MESSBARKEIT VON SECURITY

DOK FORUM 2023

Adrian Kraus

Cybersecurity Consultant

Damovo Deutschland GmbH & Co. KG

DAMOVO

© Damovo. All rights reserved

Messen? Tun wir doch!

BKA-Lagebild für 2022

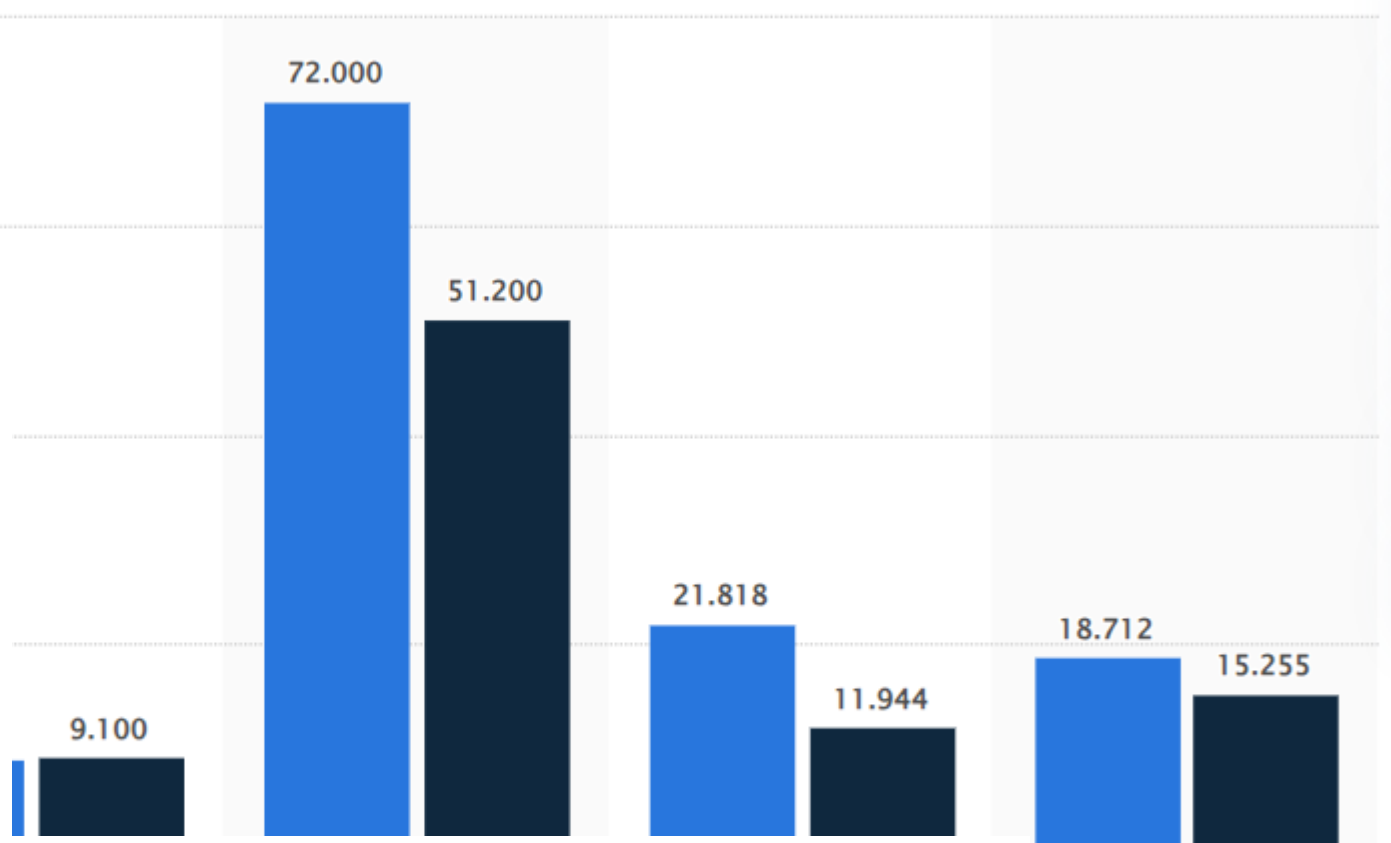
136.865 Fälle vor

Stand: 16.08

Was die BK
ist schon b
2022. Gera

USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15%

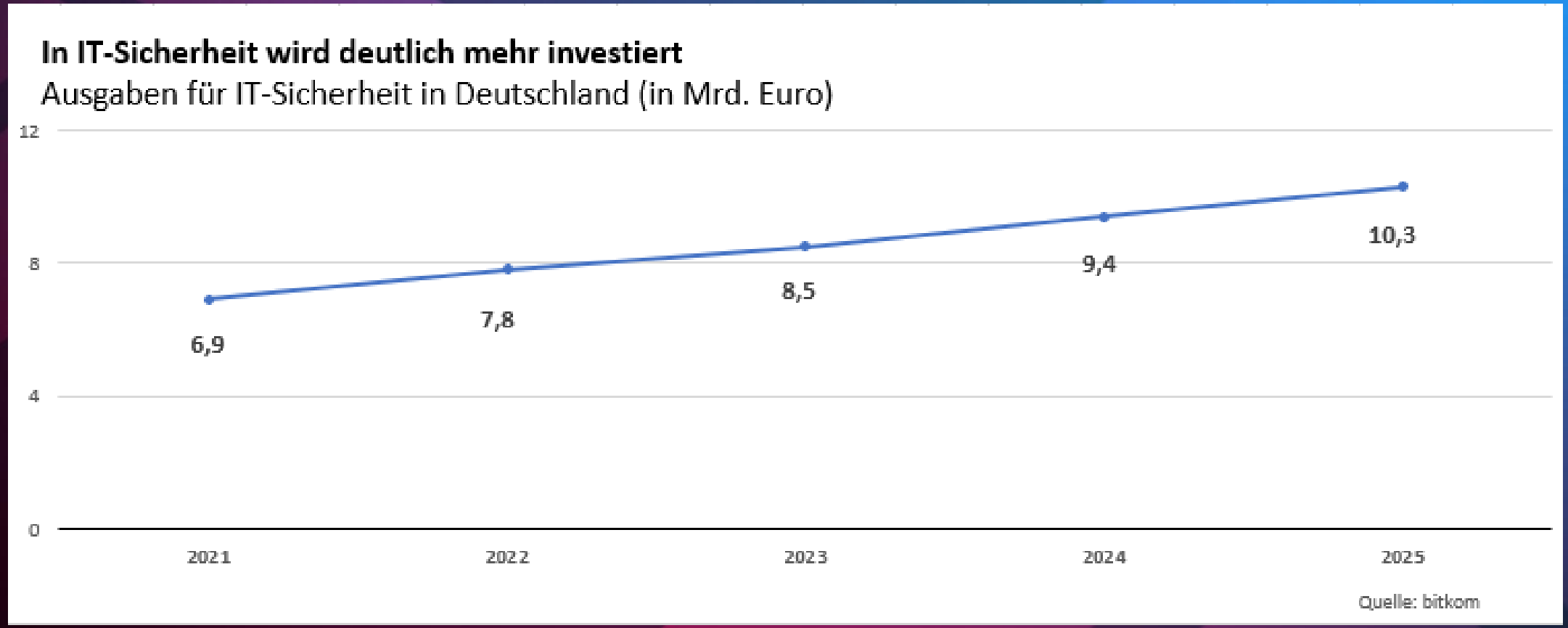


Cybercrime To Cost The World $10.5 Trillion Annually By 2025

© Damovo. All rights reserved

Was tun wir dagegen?

Wir investieren – und messen die Ausgaben



© Damovo. All rights reserved

Zusammenfassung?

