making ideas work imt.

# Cyber Resilience Act(CRA)

## Checklist

### 1. Product Classification

- ☐ All products with digital elements are identified
- ☐ Products are classified according to CRA risk levels (Standard / Class 1 / Class 2 / Critical)
- ☐ Classification is documented and justified
- ☐ Responsibilities for classification are defined
- ☐ A regular update process for classification is established

### 2. Technical Implementation in Engineering

- ☐ Security-by-Design is embedded in the development process
- ☐ Security requirements are included in the architecture phase
- ☐ Mechanisms for secure updates and patching are implemented
- ☐ Third-party dependencies are documented
- ☐ Vulnerability management process is defined and active
- ☐ Security risks are continuously assessed
- ☐ Secure development guidelines are established

### 3. Compliance & Documentation

- ☐ Technical documentation is CRA-compliant
- ☐ Product documentation is complete and up to date
- ☐ Security requirements are clearly documented
- ☐ Internal compliance processes are defined
- ☐ Audit and evidence requirements are addressed
- ☐ Interface between Engineering and Compliance is defined
- ☐ Responsibilities for regulatory updates are assigned

# Cyber Resilience Act (CRA)

## Checklist

### 4. Reporting Obligations & Incident Management

☐ Process for detecting actively exploited vulnerabilities is established
☐ Definition of "severe security incident" is clearly defined internally
☐ Escalation process is defined (Engineering → Security → Compliance)
☐ CRA reporting deadlines are implemented
☐ Communication channels with authorities are prepared
☐ Incident response team is defined and trained
☐ Reporting process has been tested

### 5. Legacy Products & Spare Parts

☐ Legacy stock is assessed for CRA compliance
☐ Re-validation process for existing stock is defined
☐ Spare parts are classified (identical / functional / new)
☐ Rules for spare parts assessment are documented
☐ Supplier requirements are aligned with CRA obligations
☐ Lifecycle strategy includes CRA requirements

### 6. Organization & Governance

☐ Cross-functional CRA ownership is defined
☐ Collaboration between Engineering, Security and Compliance is established
☐ CRA training has been conducted
☐ Regular reviews and updates are scheduled
☐ Management is informed about risks and deadlines
☐ CRA implementation roadmap is defined