika Holl, München
13. **SAP** - Alexander Schneider, Augsburg
14. **Young Professionals** - Matthias Kraft, Luxemburg



bündeln und zeigen die Expertise und Kompetenz von ISACA

- bündeln Kompetenz und Wissen der Mitglieder des ISACA Germany Chapters und machen es für die Fachwelt nutzbar
- bearbeiten relevante und zukunftsbildende Fachthemen
- bringen unterschiedliche Experten zusammen
- ermöglichen Erfahrungsaustausch und Vernetzung
- präsentieren ihre Ergebnisse über Fachzeitschriften, Vorträge auf Kongressen, Tagungen und anderen Veranstaltungen.

Was bietet die Mitarbeit in einer Fachgruppe?

- Träger von ISACA-Berufszertifizierungen wie CISA, CISM, CGEIT und CRISC erhalten für die Mitarbeit CPEs und können somit durch die Teilnahme ihre berufliche Weiterentwicklung nachweisen.
- Der fachliche Austausch fördert neue Sichtweisen auf Problemstellungen und ist in der Regel eine Win-Win-Situation. Im Idealfall bringt der Einzelne einiges an Wissen ein, gewinnt aber auch ein vielfaches an Expertise.
- Die Fachgruppen-Mitglieder erhalten zum Teil frühzeitig Einblick in die Entwürfe zukünftiger Standards und Positionspapiere und können ihr Unternehmen so frühzeitig auf kommende Veränderungen vorbereiten.
- Die ISACA-Fachgruppen tragen mit ihren Arbeitsergebnissen und ihrer Expertise zur Meinungsbildung bei Fachexperten und politischen Entscheidern bei.

Werden Sie Mitglied einer Fachgruppe, teilen Sie Ihr Wissen und tragen Sie aktiv zur Weiterentwicklung des Berufsstandes bei!

DIE Fachgruppe erwartet SIE !!!

Nun aber endlich zum eigentlichen Thema!

Die Historie:

- Die ISACA FG Informationssicherheit hat in 2017 einen Praxisleitfaden für den Aufbau eines ISMS nach ISO 27001 veröffentlicht.

- Auf dem IT-GRC Kongress 2019 haben wir einen Praxisleitfaden für ein zielorientiertes ISMS Berichtswesen angekündigt.

- Im Frühjahr 2020 haben wir den Lockdown dazu genutzt genau diesen Leitfaden zu finalisieren.

ISACA Germany Chapter

Welche ISMS Kennzahlen -/klassen sind denn sinnvoll?

Das ist eine gute Frage….

ISACA Germany Chapter

…..unsere (Praxis) Antwort sieht so aus!

Praxisleitfaden für ein zielorientiertes IS-Kennzahlensystem nach ISO/IEC 27004:2016

ISACA Germany Chapter

KPI – Key-Performance-Indikatoren

Ein Key-Performance-Indikator ist ein Wert (Soll/Ist-Vergleich), der anzeigt, wie **erfolgreich** ein Unternehmen die relevanten technischen und organisatorischen Maßnahmen sowie die Informationssicherheitsprozesse, in Bezug auf die Erreichung der Informationssicherheitsziele, umsetzt. Erfolgreich ist eine Maßnahme, wenn das gewünschte Leistungsniveau innerhalb der vorgegebenen Zeit und mit möglichst geringem Aufwand erreicht wird.

Beispielformeln:

Benötigte Zeit im Vergleich zur geplanten Zeit bei der vorgegebenen Umsetzungsrate (z.B. 80% der Mitarbeiter) einer Awareness-Kampagne.

Benötigtes Budget im Vergleich zum geplanten Budget für die Umsetzung einer Awareness-Kampagne.

ISACA Germany Chapter

KRI – Key-Risk-Indikatoren

Ein Key-Risk-Indikator ist ein Wert (Soll/Ist-Vergleich), der anzeigt, ob Veränderungen im Risikoprofil die gewünschten Toleranzgrenzen potenziell überschreiten und damit die Zielerreichung gefährden. Er ist damit ein Maß dafür, wie **risikoorientiert** ein Unternehmen die relevanten technischen und organisatorischen Maßnahmen sowie die Informationssicherheitsprozesse umsetzt. Eine Situation, die den Risikoappetit des Unternehmens überschreitet, wird durch gegensteuernde Maßnahmen wieder in den akzeptablen Risikobereich gebracht.

