Sicher und resilient auch in turbulenten Zeiten

Mit integriertem Risk & Security Management zu nachhaltigem Unternehmenserfolg

Philipp Strokosch, Martin Tanzer

Das GBTEC Team

Philipp Strokosch

Head of Product Line GRC,
Managing Director GBTEC Austria

Martin Tanzer

GRC Solution Architect

Wie ist der Status Quo im Unternehmensalltag?

GRC wird von vielen Unternehmen als Bremse gesehen

Welche Folgen sind möglich?

- Das Personal im Tower hatte keinen Zugriff auf aktuelle Systeminformationen
- Die Gepäcklogistik kam komplett zum Erliegen
- Die Terminals waren außer Betrieb
- Die Sicherheitskräfte bekamen keine Updates

Wie konnte es so weit kommen?

Was sollten Unternehmen daraus lernen?

GRC ist das Betriebssystem moderner Unternehmens-steuerung

Der Einwand: Die Kosten sind zu hoch

Welche Kosten entstehen ohne GRC?

- Reputationsschaden
- Nachrüstungskosten
- Wirschaftlicher Schaden
- Möglicher Schadenersatz

Gewinn maximieren mit GRC

Welche Vorteile bringt GRC?

- Stetiger Vertrauensgewinn
- Geringere Kosten
- Stabile Betriebskontinuität
- Planbare Ausgaben

Ein intelligentes, vorausschauendes Steuerungssystem, das sich dann bewährt, wenn es darauf ankommt – nicht wenn es zu spät ist. Denn Resilienz zeigt sich in der Wirkung, nicht in der Wahrscheinlichkeit.

Out of the Box

Was eine integrierte GRC-Lösung leisten kann

What is GRC?

G **GOVERNANCE**
... achieve objectives

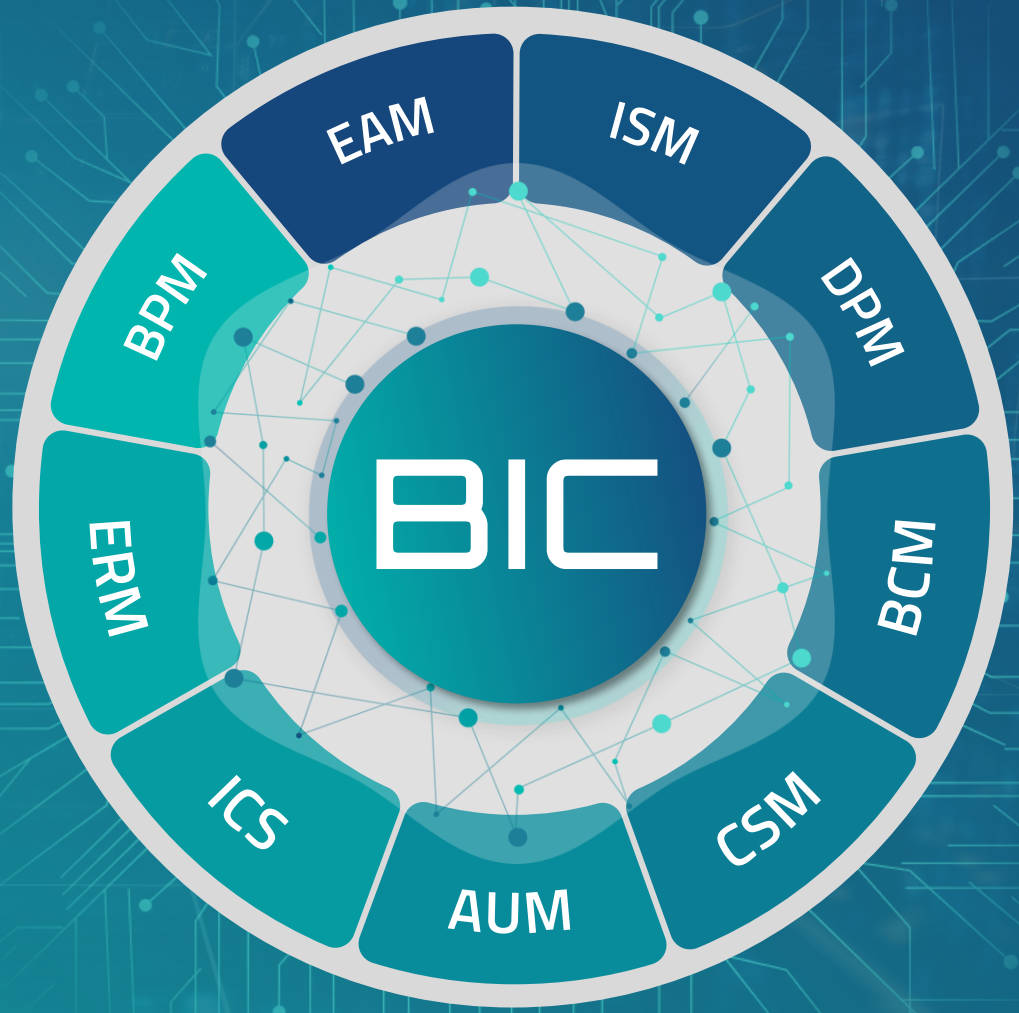
R **RISK**
... address uncertainty

C **COMPLIANCE**
... act with integrity

GRC is …

… looking **together** at the same **objectives**, but from different **perspectives**!

