



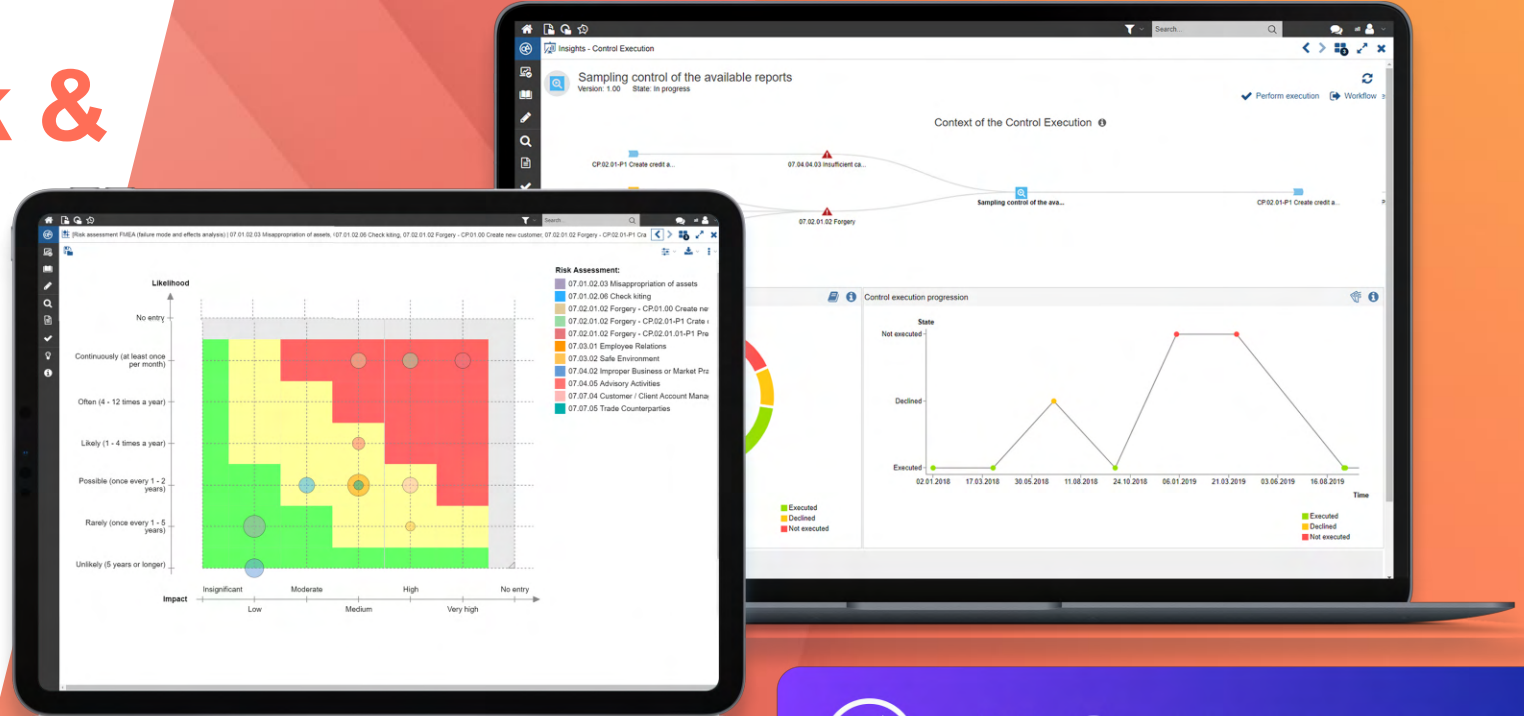
ADOGRC

Governance, Risk & Compliance Suite

BOC Group
Design Your Enterprise

Governance, Risk & Compliance in the Age of AI

Product & AI Strategy 2026f
Erik Guschlbauer, BOC Group



AI Governance

GRC is moving from obligation to business enablement.



8/10

*of the most important
global business risks are
directly related to GRC.¹*

84%

*say compliance is increasingly
becoming a business enabler.²*

82%

*plan to invest more in
GRC technology.³*



ADOGRC

Governance, Risk & Compliance Suite
by boc-group.com

Minimal Effort.
Full Compliance.



Minimal Effort. Full Compliance.

AI Governance

Scope

Embed

Assess

AI-powered GRC

Connect

Understand

Automate

Trusted Context

Assure

Improve

Confirm



ADOGRC

Governance, Risk & Compliance Suite



BOC Group

Design Your Enterprise



Focus 1

Govern Business Transformation and AI Adoption.

