LIVE-SESSION

Operational Excellence und Compliance in der digitalen Ära: Verlässliche Informationen als Schlüssel

Christian Lichka
Vorstandsmitglied BOC Group

Erik Guschlbauer
Produktmanager ADOGRC

ADOGRC
Governance, Risk & Compliance

DR. CHRISTIAN LICHKA
Member of the Board

ERIK GUSCHLBAUER
Produktmanager ADOGRC

SANDRO GERUSSI
Marketing & Kommunikation

www.boc-group.com

06. November 2024

AGENDA

1. Das Zusammenspiel von OpEX, Compliance und Digitalisierung
2. Compliance in der digitalen Ära
3. Fragerunde
4. What‘s next

Let`s make
your business
run better.

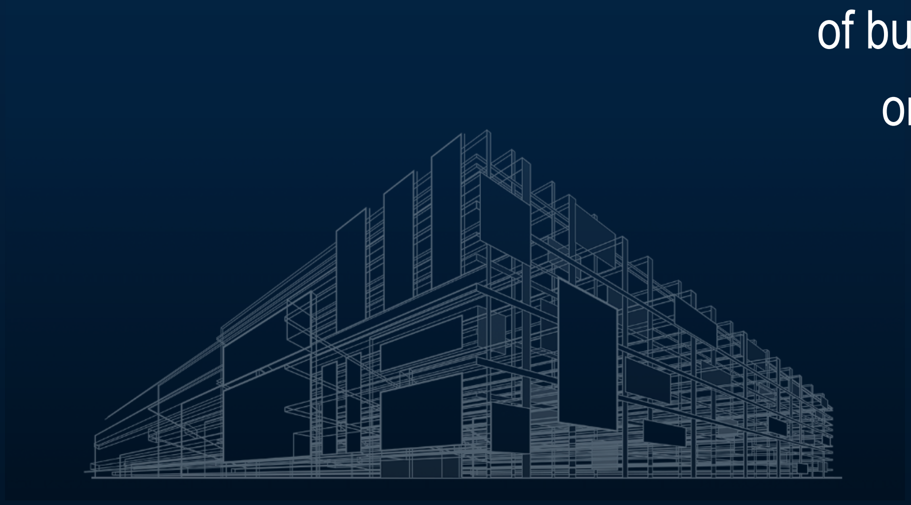
SUCCEEDING IN THE DIGITAL TRANSFORMATION JOURNEY

53%

of businesses are **just starting** or **less than half done** with digitalization[5]

82%

Consider **digitalization** a most critical factor[1]



87%

Assign the capability to manage cyber **risks** top priority in the next 2 years[4]

67%

Expect BPM to provide **efficiency gains** in their processes[2]

89%

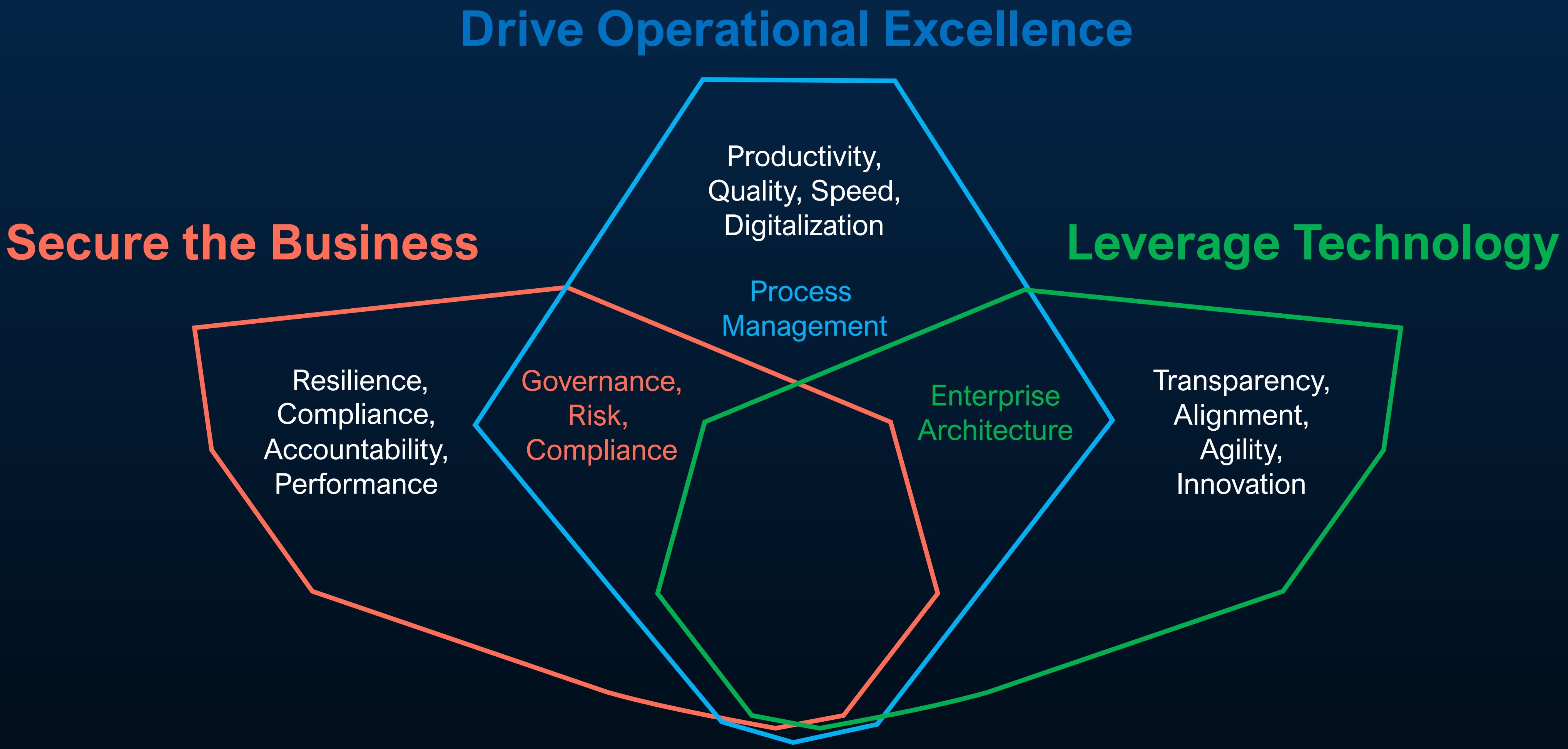
Prio 1 target: Increase **process transparency**[1]

