



**DATAGROUP**

# **DATAGROUP**

**NIS2 und BSIG – Was ist zu tun?**

**Über Risikomanagement, Sicherheitsmaßnahmen,  
Nachweis- und Meldepflichten**

Mainz, 26.02.2026





**Nils Gröne**  
Bereichsleiter GRC & IT Security

DATAGROUP

T +49 40 53007 578  
[nils.groene@datagroup.de](mailto:nilsgroene@datagroup.de)



**Dominik Wiedel**  
Head of Sales & Account Management

DATAGROUP

T +49 671 84030 209  
[dominik.wiedel@datagroup.de](mailto:dominik.wiedel@datagroup.de)



- Kurzvorstellung DATAGROUP und CORBOX
- Einführung in BSIG und NIS2
- Pflichten aus BSIG und NIS2
- Lösungsansätze von DATAGROUP

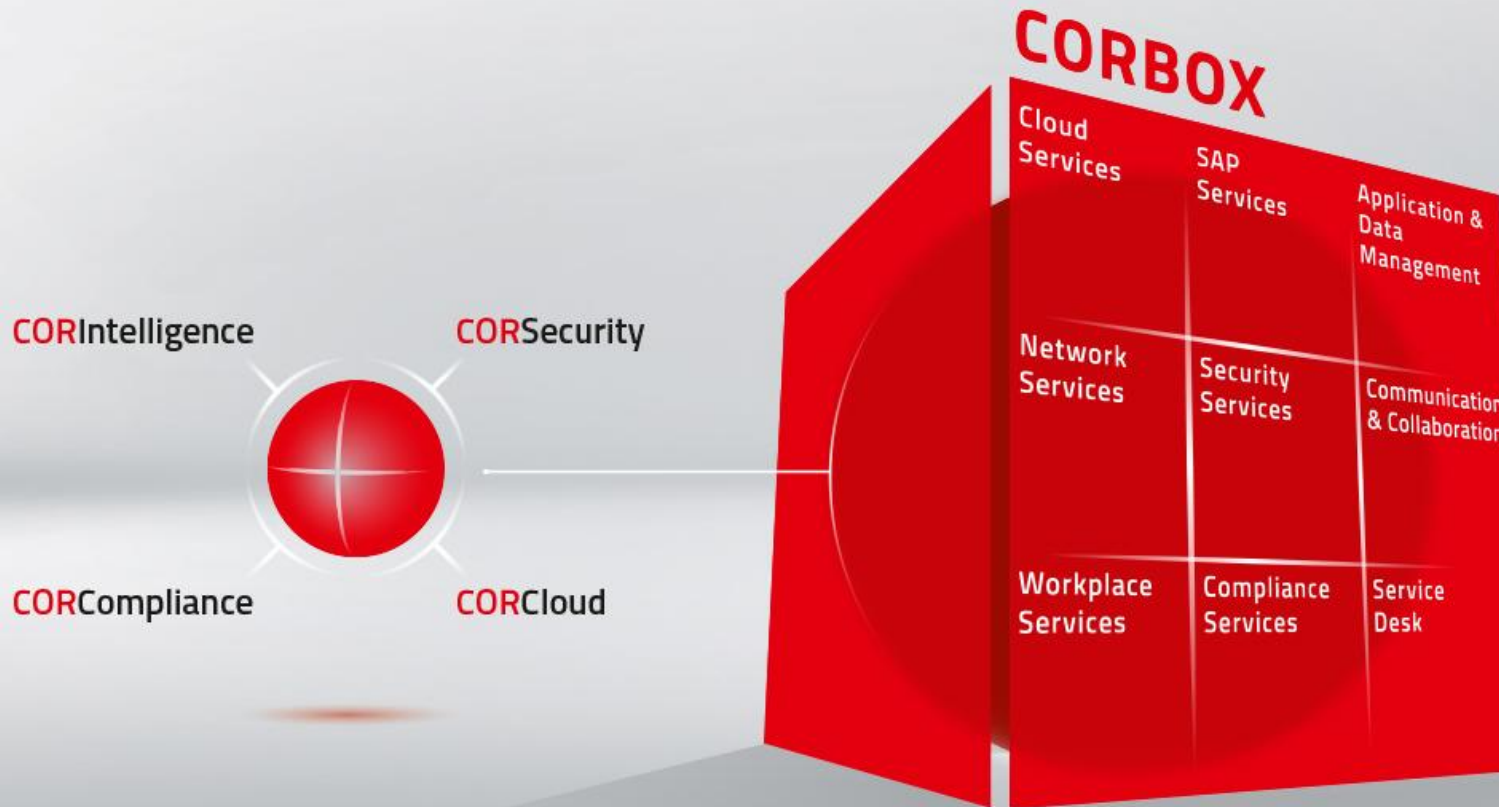
# DATAGROUP-Standorte



DATAGROUP



- Full-Service für IT- und Cloud-Services
- Für Firmen ab 150 IT-Seats
- Rund 3.700 Mitarbeiter
- Mit >30 Standorten bundesweit nah am Kunden



### CORBOX

- **Planbare IT-Kosten:**  
Transparente Preise ohne Überraschungen
- **Flexibel erweiterbar:**  
Module passend zu den Kundenbedürfnissen
- **Effizient:**  
Optimierung durch Skaleneffekte
- **Zertifizierte Qualität:**  
Höchste Standards dank ISO 20000



## CORBOX

Cloud Services	SAP Services	Application & Data Management
Network Services	Security Services	Communication & Collaboration