**Efficiency & Insights through
AI-Powered GRC**

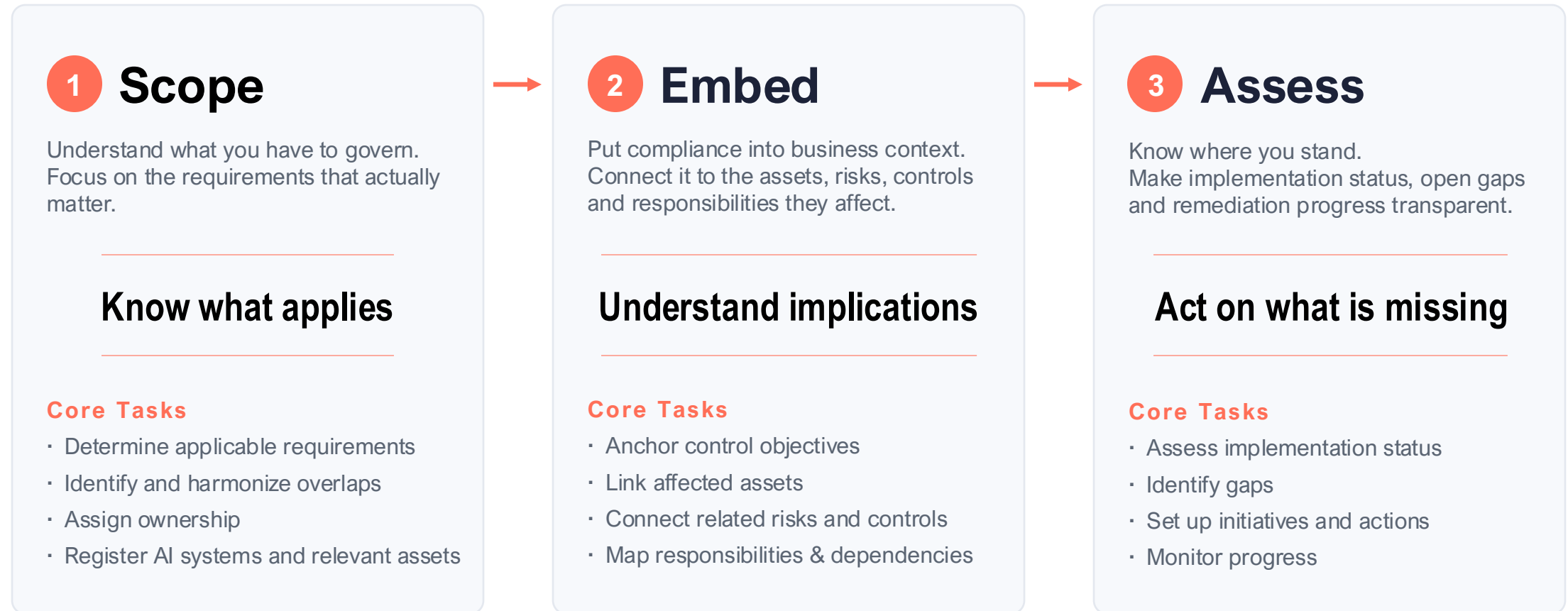
**Reliable Information
as Trusted Context.**

Turn AI requirements into governed, measurable actions.



ADOGRC

Governance, Risk & Compliance Suite
by boc-group.com



Focus on what matters – without starting from scratch.



Control Objectives Catalog

Type	Name ↑	Related Requirements
+	Artificial and Autonomous Technology (AAT)	EU AI Act • ISO/IEC 42001 • NIST AI RMF 1.0 •
+	Asset Management (AST)	EU AI Act • ISO/IEC 27001 • NIST CSF 2.0 • COBIT 2019 •
+	Business Continuity & Disaster Recovery (BCD)	EU AI Act • ISO 22301 • NIST SP 800-34 Rev.1 • DORA •
+	Capacity & Performance Planning (CAP)	EU AI Act • NIST CSF 2.0 • ISO/IEC 27001 • COBIT 2019
+	Change Management (CHG)	EU AI Act • ISO/IEC 27001 • ITIL 4 • NIST CSF 2.0 • COBIT
+	Cloud Security (CLD)	EU AI Act • ISO/IEC 27017 • ISO/IEC 27018 • CSA CCM v4
+	Compliance (CPL)	EU AI Act • ISO/IEC 37301 • ISO/IEC 19600 • NIST CSF 2.0
+	Configuration Management (CFG)	EU AI Act • CIS Controls v8 • NIST CSF 2.0 • ISO/IEC 27001
+	Continuous Monitoring (MON)	EU AI Act • NIST CSF 2.0 • ISO/IEC 27001 • NIST SP 800-13
+	Cryptographic Protections (CRY)	EU AI Act • ISO/IEC 27002 • NIST SP 800-57 Part 1 Rev.5 •
+	Cybersecurity & Data Protection Governance (GOV)	EU AI Act • NIST CSF 2.0 • ISO/IEC 27014 • NIS2 • GDPR
+	Data Classification & Handling (DCH)	EU AI Act • ISO/IEC 27001 • GDPR • NIST SP 800-60 Rev.2
+	Data Privacy (PRI)	EU AI Act • GDPR • ISO/IEC 27701 • NIST Privacy Framework
+	Embedded Technology (EMB)	EU AI Act • IEC 62443 • ISO/SAE 21434 • NIST SP 800-82 R
+	Endpoint Security (END)	EU AI Act • CIS Controls v8 • NIST CSF 2.0 • ISO/IEC 27001
+	Human Resources Security (HRS)	EU AI Act • ISO/IEC 27002 • NIST CSF 2.0 • ISO/IEC 27001
+	Identification & Authentication (IAC)	EU AI Act • NIST SP 800-63-3 • ISO/IEC 27001 • NIST SP 800-63-1
+	Incident Response (IRO)	EU AI Act • NIST SP 800-61 • ISO/IEC 27001 • NIST AI RMF 1.0
+	Information Assurance (IAO)	EU AI Act • ISO/IEC 27001 • NIST SP 800-37 Rev.2