Beispielformeln:

Prozentsatz der Mitarbeiter, die einen präparierten Phishing-Link während einer Awareness-Kampagne klicken.

Prozentsatz der IT-Systeme mit Schwachstellen, die nicht im vorgesehenen Zeitfenster geschlossen wurden.

Prozentsatz der produktiven IT-Systeme, für die kein Herstellersupport mehr besteht.

ISACA Germany Chapter

KCI – Key-Control-Indikatoren

Ein Key-Control-Indikator ist ein Wert (Soll/Ist Vergleich), der anzeigt, wie **effektiv** in Bezug auf die Zielerreichung ein Unternehmen die relevanten technischen und organisatorischen Maßnahmen sowie die Informationssicherheitsprozesse umsetzt. Effektiv ist eine Maßnahme, wenn die Steuerungsziele zuverlässig innerhalb der gewünschten Toleranzgrenzen erreicht werden.

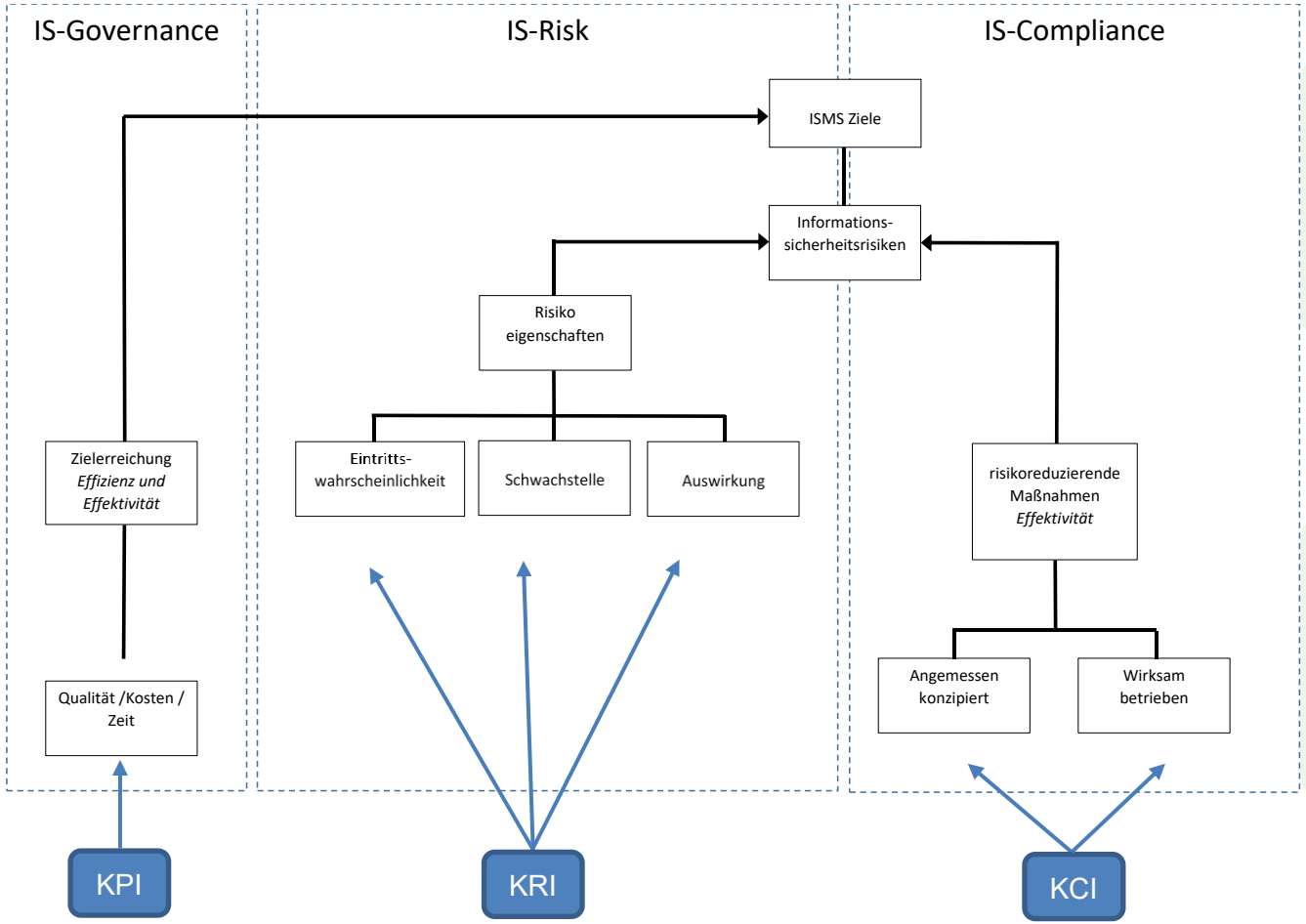
Beispiel Formeln:

Verhältnis der bisher geschulten Mitarbeiter im Vergleich zu den Planzahlen der zu schulenden Mitarbeiter bei einer Awareness-Kampagne.