… an **integrated** collection of capabilities to reliably achieve **objectives**, address **uncertainty**, and act with **integrity**.



Beispiel-Szenario: Einführung einer neuen Bürgerplattform

Anlass

Die Behörde führt einen neuen digitalen Bürgerservice ein (z.B. Online-Anträge).
Die Plattform ist "digital by design", um Effizienz und Bürgernähe zu steigern.

Auswirkung

Die neue Plattform schafft eine Angriffsfläche für externe Bedrohungen, wie Cyberangriffe und unautorisierte Zugriffe auf sensible Daten. Dies erhöht die Komplexität der Steuerung und Kontrolle.

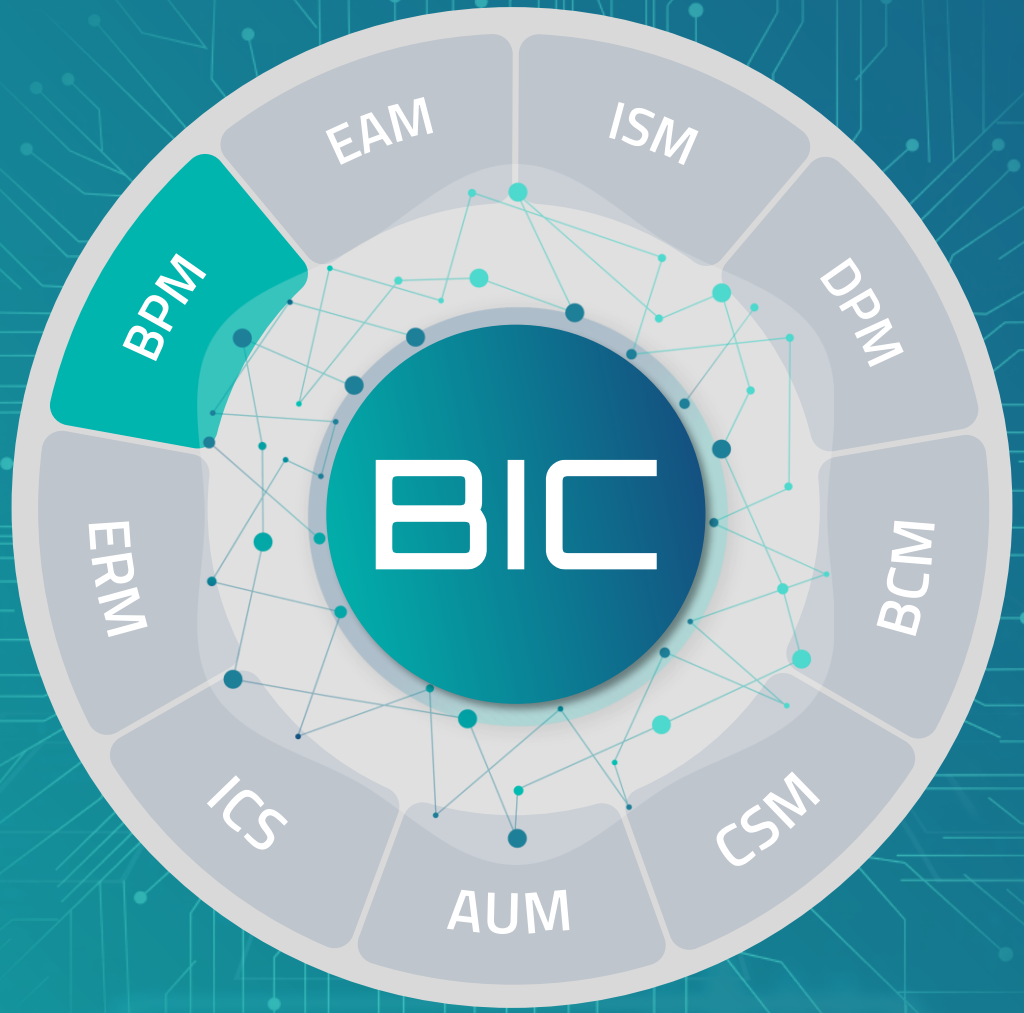
Risiko

Schwachstellen in der IT-Architektur könnten zu Datenschutzverletzungen, Systemausfällen oder Reputationsschäden führen, die das Vertrauen der Bürger nachhaltig beeinträchtigen.

Ziel

Das übergeordnete Ziel ist die Etablierung einer robusten GRC-Struktur, die die Informationssicherheit und Compliance umfassend schützt und kontinuierlich verbessert.