Workplace Services	<b>Compliance Services</b>	Service Desk



### IT Compliance Reporting (BSIG/NIS2)

- IKS auf Basis ISO 27001:2022 und den geforderten Maßnahmen von NIS2; Meldeprozesse; Reporting (IKS-Handbuch inkl. Kontrollrahmenwerk)
- Option Advanced: mit Wirtschaftsprüfungsbericht „NIS2 Assurance“ zur Wirksamkeit des IKS und regulatorischem Monitoring (NIS2/BSIG)
- Option Individual: Reporting zu IT-Sicherheit, Notfallmanagement und Risikomanagement, Kunden-individuelle Kontrollen und Regulatorisches Monitoring (NIS2/BSIG+B3S/KRITIS)
- Option Support Meldewesen
- Option Revisionsleistungen



### NIS2/KRITIS-Beratung

- Check NIS2-Readiness
- Aufbau und Beratung ISMS
- ISB-aaS
- IT-Security-aaS



### Managed IAM

- Betrieb einer Identity und Access Management Software
- Automatisierte Anlage von Benutzern, Verwaltung der Rechte, Rezertifizierung und Offboarding von Mitarbeitern
- Optional Anbindungen: SAP, Entra ID, Exchange, Cloud Connector
- Optional: IAM Consulting zur organisatorischen Vorbereitung, Einführung und fortlaufender Optimierung



### Lizenzmanagement

- Zentrale Verwaltung und Überwachung der Software-Lizenzen innerhalb des Unternehmens
- Option: Software Scanner