Die Angreifer greifen an

- Es wird gemessen.

Die Verteidiger verteidigen

- Es wird gemessen.

Die Angreifer greifen noch viel mehr

- Es wird gemessen.

Die Verteidiger verteidigen noch viel mehr

- Es wird gemessen.

Und so weiter und so fort. Zu welchem Schluss führt uns das?

Die Angriffe gehen wohl an unserer Verteidigung vorbei

© Damovo. All rights reserved

Fragen, über die wir regelmäßig diskutieren

Auch diese lassen sich mit *Messbarkeit* beantworten.

Sind wir sicher?

Was kostet Security?

Wo sind wir besonders stark?

Wo sind wir besonders schwach?

Was ist unsere größte Sicherheitslücke?

Investieren wir in die richtige Sache?

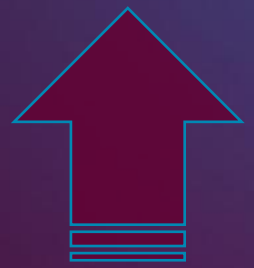
Erfüllen wir gesetzliche Vorgaben?

Tun wir die richtigen Dinge? Tun wir die Dinge richtig?

© Damovo. All rights reserved

Der Alltag in der Welt der Sicherheit

BOTTOM-UP APPROACH



© Damovo. All rights reserved

Warum schützen wir uns überhaupt?

Cybersecurity

=

Risikobehandlung

© Damovo. All rights reserved

Ausflug ins Risikomanagement

Grundlegende Fragen

Welche sind unsere kritischen Prozesse?

Was sind unsere wichtigsten Assets?

Welche Daten werden von diesen Assets verarbeitet?

Wie lange dürfen diese Assets nicht zur Verfügung stehen?

Wer greift auf diese Daten zu?

Was passiert, wenn jemand diese Daten ändert?

Welches Risiko sind wir bereit zu akzeptieren?

Welches Risiko wollen oder müssen wir komplett vermeiden?

Welches Risiko wollen wir verringern oder auslagern?