Anzahl der Mitarbeiter, die die Lernkontrolle am Ende der Awareness-Kampagne bestanden haben, im Vergleich zu den bereits geschulten Mitarbeitern bei einer Awareness-Kampagne.

ISACA Germany Chapter

Beziehungen der Kennzahlklassen



ISACA Germany Chapter

Zielgruppen der Kennzahlen

- (Senior) Management
  - Geschäftsleitung / Vorstand
  - CISO
  - CIO
- Fachbereiche
- Beispiele weiterer interessierter Parteien:
  - Interne Revisoren und Auditoren
  - Notfall-Manager und Spezialisten für die Betriebskontinuität
  - Verantwortliche für die physische Sicherheit (z.B. Leiter von Produktionsstätten)
  - Betriebsrat / Personalrat
- Externe Parteien
  - Geschäftspartner, insbesondere in Business-to-Business-Zulieferer-Netzwerken
  - Aufsichtsbehörden

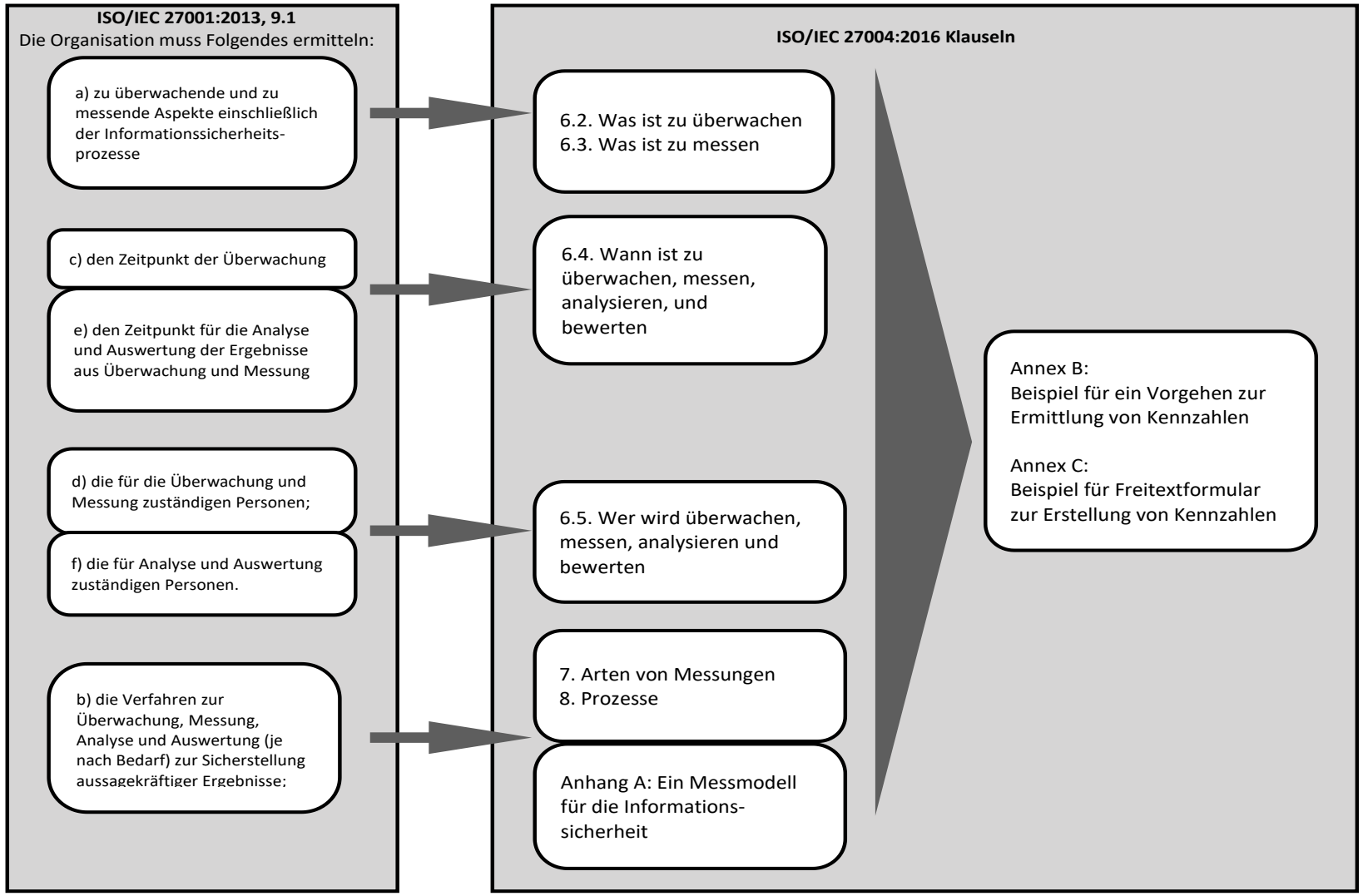
ISACA Germany Chapter

Der Blick auf Kennzahlenklassen aus Sicht von Galvanize (Auszug aus Vortrag ISACA USA Sep 2020)

INDICATOR METRIC	WHAT DOES IT MEASURE?	WHAT'S THE PURPOSE?	WHO'S THE AUDIENCE?
Key performance indicator (KPI)	KPIs measure how effectively the organization is achieving its business objectives.	They provide directional insight on how you're progressing toward strategic objectives, or the effectiveness of specific business processes or control objectives.	**Strategic KPIs** Most often executive management and the board. **Operational KPIs** Most often managers, operational process owners, and department heads.
Key risk indicator (KRI)	KRIs measure how risky certain activities are in relation to business objectives.	They provide early warning signals when risks (both strategic and operational) move in a direction that may prevent the achievement of KPIs.	**Strategic KRIs** Most often executive management and the board. **Operational KRIs** Most often managers, operational process owners, and department heads.
Key control effectiveness indicator (KCI)	KCIs measure how well controls are working.	They provide direct insight into a specific control activity, procedure, or process that wasn't implemented or followed correctly.	Most often front-line control activity owners.

