



# CYBERSECURITY- BY TAGUERI

SICHER IN DIE ZUKUNFT

MODEL:428

GMB

# Inhalt

Cybersecurity- und Software-Updates – Einführung	3
Unser Konzept – Überblick	4
Unser Konzept – Cybersecurity	6
Managementsysteme – IT-Grundschutz und Informationssicherheit	8
Cybersecurity im Produkt – FuSi, SOTIF, Safety	9
Quick Check und Risikomanagement	10
Anforderungsmanagement und Changemanagement	11
Projektmanagement	12
Prozessmanagement	13
IT-Management und Auditmanagement	15

## Cybersecurity- & Software-Updates – Einführung

# Cybersecurity

Im Zuge der digitalen Transformation ergeben sich immer wieder neue Anforderungen an die Industrie. Im Fokus neuer Normen, Regelungen und Gesetze steht der Bedarf nach einer erhöhten digitalen Sicherheit im Bezug auf Produkt und Unternehmensorganisation.

Bei immer komplexeren Strukturen in diesen Bereichen und durch die zunehmende Vernetzung der Infrastruktur im Unternehmen zeigen sich stetig neue Herausforderungen.

Die Frage nach einer Struktur in dieser Menge von neuen Anforderungen und Technologien bleibt meist unbeantwortet. Deshalb hat die Tagueri AG ein bausteinbasiertes Konzept entwickelt, um die Kernpunkte der Themen Cybersecurity- und Software-Updates anzugehen, welches wir jedem unserer Kunden individuell angepasst anbieten können.

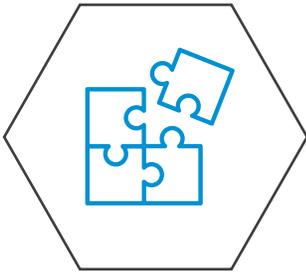
Aufbauend auf Anforderungen an die IT-Sicherheit und den IT-Grundschutz nach der ISO 27000 und BSI-Standards bieten wir Ihnen das Change-management für alle Anforderungen von TISAX bis UN-R155/UN-R156 (UNECE Managementsysteme) und ISO/SAE 21434. Der Anspruch der Tagueri AG geht dabei über die Aufnahme und Interpretation neuer Anforderungen hinaus. Wir betreuen Ihr Gesamtprojekt von der Konzeptionsphase bis zur Implementierung.

Uns liegt es am Herzen, mit Ihnen auf Augenhöhe Änderungen voranzutreiben und die Unternehmensstruktur nachhaltig zu optimieren. In dieser Informationsbroschüre stellen wir Ihnen deshalb unseren erprobten Best-Practice-Ansatz für die Umsetzung neuer Anforderungen in der Industrie vor, um Ihrem Unternehmen einen sicheren Start in die digitale Zukunft zu garantieren.



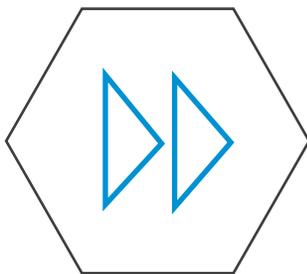
## Überblick

---



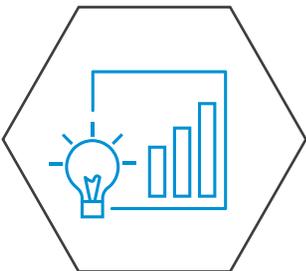
### Unser Ansatz

Kompetenzbausteine für  
Cybersecurity



### Unser Vorgehen

Praxiserprobtes  
Vorgehensmodell für eine  
erfolgreiche Umsetzung



### Unsere Expertise

Qualifizierte Projekte, Kooperationen und  
Partnerschaften für optimale Ergebnisse



## Unser Ansatz

---



Cybersecurity umfasst alle Bereiche eines Unternehmens – Vom einzelnen Mitarbeiter über die Unternehmensorganisation bis hin zu den Produkten oder Dienstleistungen.

Wir unterstützen Sie mit einem ganzheitlichen Ansatz, der nicht nur die Schulung und Unterweisung Ihrer Mitarbeiter umfasst, sondern genauso Ihre IT-Infrastruktur bis hin zu Ihren eigentlichen Umsatz- und Verkaufsargumenten.

