... gleich geht‘s los

Smart Mechatronics

UNITY
CONSULTING & INNOVATION

Fit für den Cyber Resilience Act: Bestandsschutz und Maßnahmen im Fokus

Heutige Referenten

Sven Schwarzer

Torben Lammers

Thomas Werner

Smart Mechatronics

UNITY
CONSULTING & INNOVATION

Managementberatung für **Innovation & Transformation**

Fokus auf innovieren, integrieren, transformieren und realisieren!

> 25 Jahre Erfolgsgeschichte mit 73,6 Mio. Euro Umsatz

>800 Mitarbeiter in der UNITY Innovation Alliance, davon 380 bei UNITY

100% umsetzungsstark – Hands-on-Mentalität

26 der DAX-40- und 16 der EURO-STOXX-50-Unternehmen im Kundenstamm

Partner erfolgreicher Familienunternehmen und des Mittelstands

Erfolgreiche Projekte auf allen Kontinenten

Unsere Kunden meistern den digitalen Wandel – zukunftsrobust & nachhaltig

Fokus auf Innovationskraft und Steigerung der operativen Exzellenz unserer Kunden

Beste Arbeitgeber™ Consulting – Great Place To Work. Deutschland 2024

Beste Arbeitgeber™ NRW – Great Place To Work. Deutschland 2024

Beste Arbeitgeber™ Deutschland – Great Place To Work. 2024

28.01.2025

Fit für den Cyber Resilience Act: Bestandsschutz und Maßnahmen im Fokus

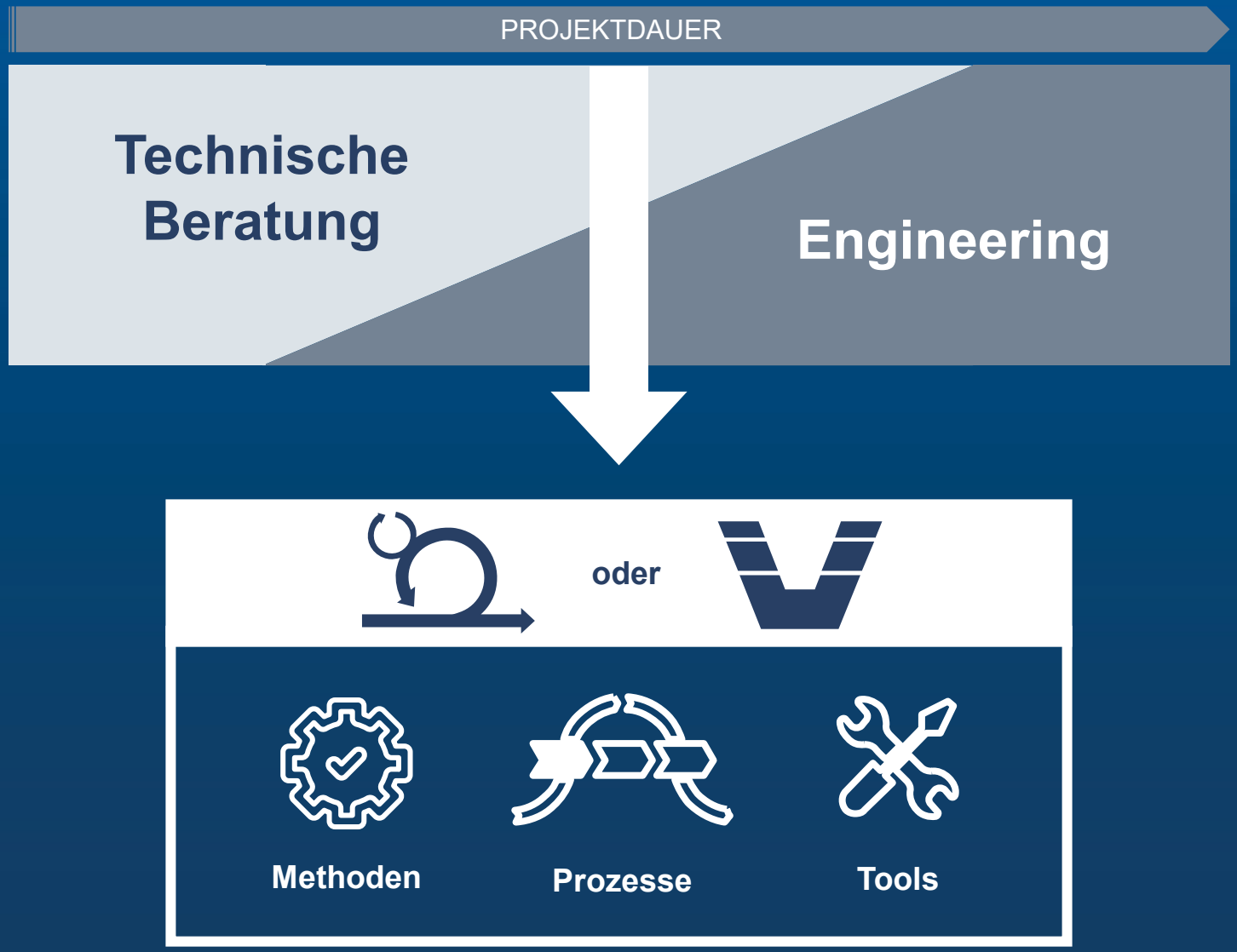
Über uns

Mitarbeiter: 130 +

Standorte:
Dortmund, Köln, München, Paderborn

Qualität:
Zertifiziert nach
DIN EN ISO 9001:2015

Gründung: 2008



Zusammenspiel UNITY / Smart

UNITY
CONSULTING & INNOVATION

- Betriebswirtschaftliche Bewertung
- Optimierung von Prozessen und Organisation
- Optimierung der IT-Architektur

Smart
Mechatronics

- Technische Bewertung
- Sicherheitsanalysen im Produkt
- Optimierung der Produktentwicklungen

Zukunftssichere Produkte

Der Cyber Resilience Act – Verpflichtungen

Hersteller tragen die Verantwortung für Cybersicherheit während des **gesamten Lebenszyklus**:

- Bewertung von Cybersicherheitsrisiken
- Meldewesen
- Schwachstellenmanagement
- Betriebsanleitung
- Sicherheitsupdates
- Konformitätserklärung (CE-Kennzeichen)