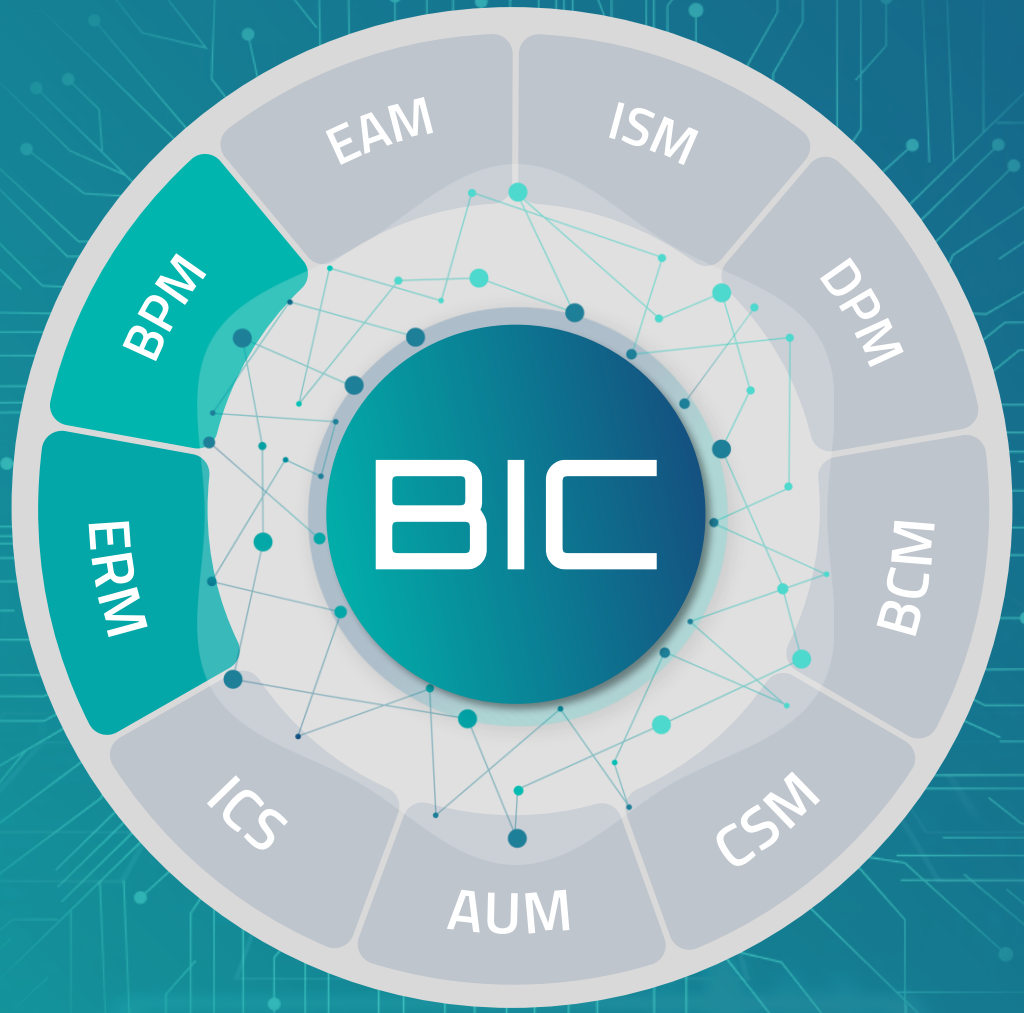
Fokus auf die Domänen …



Business Process Management

Die Behörde **modelliert** den neuen End-to-End-Prozess für Online-Anträge (z. B. für eine Meldebestätigung) in einem zentralen Prozessportal.
Medienbrüche – wie früher beim Ausdrucken und Einreichen von Formularen – werden eliminiert. Bürgerinnen und Bürger können den Antrag vollständig online abwickeln, während die internen Prozessschritte (Prüfung, Genehmigung, Zustellung) digital gesteuert werden.