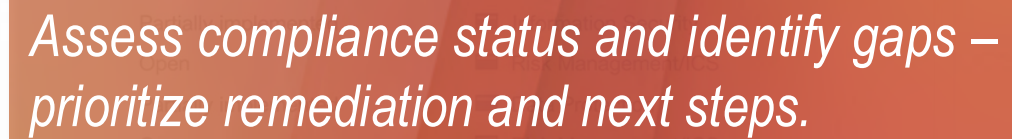
Publisher

- Publisher BSI**
 - IT-Grundschutz
 - BSI Orientierungshilfe KI
- Publisher COSO**
 - COSO Internal Control Framework
- Publisher EU**
 - EU AI Act
 - DORA
 - NIS2
 - GDPR
- Publisher ISO**
 - ISO/IEC 42001
 - ISO/IEC 27001
- Publisher NIST**
 - NIST CSF 2.0

Harmonize requirements across standards and regulations – reduce duplication and scope AI compliance faster.

Connect compliance to the business it governs.







ADOGRC

Governance, Risk & Compliance Suite

 **BOC Group**
Design Your Enterprise



Focus 2

Improve efficiency & insights through AI-Powered GRC.

**Govern Business Transformation
and AI Adoption.**

**Reliable Information
as Trusted Context.**

Turn fragmented data into key business insights.



1 Connect

Combine fragmented data into a unified, governed repository – once – and reuse it everywhere.

Rely on a single source

Core Tasks

- Unify requirements, controls, risks, etc.
- Match relationships, remove duplicates
- Reuse one repository across frameworks
- Maintain shared catalogues and lists



2 Understand

Turn connected data into decision-ready insights. Visualize dependencies and gaps – not just the data.

Gain actionable insights

Core Tasks

- Measure compliance state and coverage
- Analyze context and business impact
- Monitor status and analyze in real time
- Query, filter and share relevant insights



3 Automate

Streamline repetitive tasks with domain-aware workflows and bulk operations.

Operationalize at scale

Core Tasks

- Trigger workflows and notifications
- Schedule assessments and reviews
- Guide task execution step-by-step
- Execute bulk updates

Connect what is fragmented – without starting over.

The screenshot displays the ADOGRC web application interface. The main area is titled "Data Deduplication" and includes a search bar, a sidebar with navigation links (Overview, Home, Explore, Tasks, Processes, Workspace), and a central panel for configuring AI matching. Below this, there's a section for "Objects to Analyze (1000)" with a list of objects like "TDA-03.1 Supplier Diversity" and "IAC-15.3 Disable Inactive Accounts". A "Control Objectives" table is also visible, listing various regulatory requirements such as "EMEA EU DORA" and "EMEA EU EBA GLU/2019/04".

Data Deduplication
Use AI to discover and identify duplicate objects in your repository. Select a class and scope to analyze for potential duplicates.

Source Class
Control Objective (X) Name, Description (v)

Analysis Scope
All objects in repository (v)

Objects to Analyze (1000)

- TDA-03.1 Supplier Diversity (View Details)
- IAC-15.3 Disable Inactive Accounts (View Details)
- CRY-05 Encrypting Data At Rest

+995 more

AI Configuration: Configure the AI matching process. You can adjust the weights for the different...

Control Objectives (List Modified) (v)

Type	Name	Description
Published (0)	Work in progress (92)	
EMEA EU DORA	EU Digital Operational Resilience Act (I	
EMEA EU EBA GLU/2019/04	European Banking Authority (EBA) Gu	
EMEA EU ePrivacy [draft]	ePrivacy Directive Additional informati	
EMEA EU GDPR	General Data Protection Regulation (G	
EMEA EU NIS2	ENISA NIS2 (Directive (EU) 2022/2555	
EMEA Germany	Federal Data Protection Act Additional	
EMEA Germany Banking Supervisory Requirements for I...	Banking Supervisory Requirements for	
GOV-01 Cybersecurity & Data Protection Governance Pr...	Mechanisms exist to facilitate the imple	
GOV-02 Publishing Cybersecurity & Data Protection Doc...	Mechanisms exist to establish, maintai	
GOV-03 Periodic Review & Update of Cybersecurity & D...	Mechanisms exist to review the cybers	
GOV-04 Assigned Cybersecurity & Data Protection Resp...	Mechanisms exist to assign one or mor	
HIPAA - HICP Small Practice	Health Industry Cybersecurity Practic	
HRS-01 Human Resources Security Management	Mechanisms exist to facilitate the imple	
HRS-03 Roles & Responsibilities	Mechanisms exist to define cybers	
IAC-02 Identification & Authentication for Organizational ...	Mechanisms exist to uniquely identify a	
IRO-02 Incident Handling	Mechanisms exist to cover the prepar	
IRO-04 Incident Response Plan (IRP)	Mechanisms exist to maintain and mak	

Import data (Experimental) (x)

Method > Collect > Select data > Map columns > Map values > Verify > Result

Choose import method
Select the import method you want to use.