84%

Consider **IT / Enterprise Architecture** as critical or very critical success factor in the future[3]

[1] BPM Compass Study 2024, THM | [2] BPM Study 2023, ZHAW | [3] EA Study 2024 ZHAW, (pending publication) | [4] 12th GRM Survey, Deloitte: https://tinyurl.com/24avqz8n | [5] CEO Concerns 2024, Gartner: https://www.gartner.com/document/5415563

3 Fields of Action



Drive Operational Excellence

Productivity,
Quality, Speed,
Digitalization

Process
Management

Secure the Business

Resilience,
Compliance,
Accountability,
Performance

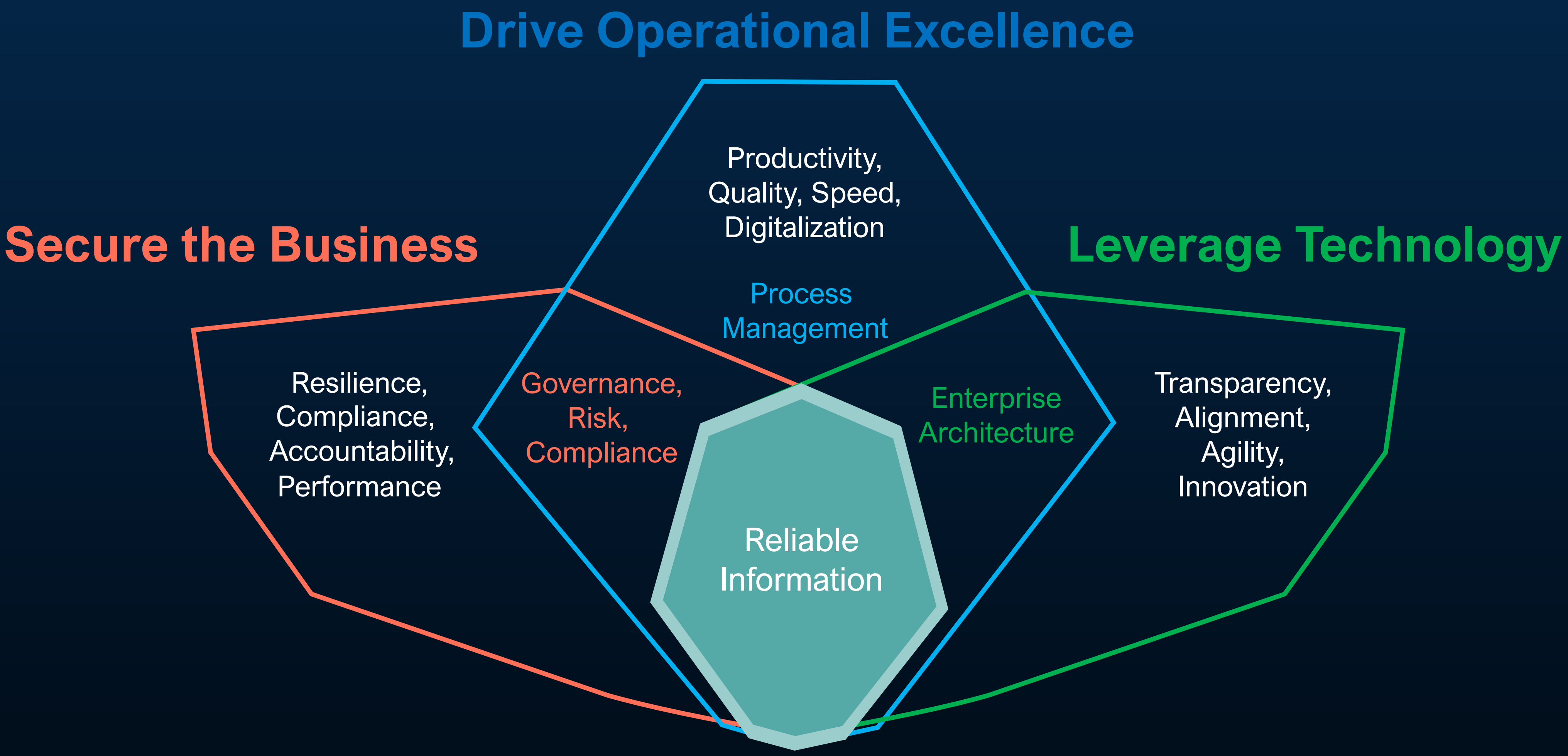
Governance,
Risk,
Compliance

Enterprise
Architecture

Leverage Technology

Transparency,
Alignment,
Agility,
Innovation

3 Fields of Action – Reliable Information



Drive Operational Excellence

Productivity, Quality, Speed, Digitalization

Process Management

Secure the Business

Resilience, Compliance, Accountability, Performance

Governance, Risk, Compliance

Leverage Technology

Transparency, Alignment, Agility, Innovation

Enterprise Architecture

Reliable Information

www.boc-group.com

Drive Operational Excellence.
Leverage Technology.
Secure the Business.

Reliable information. Better decisions.
Only with BOC Products.