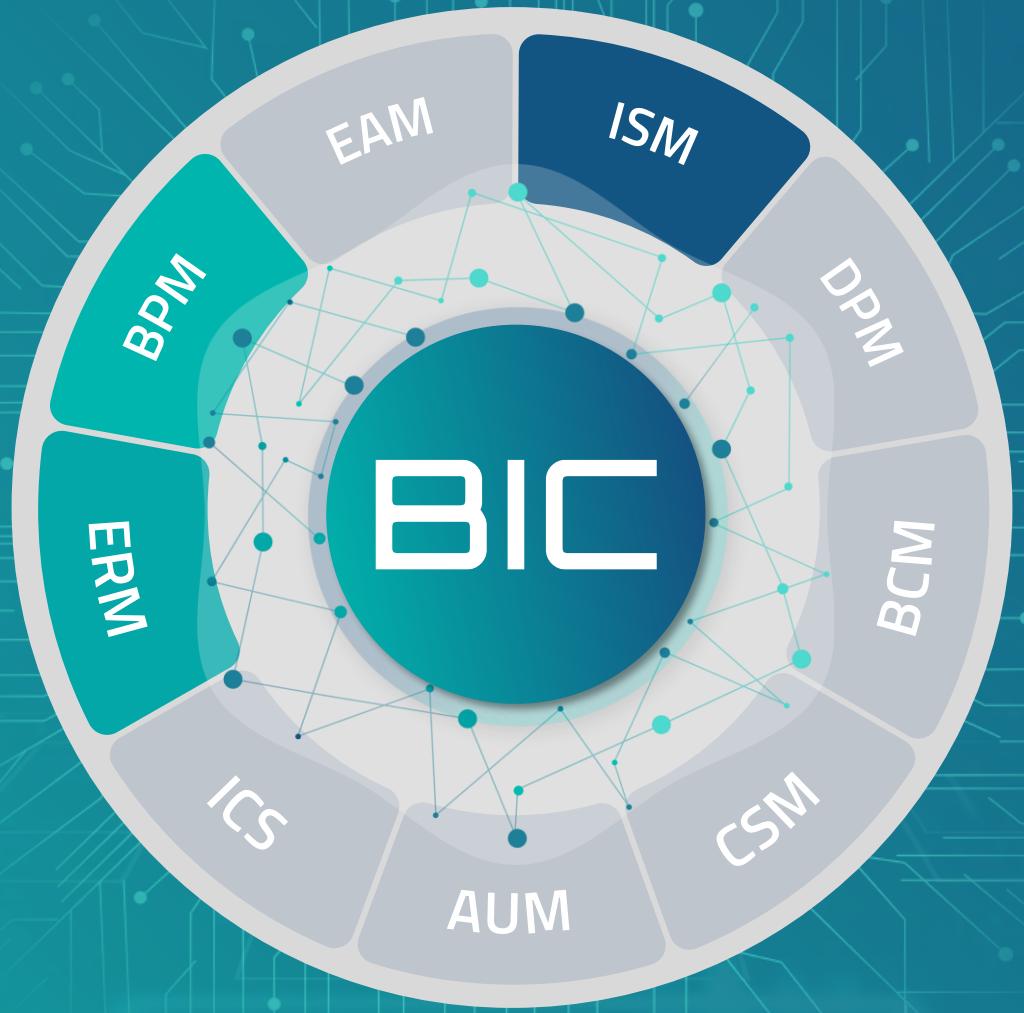
Fokus auf die Domänen …



Enterprise Risk Management

Das ERM identifiziert Risiken wie Systemausfälle, Cyberangriffe oder geringe Akzeptanz des Services durch die Bürger.
Mittels Risikobewertungen und Szenarioanalysen wird z. B. die Eintrittswahrscheinlichkeit eines Ausfalls während der Spitzenzeiten (Anmeldungen zum Studienjahr, Wahlservices) bewertet.
Maßnahmen zur Risikominimierung werden priorisiert.