Von einer gesamtheitlichen Betreuung der Analyse Ihrer Systeme und Organisationsstrukturen über die Absicherung Ihrer Produkte mit dem neuesten Stand der Technik und einschlägigen Safety-Anforderungen bis hin zu Awareness-Schulungen Ihrer Mitarbeiter und dem direkten Einfluss auf Ihren Geschäftserfolg sind wir Ihr Umsetzungspartner.

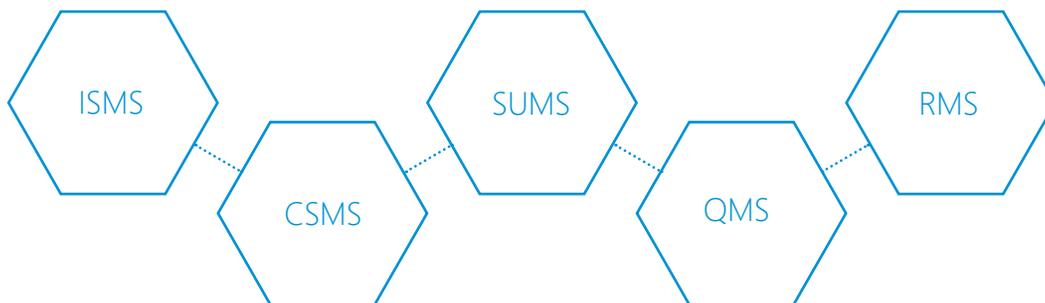
Für eine erfolgreiche Cybersecurity in Ihrer Systemlandschaft ist aufgrund einschlägiger Normen und Gesetze die Einführung sowie der Betrieb verschiedener Managementsysteme unerlässlich. Der ganzheitliche Schutz Ihrer Infrastruktur erfordert fünf grundlegende Managementsysteme, die wir Ihnen auf den folgenden Seiten kurz vorstellen möchten.

Darüber hinaus stellen wir Ihnen unsere Kompetenz im Bereich der Produktsicherheit vor, mit der wir eine Absicherung Ihrer relevanten Unternehmensbereiche gewährleisten.



# Managementsysteme

## IT-Grundschutz und Informationssicherheit



Ein Informationssicherheitsmanagementsystem stellt die Grundlage Ihrer Cybersecurity dar und sichert Daten vor unbefugten Zugriffen.

Ergänzt durch ein Cybersecurity- und Software-Update-Managementsystem erzeugen wir für Sie den Rahmen, zeitgemäße Over-the-Air-Updates, bei gleichzeitiger Maximierung der Traceability von Softwarepaketen und dazugehörigen Freigaben, sicherzustellen.

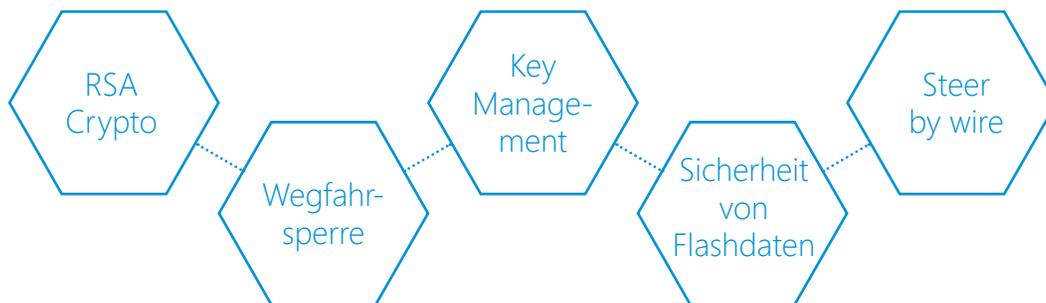
Das Qualitätsmanagementsystem gewährleistet gemeinsam mit dem Risikomanagementsystem eine Überwachung relevanter KPIs, mit der Sie Unternehmensrisiken frühzeitig erkennen, verfolgen und mit Maßnahmen belegen können, sodass sich die Eintrittswahrscheinlichkeit verringert und der wirtschaftliche Einfluss nachhaltig reduziert wird.