ADONIS
Business Transformation Suite

ADOIT
Enterprise Architecture Suite

ADOGRC
Governance, Risk & Compliance

First things first…

Lack of transparency in processes and responsibilities

Inconsistency in ways of working in silos and duplication of efforts

Vulnerable to human errors and compliance issues

75%

of **CEOs** see it as **major barrier** to operational efficiency[1]

-McKinsey 2023

70%

of **CIOs** see it as **top obstacle** to successful digital transformation initiatives[2]

-Gartner 2023

65%

of **CFOs** see as cause of **significant financial and reputational losses** due to fines and pennalties[3]

-Deloitte 2023

[1] McKinsey's Global Survey on Business Process Management 2023 | [2] Gartner's Future of Work Trends Survey 2023 | [3] Deloitte's Global Compliance and Operational Risk Study 2023

Top Prios to Drive Operational Excellence & Compliance

Observation …	Focus on …
Lack of clarity on who is doing what, when and how	**Know what's going on in the whole company**
Increased operational costs	**Do more work with the same resources**
Regulatory obligations, Audit findings, risks of reputational damage and higher costs	**Lower costs of complying, monitoring processes and people**

Top Prios to Drive Operational Excellence & Compliance

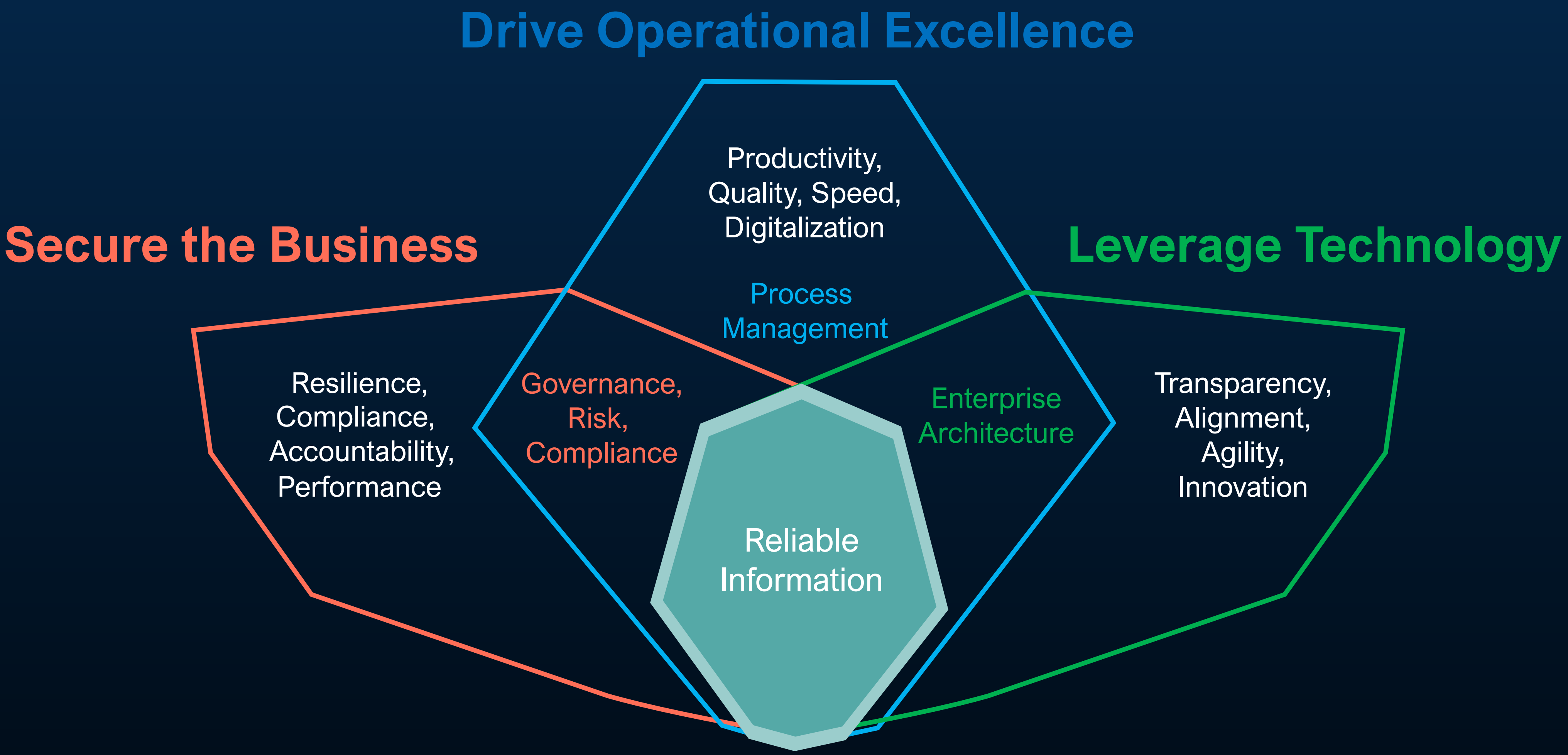
Solution …

Know what's going on in the whole company

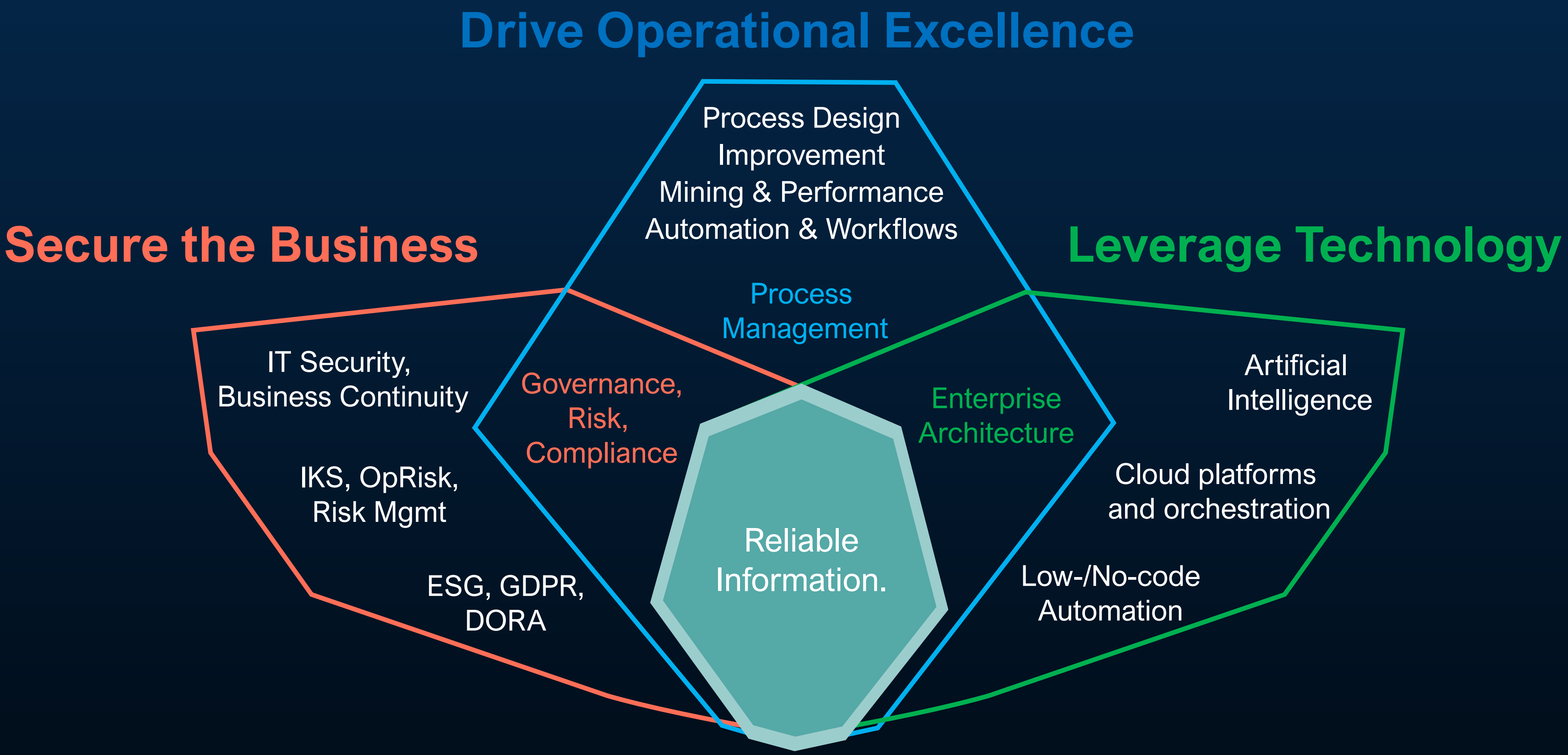
Do more work with the same resources

Lower costs of complying, monitoring processes and people

3 Fields of Action – Reliable Information


Drive Operational Excellence
Productivity, Quality, Speed, Digitalization
Process Management
Secure the Business
Resilience, Compliance, Accountability, Performance
Governance, Risk, Compliance
Leverage Technology
Transparency, Alignment, Agility, Innovation
Enterprise Architecture
Reliable Information

3 Fields of Action – Reliable Information



Drive Operational Excellence

Process Design
Improvement
Mining & Performance
Automation & Workflows

Process Management

Secure the Business

IT Security,
Business Continuity