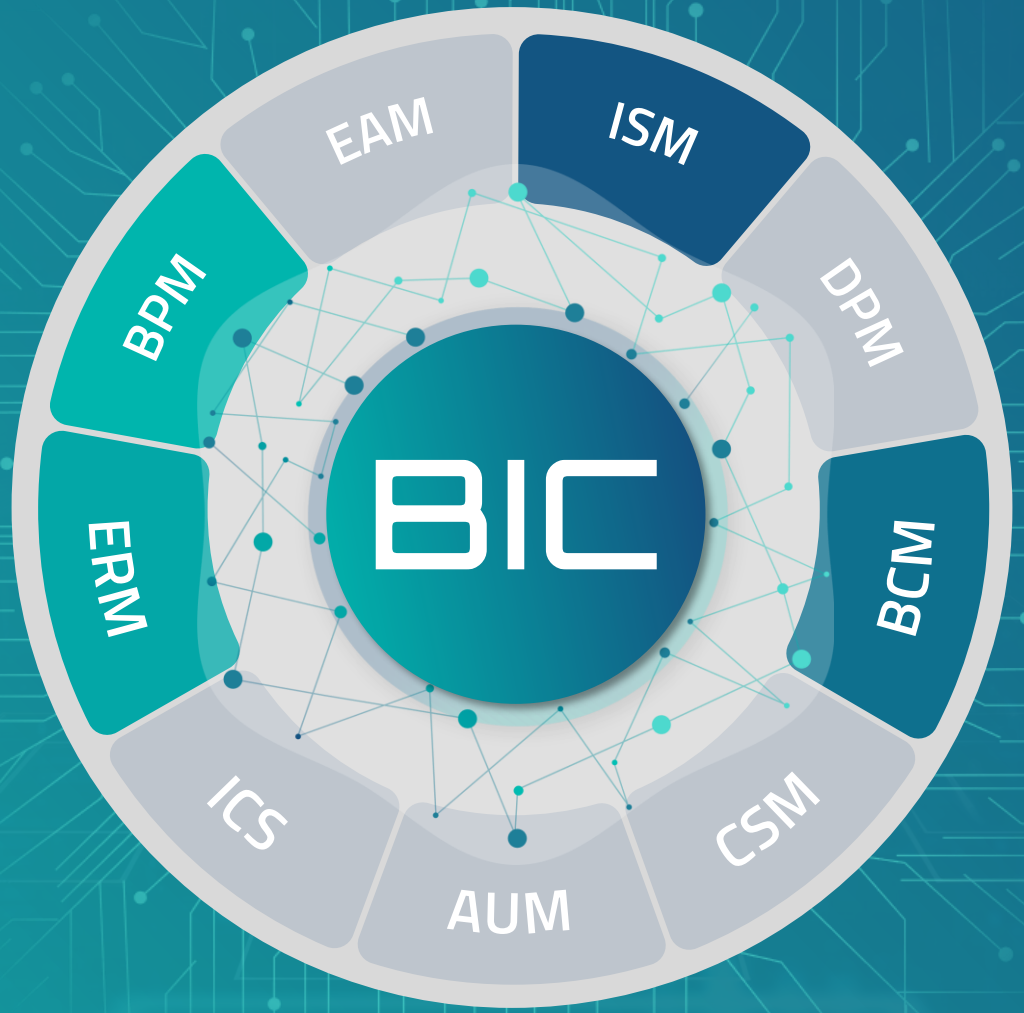
Fokus auf die Domänen …



Information Security Management

Ein ISMS stellt sicher, dass die Vertraulichkeit und Integrität sensibler Bürgerdaten (z. B. Wohnsitz, Geburtsdatum) gewährleistet ist. Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierung über die ID Austria oder Verschlüsselung bei der Datenübertragung werden implementiert.
Regelmäßige Penetrationstests decken potenzielle Schwachstellen auf.

Fokus auf die Domänen …

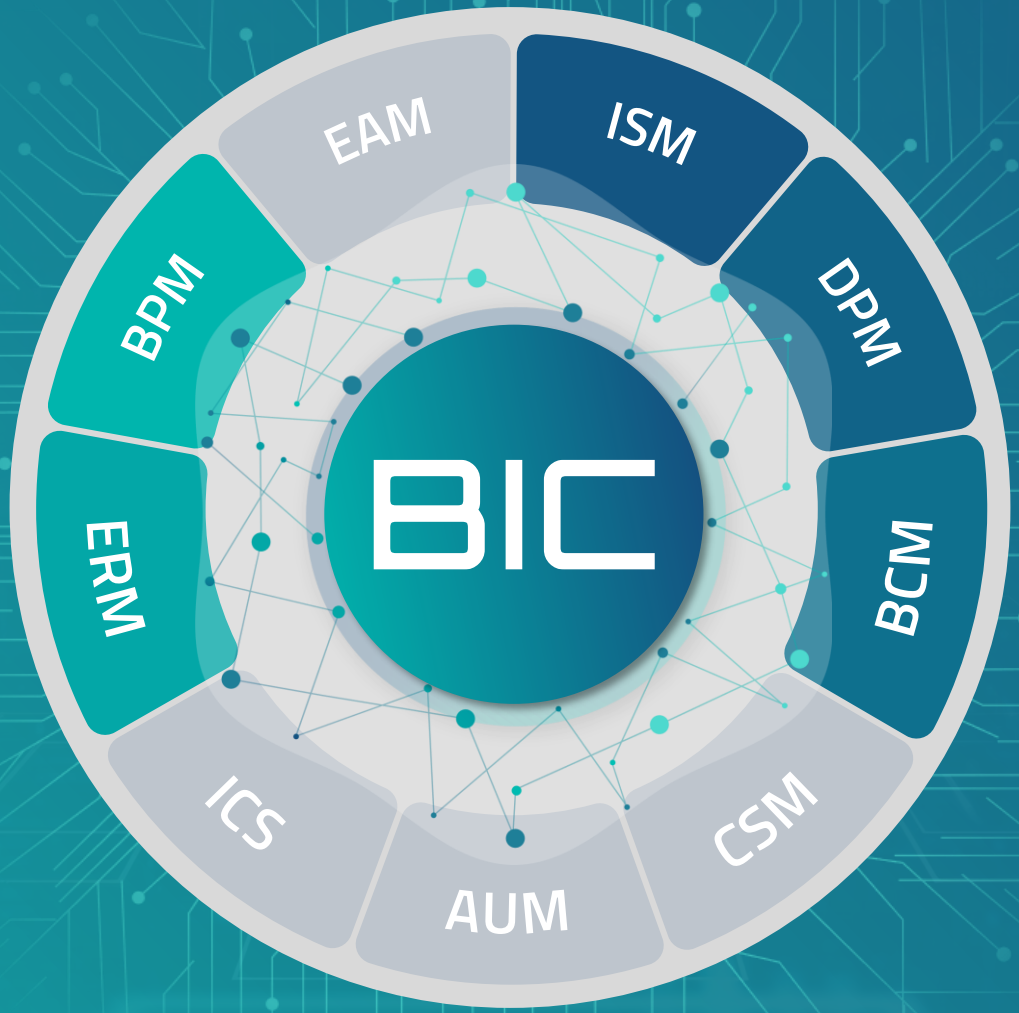


Business Continuity Management

Es wird ein Notfallkonzept erstellt, damit die Plattform auch im Krisenfall verfügbar bleibt.