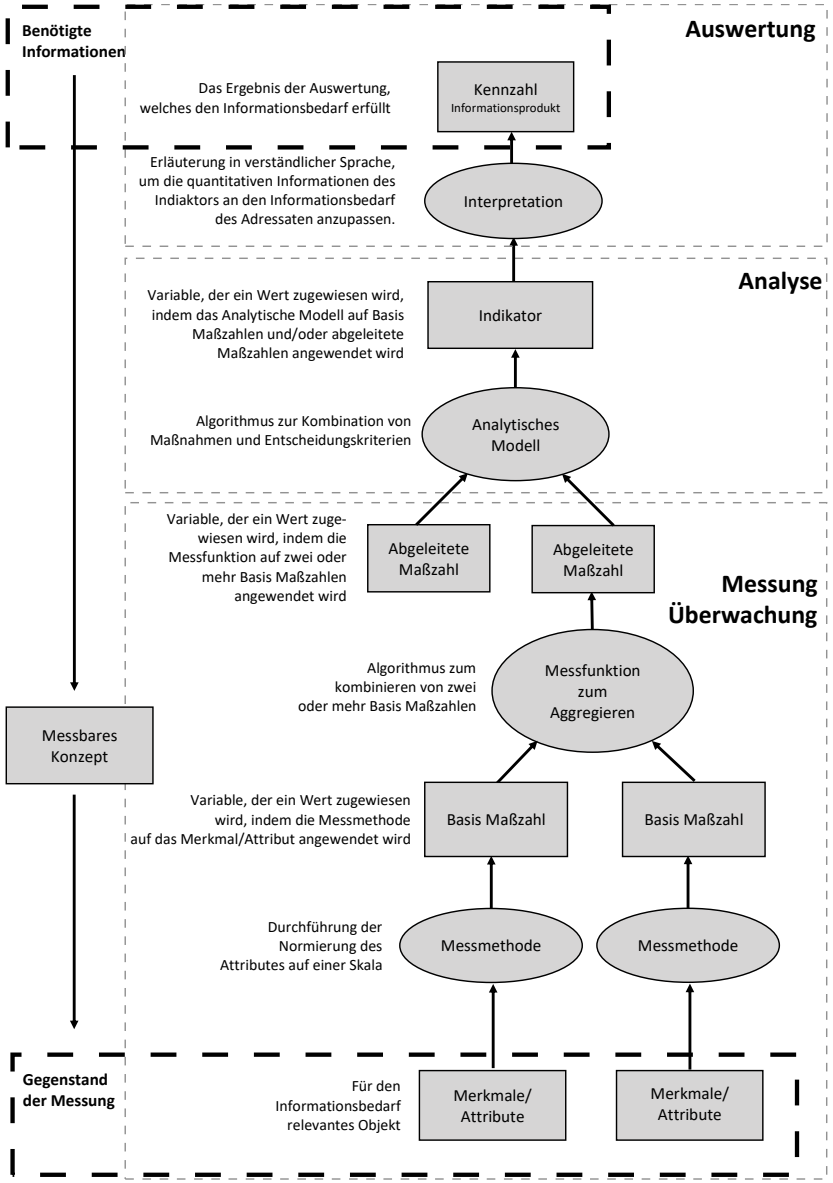
ISACA Germany Chapter

Sinnvoller Aufbau von Kennzahlen ISO/IEC 27004:2016



ISACA Germany Chapter

Messmodell nach ISO27004:2016



ISACA Germany Chapter

ISO 27004:2016 Annex B Auszug der 35 Beispiele

Related ISMS processes and controls (Clause or control number in ISO/IEC 27001:2013)	Measurement construct example names
5.1, 7.1	B.2 Resource allocation
7.5.2, A.5.1.2	B.3 Policy review
5.1, 9.3	B.4 Management commitment
8.2, 8.3	B.5 Risk exposure
9.2, A.18.2.1	B.6 Audit programme
10	B.7 Improvement actions
10	B.8 Security incidents cost
10, A.16.1.6	B.9 Learning form information security incidents
10.1	B.10 Corrective action implementation
A.7.2	B.11 ISMS training or ISMS awareness
A.7.2.2	B.12 Information security training
A.7.2.1, A.7.2.2	B.13 Information security awareness compliance
A.7.2.2	B.14 ISMS awareness campaigns effectiveness
A.7.2.2, A.9.3.1, A.16.1	B.15 Social engineering preparedness

ISACA Germany Chapter

Beispiele von Kennzahlen aus ISO 27004:2016 Annex B

B.11 ISMS training or ISMS awareness

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To measure how many employees received an ISMS related awareness training and establish control compliance with the organization's information security policy
Measure	Percentage of employees having participated to an ISMS awareness training
Formula/scoring	I1 = [Number of employees who received ISMS training/number of employees who have to receive ISMS training] * 100 I2 = [Number of employees who renewed their ISMS training in the last year / number of employee in scope] * 100
Target	Green: if I1>90 and I2>50% otherwise Yellow: if I1>60% and I2>30% otherwise Red Red – intervention is required, causation analysis must be conducted to determine reasons for non-compliance and poor performance Yellow – indicator should be watched closely for possible slippage to Red Green – no action is required
Implementation evidence	Participation lists of all awareness trainings; count of logs/registries with ISMS training field/row filler as "Received"
Frequency	Collect: Monthly, first working day of the month Analysis: Quarterly Report: Quarterly Measurement Revision: Review annually Period of Measurement: Annual
Responsible parties	Information owner: Training manager – Human resources Information collector: Training management – Human resource department Measurement client: Managers responsible for an ISMS, Chief information security officer
Data source	Employee database, training records, participation list of awareness trainings
Reporting format	Bar graph with bars colour-coded based on target. Short summary of what the measure means and possible management actions should be attached to the bar chart. OR Pie chart for current situation and line chart for compliance evolution representation.

Relationship ISO/IEC 27001:2013, A.7.2: Competence.