IKS, OpRisk,
Risk Mgmt

ESG, GDPR,
DORA

Governance,
Risk,
Compliance

Leverage Technology

Artificial
Intelligence

Cloud platforms
and orchestration

Low-/No-code
Automation

Enterprise
Architecture

Reliable
Information.

www.boc-group.com

Drive Operational Excellence.
Leverage Technology.
Secure the Business.

Reliable information. Better decisions.
Only with BOC Products.

ADONIS
Business Transformation Suite

ADOIT
Enterprise Architecture Suite

ADOGRC
Governance, Risk & Compliance

www.boc-group.com

Drive Operational Excellence.
Leverage Technology.
Secure the Business.

Reliable information. Better decisions.

Only with BOC Products.

ADONIS
Business Transformation Suite

ADOIT
Enterprise Architecture Suite

ADOGRC
Governance, Risk & Compliance

www.boc-group.com

Secure the Business.
Drive Operational Excellence.
Leverage Technology.

Reliable information. Better decisions.
With ADOGRC.

ADOGRC
Governance, Risk & Compliance

Secure the Business.

> 80%

consider GRC as Critical Success Factor[1]

Regulatory Change

is the 4th most important global Business Risk[3]

> 73%

expect a further increase of Regulatory Requirements[2]

[1] Deloitte Global Risk Management Survey 2021, PwC State of Compliance Study 2022, Gartner Integrated Risk Management Survey, OCEG GRC Maturity Survey 2022

[2] Reuters Cost of Compliance Report 2023

[3] Allianz Risk Barometer 2024

Secure the Business.

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

Risk Management

Internal Controls

Regulatory Change

is the 4th most important global Business Risk[3]

Data Protection

Compliance

Information & Cybersecurity

ESG

[3] *Allianz Risk Barometer 2024*

Secure the Business.

BAIT, VAIT, KAIT

IDW PS 951

COSO

Internal Controls

Solvency II

KonTraG

Basel IV

MaComp

ISO 37301

IDW PS 980

Compliance

ISO 9001

DCGK/ÖCGK

Green Deal

ESRS

UN SDGs

ESG

ISO 26000

CSRD

ISO 45001

Regulatory Change

is the 4th most important global Business Risk[3]

ISO 22301

MaRisk

ISO 31000

ÖNORM D4901

Risk Management

FINMA-RS Liq.R.

FINMA-RS CorpGov.