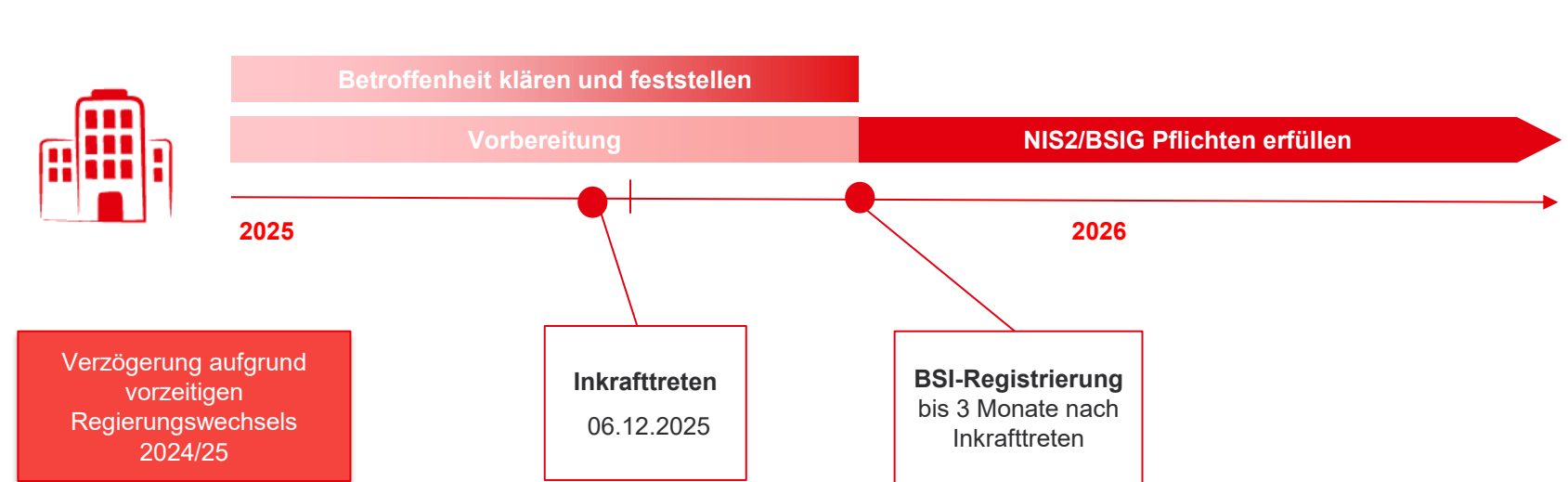
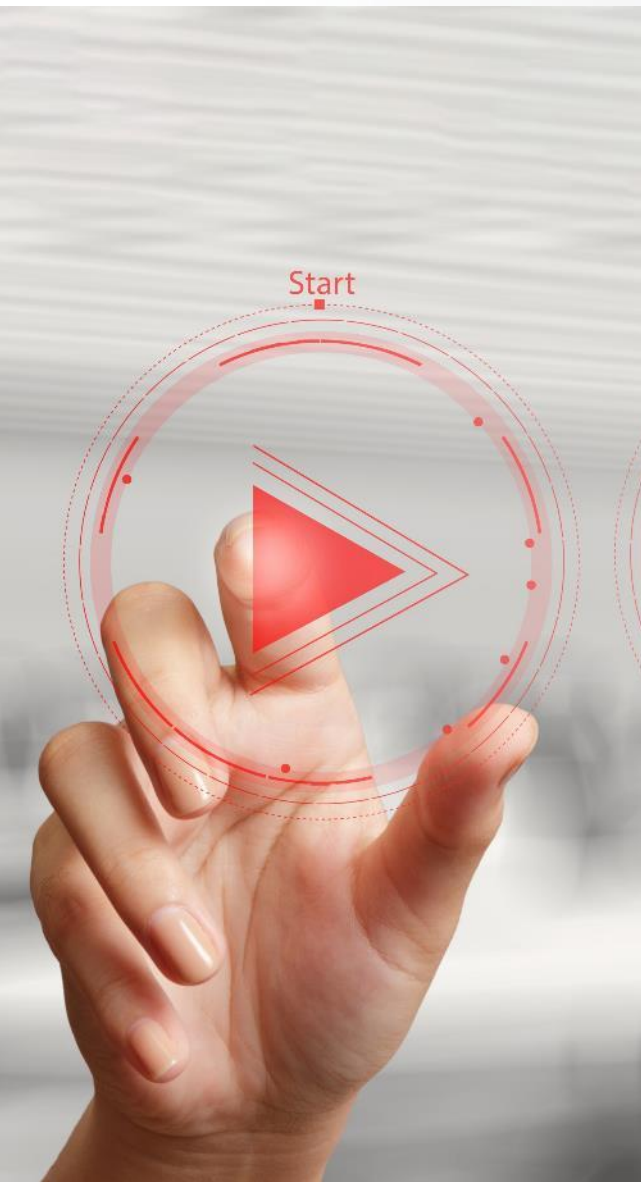
- Die Bedrohungslage in der IT steigt stark an – insbesondere durch Cyber-Angriffe
- Daher steigen regulatorische Anforderungen an IT-Sicherheit und Resilienz
- Seit Januar 2023 ist EU-Richtlinie zur Netzwerk- und Informationssicherheit (**NIS2**) in Kraft
  - Erweiterung der gesetzlichen Erwartungshaltung an ein Sicherheits- und Resilienz-Mindestniveau
  - Breiter Anwendungskreis von mittleren und großen Unternehmen aus verschiedenen Sektoren (ca. 30.000 in Deutschland, viele KMU erstmals in regulatorischer Verantwortung)
  - Verschärfte Meldepflichten bei signifikanten Störungen, Vorfällen, Bedrohungen
  - Erhöhter Handlungsdruck: Aufsichtstätigkeit des BSI und potentielle Sanktionsstrafen
  - Hohe Aufwände insb. durch Nachweis- und Dokumentationspflichten
- Deutsche NIS2-Umsetzung durch Änderung am BSI-Gesetz (**BSIG**) ist am 06.12.2025 in Kraft getreten