Durch die langjährige Erfahrung und eine hohe Abdeckung bei der Einführung und Betreuung verschiedener Managementsysteme in diversen Branchen bei namhaften Kunden sind wir immer umfassend über aktuelle Veränderungen an Normen und Gesetzen informiert.

Von diesem Know-how profitieren Sie aus erster Hand bei der Notwendigkeitsprüfung, GAP-Analyse und Umsetzung der unterschiedlichen Managementsysteme.

# Cybersecurity im Produkt

## FuSi, SOTIF, Safety



Cybersecurity umfasst sowohl Aspekte der Unternehmensorganisation als auch produktbezogene Aspekte.

Mit einer Vielzahl moderner Technologien und Schutzmechanismen bieten wir Ihnen verschiedene Services, die zusätzlich zur Absicherung Ihrer Organisationsstrukturen durch Managementsysteme eine umfassende Produktsicherheit generieren.

Die Absicherung Ihrer Produkte spielt eine entscheidende Rolle. Der Schutz Ihrer Kundendaten sichert Ihren langfristigen und nachhaltigen Unternehmenserfolg in einer digitalen Welt, in der Flexibilität ein entscheidendes Verkaufsargument ist.

Die Prozesse rund um Funktionale Sicherheit (FuSi), Safety Of The Intended Functionality (SOTIF) und generelle Safety-Themen spielen, vor allem in der Fahrzeugindustrie sowie dem Mobilitätssektor, eine entscheidende Rolle. Sie sind durch die zugrunde liegenden Normen und Standards, die sich jeweils am technologischen State of the Art orientieren, optimal auf sämtliche Branchen und Anwendungsfelder übertragbar.

Unsere Experten haben langjährige Erfahrung mit der prozessualen Bedarfsanalyse, Umsetzung und Betreuung von Schutzmechanismen in verschiedenen Produkten.

## Unser Vorgehen

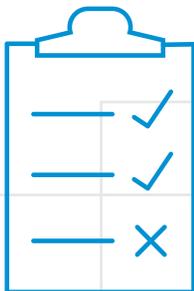
---

### Quick Check

Uns ist es wichtig, zunächst das Unternehmen und seine Prozesswelt zu verstehen, um gezielt neue Cybersecurity-Anforderungen einsteuern zu können. Wir analysieren Ihre Prozesslandschaft unter Einbezug der Nutzer hinsichtlich des Systemkontexts. Das bedeutet, dass wir ein Screening durchführen, um zu verifizieren, welche Prozesse der Gesamtorganisation in den Scope aktueller Cybersecurity-Anforderungen fallen.

Dadurch können wir für Sie im Rahmen einer Bestandsaufnahme eine Ist-System- und Prozesslandschaft erstellen, um eine belastbare Grundlage für die weiterführende Analyse zu erzeugen. Nachdem das Big Picture gemeinsam mit Ihren Prozessownern erstellt ist, grenzen wir das System vom Systemkontext ab, um Input- und Outputströme zu beschreiben.

Das ermittelte System wird ebenfalls analysiert und weiter detailliert. Wir ermitteln Swimlanes, Rollen, Prozesse und Tools und bereiten diese adressatengerecht auf. Dieser Schritt ist essentiell in der Umsetzung von neuen Anforderungen aus Gesetzen, Normen oder Standards, um ein sicheres Fundament für die weitere Projektarbeit zu erzeugen.



### Risiko- management

Nachdem das Fundament für die Bewertung erstellt wurde, müssen die Prozesse und Tools nach ihrer Dringlichkeit und Kritikalität hinsichtlich Cybersecurity bewertet werden.

Dabei hat sich eine Top-down-Analyse von Prozessgruppen auf Einzelprozess- und Aktivitätsebene bewährt, um eine maximale Durchgängigkeit in der Bewertung zu erzeugen. Bei kritischen oder unsicheren Prozessen und Systemen bieten wir Ihnen eine Stichprobenanalyse und das zugehörige Reporting an.

