

DEBIT

Jörg Deusinger

Strukturwandel braucht IT-Sicherheit



DEBIT

MADE IN MAIN - KINZIG

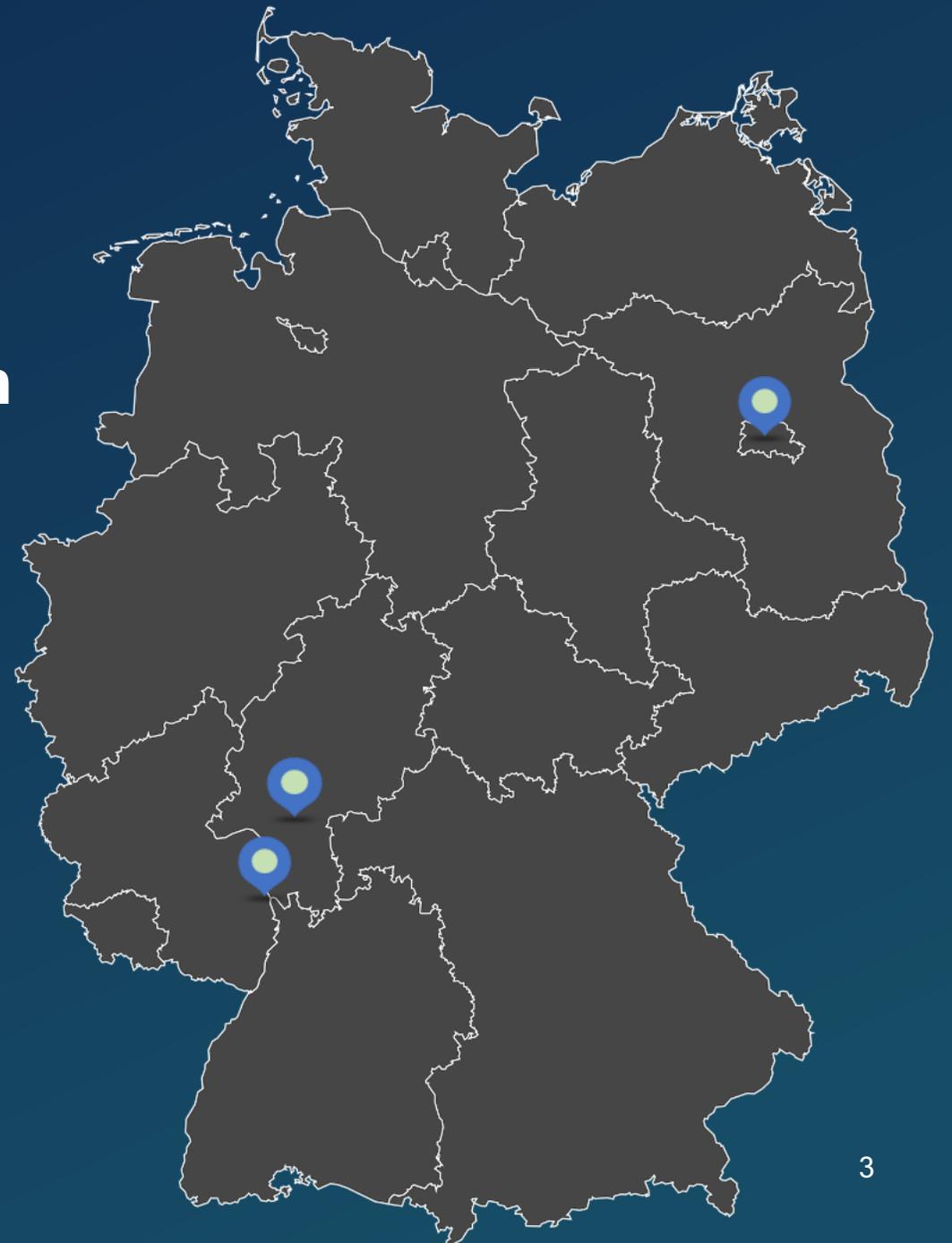
Starker Partner in der Region
24 Jahre Ausbildungsbetrieb
Hauptstandort in Gelnhausen



DEBIT

DEBIT

- Alleinstellungsmerkmale durch diverse Zertifizierungen
- 24 Jahre
- 100 Mitarbeiter
- Standorte: Gelnhausen, Mannheim, Leipzig



IT-Security

IT-Systemhaus

IT-Security

Informationssicherheit

BSI IT-Grundschutz, ISO 27001, Pentests, externer ISB, Sicherheitskonzeptionen, CERT, Schwachstellenmanagement, uvm.