B.12 Information security training

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate compliance with annual information security awareness training requirement
Measure	Percentage of personnel who received annual information security awareness training
Formula/scoring	[Number of employees who received annual information security awareness training/number of employees who need to receive annual information security awareness training] * 100
Target	0-60% - Red; 60-90% - Yellow; 90-100% Green. For Yellow, if progress of at least 10% per quarter is not achieved, rating is automatically red. Red – intervention is required, causation analysis must be conducted to determine reasons for non-compliance and poor performance. Yellow – indicator should be watched closely for possible slippage to Red. Green – no action is required.
Implementation evidence	Count of logs/registries with annual information security awareness training field/ row filler as "Received"
Frequency	Collect: Monthly, first working day of the month Analysis: Quarterly Report: Quarterly Measurement Revision: Review annually Period of Measurement: Annual
Responsible parties	Information owner: Information security officer and Training manager Information collector: Training management – Human resource department Measurement client: Managers responsible for an ISMS; Security management; Training management
Data source	Employee database, training records
Reporting format	Bar graph with bars colour-coded based on target. Short summary of what the measure means and possible management actions should be attached to the bar chart.

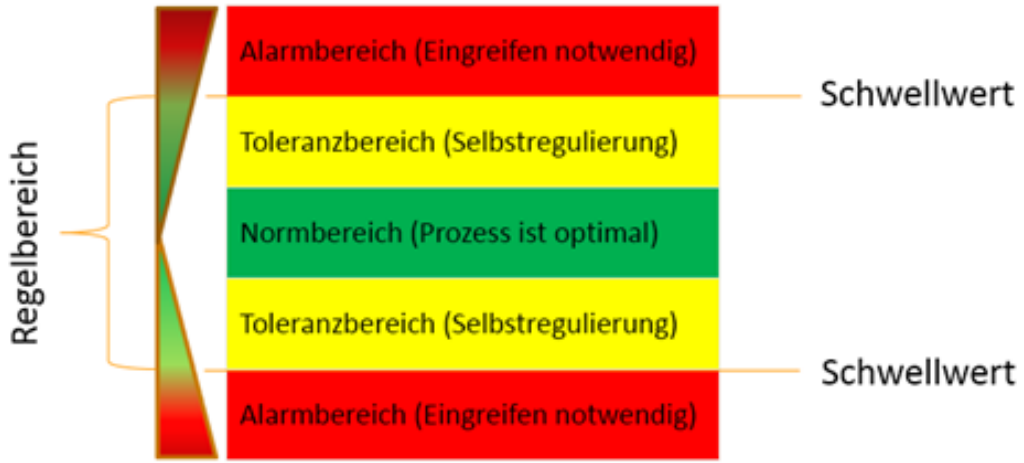
Relationship ISO/IEC 27001:2013, A.7.2.2: Information security awareness, education and training.

ISACA Germany Chapter

Steuerung durch Kennzahlen

„*Was man nicht messen kann, kann man nicht lenken.*“
(Zitat von Peter F. Drucker)

Die Steuerungsmaßnahmen müssen in der Lage sein, sowohl die Governance- und Compliance-Anforderungen der Organisation zu befriedigen als auch die vorhandenen Risiken der Organisation zu identifizieren und auf ein angemessenes Niveau zu senken.



ISACA Germany Chapter

Bewertung vorhandener Konzepte – VDA ISA / TISAX

VDA ISA / TISAX

Seit 2017 betreibt die ENX Association mit TISAX einen Prüf- und Austauschmechanismus für die Informationssicherheit von Unternehmen und ermöglicht eine gemeinsame Anerkennung von Prüfergebnissen zwischen den Teilnehmern. Dieser wird bereits von mehr als 1.200 Unternehmen in mehr als 40 Ländern eingesetzt. Grundlage für die Prüfungen ist der VDA-ISA-Fragenkatalog.

Der VDA hat für relevante Controls aus dem Fragenkatalog 20 Beispiel-KPIs für das Reporting definiert, die sich an den Annex A der ISO/IEC 27001:2013 anlehnen, allerdings ohne die Bewertung des ISMS selbst