Der Cyber Resilience Act ist in Kraft getreten

Smart Mechatronics

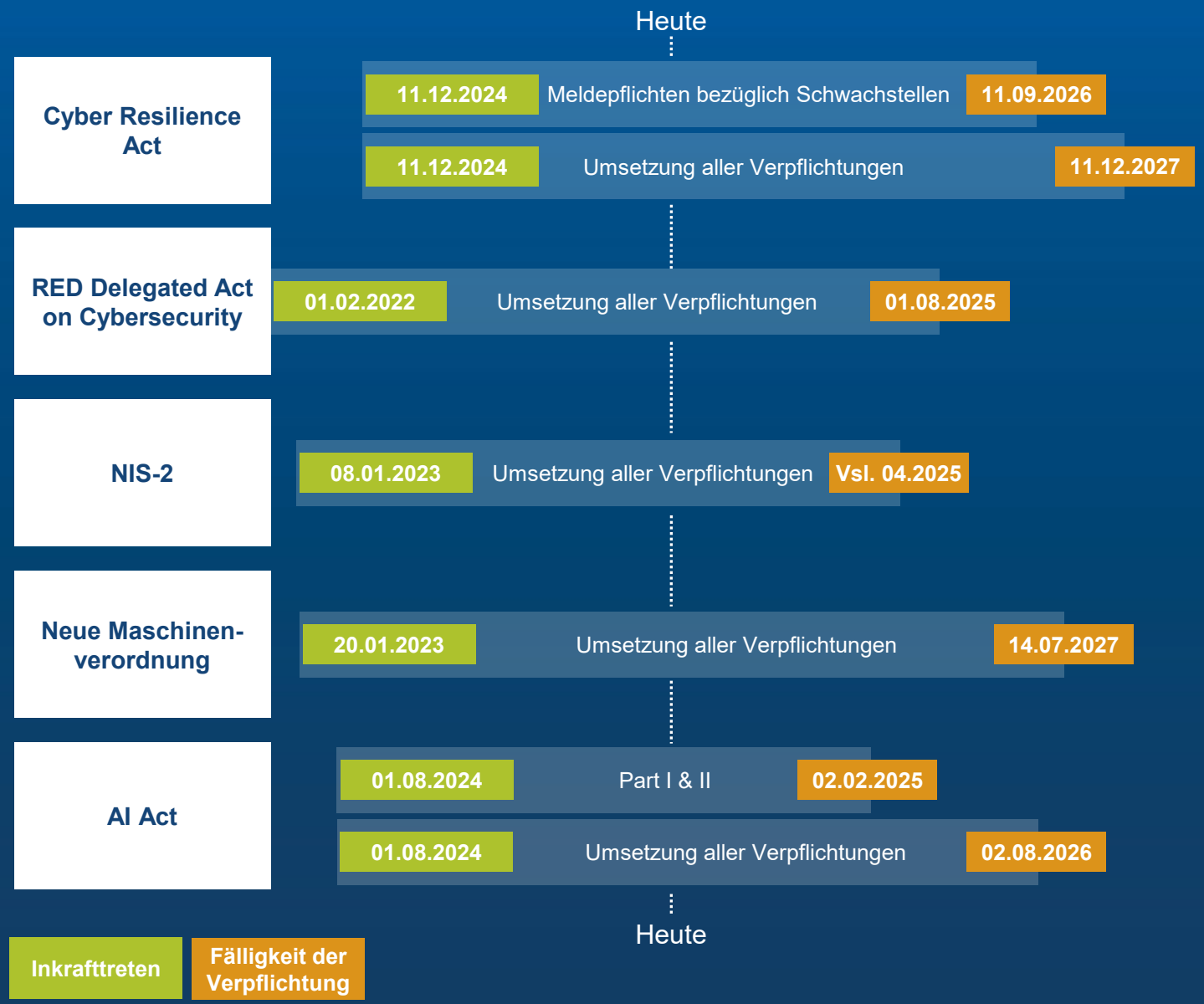
UNITY CONSULTING & INNOVATION

Achtung kein Bestandsschutz!