FINMA-RS OpRisk

ISO 27701

DSGVO

Data Protection

NIST Privacy

revDSG

EDPB

NIST CSF 2.0

ISO 27001

Information & Cybersecurity

DORA

NIS-2

[3] *Allianz Risk Barometer 2024*

Compliance affects us all.

Compliance affects us all.

Understand your compliance challenges better.

Understand your compliance challenges better.

Bundesamt für Sicherheit in der Informationstechnik
BSI 200-1

ISO

NIST
CSF 2.0, 800

COSO

DORA

NIS-2

GDPR

COBIT 2019

ISACA

PCI DSS

HIPAA

...

> 30 Standards & Sources

> 40 Domains & Principles

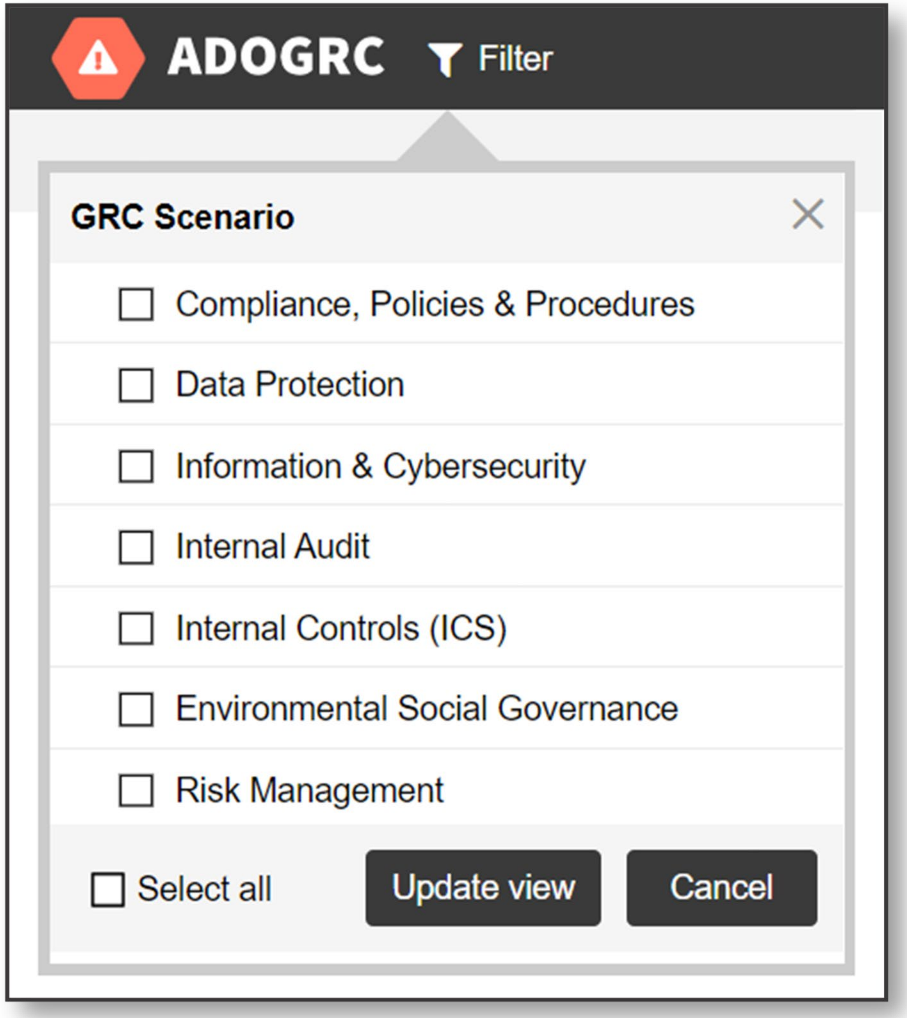
> 1,000 Control Objectives & Best Practices

ADOGRC Compliance Library

based on the Secure Controls Framework* and BOC Best Practices

* https://securecontrolsframework.com/

Understand your compliance challenges better.



GRC Scenario

- □ Compliance, Policies & Procedures
- □ Data Protection
- □ Information & Cybersecurity
- □ Internal Audit
- □ Internal Controls (ICS)
- □ Environmental Social Governance
- □ Risk Management

□ Select all

> 30 Standards & Sources

> 40 Domains & Principles

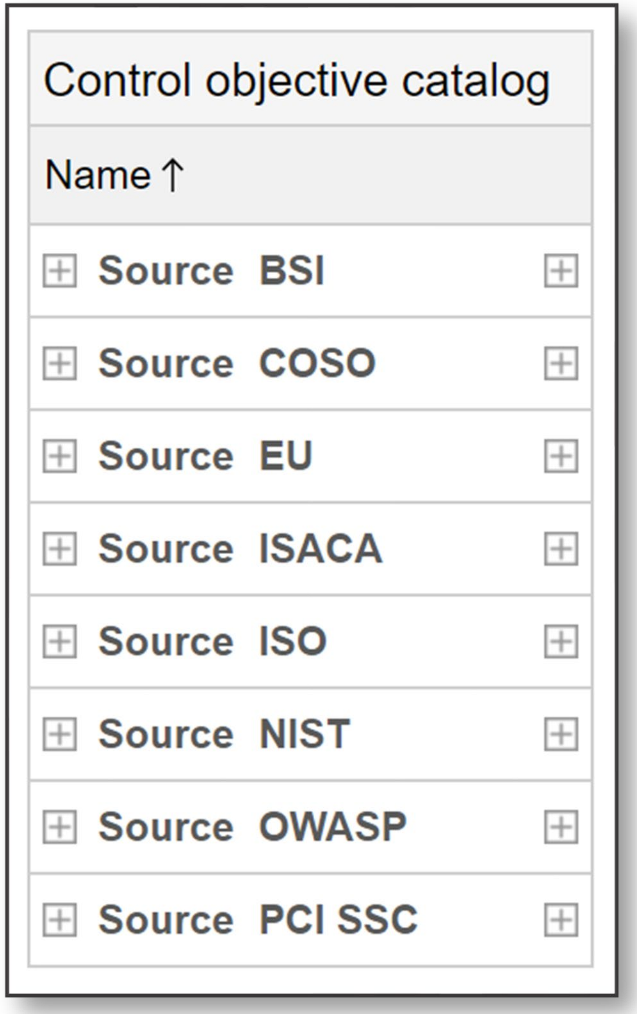
> 1,000 Control Objectives & Best Practices

ADOGRC Compliance Library

powered by Secure Controls Framework and BOC Best Practices

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

Understand your compliance challenges better.



