TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-interner Workshop

Berlin, 25.06.2026

Ein standardübergreifendes Reifegradmodell für Cyberresilienz

Svenja Mischur, APT GmbH | Advanced Prevention Time

Wir haben genug Standards.
Aber keine gemeinsame Messbarkeit.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Organisationen investieren in Cybersecurity.
- Aber sie können Fortschritt kaum objektiv vergleichen.

THE CYBER KILL CHAIN®
LOCKHEED MARTIN

Swift

D3FEND™

NIST SP 800-171 Rev. 2
NIST SP 800-53 Rev. 5

DORA - Digital Operational Resilience Act

TISAX

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

ATT&CK®

SAMM

CIS Critical Security Controls®

Federal Office for Information Security
Cloud Computing (C5)

ISO/IEC 27001 – Informationssicherheits-Managementsystem (ISMS)
ISO/IEC 27002 – Maßnahmenkatalog (Controls)
ISO/IEC 27005 – Risikomanagement
ISO/IEC 22301 – Business Continuity Management (Resilienz-Aspekt!)
ISO/IEC 27701 – Datenschutz-Erweiterung

IT-Grundschutz-Kompendium –
Werkzeug für Informationssicherheit

Edition 2023

CSMS

Das eigentliche Problem.

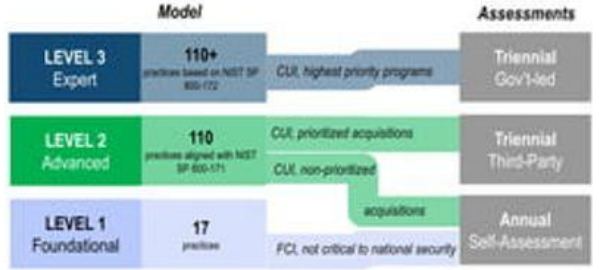
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

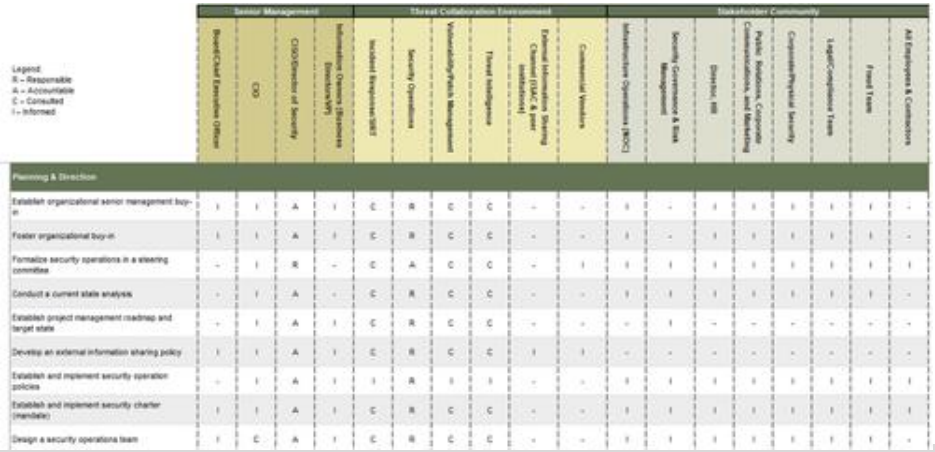
Cybersecurity ist überstandardisiert und unterintegriert

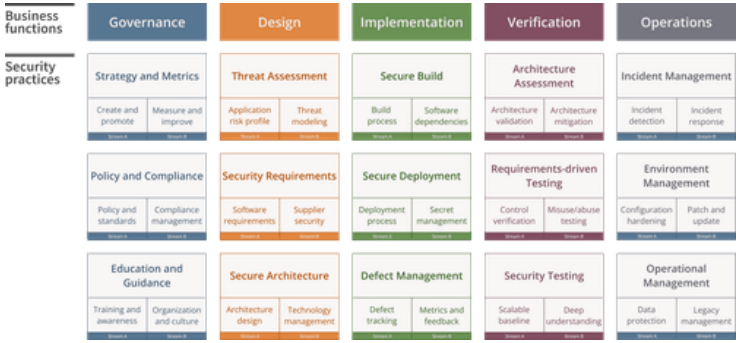
- zahlreiche Frameworks und Modelle
- unterschiedliche Logiken und Bewertungsansätze
- fehlende Vergleichbarkeit

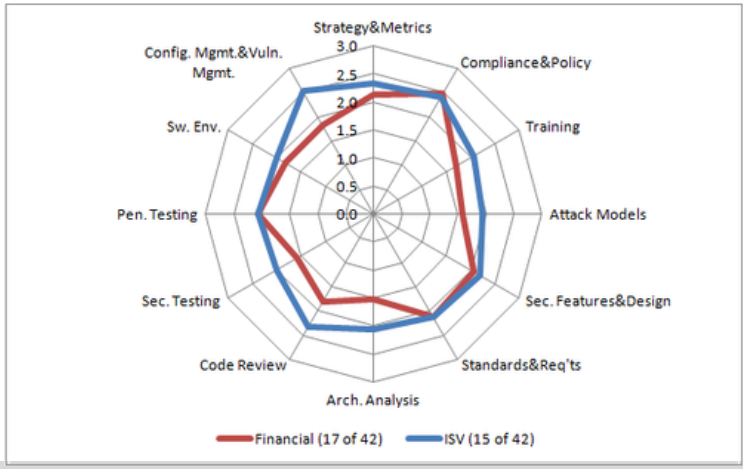
Ergebnis:

- Jede Organisation bewertet sich in ihrem eigenen System.