# Compliance Services

## BSIG/NIS2: Timeline



DATAGROUP



Stand: Feb. 2026

# Compliance Services

## BSIG/NIS2: Übersicht der Pflichten



Risikomanagement



Meldepflichten



Registrierung



Nachweise



Dokumentation



Informationspflichten



Governance

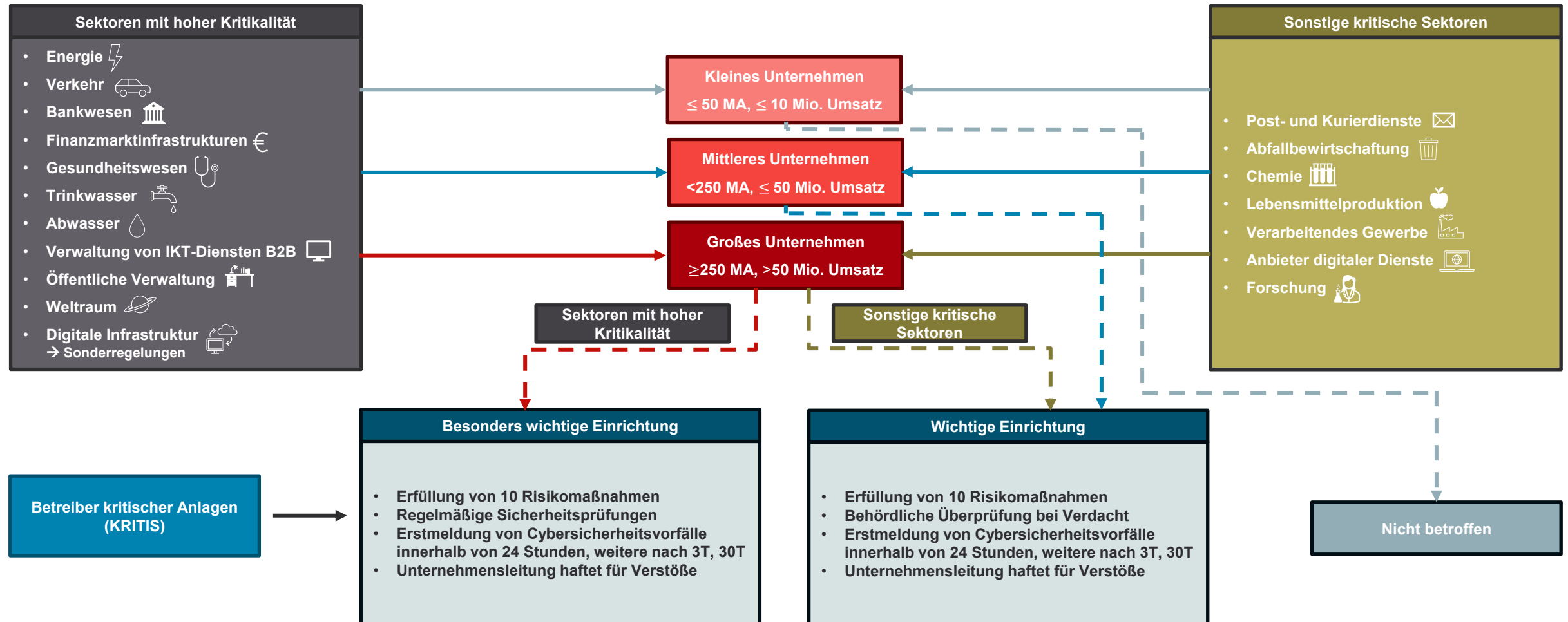
*NIS2-Pflichten (in Anlehnung an OpenKRITIS)*