Control objective catalog
Name ↑
⊞ Source BSI ⊞
⊞ Source COSO ⊞
⊞ Source EU ⊞
⊞ Source ISACA ⊞
⊞ Source ISO ⊞
⊞ Source NIST ⊞
⊞ Source OWASP ⊞
⊞ Source PCI SSC ⊞

> 30 Standards & Sources

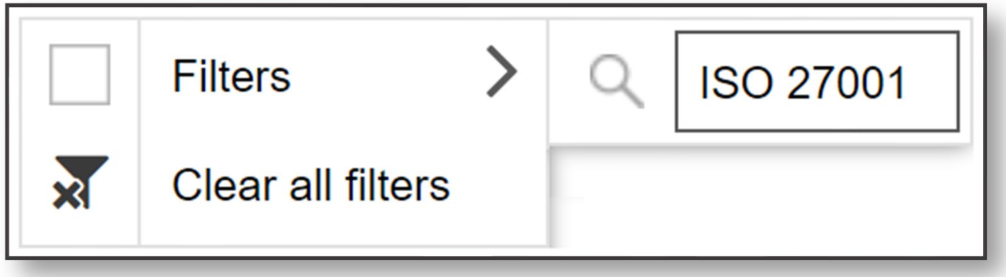
> 40 Domains & Principles

> 1,000 Control Objectives & Best Practices

ADOGRC Compliance Library

powered by Secure Controls Framework and BOC Best Practices

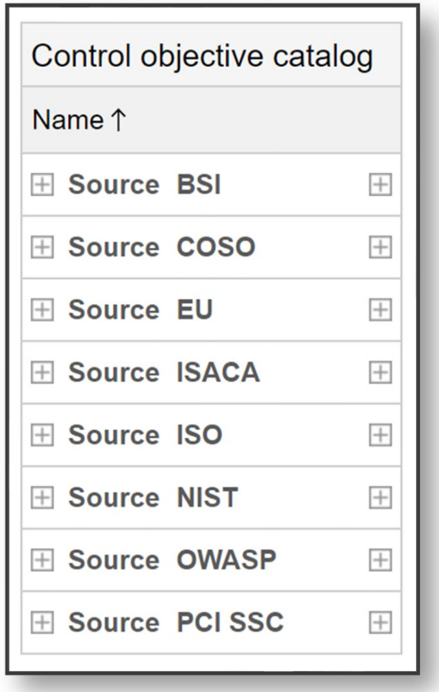
Understand your compliance challenges better.



□ Filters >

Clear all filters

ISO 27001



Control objective catalog

Name ↑

⊞ Source BSI ⊞

⊞ Source COSO ⊞

⊞ Source EU ⊞

⊞ Source ISACA ⊞

⊞ Source ISO ⊞

⊞ Source NIST ⊞

⊞ Source OWASP ⊞

⊞ Source PCI SSC ⊞

> 30 Standards & Sources

> 40 Domains & Principles

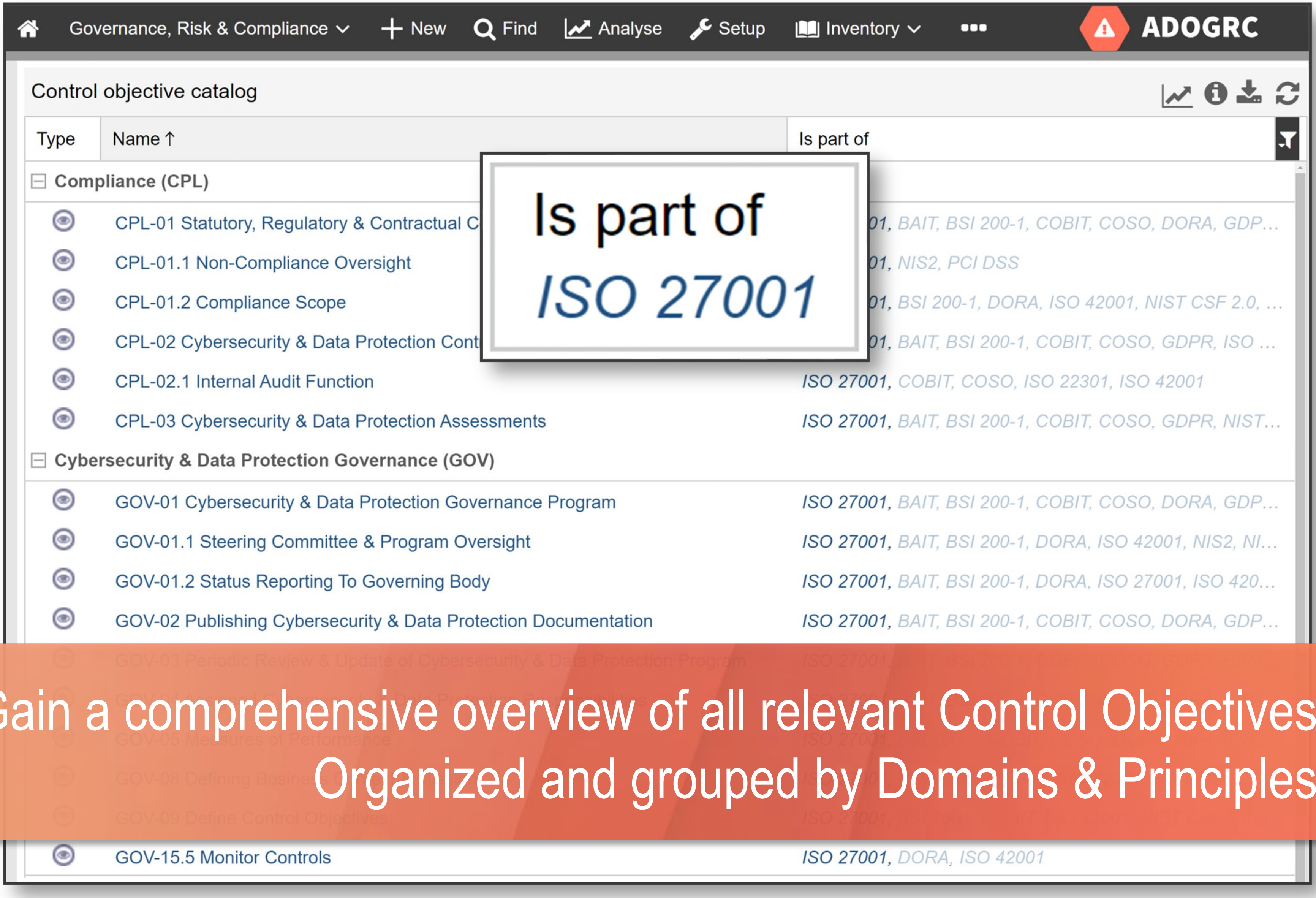
> 1,000 Control Objectives & Best Practices