Der blinde Fleck.

Selbst Reifegradmodelle lösen das Problem nicht

- C2M2 (organisationales Reifegradmodell)
- BSIMM (empirisches Software-Security-Modell)
- OWASP SAMM (Software-Sicherheit)
- CMMC (Zertifizierungsmodell mit Reifegradstufen)

Fokus: Bewertung und Entwicklung von Fähigkeiten

- unterschiedlich aufgebaut
- auf einzelne Bereiche begrenzt
- nicht kompatibel

Cybersecurity Maturity Model Certification 2.0 Program

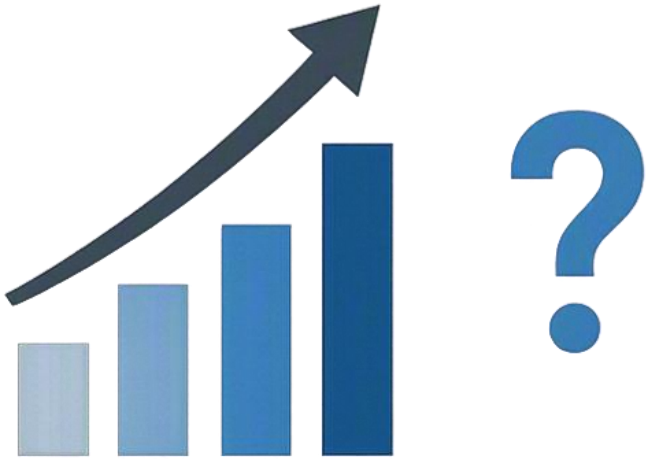
Es gibt keinen gemeinsamen Maßstab.

C2M2 | Cybersecurity Capability Maturity Model

Cyberresilienz bleibt schwer steuerbar

- Fortschritt ist schwer messbar
- Vergleiche sind kaum möglich
- Entscheidungen basieren oft auf Annahmen

Wir messen Aktivitäten – aber nicht Reife.

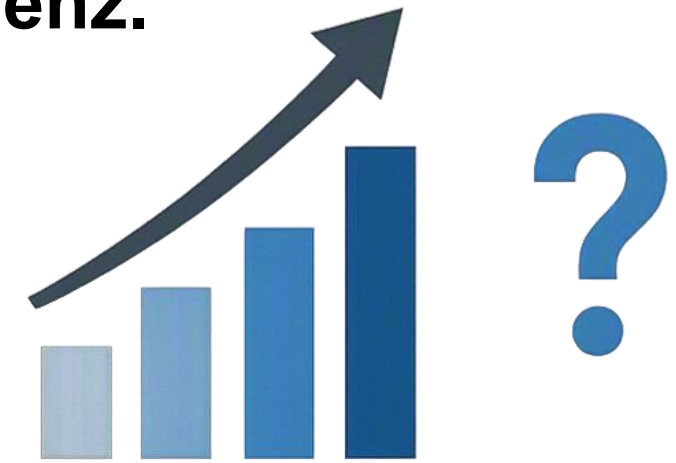


Die Idee.

Ein standardübergreifendes Reifegradmodell

- bestehende Frameworks verbinden, nicht ersetzen
- eine gemeinsame Bewertungslogik schaffen
- Reifegrade messbar und vergleichbar machen

Ein gemeinsamer Bezugsrahmen für Cyberresilienz.

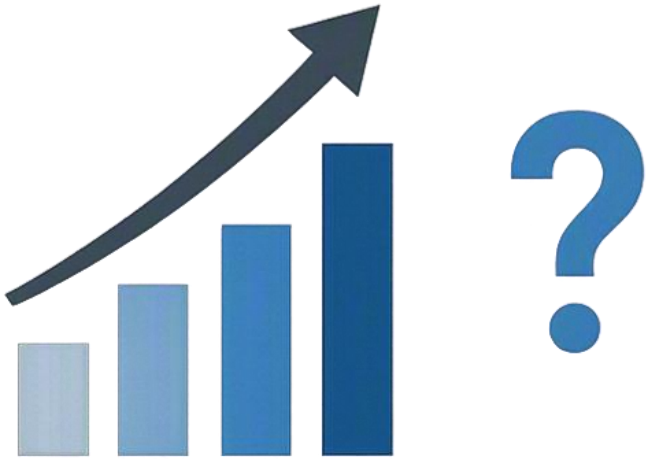


Der Ansatz.

Ein verbindender Bewertungs-Layer

- Integration bestehender Standards
- Mapping auf eine gemeinsame Struktur
- einheitliche Reifegradlogik
- Scoring-Modell entwickeln
- Grundlage für Benchmarking

Eine Art gemeinsame Sprache für Cyberresilienz.



Call to Action.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Entwicklung eines ersten Modells
- iterative Validierung im Netzwerk

Ziel:

- Ein gemeinsamer, praxisnaher Standard für Reifegradmessung.