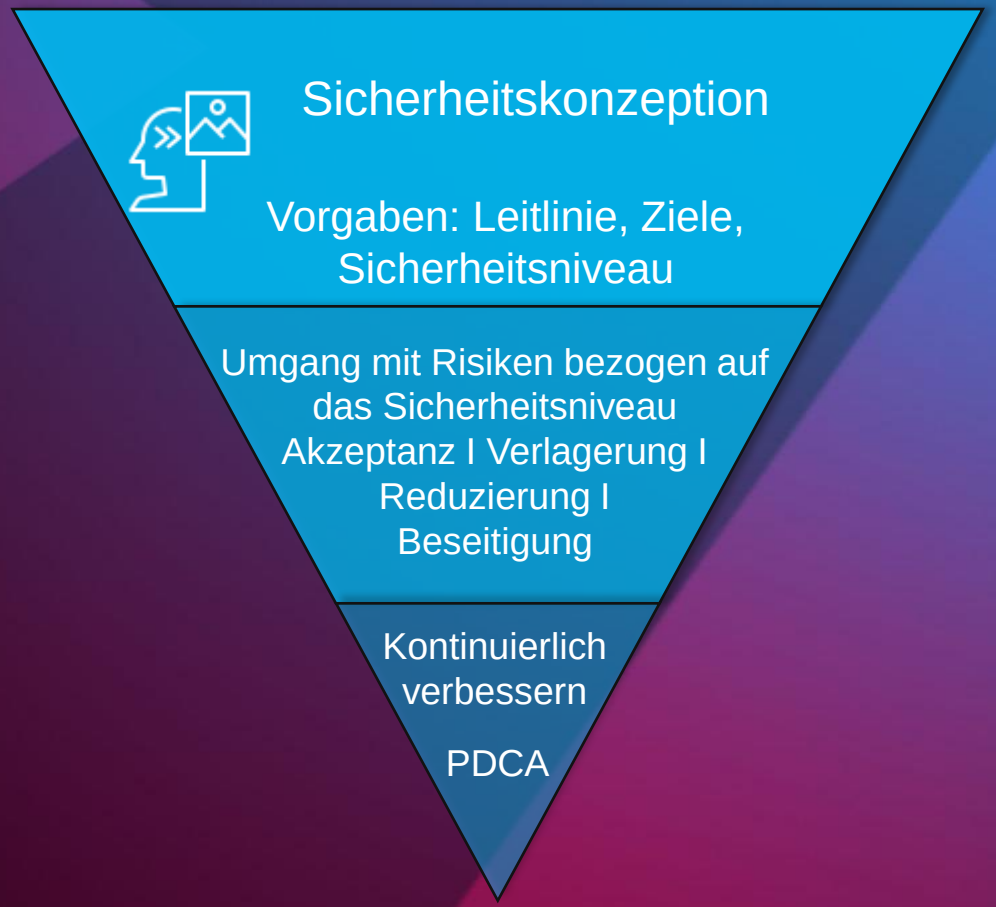
© Damovo. All rights reserved

Beispiel einer Risikomatrix

existenzbedrohend	Mittel	Hoch	Sehr hoch
beträchtlich	Gering	Mittel	Hoch
begrenzt	Information	Gering	Mittel
Schadensausmaß Eintrittswahrscheinlichkeit	Selten	Manchmal	Häufig

© Damovo. All rights reserved

Ist das der bessere Weg?