Im Rahmen des Projektmanagement-Office unterstützen wir Sie natürlich auch in der Aufbereitung von relevanten Unterlagen und der Einsteuerung dieser in die Gesamtunternehmensorganisation.



## Unser Vorgehen

# Anforderungsmanagement

Anschließend erzeugen wir für Sie, abgeleitet aus der vorher erstellten Outputbeschreibung, Anforderungen und generieren einen Umsetzungsplan mit zeitlichen Meilensteinen anhand der vorangegangenen Risikoanalyse.

Durch Aufzeigen einer maßgeschneiderten Soll-Systemlandschaft in Form eines Zielbildes für Ihr Unternehmen detaillieren wir die Umsetzungsanforderungen auf System- und IT-Tool-Ebene. Als Ergebnis entstehen User-Stories zur Anforderungsbeschreibung und Akzeptanzkriterien zur Einsteuerung in die Umsetzungsplanung der spezifischen IT-Tools.

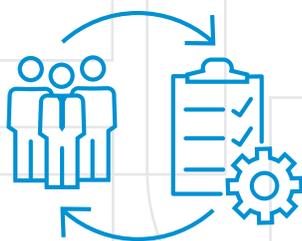
# Change-management

In der Phase der Implementierung steht die Umsetzung der Anforderungen in der System- und Prozesslandschaft im Fokus.

Hierbei legen wir vor allem Wert auf die Anpassung von gelebten Prozessen sowie zu den Prozessen passende IT-Systeme.

Wir führen gemeinsam mit Ihnen eine Rollout-Planung durch und betreuen die Dokumentation der Anpassungen an Ihren Prozessen und Tools. Durch Awareness-Schulungen für Mitarbeiter sowie die Erstellung und regelmäßige Durchführung von WBTs, Remote Trainings und On-Site-Trainings stellen wir den nachhaltigen Erfolg des Projektes sicher. Darüber hinaus verwenden wir zur Prüfung des Umsetzungserfolges verschiedene Methoden des Security- sowie Awareness-Testings.

Nach Projektabschluss stellen wir Ihnen gerne Mitarbeiter zur Betreuung eines Servicedesks sowie zur Durchführung weiterer Anpassungen und Optimierungen zur Verfügung.



## Unser Vorgehen

---

Unser Vorgehen wird von vier Kernelementen begleitet. Wir führen durchgängig Tätigkeiten in den Bereichen **Projektmanagement**, **Prozessmanagement**, **IT-Management** und **Auditmanagement** durch, um eine erfolgreiche Umsetzung der Cybersecurity-Anforderungen sicherzustellen.

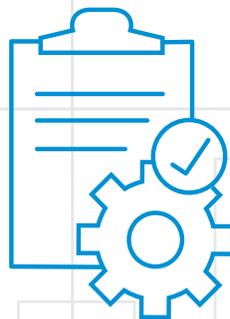
# Projektmanagement

Um einen ganzheitlichen Rahmen für das Vorgehen zu bilden und den Überblick zu behalten, setzen wir für Ihren Erfolg ein Projektmanagement-Office auf. Für eine individuelle und flexible Betreuung Ihrer Anforderungen und eine Bereitstellung von regelmäßigen, qualitätsgesicherten Zwischenergebnissen verwenden wir einen hybriden Projektmanagement-Ansatz.

Das hybride Projektmanagement umfasst die klassischen Projektschritte von der Initialisierung Ihres Projektes bis zum Projektabschluss, setzt jedoch agile Akzente in der Durchführung. Beispielsweise kann durch den repetitiven Charakter und durch das Aufsetzen von Aufgabensprints innerhalb einzelner Projektschritte sowohl eine zeitliche, qualitative Optimierung als auch eine frühzeitige Fehlervermeidung erzielt werden.

Mithilfe unserer regelmäßigen Statusberichte und eines bereichsübergreifenden Trackings, für das wir Best-Practice-Toolösungen nutzen, bieten wir Ihnen jederzeit einen transparenten Einblick in jede Aktivität. Wir unterstützen Ihre Entscheidungsträger dabei, mögliche Handlungsfelder und potentielle Risiken frühzeitig zu erkennen.