Datenschutz

Externer DSB, Sensibilisierungen

Auditierung

ISO 27001, BSI IT-Grundschutz, KRITIS-Audits, interne Audits

Cloudbasierte Möglichkeiten

IT-Support

User-Help-Desk (UHD)

- mehrsprachig
- 24/7

Backup, Monitoring, Virtualisierung, Netzwerktechnik, Server/Storage

IT-

Beschaffungsmanagement

Beschaffung von Hardware, Beschaffung von Software

Karriereleiter de-bit





Strukturwandel braucht IT-Sicherheit

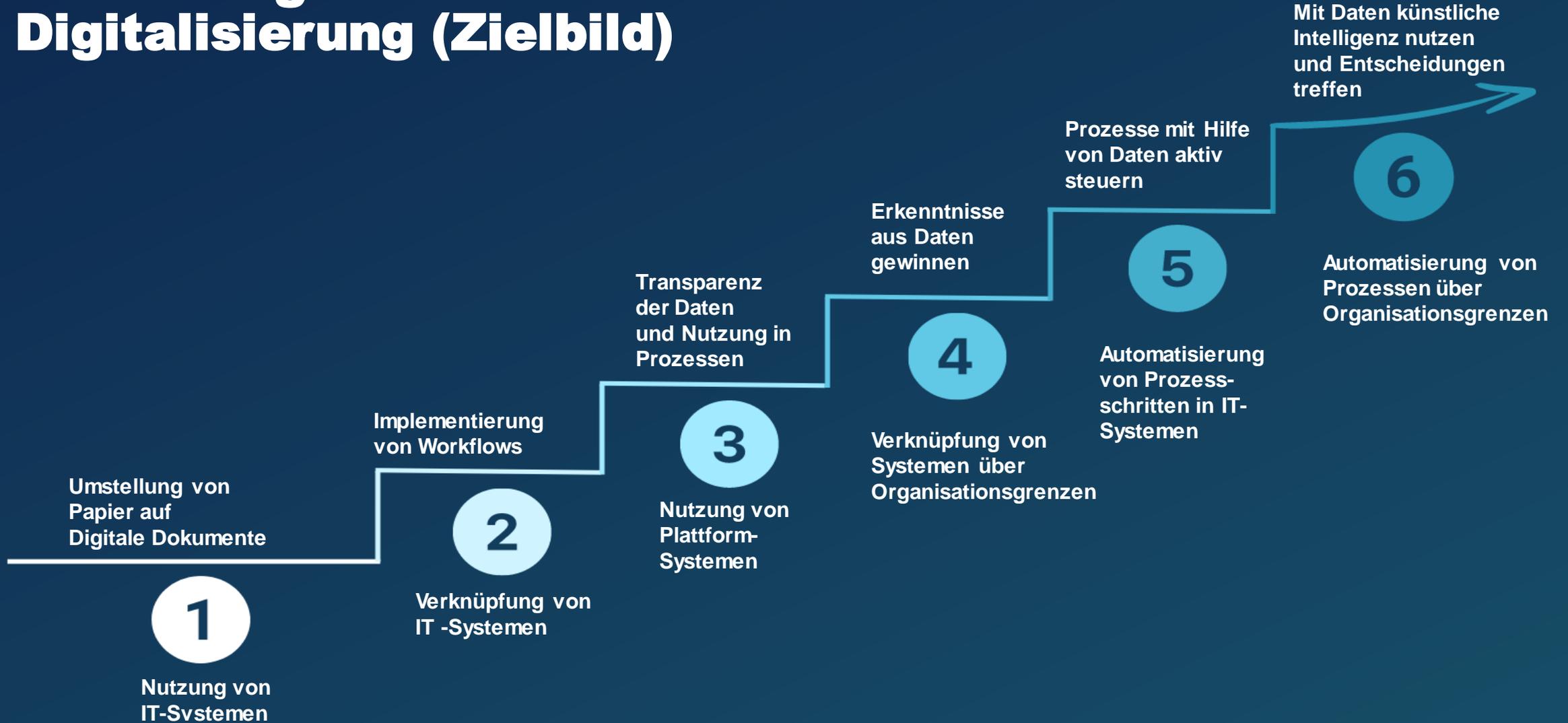
Was bedeutet Strukturwandel durch Digitalisierung und Automatisierung?