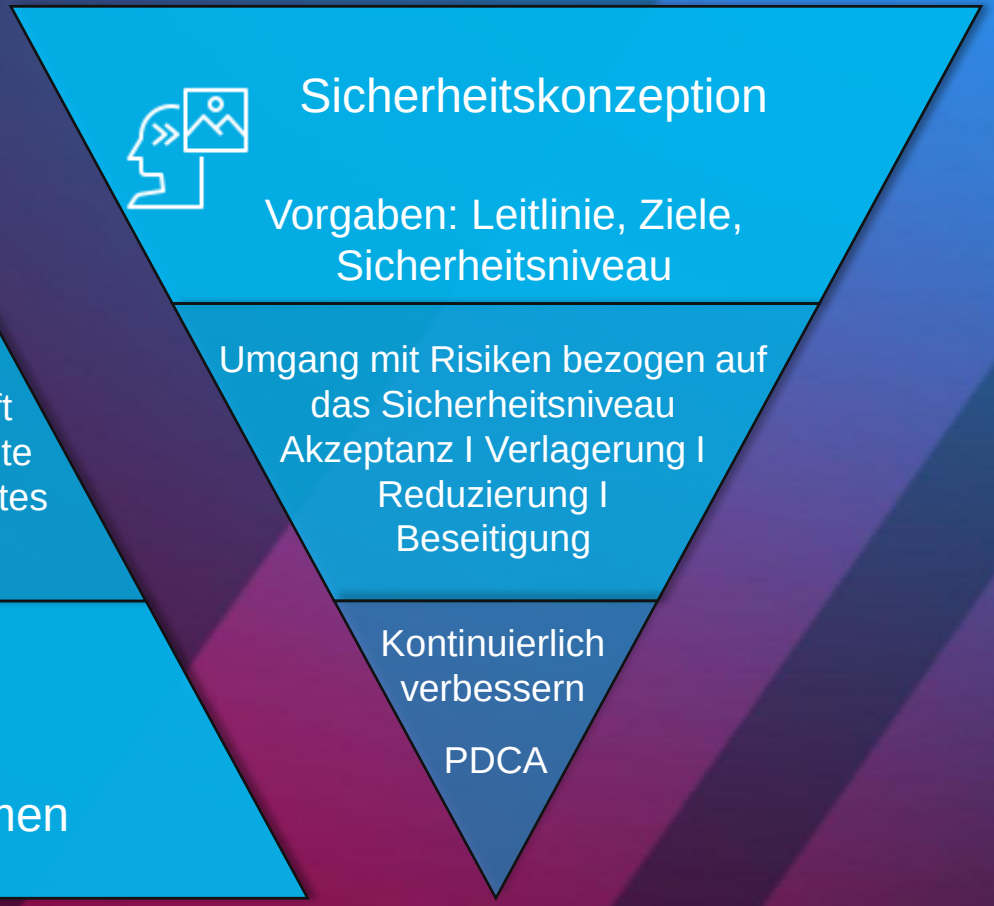
TOP-DOWN APPROACH

DAMOVO

© Damovo. All rights reserved

BOTTOM-UP und TOP-DOWN

BOTTOM-UP APPROACH



TOP-DOWN APPROACH

© Damovo. All rights reserved

Ein Blick in die Normen und Standards

ISO27001/27035 – Risk Management & Monitoring, measurement, analysis and evaluation

“The organization shall define and apply an information security risk assessment process that:

- establishes and maintains information security risk criteria
- ensures that repeated information security risk assessments produce consistent, valid and comparable results;
- identifies the information security risks;
- analyses the information security risks;
- evaluates the information security risks;”

“The organization shall determine:

- what needs to be monitored and measured, including information security processes and controls
- the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;
- (…)“

© Damovo. All rights reserved

Ein Blick in die Normen und Standards

Bundesamt für Sicherheit in der Informationstechnik

- Das BSI hat mit dem Dokument 200-3 einen eigenen Standard zum Risikomanagement hervorgebracht.
- Beispiele für Kennzahlen:

1 Beispiele für Kennzahlen

Kurz-bezeichnung	Ziel der Messung	Kennzahl/Formel	Zielobjekt, Wo-ran wird gemes-sen/analysiert? (Objekt/Prozess)	Art der Kenn-zahl (Umsetzung, Wirksamkeit)	Anwendungszweck bzw. Erkenntnisse aus der Kennzahl
U-Dokumen-tenaktualität	Bestimmung der Aktualität der BCM-Dokumenta-tion	Anzahl aktueller BCM-Dokumente gemäß den Vorgaben der Dokumen-tenlenkung/Gesamtzahl aller BCM-Dokumente	BCM-Dokumente (Prozessbeschrei-bungen, Ergebnis-objekte, Pläne)	Umsetzung	Wurden alle Dokumente bis zum vorgege-benen Datum aktualisiert? Wurde das Dokument bei einer Sachände-rung (z. B. Reorganisation, Prozessent-wicklung, Änderung der Zuständigkeiten) aktualisiert?
U-Dokumen-tenkonformi-tät	Einhaltung der Vorgaben zur BCM-Dokumentation	Anzahl als vollständig bewerteter Dokumente/Anzahl geprüfter Doku-mente	BCM-Dokumente (Prozessbeschrei-bungen, Ergebnis-objekte, Pläne)	Umsetzung	Entspricht der Aufbau der BCM-Doku-mente der jeweiligen Dokumentenvor-lage oder der üblichen Struktur dieses Do-kumententyps (z. B. Gliederung)? Ist der Umfang und Detaillierungsgrad der Dokumente angemessen?
W-Dokumeen-tenverständ-lichkeit	Verbesserung der Verständlichkeit der BCM-Doku-mentation	Anzahl als verständlich bewerteter Dokumente/Anzahl geprüfter Doku-mente	BCM-Dokumente (Prozessbeschrei-bungen, Ergebnis-objekte, Pläne)	Wirksamkeit	Ist das Dokument für einen fachkundigen Anwender verständlich?
W-Dokumen-tenkonsistenz	Sicherstellung der Konsistenz der BCM-Dokumenta-tion	Anzahl als konsistent bewerteter Do-kumente/Anzahl geprüfter Doku-mente	BCM-Dokumente (Prozessbeschrei-bungen, Ergebnis-objekte, Pläne)	Wirksamkeit	Sind die Daten innerhalb der BCM-Doku-mente konsistent? (Genauigkeit und Wi-derspruchsfreiheit)

Wie also helfen Normen und Standards?