# Compliance Services

## BSIG/NIS2: Betroffene Unternehmen



DATAGROUP





### BSIG §30 Abs. 1 Risikomanagementmaßnahmen

- **Ziel:** Störungen der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering halten
- Umfangreiche Risikoanalyse und –bewertung
- Einleiten von geeigneten, verhältnismäßigen und wirksamen technischen und organisatorischen Maßnahmen
- Dokumentations-, Prüf- und Nachweispflichten

### BSIG §30 Abs. 2: Mindestmaßnahmen (Kurzübersicht):

1. Konzepte in Bezug auf die Risikoanalyse und Informationssicherheit
  2. Bewältigung von Sicherheitsvorfällen
  3. Backup- sowie Notfall- und Krisenmanagement
  4. Sicherheit der Lieferkette (insb. unmittelbare Anbieter)
  5. Security-by-Design und Schwachstellenmanagement
  6. Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
  7. Schulung und Sensibilisierung zur IT-Sicherheit
  8. Kryptographische Verfahren
  9. Konzepte für Sicherheit des Personals, Zugriffskontrolle und Verwaltung von IKT-Systemen/Produkten/Prozessen
  10. Lösungen für Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation, ggf. gesicherte Notfallkommunikationssysteme
- **Die Einhaltung dieser Pflichten ist zu dokumentieren**
  - **Unternehmen sollten sich risikobasiert über die Mindestmaßnahmen hinaus schützen**
  - **Achten Sie stets auf die Verknüpfung von IT und OT**

### Besondere Anforderungen an Betreiber kritischer Anlagen:

Für den Betrieb der für die Funktionsfähigkeit der kritischen Anlagen maßgeblichen Komponenten, Systeme und Prozesse:

- kann ein **höheres Schutzniveau mit umfangreicherer Maßnahmenumsetzung** als verhältnismäßig angesehen werden (BSIG §31 Abs. 1)
- sind **Systeme zur Angriffserkennung (SZA)** einzusetzen (BSIG § 31 Abs. 2)
  - SZA müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten.
  - Ziel: fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.
  - Zum Beispiel:
    - ✓ Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
    - ✓ Security Information and Event Management (SIEM)
    - ✓ Endpoint Detection and Response (EDR)



### Erheblicher Sicherheitsvorfall

- tritt auf
- wird erkannt
- validiert / bewertet

### Meldung spätestens **24 Stunden** ab Kenntniserlangung:

- Frühwarnung
- Verdacht auf rechtswidrige oder böswillige Handlungen?
- Grenzüberschreitende Auswirkungen?

### Meldung spätestens **72 Stunden** ab Kenntniserlangung

- Aktualisierung der Erstmeldung
- Bewertung des Vorfalls
- Schweregrad
- Auswirkungen
- Kompromittierungsindikatoren

### Spätestens **1 Monat** nach Meldung

- Abschluss- oder Fortschrittmeldung mit ausführlicher Beschreibung, inkl. Schweregrad und Auswirkungen
- Angaben zu Art der Bedrohung / Ursache, getroffene und laufende Abhilfemaßnahmen, grenzüberschreitende Auswirkungen

Partner / Dienstleister müssen regulierte Unternehmen in die Lage versetzen, die notwendigen Informationen fristgerecht vorliegen zu haben sowie bewerten und melden zu können

Schweregrad der Betriebsstörungen, finanzielle Verluste, materielle oder immaterielle Schäden

### Anforderungen

- NIS2 / BSIG
- KRITIS / B3S
- DORA / MaRisk / EBA-GL
- DSGVO
- ...

### Umsetzung

- Internes Kontrollsystem
- Interne Richtlinien
- Risikomanagement
- ISMS
- BCM / ITSCM
- Service- und Security-Prozesse
- Sicherer Betrieb
- Audits
- Kommunikations- und Meldewege

### Nachweise

- Servicebezogener Kontrollrahmen
- Vollständiger Bericht über Angemessenheit und Wirksamkeit des Kontrollsystems zum ISMS
  - Services
  - Prozesse
  - Kontrollen
  - Nachweise
- Prüfung / Bestätigung durch WP
- ISO-Zertifikate
- GRC-Reports / Audits



### Risikoanalyse und Informationssicherheit

- Security Assessment
- Security Consulting
- Pentesting
- IT Compliance Reporting (BSIG/NIS2)