Wo liegen die Chancen aber auch Risiken dieses Wandels?

Welche gesetzlichen Regelungen gibt es?

Was können Unternehmen tun, um diesen Wandel sicher zu vollziehen?

Bedeutung des Strukturwandels durch Digitalisierung (Zielbild)





Strukturwandel braucht IT-Sicherheit

Was bedeutet Strukturwandel durch Digitalisierung und Automatisierung?

Wo liegen die Chancen aber auch Risiken dieses Wandels?

Welche gesetzlichen Regelungen gibt es?

Was können Unternehmen tun, um diesen Wandel sicher zu vollziehen?



Chancen und Risiken des Wandels

Chancen

- **Effizienzsteigerung durch schnellere Prozessabläufe**
- **Kostenreduktion durch Automatisierung**
- **Innovation durch strukturierte Prozesse**
- **Flexibilität durch ständige Verfügbarkeit der Informationen und Daten**

Chancen und Risiken des Wandels

Risiken:

- Erhöhte Bedrohungslage durch Cyberangriffe durch die Vernetzung
- Prozessfehler durch Fehlkonfiguration
- Technologische Abhängigkeit
- Mangelnder Wissenstransfer und unzureichende Dokumentation



Strukturwandel braucht IT-Sicherheit

Was bedeutet Strukturwandel durch Digitalisierung und Automatisierung?

Wo liegen die Chancen aber auch Risiken dieses Wandels?

Welche gesetzlichen Regelungen gibt es?

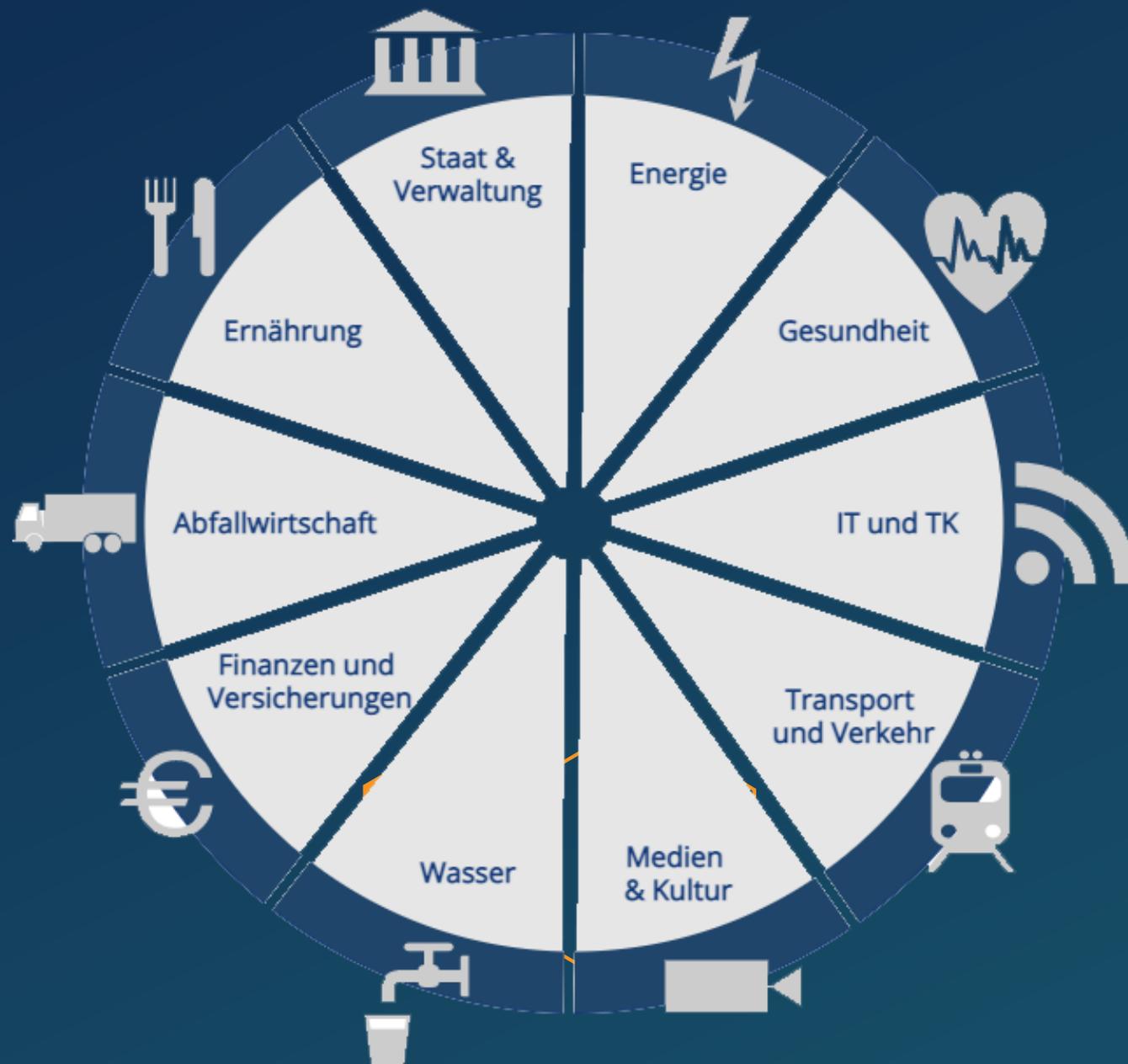
Was können Unternehmen tun, um diesen Wandel sicher zu vollziehen?