Leider kaum. Deswegen ein paar Ideen aus der Praxis:

Scope definieren und innerhalb dieses Scopes Sichtbarkeit schaffen!

Messbarkeit des Schadens

- Wie hoch wäre der Schaden für unsere Assets und damit für unser Unternehmen?
- Welcher Schaden kann akzeptiert werden?
- Wie verändert sich der Schaden, wenn wir Maßnahmen dagegen setzen?

Messbarkeit der Maßnahmen

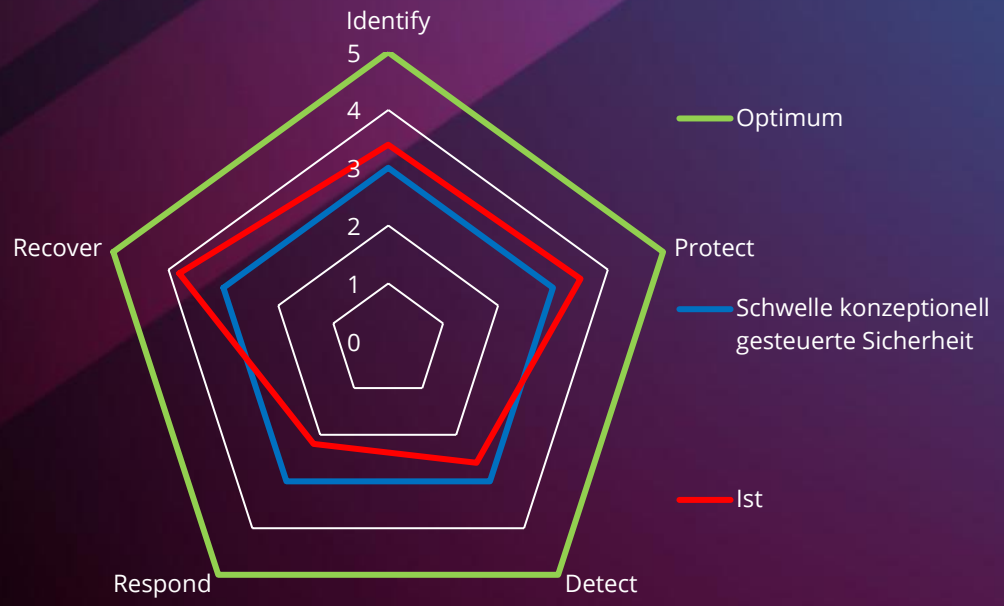
- Wie viele Assets werden von unseren Maßnahmen geschützt?
- Zu welchem Grad werden die beschlossenen Maßnahmen umgesetzt?
- Halten die Maßnahmen ein, was sie versprochen haben?

Die Messungen müssen permanent durchgeführt werden und mit dem Management besprochen werden.

© Damovo. All rights reserved

Beispiel einer umfassenden Messung der Security

NIST-Security Framework V1.1



Cyber-Security Fähigkeit	Bewertung
Identify	3,4
Protect	3,5
Detect	2,6
Respond	2,2
Recover	3,8