Relevante EU-Regularien im Bezug zum CRA

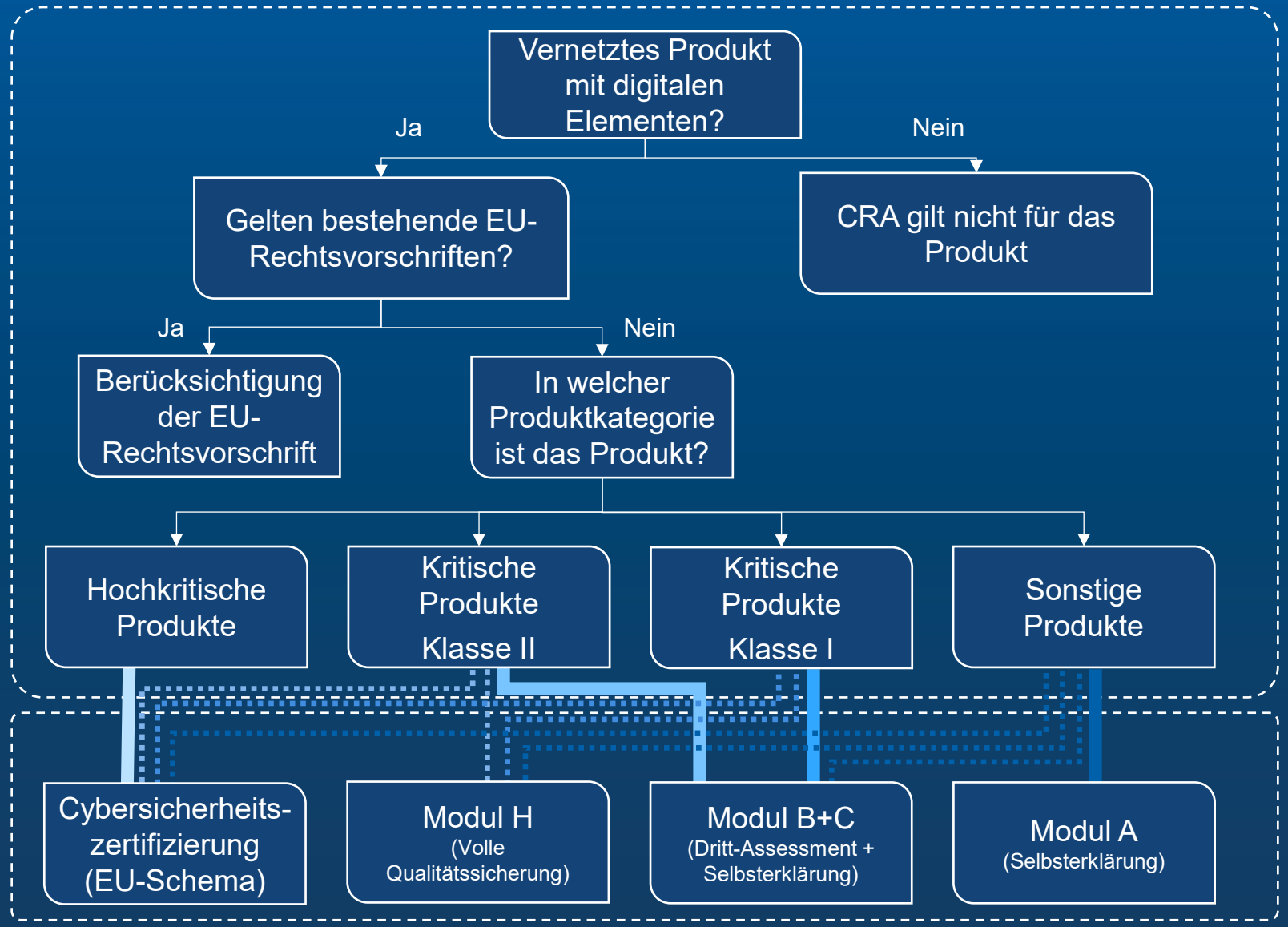
Smart Mechatronics

UNITY CONSULTING & INNOVATION



	Überschneidungen mit dem CRA	Hauptunterschiede zum CRA
Cyber Resilience Act		
RED Delegated Act on Cybersecurity	Fokus auf Produktsicherheit	Betrifft mit dem Internet verbundene Funkgeräte
NIS-2	Meldung von Vorfällen Risikomanagement	Betrifft Organisationen und ihre IT-Infrastruktur
Neue Maschinen-verordnung	Fokus auf Produktsicherheit	Betrifft den Maschinen- und Anlagenbau
AI Act	Fokus auf Produktsicherheit	Betrifft Produkte mit KI

Der Weg zum CE-Kennzeichen: Konformitätsbewertung



Ermittlung durch
CRA Readiness Check

Konformitätsbewertungsverfahren
(vereinfachte Darstellung)

Klassischer Ablauf zur CRA-Konformität

Smart Mechatronics

UNITY CONSULTING & INNOVATION

Positionsbestimmung

Befragung von externen Experten:

- Anwälte
- Technische Ansprechpartner
- Spezialisierte Berater
- …

Identifikation Handlungsfelder

- Entwicklung
- Prozess
- Qualität/ Normenstellen
- …

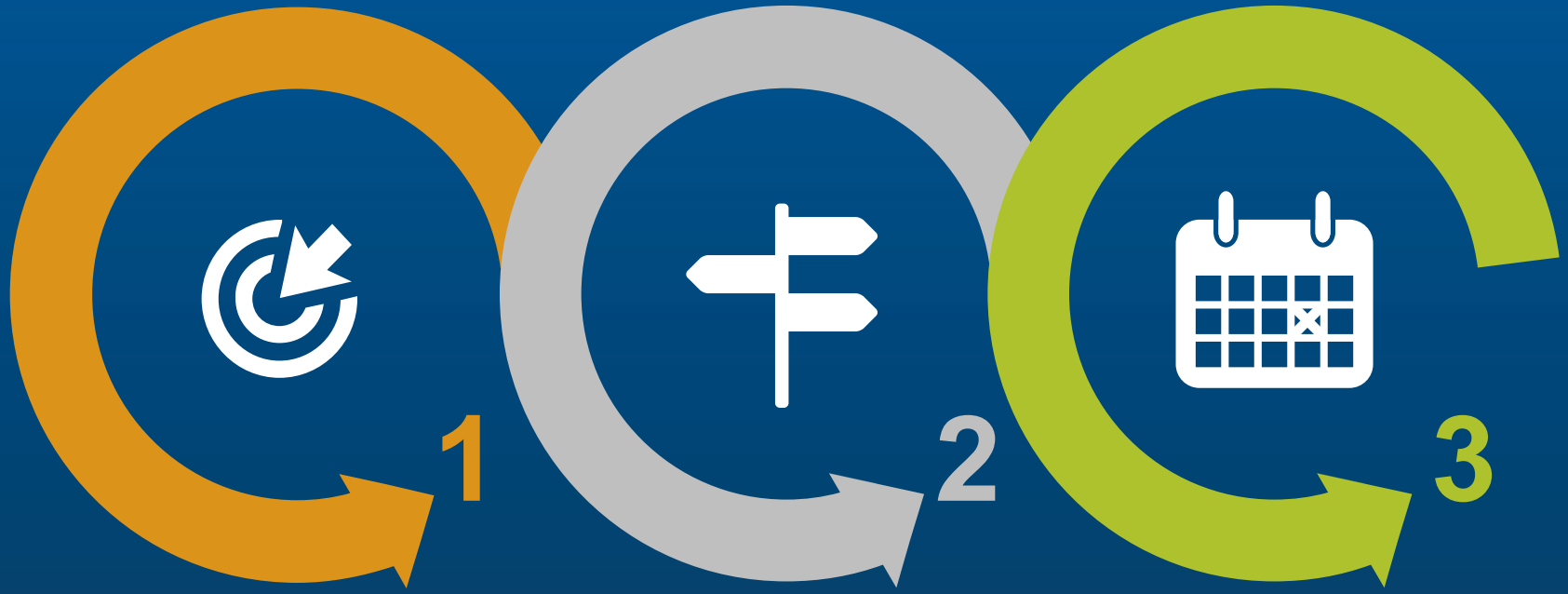
Umsetzung Handlungsfelder

- Diverse Projekte
- Eigene Projektleitung
- Eigene effiziente Methoden
- …

CRA Konformität

- Sichere Produkte
- Konforme Prozesse

3-Phasen-Ansatz zur Umsetzung des CRA



CRA Readiness Check

Bestimmung der Position als Basis für die weitere Umsetzung

Pilotumsetzung & Überwachung

Planung und erste Umsetzung von Sofortmaßnahmen

Überwachungsmaßnahmen

Abschluss Pilot & Rollout

Planung und Umsetzung von nachgelagerten Maßnahmen

Flächendeckender Rollout über alle erforderlichen Bereiche

3-Phasen-Ansatz zur Umsetzung des CRA

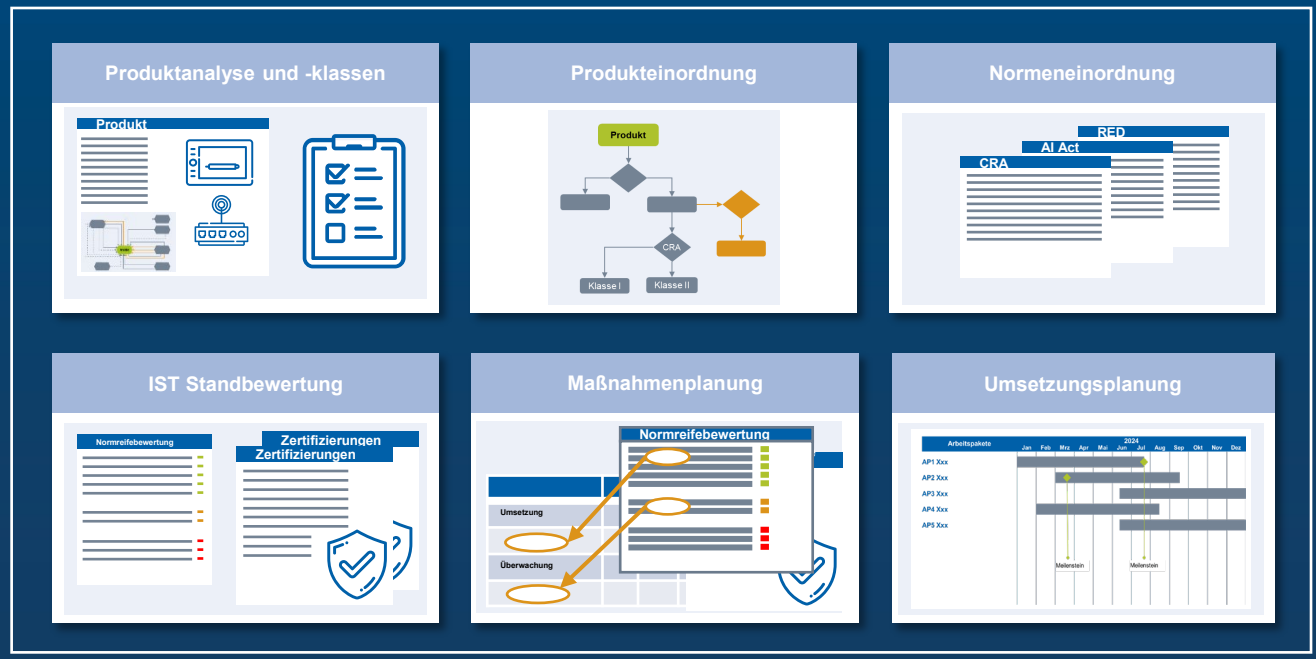
1 CRA Readiness Check

- Definition von **Beispielproduktklassen** mit gemeinsamen Merkmalen und Identifikation von **Referenzprodukten**
- Bestimmung **SOLL-Konformitätsverfahren** für Referenzprodukte
- Einordnung in die aktuelle **Normen- und Verordnungslandschaft** (z.B. CRA, RED-DA, MVO)
- Betrachten bereits **angewandter Normen** (z.B. IEC 62443) und der **Reifegrade neuer Vorgaben**
- Ableiten von **Maßnahmen**
- **Umsetzungsplanung** für Direktmaßnahmen und Pilotprojekt