ISACA Germany Chapter

Die VDA ISA Fragenkatalog KPIs

7.2 Sensibilisierung und Schulung der Mitarbeiter (Als Beispiel im nächsten Abschnitt)

9.2 Benutzerregistrierung

12.1 Änderungsmanagement

12.3 Schutz vor Schadsoftware

12.4 Informationssicherung (Back-Up)

12.7 Verfolgung von Schwachstellen (Patch Management)

16.2 Bearbeitung von Informationssicherheitsvorfällen

5.1 Informationssicherheitsrichtlinie

6.2 Informationssicherheit in Projekten

6.3 Mobile Endgeräte

11.1 Sicherheitszonen

11.3 Schutzmaßnahmen im Anlieferungs- und Versandbereich

12.5 Event-Logging

12.6 Protokollierung Administrationstätigkeiten

12.8 Systemaudits

13.2 Netzwerkdienste

13.5 Geheimhaltungsvereinbarungen

14.1 Anforderungen an die Beschaffung von Informationssystemen

14.2 Sicherheit im Software-Entwicklungsprozess

18.4 Wirksamkeitsprüfung

ISACA Germany Chapter

Beispiel VDA ISA KPI Steckbrief

Control	7.2 Sensibilisierung und Schulung der Mitarbeiter	
VDA-ISA Zielreifegrad	4	
Bereich	ABDECKUNG	EFFEKTIVITÄT
ID	Abdeckungsgrad Awareness-Maßnahmen	Effektivität von Awareness-Maßnahmen
Beschreibung	Sensibilisierte Mitarbeiter stellen eine wichtige Säule für die Informationssicherheit im Unternehmen dar. Awareness-Maßnahmen sollten möglichst alle Mitarbeiter erreichen. Der KPI misst den Abdeckungsgrad von Schulungen, wie z.B. E-Learnings, Präsenz-Trainings.	Die Inhalte von Awareness-Maßnahmen sollten Erkenntnisse aus Informationssicherheitsvorfällen berücksichtigen. Der KPI misst die Effektivität von Awareness-Maßnahmen durch eine Erfassung (Anzahl- oder Kosten-bezogen) der Sicherheitsvorfälle mit menschlichen Fehlhandlungen als Ursache.
Ziel (Vision)	Alle Mitarbeiter sind hinsichtlich Informationssicherheit geschult.	Keine Informationssicherheitsvorfälle mit menschlichem Fehlverhalten als Ursache.
Adressaten / Empfänger	Informationssicherheit, Vorgesetzte	Informationssicherheit
Frequenz (Reporting)	individuell zu bestimmen (z.B. jährlich)	individuell zu bestimmen (z.B. jährlich)
Schwellwerte	individuell zu bestimmen (z.B. Grün: > 90%, Gelb: 70-90%, Rot: < 70%)	individuell zu bestimmen (0-20…gering, 20-50 mittel, 50+ hoch) mögliche Ausprägung zur Vergleichbarkeit von Unternehmenseinheiten: Bezug auf Mitarbeiteranzahl z.B. Einheit: Vorfälle/100 MA
Messung	Auswertung Schulungsmanagement Quotient: Anzahl Teilnehmer / Gesamtzahl der Mitarbeiter	Erhebung der Anzahl von Sicherheitsvorfällen mit menschlichem Fehlverhalten als Ursache
Frequenz (Messung)	individuell zu bestimmen (z.B. jährlich)	individuell zu bestimmen (z.B. jährlich)
Schnittstellen	HR - Schulungsabteilung - IKS - Interne Revision	Incident Management
Komponenten	E-Learnings, Präsenzschulungen, Schulungsplan, Schulungsregister	Incident Mgmt. Tool, Ticket System, ISMS-Tool
Datenarchivierung	5 Jahre	5 Jahre

ISACA Germany Chapter

Bewertung vorhandener Konzepte – PRAGMATIC

PRAGMATIC ist ein praxisorientierter, in Buchform veröffentlichter Ansatz zur Erstellung von Informationssicherheits-Metriken. Zunächst erfolgt eine detaillierte Darlegung der Vorteile, der Gründe für die Erhebung sowie der unterschiedlichen Zielgruppen für Informationssicherheits-Metriken. Hierbei wird auch ein ausführlicher Blick auf verschiedene Quellen von Informationssicherheits-Metriken geworfen, u.a. das Business Model for Information Security (BMIS) der ISACA, das Capability Maturity Model (CMM), die ISO/IEC 27004:2016 und die Veröffentlichungen des National Institute of Standards and Technology (NIST).

Erfolgsfaktoren aus der Praxis

Vier Schritte zum Erfolg beim Aufbau eines IS-Kennzahlensystems

1. Definition von messbaren ISMS Zielen
2. Konkrete Kennzahlen und Schwellwerte
3. Überprüfung der Effektivität der definierten Steuerungsmasnahmen
4. Überprüfung des Zielerreichungsgrad und der Auswirkung auf die Risikoreduktion (Siehe Anhang A des Leitfadens)

ISACA Germany Chapter

Erfolgsfaktoren aus der Praxis

Funktionale Datenquellen für Indikatoren bzw. Metriken

- **Technische Systeme: SIEM, AV, Patch MGT, Firewalls**
- **Tools/Werkzeuge: IAM, Service MGT, HR**
- **Berichte: Revision, Pentest, Audits**

ISACA Germany Chapter

Erfolgsfaktoren aus der Praxis

Angemessene Anzahl Kxls im Reporting

Wenn ich vorhabe, 1-3 Dinge zu tun, werde ich 1-3 Dinge erreichen.

