

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.

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

THE CYBER KILL CHAIN®

LOCKHEED MARTIN



D3FEND™

NIST SP 800-171 Rev. 2

NIST SP 800-53 Rev. 5

DORA - Digital Operational Resilience Act



ATT&CK®



CIS Critical Security Controls®



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



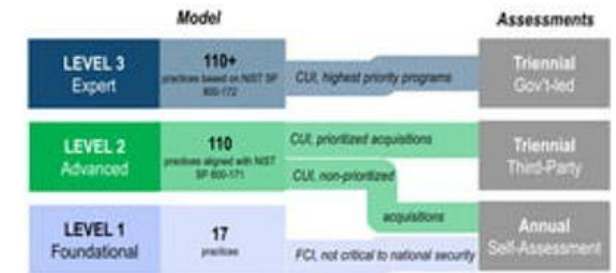
Das eigentliche Problem.

Cybersecurity ist überstandardisiert und unterintegriert

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

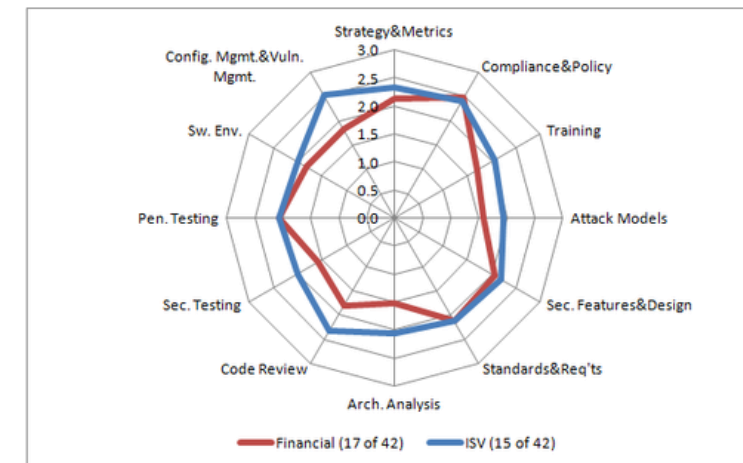
Ergebnis:

- Jede Organisation bewertet sich in ihrem eigenen System.



	Senior Management				Threat Collaboration Environment				Stakeholder Community				All Employees & Contractors			
	CEO	COO/Chief of Security	Chief Information Officer	Chief Security Officer	Incident Response Unit	Security Operations	Threat Intelligence	External Information Sharing Channel (CISAC & peer institutions)	Commercial Partners	Interagency Operations (JPOC)	Security Governance & Risk Management	Private Industry, Government Contractors, and Academia	Competitive/Physical Security	Target/Compromise Team	Front Lines	
Legend: R = Responsible A = Accountable C = Consulted I = Informed																
Planning & Direction																
Establish organizational senior management buy-in	I	I	A	I	C	R	C	C	-	-	-	-	-	-	-	-
Formalize security operations in a steering committee	-	I	R	-	C	A	C	C	-	I	I	I	I	I	I	I
Conduct a current state analysis	-	I	A	-	C	R	C	C	-	I	I	I	I	I	I	I
Establish project management roadmap and target state	-	I	A	I	C	R	C	C	-	-	-	-	-	-	-	-
Develop an external information sharing policy	I	I	A	I	C	R	C	C	-	I	I	I	I	I	I	I
Establish and implement security operation policies	-	I	A	I	R	I	I	-	-	I	I	I	I	I	I	I
Establish and implement security charter (mandatory)	I	I	A	I	C	R	C	C	-	I	I	I	I	I	I	I
Design a security operations team	I	C	A	I	C	R	C	C	-	I	I	I	I	I	I	I

Business functions	Governance	Design	Implementation	Verification	Operations
Security practices	Strategy and Metrics Create and promote Measure and improve	Threat Assessment Application risk profile Threat modeling	Secure Build Build process Software dependencies	Architecture Assessment Architecture validation Architecture mitigation	Incident Management Incident detection Incident response
	Policy and Compliance Policy and standards Compliance management	Security Requirements Software requirements Supplier security	Secure Deployment Deployment process Secret management	Requirements-driven Testing Control verification Misuse/abuse testing	Environment Management Configuration hardening Patch and update
	Education and Guidance Training and awareness Organization and culture	Secure Architecture Architecture design Technology management	Defect Management Defect tracking Metrics and feedback	Security Testing Scalable baseline Deep understanding	Operational Management Data protection Legacy management