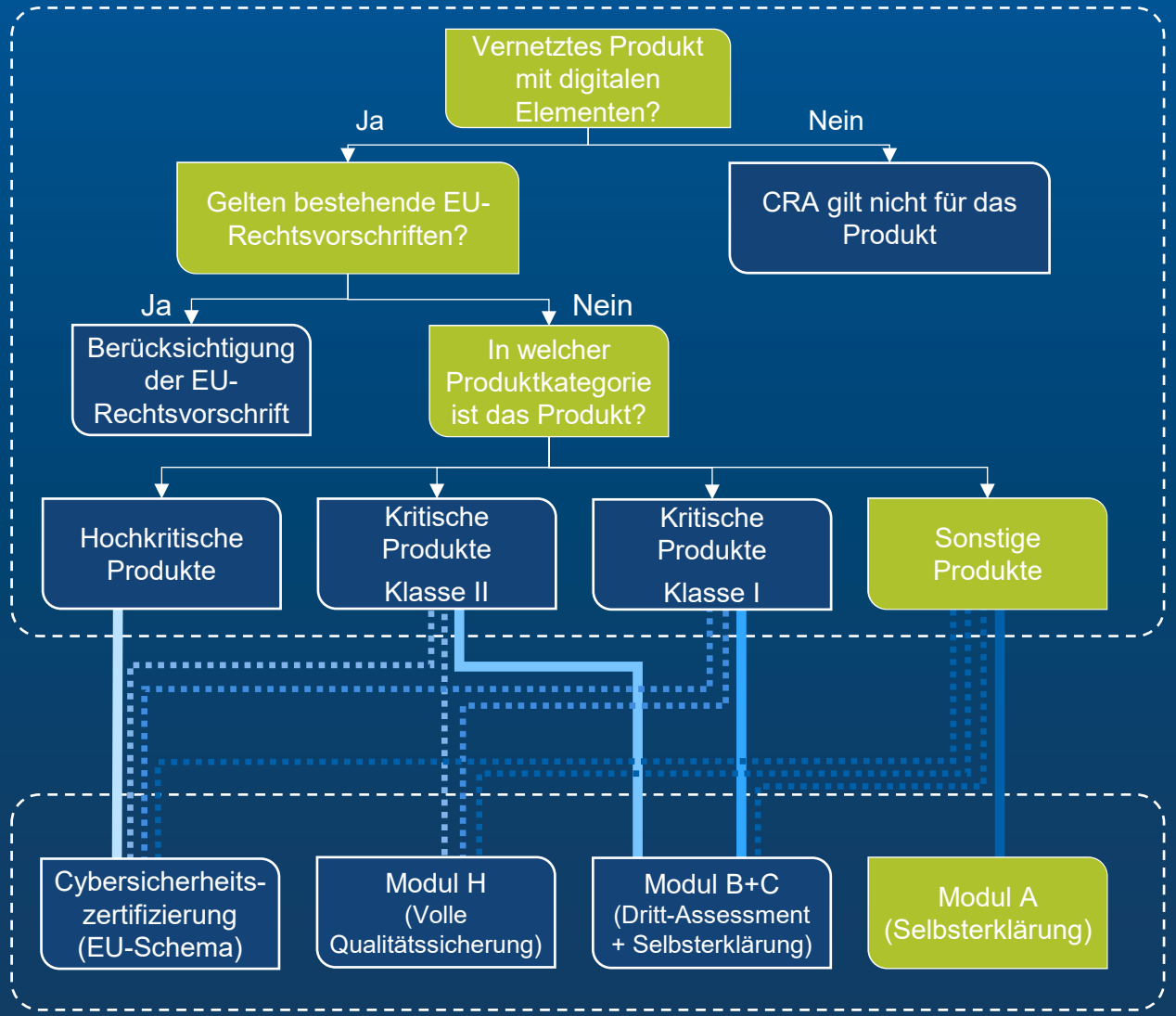
Analyse

Planung

Readiness Analyse



Einordnung



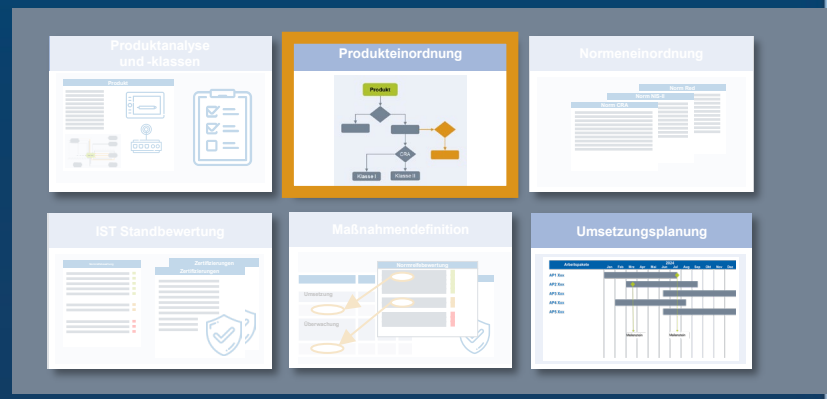
Ermittlung durch CRA Readiness Check

Konformitäts-bewertungs-verfahren
(vereinfachte Darstellung)

Smart Mechatronics

UNITY CONSULTING & INNOVATION

Ergebnisbeispiel



Umsetzungsplanung

Ergebnisbeispiel

2024 Q4 | 2025 Q1 Q2 Q3 Q4 | 2026 Q1 Q2 Q3 Q4 | 2027 Q1 Q2 Q3 Q4 | 2028 Q1 Q2 Q3 Q4

Zeitschiene CRA

Cyber Resilience Act (Legislative)

- 0: 11.12.2024 Inkrafttreten
- +21: 11.09.2026 Meldepflichten der Hersteller
- +36: **11.12.2027 Alle Herstellerpflichten** Ab hier CRA-Konformität

Harmonisierte Europäische Norm (hEN)

- -25: Harmonisierungsauftrag an Arbeitsgruppe
- -12: ~ Dezember 2025 Entwurf hEN
- 0: ~Dezember 2026 Veröffentlichung hEN

Unternehmensweite Maßnahmen (UM)

- UM01: Anpassung Produktlebenszyklus hin zu Secure Development Lifecycle
- UM02: Etablierung von Struktur und Prozessen für Berichtspflichten
- UM03: Einrichtung Schwachstellenmanagement
- Anmeldung Marktaufsichtsbehörde und Schwachstellendatenbank
- UM04: Überarbeitung der Anforderungen für M&A (Fusion und Übernahme)
- UM05: Interne CRA Audits durchführen
- UM06: Monitoring Harmonisierung EU-Normen
- CM07: Einführung von Tools zur Compliance-Dokumentation
- CM08: Anpassung der Templates für Dokumentation
- UM09: Technische Dokumentation & Handbuch
- UM10: Erweiterung Lieferantenmanagement

Produktbezogene Maßnahmen (PM)

Pilotprodukt

- PM01: Security Analyse
- PM02: Identifizierung und Bewertung von Schwachstellen
- PM03: Auflösen von Produktschwachstellen
- Weiterentwicklung und Anpassung Threat Model
- PM04: Security Testing
- PM05: Automatisierte (Sicherheits-)Updates
- PM06: Monitoring und Logging
- PM07: Einführung von Tools zur Unterstützung produktbezogener Prozesse
- Konformitätserklärung Pilotprodukt

Pilotierung der neuen Prozesse & Maßnahmen

- PM08: Minimierung der Erhebung von Daten
- PM09: Minimierung der Angriffsfläche
- PM10: Minimierung des Impacts

Restliches Produktportfolio

- Rollout Prozesse und Maßnahmen auf Produkt A
- Konformitätserklärung Produkt A
- Rollout Prozesse und Maßnahmen auf weitere Produkte (B bis n)
- Konformitätserklärung Produkt n

Umsetzungsplanung

Ergebnisbeispiel

	2024				2025				2026				2027				2028			
	Q4				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Zeitschiene CRA																				
Cyber Resilience Act (Legislative)	0	11.12.2024 Inkrafttreten										+21	11.09.2026 Meldepflichten der Hersteller			+36	**11.12.2027 Alle Herstellerpflichten** Ab hier CRA-Konformität			
Harmonisierte Europäische Norm (hEN)	-25	Harmonisierungsauftrag an Arbeitsgruppe					-12	~ Dezember 2025 Entwurf hEN				0	~Dezember 2026 Veröffentlichung hEN							

Unternehmensweite Maßnahmen (UM)

- UM01: Anpassung Produktlebenszyklus hin zu Secure Development Lifecycle
- UM02: Etablierung von Struktur und Prozessen für Berichtspflichten
- UM03: Einrichtung Schwachstellenmanagement
- Anmeldung Marktaufsichtsbehörde und Schwachstellendatenbank
- UM10: Erweiterung Lieferantenmanagement
- UM05: Interne CRA Audits durchführen
- UM06: Monitoring Harmonisierung EU-Normen
- CM07: Einführung von Tools zur Compliance-Dokumentation
- CM08: Anpassung der Templates für Dokumentation
- UM09: Technische Dokumentation & Handbuch
- UM10: Erweiterung Lieferantenmanagement

Produktbezogene Maßnahmen (PM)

Pilotprodukt

- PM01: Security Analyse
- PM02: Identifizierung und Bewertung von Schwachstellen
- PM03: Auflösen von Produktschwachstellen
- Weiterentwicklung und Anpassung Threat Model
- PM04: Security Testing
- PM05: Automatisierte (Sicherheits-)Updates
- PM06: Monitoring und Logging
- PM07: Einführung von Tools zur Unterstützung produktbezogener Prozesse
- Konformitätserklärung Pilotprodukt

Pilotierung der neuen Prozesse & Maßnahmen

- PM08: Minimierung der Erhebung von Daten
- PM09: Minimierung der Angriffsfläche
- PM10: Minimierung des Impacts

Restliches Produktportfolio

- Rollout Prozesse und Maßnahmen auf Produkt A
- Konformitätserklärung Produkt A
- Rollout Prozesse und Maßnahmen auf weitere Produkte (B bis n)
- Konformitätserklärung Produkt n