- CSV**
Import data from comma-separated values files
- Excel**
Import data from Excel spreadsheets (.xlsx, .xls)
- ADONIS**
Import objects from an ADONIS repository
- ADOIT**
Import objects from an ADOIT repository
- ADOGRC**
Import objects from an ADOGRC repository

Upload your files

Drag and drop file here

Consolidate fragmented GRC information in one place – matched, deduplicated and ready to use.

Transform GRC data into actionable intelligence.



The top screenshot displays the ADOGRC 'OVERVIEW' page. It features a sidebar with navigation options like Home, Explore, Tasks, Favorites, and a Workspace section with folders for Assets, Audit Management, Business Continuity, Compliance, Data Protection, Information & Cybers..., Internal Controls, Risk Management, and Taxonomies. The main content area shows three readiness score cards: 'EU AI Act' with a 72% score, 'ISO 27001' with a 56% score, and 'BSI Orientierungshilfe KI' with an 84% score. Each card includes a 'Setup progress' bar and a start date.

The bottom screenshot shows the 'Dashboards' page. It features a similar sidebar and a grid of six dashboard cards: 'Enterprise Risk Management Dashboard', 'Compliance & Regulatory Dashboard', 'Internal Control Dashboard', 'Audit Management Dashboard', 'Business Continuity & Resilience Dashboard', and 'AI Governance Dashboard'. Each card shows creation and last changed dates.

Combine readiness scoring with drill-down dashboards – give every role the insights they need.

Automate what follows – without losing control.



The screenshot displays the ADOGRC user interface. At the top, a red header bar contains the ADOGRC logo, a search bar, and a user profile icon (EG). Below the header, a dashboard section titled 'Good morning, GRC' shows a summary of tasks: 'You have 9 open tasks - 1 needs attention'. A filter bar allows searching tasks, columns, group (Urgency), and sort (Soonest). The main task list is divided into three sections: 'Do now' (3 tasks), 'Scheduled' (3 tasks), and 'Anytime' (3 tasks). The 'Do now' section highlights a task 'Perform an assessment: Control Test Q1' which is 'Overdue by 2 days'. To the right, a detailed view of 'Control Test Q1' is shown, featuring a progress bar with three steps: 1. Guide (highlighted), 2. Form, and 3. Confirm. Below the progress bar, a section titled 'How to complete this assessment' provides a quick guide with four steps: 1. Open Control Test Q1 and review the control or process being tested. 2. Perform the required tests and gather evidence. 3. Select the appropriate test result. 4. Continue to record your findings and evidence. A purple callout box states: 'Your entries are kept as you go — you can step back at any point before submitting.' At the bottom of the workflow view, there are 'Back' and 'Continue' buttons.

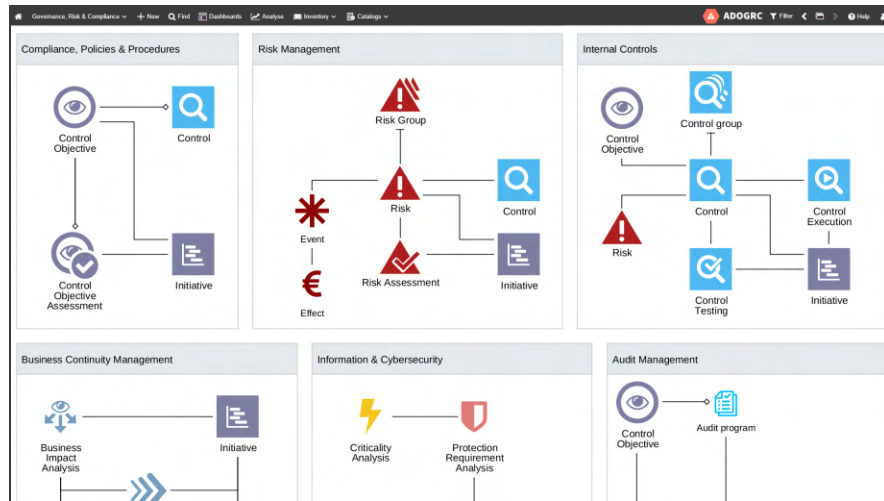
Tasks	Due date	Type
Do now 3		
Perform an assessment: Control Test Q1	Overdue by 2 days	Control Test
Review: Access Review — Finance	Due tomorrow	Access Review
Complete mandatory fields: Risk Treatment Plan	Due in 2 days	Risk
Scheduled 3		
Complete mandatory fields: Process — Order Fulfillment	Due in 18 days	Business Process
Perform an assessment: Control Test Q2	Due in 20 days	Control Test
Review: Business Continuity Plan Review	Due in 25 days	Bcm Plan
Anytime 3		

Support recurring GRC activities with guided workflows — streamline execution and keep responsibilities on track.

Our current release. And the next generation.

Out
now

ADOGRC 15.0 LTS



Audit Program Audit Finding Event Effect AI Assistant

Configurable Dashboards MCP Services REST API OAuth & OIDC

Enhanced Authentication Administration Audit Log Super Admin

Starting
2027

ADOGRC Next Generation

The screenshot shows the ADOGRC Next Generation interface, specifically the 'Risks' section. The table displays a list of risks with the following columns: Type, Name, Description, Frequency of, and Responsible Person.