Zum Beispiel: Fällt das Rechenzentrum aus, erfolgt ein automatischer Failover zu einem Ausweichstandort. Für Bürger:innen wird ein „Fallback-Service“ bereitgestellt (z. B. Hotline oder vereinfachtes Ersatzformular), um die Bearbeitung sicherzustellen.

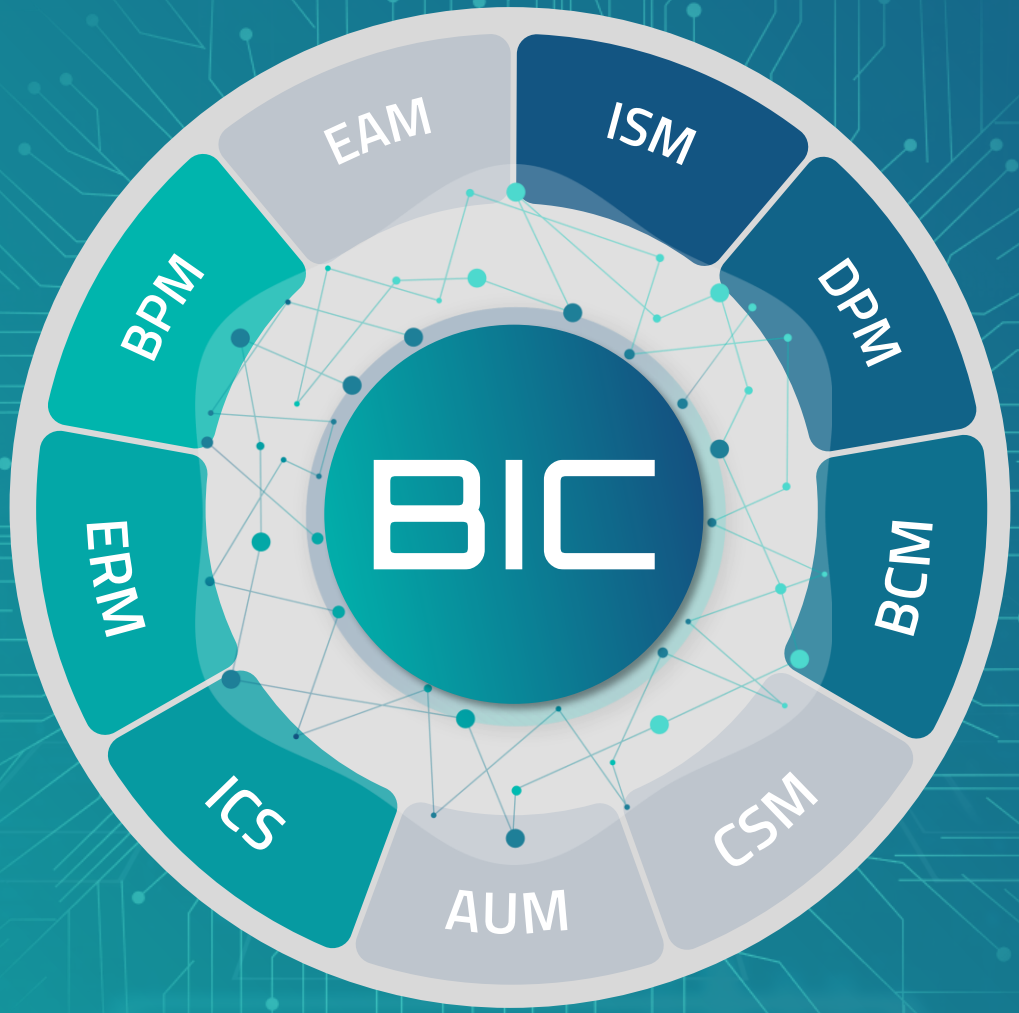
Fokus auf die Domänen …



Data Protection Management

Der digitale Bürgerservice wird DSGVO-konform gestaltet.
Bürger:innen erhalten transparente Informationen über die Verarbeitung ihrer Daten und können ihre Rechte (Auskunft, Berichtigung, Löschung) direkt online ausüben.
Daten werden nur für den klar definierten Zweck des Antrags erhoben und nach Ablauf gesetzlicher Aufbewahrungsfristen gelöscht.