UM10: Erweiterung Lieferantenmanagement

Smart Mechatronics

UNITY CONSULTING & INNOVATION

Ergebnisbeispiel

Allgemeines

Ziel: Adaption der Einkaufs- und Lieferantenmanagementprozesse: Sicherstellung der CRA-Konformität von bezogener Software und Komponenten mit digitalen Elementen

Verantwortung: Management Global Sales- & Purchasing-Department

Betroffenheit:

- [x] Unternehmen
- [ ] Produktportfolio
- [ ] Einzelnes Produkt

Motivation & Zielstellung

Einordnung

- Projektübergreifende Lieferantenqualifizierung

IST-Zustand

- Die CRA-Konformität ist in den aktuellen Verträgen und bei den aktuellen Lieferantenaudits nicht berücksichtigt

Soll-Zustand:

- Die neuen Lieferantenmanagementprozesse müssen gewährleisten, dass alle zugekauften Softwareprodukte und Komponenten mit digitalen Elementen CRA-konform sind
- Erweiterung der Lieferantenprozesse entsprechend der neuen normativen Vorgaben (z.B. aus ISO 27001, ISO 28000, aber auch IEC 62443-4-2)

Konkrete Aktivitäten

- Sichtung bestehender Lieferantenverträge und AGBs
- Erweiterung der Lieferantenstrategie um CRA Compliance (Audits, Selbsterklärungen)
- Anpassung der Vertragsbedingungen und AGBs, um die Einhaltung der CRA-Standards durch die Lieferanten sicherzustellen.
- Compliance mit dem CRA fortlaufend kontrollieren

Bewertung & Nutzen

Wichtigkeit: 1 – sehr wichtig

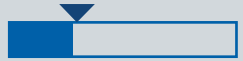
Priorität: 2 – dringend

Nutzen:

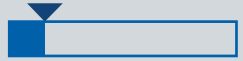
- Absicherung der Compliance der zugekauften Produkte
- Ausweitung des CRA-Risikomanagements auf die eigenen Lieferanten

Aufwandsabschätzung

Aufwand (PT):



Kosten:



Dauer: 12-18 Monate

Erforderliche Ressourcen

- Global Sales- & Purchasing Department
- Rechtsabteilung (ggf. externe Experten)
- Security Engineers
- Produktmanagement

Abhängigkeiten und Voraussetzungen

- Sicherheitsstandards für die Supply Chain (ISO 28000) sowie die Veröffentlichung der harmonisierten EU-Norm zum Cyber Resilience Act.

Umsetzungsplanung

Ergebnisbeispiel

2024				2025				2026				2027				2028			
Q4				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Zeitschiene CRA

Cyber Resilience Act (Legislative)

- 0: 11.12.2024 Inkrafttreten
- +21: 11.09.2026 Meldepflichten der Hersteller
- +36: **11.12.2027 Alle Herstellerpflichten** Ab hier CRA-Konformität

Harmonisierte Europäische Norm (hEN)

- -25: Harmonisierungsauftrag an Arbeitsgruppe
- -12: ~ Dezember 2025 Entwurf hEN
- 0: ~Dezember 2026 Veröffentlichung hEN

Unternehmensweite Maßnahmen (UM)

- UM01: Anpassung Produktlebenszyklus hin zu Secure Development Lifecycle
- UM02: Etablierung von Struktur und Prozessen für Berichtspflichten
- UM03: Einrichtung Schwachstellenmanagement
- Anmeldung Marktaufsichtsbehörde und Schwachstellendatenbank
- UM04: Überarbeitung der Anforderungen für M&A (Fusion und Übernahme)
- UM05: Interne CRA Audits durchführen
- UM06: Monitoring Harmonisierung EU-Normen
- CM07: Einführung von Tools zur Compliance-Dokumentation
- CM08: Anpassung der Templates für Dokumentation
- UM09: Technische Dokumentation & Handbuch
- UM10: Erweiterung Lieferantenmanagement

Produktbezogene Maßnahmen (PM)

Pilotprodukt

- PM01: Security Analyse
- PM02: Identifizierung und Bewertung von Schwachs…
- PM03: Weiterentwicklung und Anpassung Threat Model
- PM04: Security Testing
- PM05: Automatisierte (Sicherheits-)Updates
- PM06: Monitoring und Logging
- PM07: Einführung von Tools zur Unterstützung produktbezog…
- PM01: Security-Analyse
- Konformitätserklärung Pilotprodukt

Pilotierung der neuen Prozesse & Maßnahmen

- PM08: Minimierung der Erhebung von Daten
- PM09: Minimierung der Angriffsfläche
- PM10: Minimierung des Impacts

Restliches Produktportfolio

- Rollout Prozesse und Maßnahmen auf Produkt A
- Konformitätserklärung Produkt A
- Rollout Prozesse und Maßnahmen auf weitere Produkte (B bis n)
- Konformitätserklärung Produkt n

PM01: Security-Analyse

Smart Mechatronics

UNITY CONSULTING & INNOVATION

Ergebnisbeispiel

Allgemeines

Ziel: Bewertung der Cybersicherheitsrisiken für ein konkretes Produkt

Verantwortung: Entwicklungsabteilung

Betroffenheit:

- [ ] Unternehmen
- [ ] Produktportfolio
- [x] Einzelnes Produkt

Motivation & Zielstellung

Einordnung

- EU Cyber Resilience Act: Artikel 13 Pflichten der Hersteller Absatz 2
- EU Cyber Resilience Act: Anhang I Grundlegende Anforderungen Teil I Absatz 1

IST-Zustand

- Für das konkrete Produkt hat noch keine Analyse stattgefunden

Soll-Zustand:

- Analysiertes Produkt entsprechend den Anforderungen des CRA
- Identifizierte Schwachstellen als Basis für Abstell- bzw. Managementmaßnahmen

Konkrete Aktivitäten

- Security-Analyse Workshop *CONCRY* (Threat Analysis and Risk Assessment)

Bewertung & Nutzen

Wichtigkeit: 1 – sehr wichtig

Priorität: 1 – sehr hoch

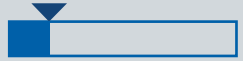
Nutzen:

- Erfüllung der normativen Anforderungen des CRA
- Identifikation erforderlicher Schutzmaßnahmen gegen Angriffe gegen das konkrete Produkt
- Basis für zukünftige Betrachtungen, wenn das Produkt weiterentwickelt wird und weitere Features ergänzt werden (Basis laufender Analysen, z.B. bei Bauteilwechseln oder Lieferantenwechseln)