Type	Name	Description	Frequency of	Responsible Person
▲	07.07.02.01 Failed ma...	Not fulfilling legal or regulatory requiremen...	Year	gnc_admin
▲	07.08.03.04 Unauthorised modifi...	Unbefugte IKT-Manipulationen infolge von ...	Month	gnc_admin
▲	07.08.01.02 Disruptive and destru...	Angriffe zu unterschiedlichen Zwecken (z. ...	Month	gnc_admin
▲	07.04.01.03 Retail con...	Non-compliance with disclosure requireme...	Year	gnc_admin
▲	07.04.04.03 Lack of due-diligence...	Failing to thoroughly assess the risk and v...	Year	gnc_admin
▲	07.08.03.02 Misuse or theft of ass...	Misuse or theft of ICT assets via physical a...	Year	gnc_admin
▲	07.04.05.02 Lack of knowledge / ...	Insufficient expertise to properly assess gu...	Year	gnc_admin
▲	07.02.01.02 Forgery	Forgery involves the creation or alteration ...	Year	gnc_admin
▲	07.07.01.03 Missed deadline or re...	Failing to meet critical deadlines or fulfill re...	Year	gnc_admin
▲	07.03.02.02 Employee health and...	Incidents involving the violation of health a...	Year	gnc_admin

Magic Connector Micro Frontend Control Execution 1st Line Task List

Holistic, semantic meta model Program Browser Connected Compliance

2nd Line Workspace Evidence Collection Smart Lists Automation Engine

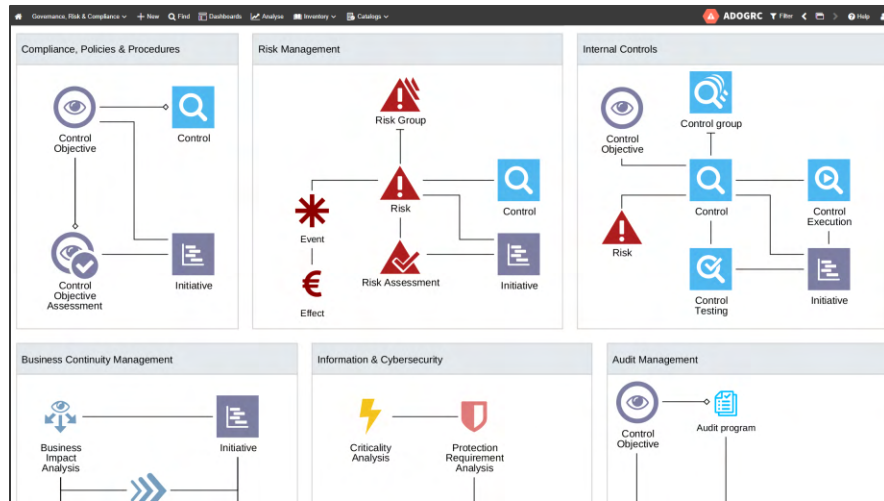
Ready for today's challenges. ➔ [ADOGRC.com](https://www.adogrc.com) ➔ Built for what's next.

Stay up to date.

Our current release. And the next generation.

Out
now

ADOGRC 15.0 LTS



Audit Program Audit Finding Event Effect AI Assistant

Configurable Dashboards MCP Services REST API OAuth & OIDC

Enhanced Authentication Administration Audit Log Super Admin

Starting
2027

ADOGRC Next Generation

The screenshot displays the ADOGRC Next Generation interface, specifically the 'Risks' section. It features a sidebar menu with 'OVERVIEW' and 'Home'. The main content area shows a table of risks with the following columns: Type, Name, Description, Frequency of, and Responsible Person. The table contains 24 rows of data, with the first 10 rows visible. The table is filtered to show 27 published risks and 75 work in progress risks.

Type	Name	Description	Frequency of	Responsible Person
▲	07.07.02.01 Failed ma...	Not fulfilling legal or regulatory requiremen...	Year	gnc_admin
▲	07.08.03.04 Unauthorised modifi...	Unbefugte IKT-Manipulationen infolge von ...	Month	gnc_admin
▲	07.08.01.02 Disruptive and destru...	Angriffe zu unterschiedlichen Zwecken (z. ...	Month	gnc_admin
▲	07.04.01.03 Retail con...	Non-compliance with disclosure requireme...	Year	gnc_admin
▲	07.04.04.03 Lack of due-diligence...	Failing to thoroughly assess the risk and v...	Year	gnc_admin
▲	07.08.03.02 Misuse or theft of ass...	Misuse or theft of ICT assets via physical a...	Year	gnc_admin
▲	07.04.05.02 Lack of knowledge / ...	Insufficient expertise to properly assess gu...	Year	gnc_admin
▲	07.02.01.02 Forgery	Forgery involves the creation or alteration ...	Year	gnc_admin
▲	07.07.01.03 Missed deadline or re...	Failing to meet critical deadlines or fulfil re...	Year	gnc_admin
▲	07.03.02.02 Employee health and...	Incidents involving the violation of health a...	Year	gnc_admin

Magic Connector Micro Frontend Control Execution 1st Line Task List

Holistic, semantic meta model Program Browser Connected Compliance

2nd Line Workspace Evidence Collection Smart Lists Automation Engine

Ready for today's challenges. ➔ [ADOGRC.com](https://www.adogrc.com) ➔ Built for what's next.