Zusätzlich gibt Ihnen die organisatorische Betreuung von Meetings und Workshops die Möglichkeit, Ihren Blick auf das Wesentliche zu richten. Unsere erfahrenen Projektmanager stehen Ihnen dabei jederzeit zur Verfügung.



## Unser Vorgehen

# Prozessmanagement

Die detaillierte Betrachtung von Prozessen bei der Umsetzung von Cybersecurity-Anforderungen ist ein essentieller Bestandteil im Cybersecurity-Konzept der Tagueri AG.

Dabei fokussieren wir uns auf die Identifikation, Gestaltung, Dokumentation, Implementierung und Steuerung von Geschäftsprozessen. Wir wenden einen ganzheitlichen Ansatz zur Analyse der Gesamtprozesse an, um organisatorische wie auch technische Aspekte durchgängig berücksichtigen zu können. Das Prozessmanagement gliedert sich in drei Level auf, die wir im Folgenden am Beispiel der UNECE WP.29 Regulierungen darstellen.

**Level 1:** Einordnung der Anforderungen in die Gesamtorganisation und Bewertung von In- und Outputs.

*Beispiel:* (1) Input: Änderungsbegehren für Fahrzeugkonfigurationen; (2) System: UNECE WP.29 Cybersecurity UN-R155; (3) Output: Abgesicherte Steuergerätedaten und - Parameter.

**Level 2:** Identifikation von Teilprojekten und Hauptaktivitäten innerhalb des Systems.

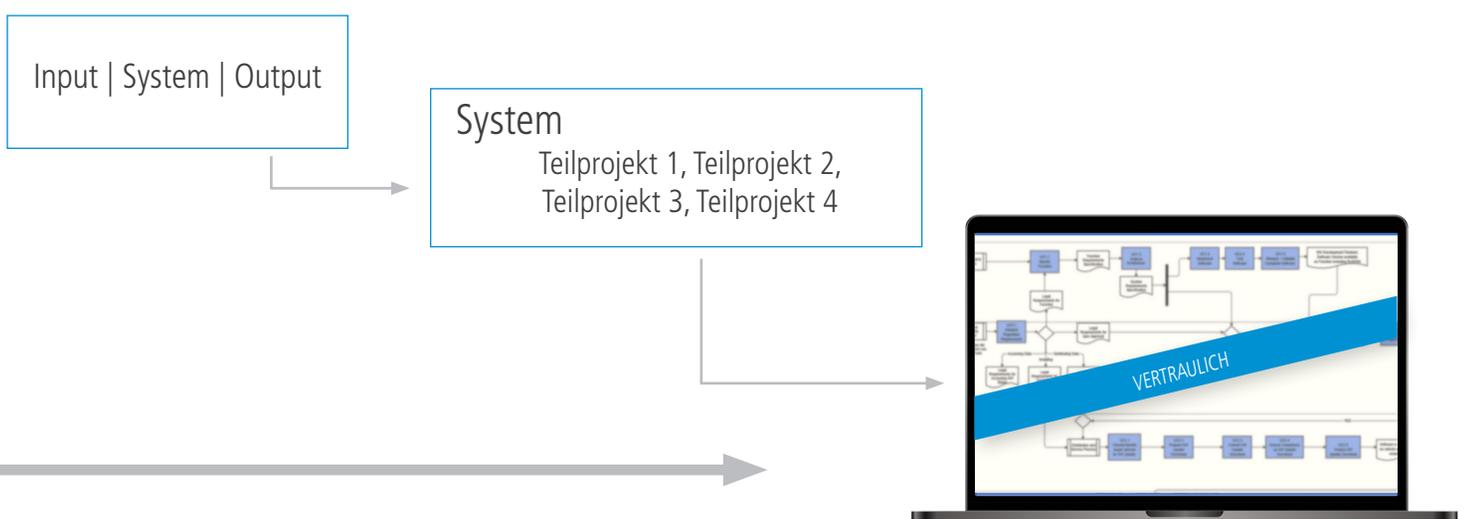
*Beispiel:* Die Anwendung von Prüfsummenergebnissen bei der Übertragung von Daten zum Steuergerät bildet ein eigenes, identifizierbares Teilprojekt.