ADOGRC Compliance Library

powered by Secure Controls Framework and BOC Best Practices

Understand your compliance challenges better.

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



Control objective catalog

Type	Name ↑	Is part of
Compliance (CPL)		
	CPL-01 Statutory, Regulatory & Contractual C	01, *BAIT, BSI 200-1, COBIT, COSO, DORA, GDP…*
	CPL-01.1 Non-Compliance Oversight	01, *NIS2, PCI DSS*
	CPL-01.2 Compliance Scope	01, *BSI 200-1, DORA, ISO 42001, NIST CSF 2.0, …*
	CPL-02 Cybersecurity & Data Protection Cont	01, *BAIT, BSI 200-1, COBIT, COSO, GDPR, ISO …*
	CPL-02.1 Internal Audit Function	*ISO 27001, COBIT, COSO, ISO 22301, ISO 42001*
	CPL-03 Cybersecurity & Data Protection Assessments	*ISO 27001, BAIT, BSI 200-1, COBIT, COSO, GDPR, NIST…*
Cybersecurity & Data Protection Governance (GOV)		
	GOV-01 Cybersecurity & Data Protection Governance Program	*ISO 27001, BAIT, BSI 200-1, COBIT, COSO, DORA, GDP…*
	GOV-01.1 Steering Committee & Program Oversight	*ISO 27001, BAIT, BSI 200-1, DORA, ISO 42001, NIS2, NI…*
	GOV-01.2 Status Reporting To Governing Body	*ISO 27001, BAIT, BSI 200-1, DORA, ISO 27001, ISO 420…*
	GOV-02 Publishing Cybersecurity & Data Protection Documentation	*ISO 27001, BAIT, BSI 200-1, COBIT, COSO, DORA, GDP…*
	GOV-03 Periodic Review & Update of Cybersecurity & Data Protection Program	*ISO 27001,* [illegible]
	GOV-04 Assigned Cybersecurity & Data Protection Responsibilities	[illegible]
	GOV-05 Measures of Performance	*ISO 27001,* [illegible]
	GOV-08 Defining Busine[illegible]	[illegible]
	GOV-09 Define Control Objectives	*ISO 27001,* [illegible]
	GOV-15.5 Monitor Controls	*ISO 27001, DORA, ISO 42001*