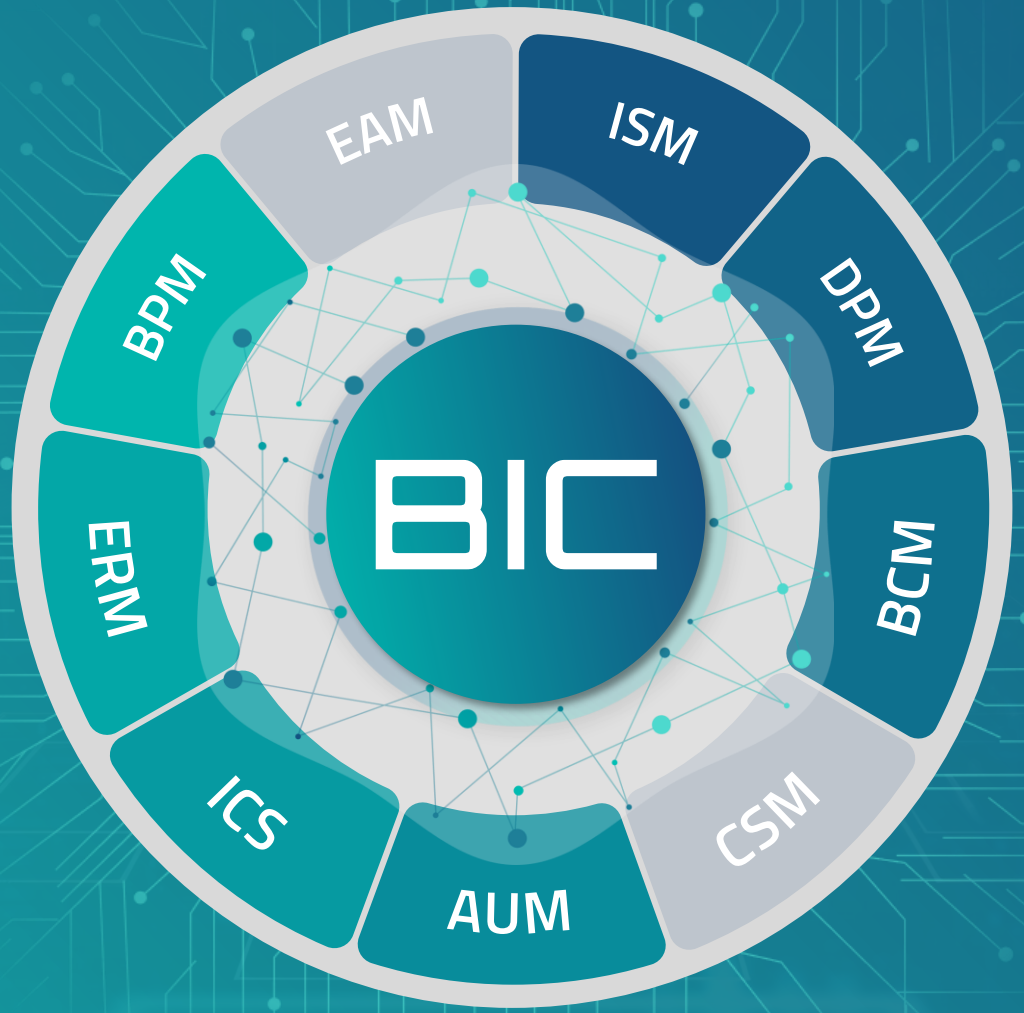
Fokus auf die Domänen …



Internal Control System

Das IKS stellt sicher, dass die korrekte Bearbeitung der Online-Anträge durch Kontrollen unterstützt wird.
Beispielsweise gibt es automatisierte Prüfschritte, die sicherstellen, dass ein Antrag nur dann genehmigt wird, wenn alle erforderlichen Unterlagen vorliegen.
Auch Zugriffsrechte für Mitarbeitende sind klar geregelt und werden regelmäßig kontrolliert.

