

PREPARE

PROTECT

DETECT

RESPOND

IMPROVE

# Handlungsfähig, wenn es darauf ankommt. Business Continuity Management.

BCM sorgt dafür, dass geschäftskritische Prozesse bei Cyberangriffen, IT-Ausfällen oder Krisen weiterlaufen oder schnellstmöglich wieder anlaufen. Argos baut mit Ihnen ein praxistaugliches BCM auf, das über Papier hinausgeht.

&gt;600

Kunden

100+

Security-  
Experten

24/7

Cyber Defense  
Center

seit 1999

Managed  
Security

ISO 27001

TÜV-SÜD-  
zertifiziert

NIS-2

DSGVO- & ISO-  
27001-Nachweise  
unterstützt

## Das leistet der Service für Sie.



### Business Impact Analyse

Die BIA ermittelt Ihre wirklich geschäftskritischen Prozesse – statt generischer Vorlagen entsteht ein BCM, das zu Ihrem Unternehmen passt.



### Wiederanlaufziele

Belastbare Wiederanlaufziele (RTO/RPO) je Prozess definieren, was wann wieder laufen muss – die Grundlage für Notfall- und Wiederanlaufpläne.



### Notfallorganisation

Notfall- und Wiederanlaufpläne mit klaren Rollen und Eskalationswegen sowie eine handlungsfähige Notfallorganisation, die im Ernstfall trägt.



### Übungen & Reviews

Vorbereitete Krisenkommunikation, Integration mit Incident Response und regelmäßige Übungen und Reviews halten das BCM wirksam und aktuell.

**Für wen:** Für Organisationen, die ihre kritischen Prozesse gegen Ausfälle absichern müssen – mit Orientierung an ISO 22301 und konform zu KRITIS-, DORA- und NIS-2-Anforderungen.



**BCM aus generischen Vorlagen bleibt Papier – im Ernstfall trägt es nicht.** Argos ermittelt Ihre wirklich geschäftskritischen Prozesse und verzahnt BCM nahtlos mit Incident Response und Krisenprozessen – ein BCM aus einem Guss, mit klaren Wiederanlaufzielen und geübten Abläufen.

# Argos Business Continuity Management vs. klassischer Ansatz

der Vergleich auf einen Blick

| Kriterium     | Klassischer Ansatz                      | Argos Business Continuity Management                                          |
|---------------|-----------------------------------------|-------------------------------------------------------------------------------|
| Ausgangspunkt | Generische Vorlagen und Musterpläne     | Ihre geschäftskritischen Prozesse ermittelt über eine Business Impact Analyse |
| Ziele         | Unklare Erwartungen an den Wiederanlauf | RTO/RPO je Prozess definiert                                                  |
| Ernstfall     | Pläne bleiben Papier, Rollen unklar     | Geübte Abläufe, klare Rollen mit Eskalationswegen und Notfallorganisation     |
| Integration   | BCM und Incident Response getrennt      | Nahtlos mit IR verzahnt inklusive vorbereiteter Krisenkommunikation           |
| Compliance    | Nachweise mühsam zusammengetragen       | Orientierung an ISO 22301 konform zu KRITIS-, DORA- und NIS-2-Anforderungen   |

## Ihr Leistungsumfang im Überblick

- ✓ Business Impact Analyse (BIA)
- ✓ Wiederanlaufziele (RTO/RPO) je Prozess
- ✓ Notfall- und Wiederanlaufpläne mit Rollen und Eskalationswegen
- ✓ Handlungsfähige Notfallorganisation
- ✓ Vorbereitete Krisenkommunikation und IR-Integration
- ✓ Regelmäßige Übungen und Reviews

**Für Ihre Geschäftsleitung:** Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, >600 Kunden) · Überwachung erfüllbar (Reporting an die Geschäftsleitung) · Leistungsumfang vertraglich klar definiert.

**Ihr Part:** benannte Ansprechpartner und Dokumentenzugang – Rollen, Zuständigkeiten und Berichtswege werden gemeinsam festgelegt. Details (Leistungsbeschreibung, AVV/TOM) im Erstgespräch.

## Souverän. Deutsch. Nachweisbar.

- » Deutscher Anbieter – seit 1999, Sitz in München
- » 100+ Security-Expertinnen und -Experten
- » ISO/IEC 27001 zertifiziert (TÜV SÜD)
- » Unterstützt NIS-2-, DORA- und ISO-27001-Nachweise
- » DSGVO-konforme Verarbeitung – AVV (Art. 28) & TOM auf Anfrage
- » Angebunden an das 24/7 Cyber Defense Center

## So starten Sie mit dem Service

### 01

#### Erstgespräch & Analyse

Wir identifizieren in der Business Impact Analyse Ihre geschäftskritischen Prozesse und die Auswirkungen von Ausfällen auf Ihr Geschäft.

### 02

#### Ziele & Pläne

Gemeinsam definieren wir Wiederanlaufziele (RTO/RPO) je Prozess und erstellen Notfall- und Wiederanlaufpläne mit Rollen und Eskalationswegen.

### 03

#### Üben & Verankern

Die Notfallorganisation wird aufgebaut, mit Incident Response verzahnt und in regelmäßigen Übungen und Reviews trainiert und aktuell gehalten.

## Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Business Continuity Management auf Ihre Organisation und Ihre Anforderungen zugeschnitten wird.



Dr. Nils Kaufmann  
Chief Sales Officer

+49 89 45 24 24-100

kontakt@argos.security · [www.argos.security](http://www.argos.security)

Mehr zur Leistung: [argos.security/leistungen/bcm](https://argos.security/leistungen/bcm) →



Termin buchen