Stay up to date.



ADOGRC

Governance, Risk & Compliance Suite

 **BOC Group**
Design Your Enterprise



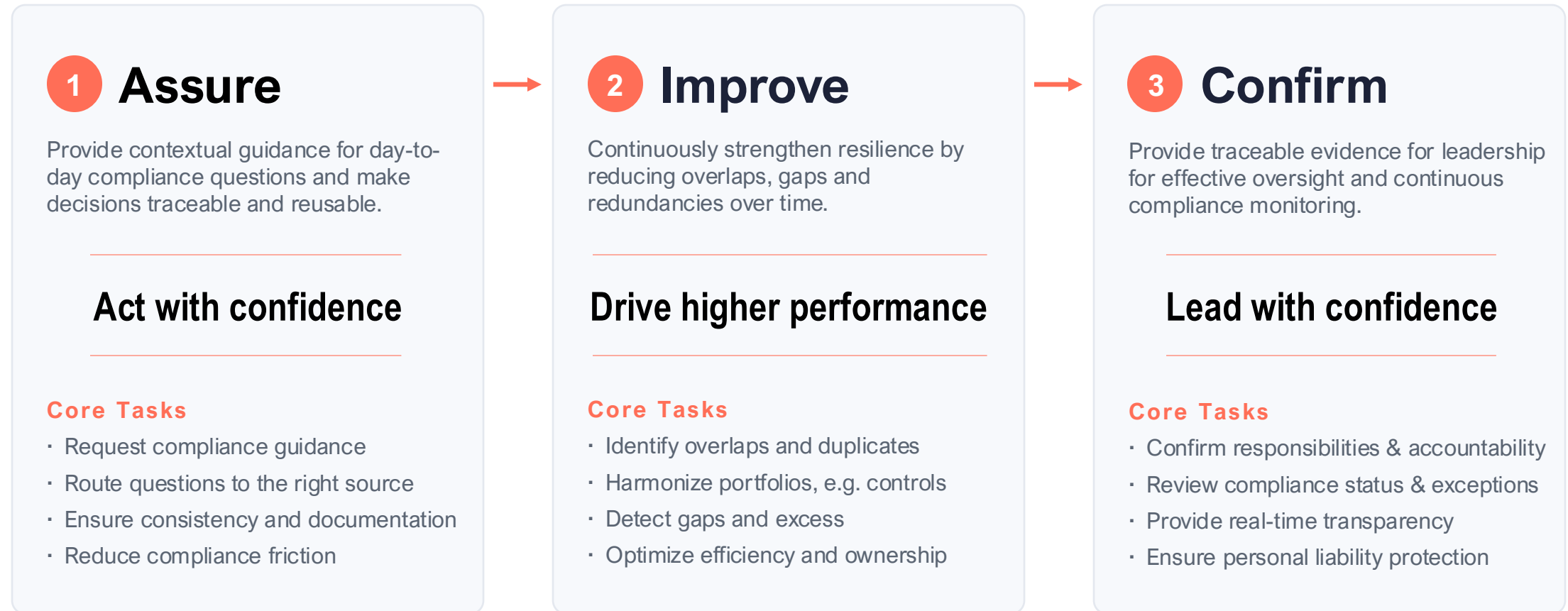
Focus 3

Leverage Reliable Information as Trusted Context.

**Govern Business Transformation
and AI Adoption.**

**Efficiency & Insights through AI-
Powered GRC**

Turn trusted context into confidence at every level.



Get the right guidance – when the answer is not obvious.



ADOGRC

Governance, Risk & Compliance Suite
by boc-group.com

The screenshot shows the ADOGRC interface. On the left is a sidebar with navigation options: OVERVIEW (Home, Explore, Tasks), WORKSPACE (Assets, Audit Management, Business Continuity, Compliance Policies, Data Protection), and a search bar. The main area displays a 'Policies' list with columns for Type and Name. A table shows one policy: 'Gifts & Hospitality Policy' under the 'BOC Group'. A purple line connects this policy to a detailed view on the right. The detailed view shows a question: 'I will give a presentation at BOC's Business Excellence Circle. What tokens of appreciation are acceptable?' with a red circle labeled 'EG' next to it. Below the question, a box titled 'For an employee presenting at a supplier-hosted event, the following applies:' contains three items: 'Acceptable' (Branded merchandise, flowers, a bottle of wine or the event meal — keep it and log it if the value is up to €50.), 'Approval needed' (Gifts of €50–€150, or travel and accommodation paid by the host — get manager sign-off and record it in the gift register.), and 'Not acceptable' (Cash or vouchers, gifts above €150, or anything offered while a tender or procurement decision with the supplier is active.). At the bottom, a 'Source' field shows 'Gifts & Hospitality Policy (COM-04) · §3 Events'. A purple circle with a star icon is at the bottom left of the detailed view.

I will give a presentation at BOC's Business Excellence Circle. What tokens of appreciation are acceptable?