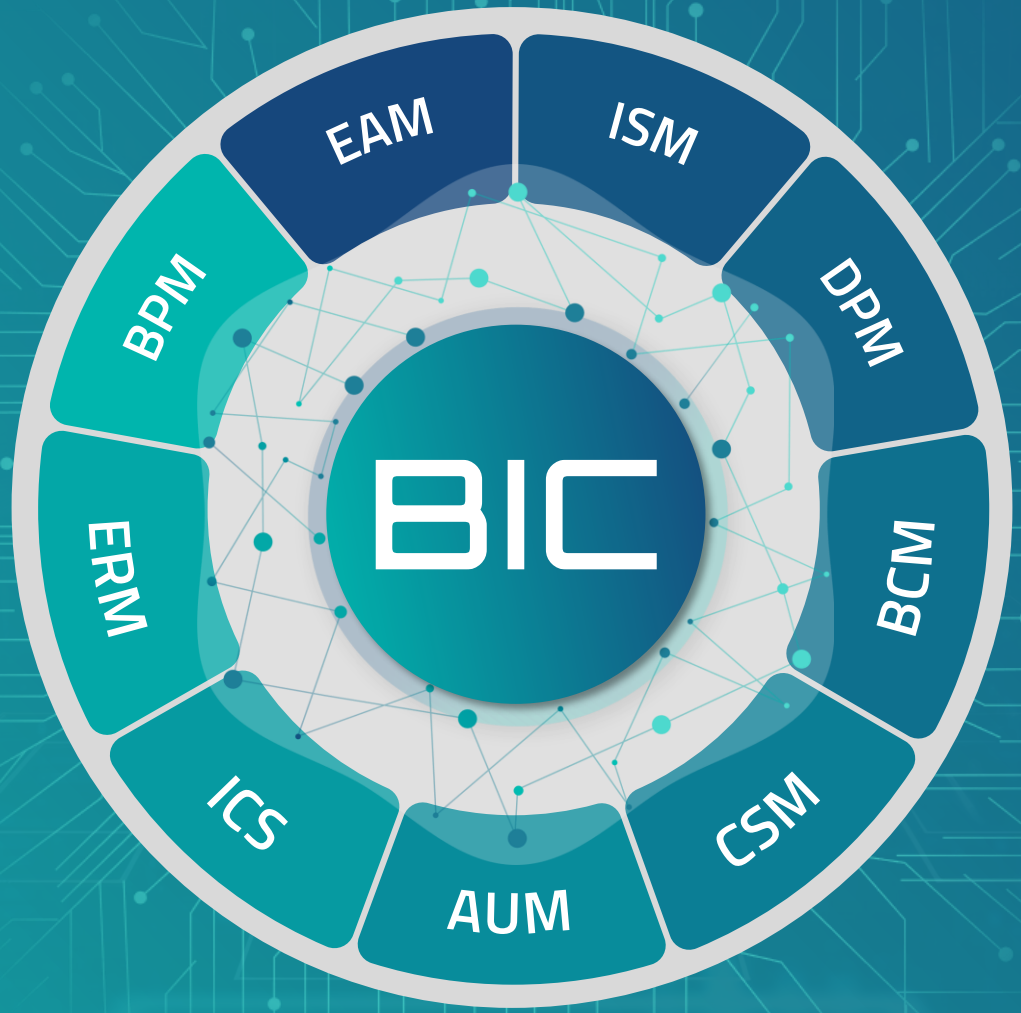
Fokus auf die Domänen …



Audit Management

Interne und externe Audits überprüfen, ob der digitale Bürgerservice den rechtlichen und organisatorischen Vorgaben entspricht Beispielsweise kontrolliert der Rechnungshof, ob der Service effizient implementiert wurde, während interne Audits die Einhaltung der Datenschutz- und IT-Sicherheitsmaßnahmen prüfen.

Fokus auf GRC!



Relevante GRC-Domänen

Business Process Management (BPM)

…sorgt für effiziente, transparente Abläufe und erleichtert Bürgerinnen und Bürgern den schnellen Zugang zu digitalen Services.

Enterprise Risk Management (ERM)

…ermöglicht, Risiken wie Systemausfälle oder Cyberangriffe frühzeitig zu erkennen und gezielt zu steuern.

Information Security Management (ISM)

…gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Bürgerdaten.

Business Continuity Management (BCM)

…stellt sicher, dass der digitale Service auch bei Störungen oder Krisen verfügbar bleibt.

Relevante GRC-Domänen

Data Protection Management (DPM)

…schafft Vertrauen, indem personenbezogene Daten rechtskonform und transparent verarbeitet werden.

Internal Control System (ICS)

…sorgt für die regelkonforme, sichere und nachvollziehbare Bearbeitung aller digitalen Anträge.

Audit Management (AUM)

…überprüft die Wirksamkeit der Systeme und Nachweise gegenüber internen wie externen Prüfinstanzen.

Vorteile durch verzahnte GRC-Systeme

Transparenz

Zentrale Erfassung aller Risiken, Kontrollen und Anforderungen für ganzheitliche Steuerung

Effizienz

Vermeidung von Redundanzen senkt Dokumentations- und Prüfaufwand

Synergien

Wechselwirkungen zwischen Risiken werden sichtbar und gezielt adressiert

Resilienz

Integration von BCM, ISMS, Datenschutz und IKS stärkt Krisenfestigkeit

Compliance

Einheitliche Umsetzung und Nachweis regulatorischer Anforderungen

Steuerung

Fundierte, informierte Entscheidungen auf Basis konsolidierter Informationen

Sehen Sie hier weitere konkrete integrierte GRC Use Cases!

Einfache und zeitsparende Integration von:

BCM, CSM, BPM

BCM, ERM, BPM

ISM, ERM, IKS, AUM

Questions & Answers