Wenn ich vorhabe, 4-10 Dinge zu tun, könnte ich 1 oder 2 erreichen.

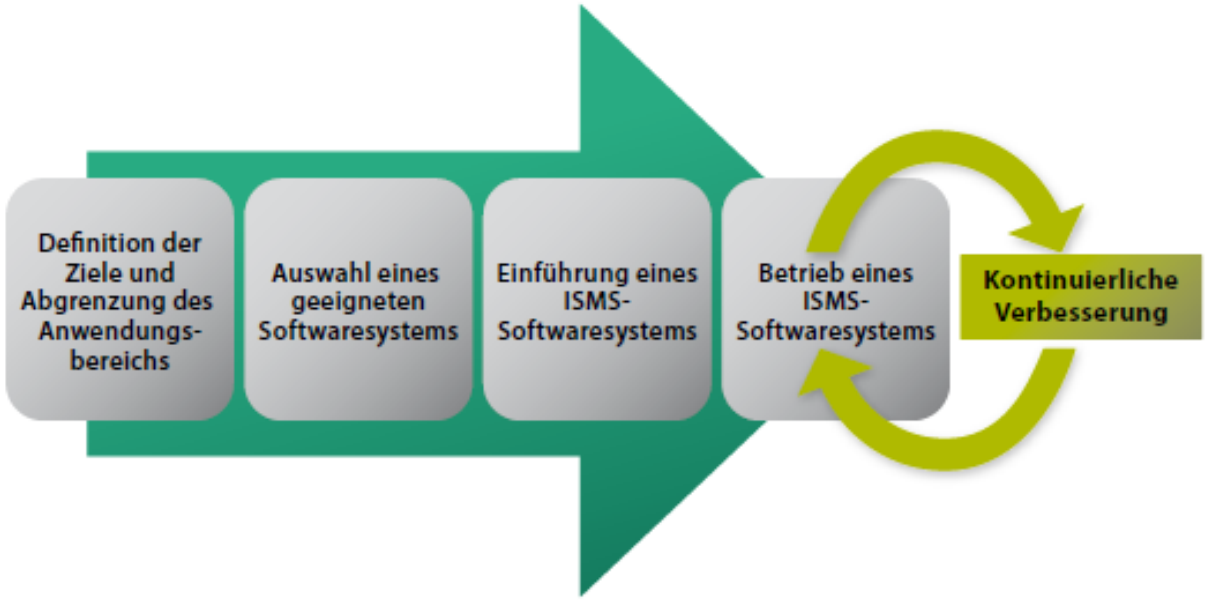
Wenn ich vorhabe, mehr als 10 Dinge zu tun, werde ich nichts erreichen.

ISACA Germany Chapter

Erfolgsfaktoren aus der Praxis

ISMS-/SIEM-Tools können eine große Hilfe sein

…..oder die “Hölle auf Erden”



ISACA Germany Chapter

Praxisleitfaden Anhang A:

Wir haben die ultimative Antwort gefunden!

ISO 27004:2016 ist gut mit 35 Kennzahlen, aber wir haben 42!

- Weit über 100 Vorschläge für KxI´s wurden in der Fachgruppe erarbeitet
- Daraus haben wir die 42 “besten” ausgewählt als Anlage zu unserem Leitfaden mit dem Mapping auf die ISO 27001 Controls und der Kennzahlklasse
- Ein wichtiges Kriterium war hierbei auch die Umsetzbarkeit im Mittelstand, ohne SOC, IRT und Co

ISACA Germany Chapter

Danksagung

An die Arbeitsgruppe:

Holger Schrader, Andrea Rupprich, Andreas Kirchner, Michael Schmidt, Nico Müller, Nikolay Jeliazkov

Unseren Lektoren:

Julia Hermann, Angelika Holl, Melanie Holtz und Dr. Tim Sattler

Und natürlich dem gesamten ISACA Vorstand dafür, dass wir uns hier ehrenamtlich einbringen durften ☺

ISACA
Germany Chapter