EG

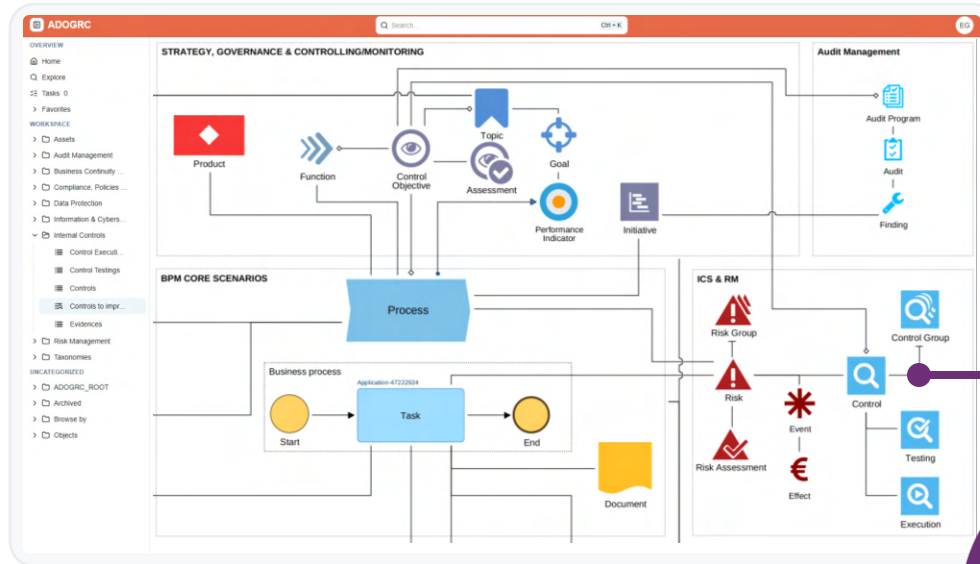
For an employee presenting at a supplier-hosted event, the following applies:

- Acceptable** Branded merchandise, flowers, a bottle of wine or the event meal — keep it and log it if the value is up to €50.
- Approval needed** Gifts of €50–€150, or travel and accommodation paid by the host — get manager sign-off and record it in the gift register.
- Not acceptable** Cash or vouchers, gifts above €150, or anything offered while a tender or procurement decision with the supplier is active.

Source Gifts & Hospitality Policy (COM-04) · §3 Events

Provide reliable answers to day-to-day compliance questions – with confidence, consistency and a clear rationale.

Strengthen your portfolio – without growing it blindly.



I am the ICS responsible. Help me review the current control portfolio to identify opportunities to simplify, harmonize and optimize it.

EG

Based on the current portfolio, these are the highest-priority opportunities:

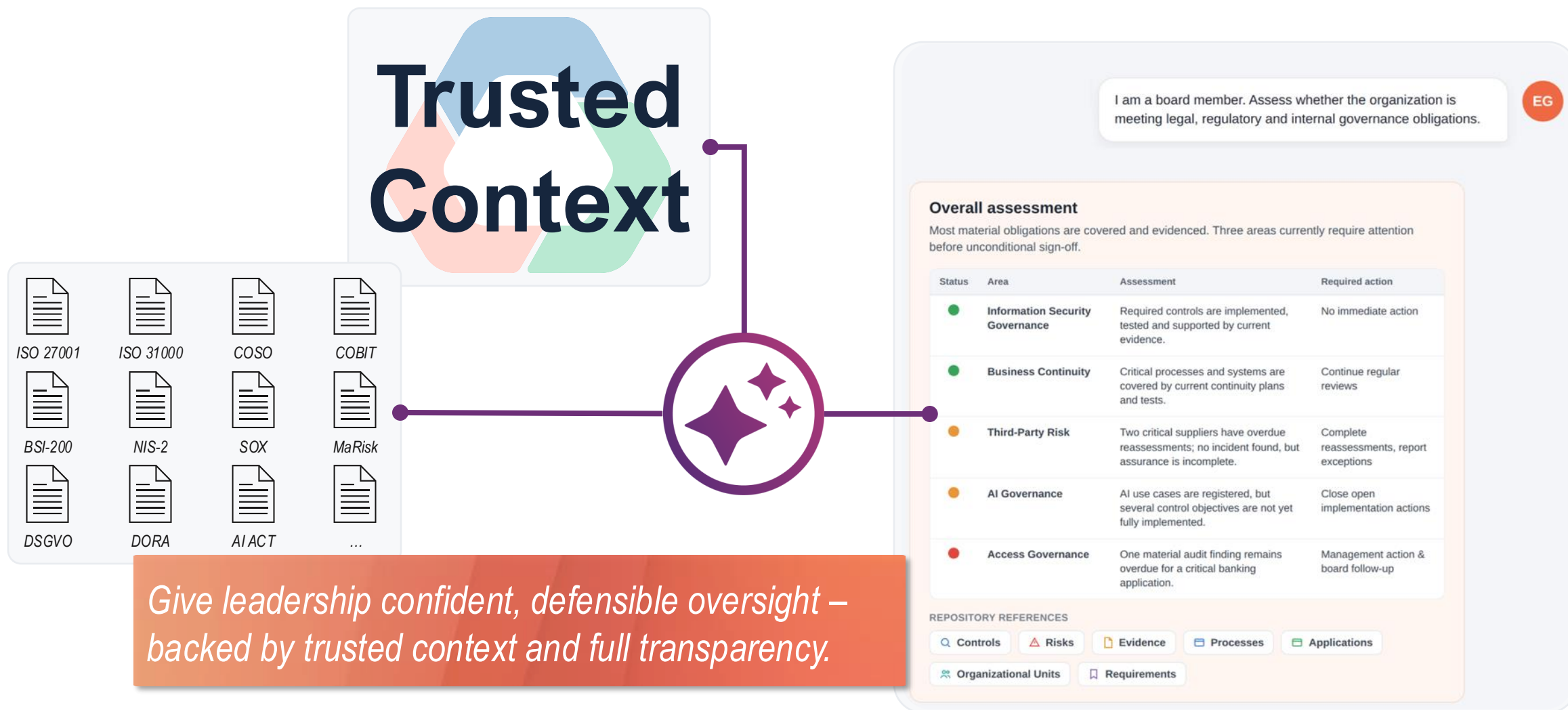
Finding	Recommendation	Risk impact	Effort reduction
Duplicate access reviews	Merge into one standardized access-review control with application-specific scope.	High	High
Overlapping third-party controls	Harmonize the assessments and reuse common control evidence across functions.	High	High
Repeated evidence collection	Reuse evidence and automate collection from source systems.	Medium	High