Aufwandsabschätzung

Aufwand (PT):

Kosten:



Dauer: 3 Wochen

Erforderliche Ressourcen

- Produktmanager
- Firmware-Entwickler
- System-Engineer
- Security-Engineer

Abhängigkeiten und Voraussetzungen

- Idealerweise vorliegende Systemarchitektur des Produktes
- Nachfolgender Schritt: Behebung von Schwachstellen im Produkt

Umsetzungsplan

Smart Mechatronics

UNITY CONSULTING & INNOVATION

Ergebnisbeispiel

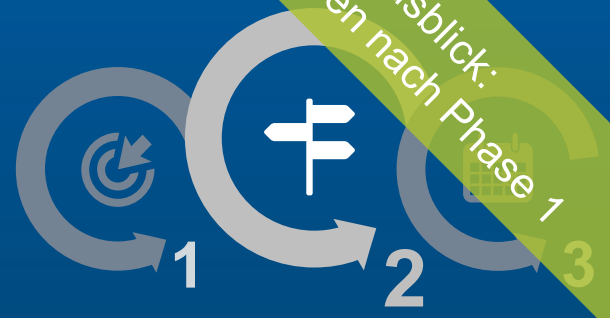
Nr.	Maßnahme	Aktivitäten	Externe Kosten	Aufwand Kunde (PT)	Aufwand Beratung (PT)	Aufwand Engineering (PT)	Aufwand Extern (PT)	Dauer (Monate)	Annahmen	Budget
PM 01	Security-Analyse	• Aufstellen von Context-Diagrammen • Einzeichnen von Trust Boundaries • Identifizierung von Threats • Bewertung der Risiken • Auflisten der Assets • Definition von Maßnahmen • Analyse von Threat Agents und Use Cases	XXX €	X	X	X	X	X	Personen seitens Kunde: Produktmanager, Systems Engineer / Architekt, HW-Entwickler, SW-Entwickler, ggf. Projektleiter Aufwand Kunde: X Personen im 1-Tages-WS + X Personen im Halbtages-WS-Risikoabschätzung + X Personen 2h-Abschlusspräsentation + X Personen halben Tag Bereitstellung Unterlagen = X Threat Modeling Tooling für ca. XXXX EUR / 1 Jahr Aufwand Engineering ...	**XXX €**
UM 10	Erweiterung des Lieferanten-managements	• Überprüfung der aktuellen Lieferantenverträge und AGBs auf CRA-Konformität. • Anpassung der Vertragsbedingungen und AGBs, um die Einhaltung der CRA-Standards durch die Lieferanten sicherzustellen. • Entwicklung und Implementierung einer überarbeiteten Lieferantenstrategie, die die Risiken und Anforderungen des CRA berücksichtigt (ggf. über gängige Standards, spätestens zu hEN CRA) • Klärung der Beschaffungspolitik für spezifische Komponenten wie Rechner (Microsoft Windows) und Waagen im Hinblick auf CRA-Anforderungen.	XXX €	X	X	X	X	X	• X PT Einarbeitung Einkauf in die Thematik CRA und Ableiten von Konsequenzen • X PT Identifizierung notwendiger Anpassungen der bestehenden Lieferantenverträge zwischen Einkauf, Rechtsabteilung und Entwicklung • X PT Anpassung von Richtlinien oder Prozessen zum strategischen und operativen Lieferantenmangement. • X PT für Kommunikation, Verhandlung, Änderung von aktiven Lieferantenbeziehungen für angenommen X wichtige Lieferanten (für elektonische Bauteile). • vermutlich keine Software benötigt (vermutlich unverhältnismäßig für Einsatz bei Elementar) • X PT Beratung: Unterstützung Anforderungsklärung und Einbringung Best Practices im Lieferantenmanagement (Secure Supplier Management).	**XXX €**
UM 06	Monitoring harmonisierte EU-Normen (hENs)	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3-Phasen-Ansatz zur Umsetzung des CRA

Smart Mechatronics

UNITY CONSULTING & INNOVATION

Ausblick: Vorgehen nach Phase 1



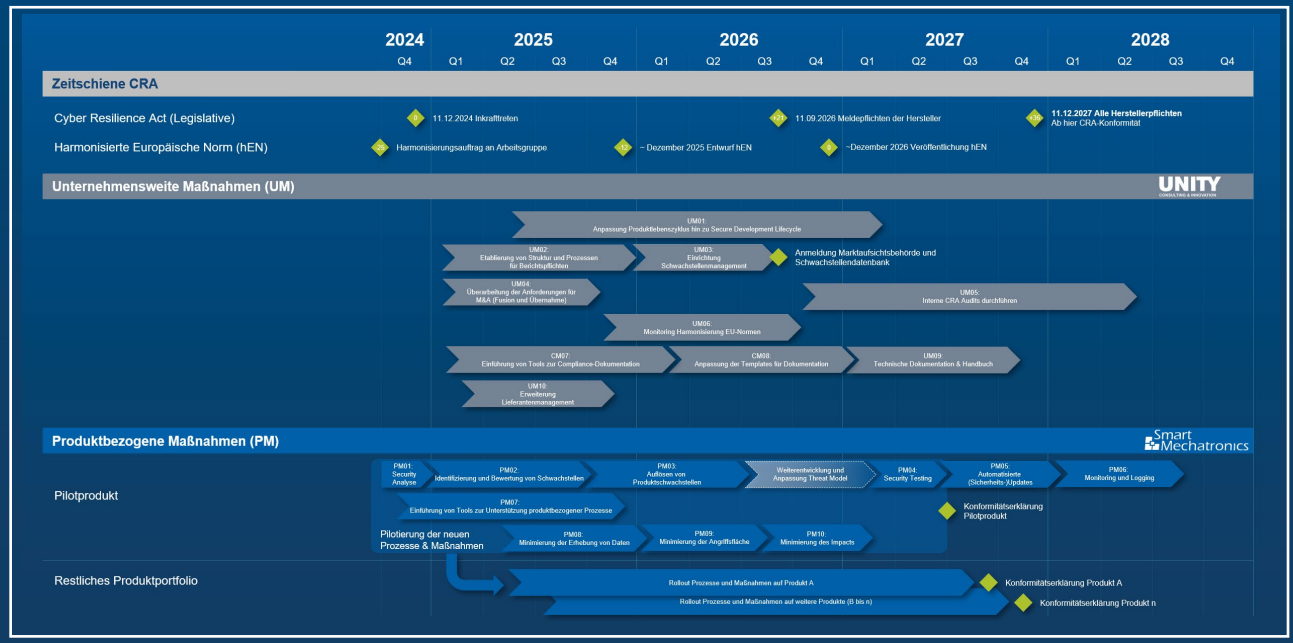
2 Pilotumsetzung & Überwachung

Direktmaßnahmen Pilotprodukt

- Produkt (Beispiele)
  - Bedrohungsanalyse (C⬢NCRY)
  - SBOM (z.B. nach TR-03183)
  - Schwachstellenmanagement
  - Systemarchitektur
- Prozesse (Beispiele)
  - Prozessanpassung (PEP)
  - Lieferantenmanagement
  - Security Testing
  - Risiko/Incident Management
- IT
- Produktion
- Organisation…