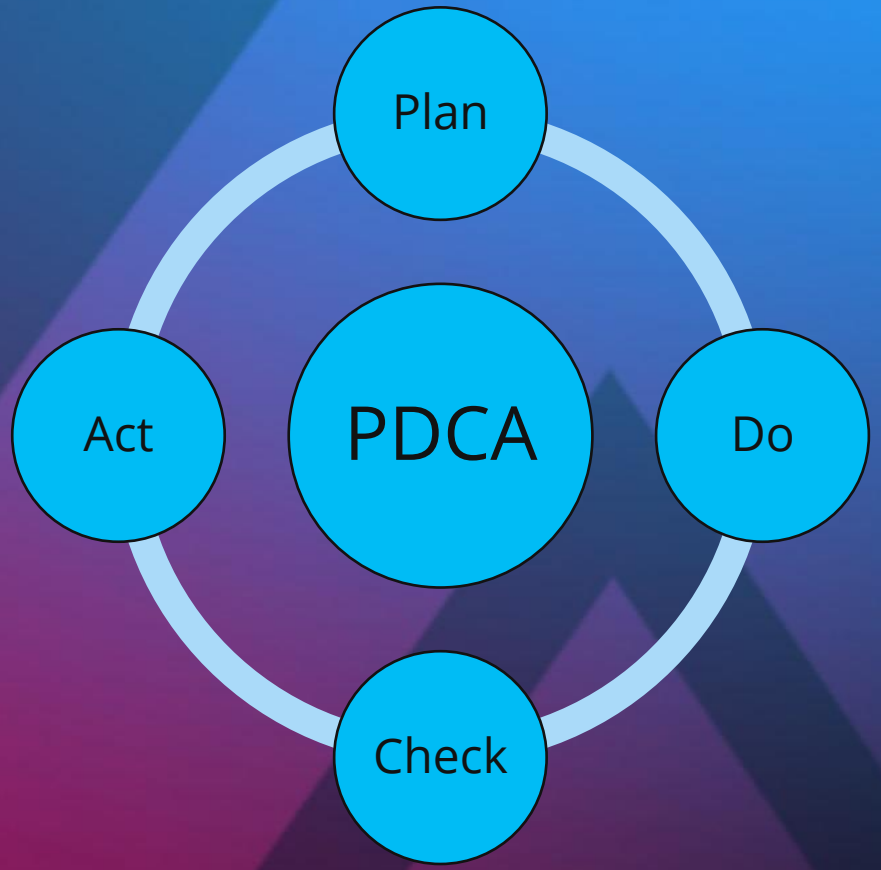
Referenz	Bewertung
Fähigkeit nicht vorhanden	0
Fähigkeit geplant, aber nicht umgesetzt	1
Fähigkeit teilweise umgesetzt	2
Fähigkeit umgesetzt und dokumentiert	3
Fähigkeit gesteuert, umgesetzt, geprüft und verbessert – aber mit (bekanntem) Verbesserungspotenzial	4
Fähigkeit auf optimalem Stand	5

DAMOVO

© Damovo. All rights reserved

Kontinuierlicher Verbesserungsprozess

- Messungen kontinuierlich durchführen und bei Maßnahmen gegensteuern, wenn sich die KPI's nicht verbessern.
- Nicht nur die Messungen selbst im Auge behalten, sondern auch prüfen, ob wir überhaupt noch das Richtige messen.
- Regelmäßiger Austausch mit den Risiko-Trägern – in der Regel die Geschäftsführung



DAMOVO

© Damovo. All rights reserved

Noch ein paar Tipps vor dem Abendessen

Messungen bieten die Fakten, auf die wir unsere Entscheidungen fußen lassen können.

Das Risikomanagement dient der Entscheidungsfindung. Die Messungen zeigen, ob wir auf dem richtigen Weg sind.

Maßnahmen zu definieren, ohne auch nur einen Gedanken an den Sicherheitsprozess zu verschwenden, wird schiefgehen – oder zumindest schräg verlaufen.

Seien Sie bei den Vorgaben der Messungen/KPI konkret. Sie lassen sich im Laufe des KPI noch immer anpassen, wenn sie ihren Zweck nicht erfüllen.

Der Genuss von Wein beim Abendessen wirkt sich auf die körperliche und geistige Verfügbarkeit beim Frühstück aus. Maßnahmen zur Risikominimierung und zur *Incidence Response* erhalten Sie in der Apotheke.

© Damovo. All rights reserved

VIELEN DANK!

DAMOVO

© Damovo. All rights reserved