Repository references

Controls Risks Evidence Processes
Applications Organizational Units Requirements

*Reveal overlaps, gaps and redundancies –
reduce complexity and strengthen your overall portfolio.*

Confirm that governance works – with evidence to prove it.





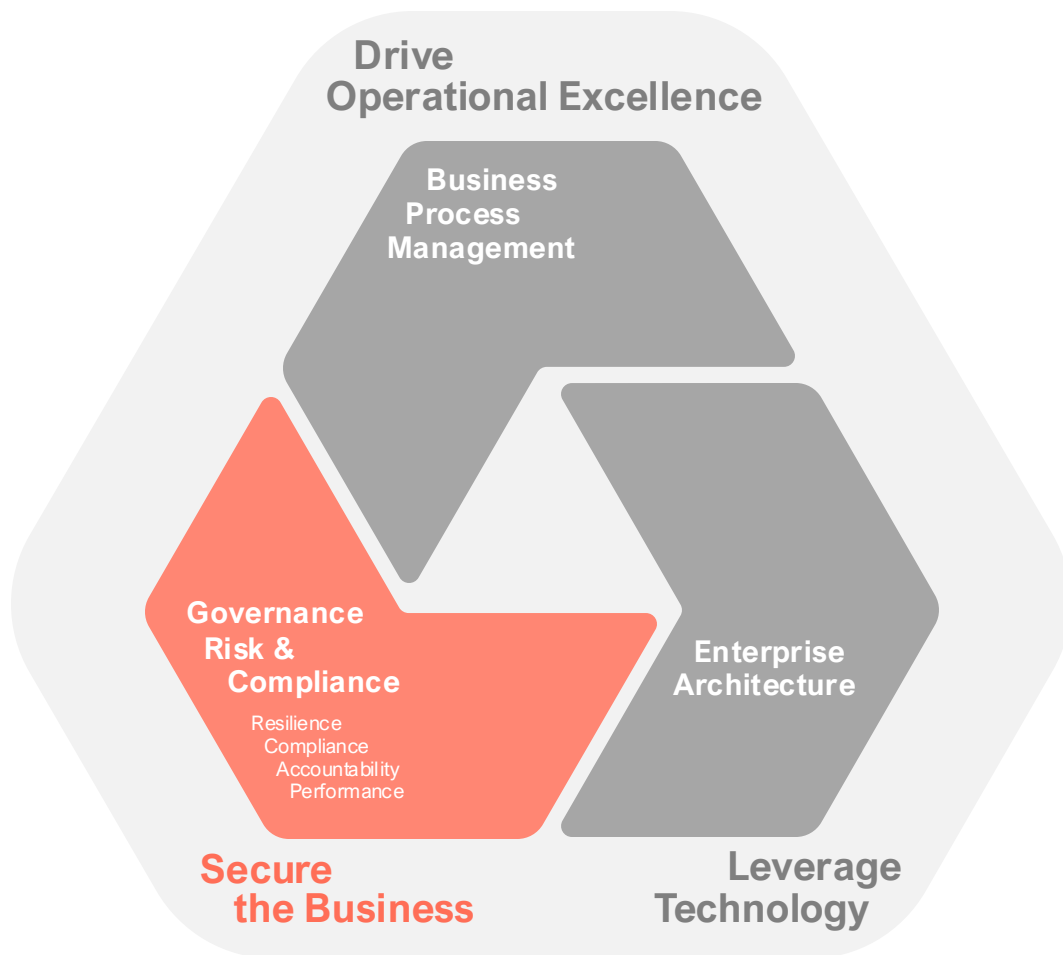
ADOGRC

Governance, Risk & Compliance Suite



BOC Group

Design Your Enterprise



**Minimal Effort.
Full Compliance.
With ADOGRC.**



AI Governance