### Incident Handling

- Managed SOC
- Managed SIEM
- Managed EDR
- Managed XDR
- Incident Response



### Business continuity

- Managed SOC
- Managed Backup / Option immutable Backup
- CORBOX Services (SLA Business Critical)



### Supply Chain Security

- Security Assessment (Audit)
- Pentesting
- External Attack Surface Management (EASM)
- VMS



### Sicherheitsmaßnahmen für IT-Systeme und Schwachstellenmanagement

- VMS, EASM
- Client Management / Managed MDM
- Pentesting
- Managed Net Security
- Managed LAN / WLAN (Option NAC / Authent.)
- Managed EDR
- Managed XDR



### Cyberhygiene und Schulungen zur IT-Sicherheit

- Security Awareness Training
- Phishing Simulation



### Kryptografie und Verschlüsselung

- Managed Landing Zone (Hyperscaler Cloud)
- Managed M365
- Verschlüsselung und Optionen in div. CORBOX Services



### Zugriffskontrolle

- IAM Consulting
- Managed IAM
- Managed AD
- Managed M365
- Managed SASE



### MFA oder kontinuierliche Authentifizierung

- Managed M365
- Managed AD
- Managed RAS (Option MFA/ Zerotrust)



### Bewertung und Nachweis der Wirksamkeit

- IT Compliance Reporting (BSIG/NIS2)

# Compliance Services

## BSIG/NIS2: Herausforderungen



DATAGROUP



- Kurzfristig: Klärung der individuellen Betroffenheit (BSIG § 28) und Registrierungspflicht (BSIG § 33)
- Geschäftsführung ist für Umsetzung und Überwachung der Risikomanagementmaßnahmen verantwortlich und haftbar (BSIG §38)
  - Schulung der Geschäftsführung
  - Verantwortliche zur Koordination der NIS2-Umsetzung und Ausbau der IT-Sicherheit benennen
- Aufbau/Weiterentwicklung eines BSIG/NIS2-konformen Informationssicherheitsmanagements
  - Bestandsaufnahme und Risikoanalyse der IT-Sicherheit
  - Risikomanagementmaßnahmen aus BSIG/NIS2 ins ISMS des Unternehmens integrieren und auf unterschiedliche Bedrohungsszenarien anpassen
  - Angemessen, wirksam und nachweisbar umsetzen
  - Maßnahmen, Prozesse, Kontrollen und operative Sicherheit miteinander verzahnen
- Melde- und Auskunftswege in Richtung BSI etablieren
- Umfangreiche Dokumentations- und Nachweispflichten
- Lieferkettensicherheit: Dienstleister vertraglich verpflichten, steuern und kontrollieren



### CORBOX

Cloud Services	SAP Services	Application & Data Management
Network Services	Security Services	Communication & Collaboration
Workplace Services	<b>Compliance Services</b>	Service Desk

- Viele Unternehmen sind noch nicht auf die NIS2/BSIG-Regulatorik vorbereitet bzw. sehen sich mit der Umsetzung herausgefordert
- DATAGROUP Compliance Services:
  - ✓ Beratung zum Erfüllen von NIS2/KRITIS-Anforderungen
    - Einstieg z. B. über „NIS2-Starterpaket“
  - ✓ Angebot von IT-Services auf Regulatorik-konformen Niveaus (inkl. Reporting und Nachweisführung, Sicherheitsstandards und IT-Sicherheitslösungen)
  - ✓ DATAGROUP versorgt Kunden mit benötigten Berichten und Nachweisen für ihr Risiko- und Compliance-Management
  - ✓ Laufendes Monitoring der Bedrohungs-/Gefährdungslage und der Compliance-Anforderungen

Danke für Ihre Aufmerksamkeit.  
Welche Fragen sind bei Ihnen offen geblieben?



**DATAGROUP**

Spätere Fragen gern an:

**Nils Gröne**

T +49 40 53007 578

[nils.groene@datagroup.de](mailto:nils.groene@datagroup.de)



# NIS2 Starterpaket



DATAGROUP

 DATAGROUP

**SIND SIE BEREIT FÜR NIS2?**

**Buchen Sie jetzt unser Starterpaket!**

Wir prüfen, wo Ihr Unternehmen steht und zeigen, welche **Maßnahmen** nötig sind – schnell, transparent und zum **Festpreis von 4.990 €.**

**Jetzt starten!**