Selbst Reifegradmodelle lösen das Problem nicht



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

- unterschiedlich aufgebaut
- auf einzelne Bereiche begrenzt
- nicht kompatibel



Fokus: Bewertung und Entwicklung von Fähigkeiten



Cybersecurity Maturity Model Certification 2.0
Program

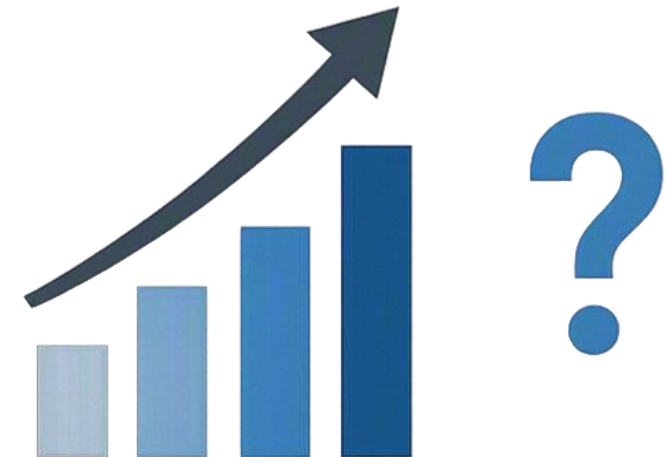
Es gibt keinen gemeinsamen Maßstab.



Cyberresilienz bleibt schwer steuerbar

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

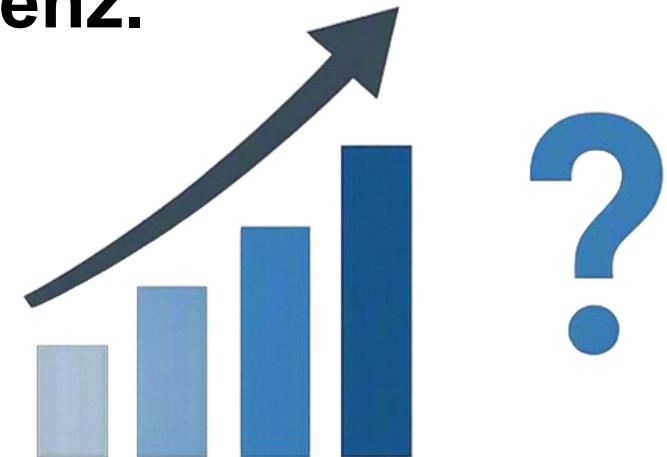
Wir messen Aktivitäten – aber nicht Reife.



Ein standardübergreifendes Reifegradmodell

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

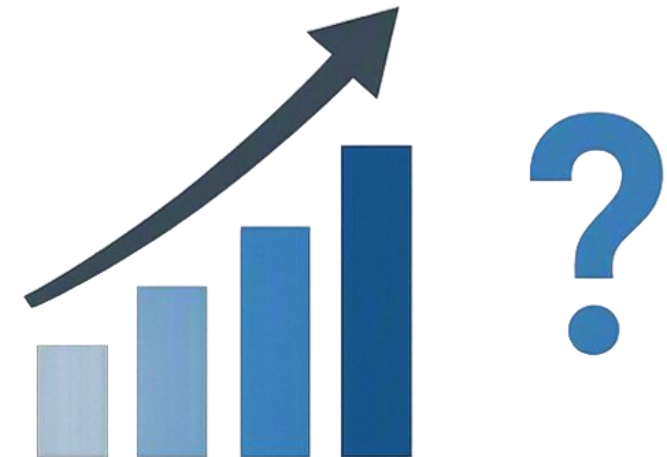
Ein gemeinsamer Bezugsrahmen für Cyberresilienz.



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.

- Entwicklung eines ersten Modells
- iterative Validierung im Netzwerk

Ziel:

- Ein gemeinsamer, praxisnaher Standard für Reifegradmessung.