Überwachungsmaßnahmen z.B. harmonisierte Europäische Norm, Tools, Lieferanten

Maßnahmen



UM10: Erweiterung Lieferantenmanagement

Smart Mechatronics

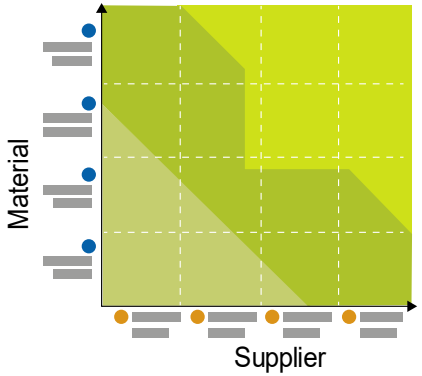
UNITY CONSULTING & INNOVATION

Ausblick: Vorgehen nach Phase 1

Bestehenden Verträge prüfen

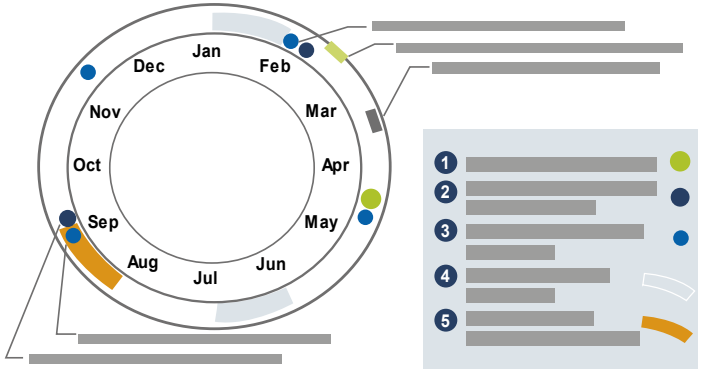
Risk Management		☑	☐	☑
		☐	☑	☑
Performance Management		☑	☑	☑
		☐	☑	☑
Contract Management		☐	☑	☑
		☐	☐	☑
Supplier Integration/ Development		☑	☐	☐
		☐	☑	☑

Lieferantenstrategie erweitern



Vertragsbedingungen anpassen

CRA Compliance kontrollieren



PM01: Security-Analyse

Smart Mechatronics

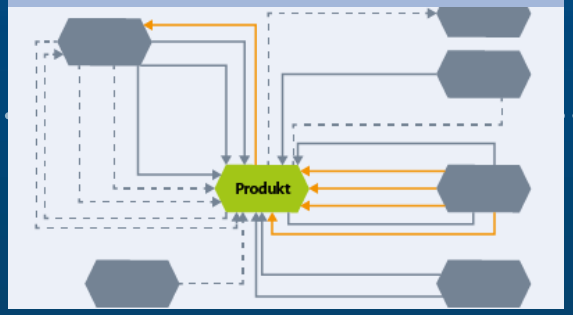
UNITY CONSULTING & INNOVATION

Ausblick: Vorgehen nach Phase 1

Produktbezogene Maßnahmen (PM)

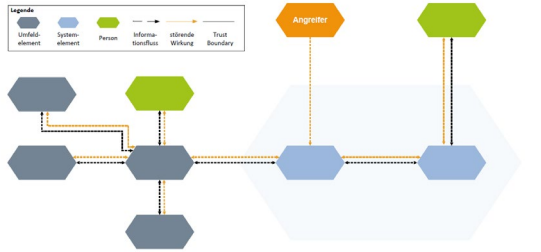
Produkt-analyse

Umfeld



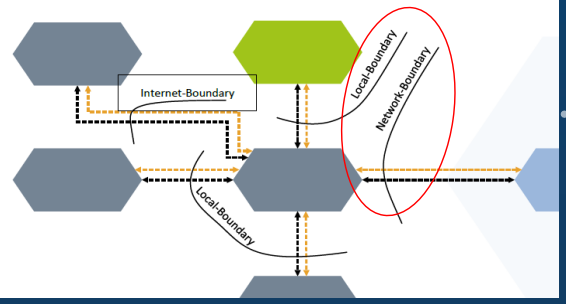
Personas und Use Cases

Wirkungsanalyse und Assets

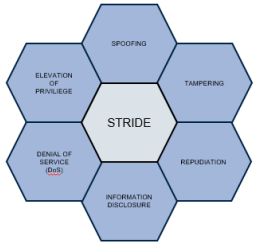


Security-analyse

Datenfluss und Vertrauensgrenzen



Bedrohungen und Angriffsvektoren



Risikoabschätzung und Handlungsempfehlungen

3-Phasen-Ansatz zur Umsetzung des CRA

Smart Mechatronics | UNITY CONSULTING & INNOVATION

Vorgehen nach Phase 1 | Ausblick: 3

3 Abschluss Pilot & Rollout

Abschluss Pilotprodukt (mittelfristig)

- Technische Dokumentation
- Informationen für den Benutzer
- Erstellung Konformitätserklärung (finale oder Übergangslösung)
- Interne Prüfung oder durch externe Prüfstelle
- …

Rollout: Umsetzung nachgelagerte Maßnahmen (kurzfristig)

- Ausweitung auf weitere betroffene Produkte
- IT-Umsetzung
- Weiterentwicklung der Prozesse (PEP, IT,..)
- Risikomanagement etablieren
- Schwachstellenmanagement
- …

Cybersicherheit ist ein Prozess…

Ihr Produkt ist CRA-Ready

Harmonisierte EU-Normen (hEN)

Monitoring & graduelle Umsetzung

NOCH FRAGEN?

Wir stehen Ihnen gerne zur Verfügung!

Sven Schwarzer

Sven.Schwarzer@smartmechatronics.de

Torben Lammers

Torben.Lammers@smartmechatronics.de

Thomas Werner

Thomas.Werner@unity.de

www.smartmechatronics.de | www.unity.de