**Level 3:** Analyse der Teilprojekte und Identifikation von Aktivitäten und Rollen mithilfe einer BPMN-Methodik und Einordnung in den Gesamtprozessablauf.

*Beispiel:* Im Teilprojekt „Prüfsummenergebnis bilden“ haben sich weitere Teilaktivitäten und Arbeitspakete ergeben. Diese werden den zuständigen Rollen in einer festgelegten Swimlane zugeordnet.

Aus den Erkenntnissen der Analyse erstellen wir gemeinsam mit Ihnen eine Prozesslandkarte, die das Fundament für eine strukturierte Betrachtung von Cybersecurity-Anforderungen bildet.

Dieser praxiserprobte Ansatz des Prozessstrackings erhöht die Traceability in der Implementierung und unterstützt Anwender und Prozessowner in der Anpassung ihrer Prozesse.





## Unser Vorgehen

---

# IT- Management

Im Kern einer jeden Betrachtung der Cybersecurity steht vor allem Ihre IT-Systemlandschaft, auch wenn diese im Gesamtkontext der Cybersecurity keine gesonderte Stellung besitzt.

Durch die Analyse Ihrer IT-Systemlandschaft, Generierung von standardkonformen Systemdarstellungen und Durchführung von GAP-Analysen decken wir Bedarfe auf und unterstützen mit zertifizierter Expertise im IT-Anforderungsmanagement bei der Umsetzung der erforderlichen Anpassungen an Ihren Tools.

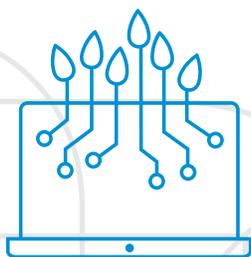
Gerne übernehmen wir mit unseren Produktmanagern auch eine Interims-Product-Ownership für neu entwickelte Tools nach verschiedenen Vorgehensmodellen (Wasserfall, Agile...) in Ihrem Unternehmen, bis sie durch eigene Ansprechpartner weiterbetreut werden. Über den gesamten Zeitraum der Analyse sowie der Umsetzung führen wir ein umfassendes Fehlermanagement in bestehenden und neuen IT-Systemen durch.

Wir unterstützen Ihre IT-Experten bei der Umsetzung neuer Anforderungen zur Sicherstellung einschlägiger Cybersecurity-Normen, Standards und Gesetze, sodass Ihre Systemlandschaft optimal auf entsprechende Auditierungen und Zertifizierungen vorbereitet ist.

# Audit- management

Nach erfolgter Analyse und Umsetzung von Prozess- und IT-Anpassungen steht zur Erfolgsmessung der Maßnahmen die Vorbereitung eines Assessments an. Zur Durchführung des Assessments in Ihrem Unternehmen bereiten wir die Teilnehmer unter Anwendung unserer praxiserprobten Self-Assessment-Methodik optimal vor. Wir unterstützen Sie bei der Auswahl der Zertifizierungsstelle und der notwendigen Kommunikation mit dieser ihr sowie der Nachbereitung des durchgeführten Assessments.

Nach dem erfolgten Audit stellen wir die Behebung eventueller Non-conformities sicher, sodass der Zertifikatsvergabe als Beleg für Ihre Cybersecurity nichts mehr im Weg steht.





## Unsere Expertise

- ISO/IEC 27001 und BSI 200 IT-Grundschutz
- VDA TISAX
- UNECE Software-Updates/ Cybersecurity (UN-R155/UN-R156)
- ISO/SAE 21434
- Risiko-Identifikation
- Cybersecurity Awareness Training
- Incident Monitoring
- Thread Analysis & Risk Assessment (TARA)
- Code Review
- Static Code Analysis (SCA)
- Security Testing/ Penetration Testing
- ITIL V3/V4

## Ihre Ansprechpartner

Aaron Machmer

Tel.: +49 1525 522 4472

Benedict Nienhaus

Tel.: +49 1525 499 3549

E-Mail Kontakt:

[cybersecurity@tagueri.com](mailto:cybersecurity@tagueri.com)