A background image showing a pair of golden scales of justice on a wooden surface, with several books stacked behind them. The image is partially obscured by a dark blue diagonal overlay on the right side.

Gesetzliche Anforderungen NIS2 & KRITIS Dachgesetz

- **Gesetzliche Anforderungen zur Steigerung der Cyberresilienz**
- **NIS2: Unternehmen ab 50 Mitarbeiter & 10 Mio. Umsatz die in definierten Sektoren tätig sind**
- **KRITIS: Unternehmen die einem der Krisis Sektoren angehören**

KRITIS - Sektoren





NIS - Sektoren

Wesentliche Einrichtungen

In 11 Sektoren mit höhere Kritikalität

- Energie
- Gesundheit
- ICT Service Management
- Transport
- Trinkwasser
- Öffentliche Verwaltung
- Bankwesen
- Abwasser
- Digitale Infrastruktur
- Finanzmärkte
- Weltraum

Wichtige Einrichtungen

In 7 sonstigen Kriterien

- Post
- Industrie
- Digitale Dienste
- Abfall
- Forschung
- Chemikalien
- Lebensmittel

Nationale Umsetzung von NIS2 und RCE



EU RCE Umsetzung durch KRITIS-DachG

- Fokus: Physische Sicherheit und Resilienz
- Betroffen: KRITIS-Betreiber (kritische Anlagen)
- Schutzobjekt: Kritische Anlagen in DE und EU
- Deutsche Aufsicht (BBK)

EU NIS2 Umsetzung durch NIS2UmsuCG

- Fokus: Cybersecurity und Informationstechnik
- Betroffen: KRITIS-Betreiber + besonders wichtige
- Einrichtungen + wichtige Einrichtungen
- Schutzobjekt: Große Teile der Wirtschaft
- Deutsche Aufsicht (BSI) + EU



Strukturwandel braucht IT-Sicherheit

Was bedeutet Strukturwandel durch Digitalisierung und Automatisierung?

Wo liegen die Chancen aber auch Risiken dieses Wandels?

Welche gesetzlichen Regelungen gibt es?

Was können Unternehmen tun, um diesen Wandel sicher zu vollziehen?

Best Practices für die Transformation



- **Entwicklung einer ganzheitlichen Informationssicherheitsstrategie**
- **Implementierung eines ISMS mit technischen und organisatorischen Maßnahmen**
- **Fortlaufende Sensibilisierung der Beschäftigten zur Steigerung des Sicherheitsbewusstseins**



DEEBIT