Is part of

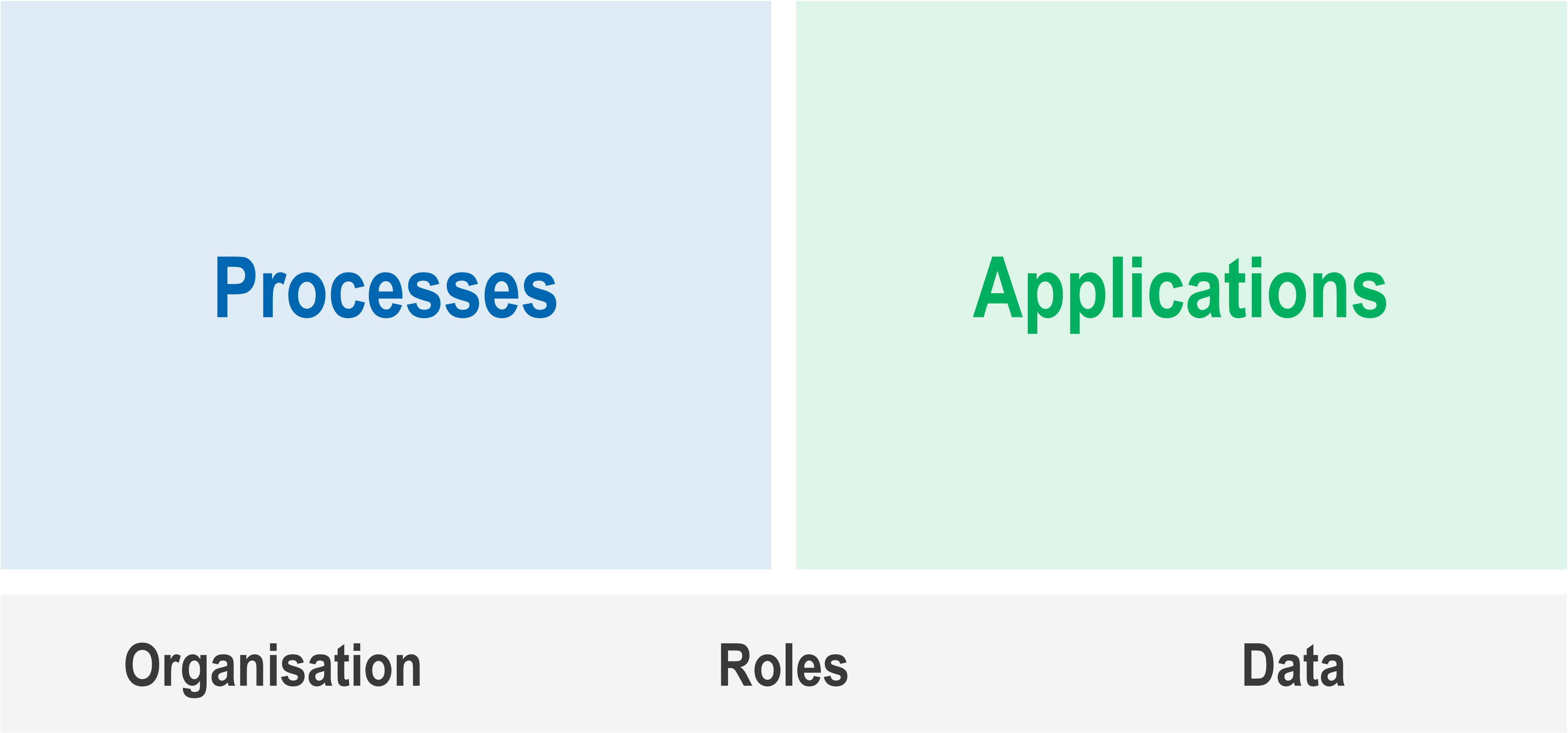
ISO 27001

Gain a comprehensive overview of all relevant Control Objectives.
Organized and grouped by Domains & Principles.

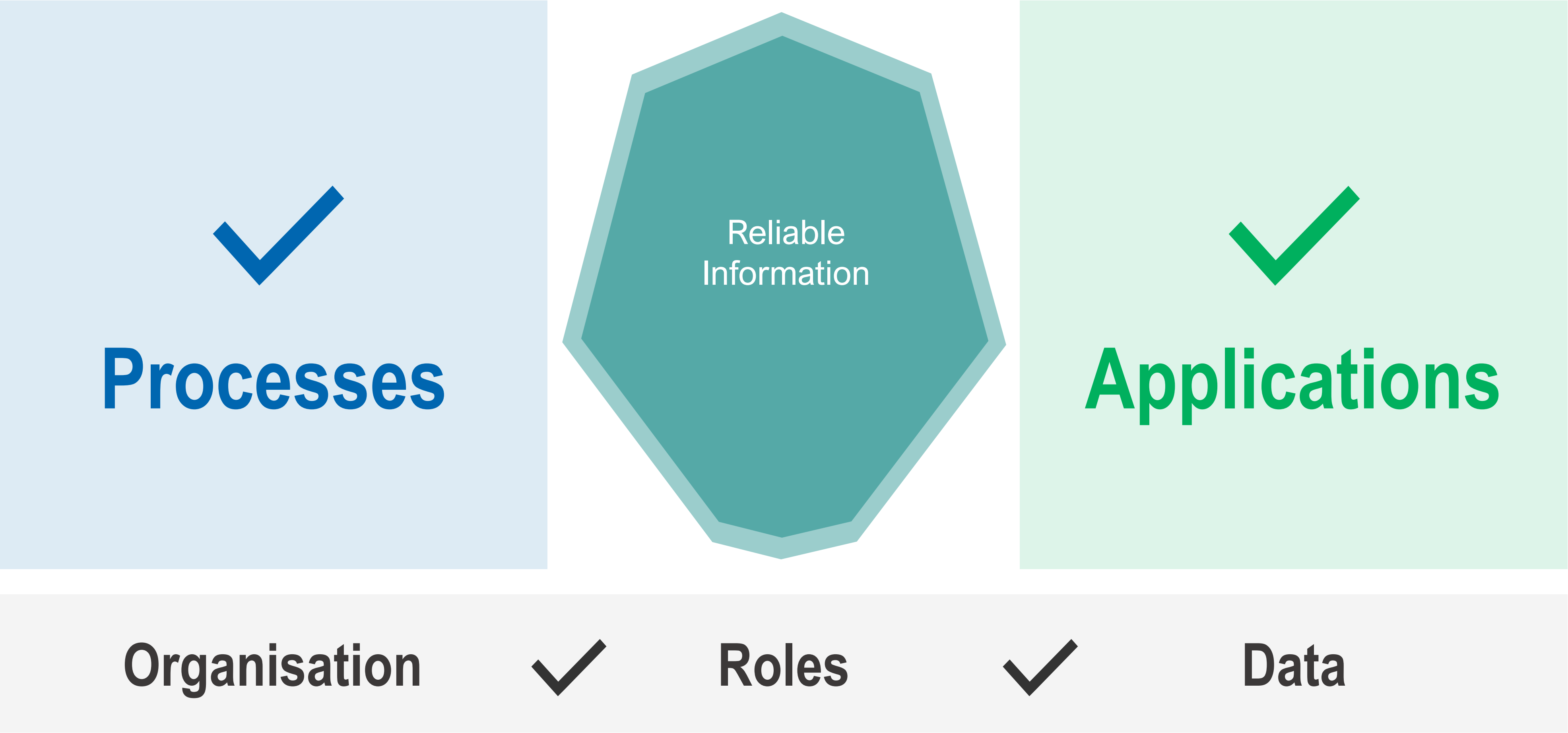
- ✓ **Understand your compliance challenges better.**
- Leverage your existing data.
- Assess what matters.

- ✓ Understand your compliance challenges better.
- **Leverage your existing data.**
- Assess what matters.

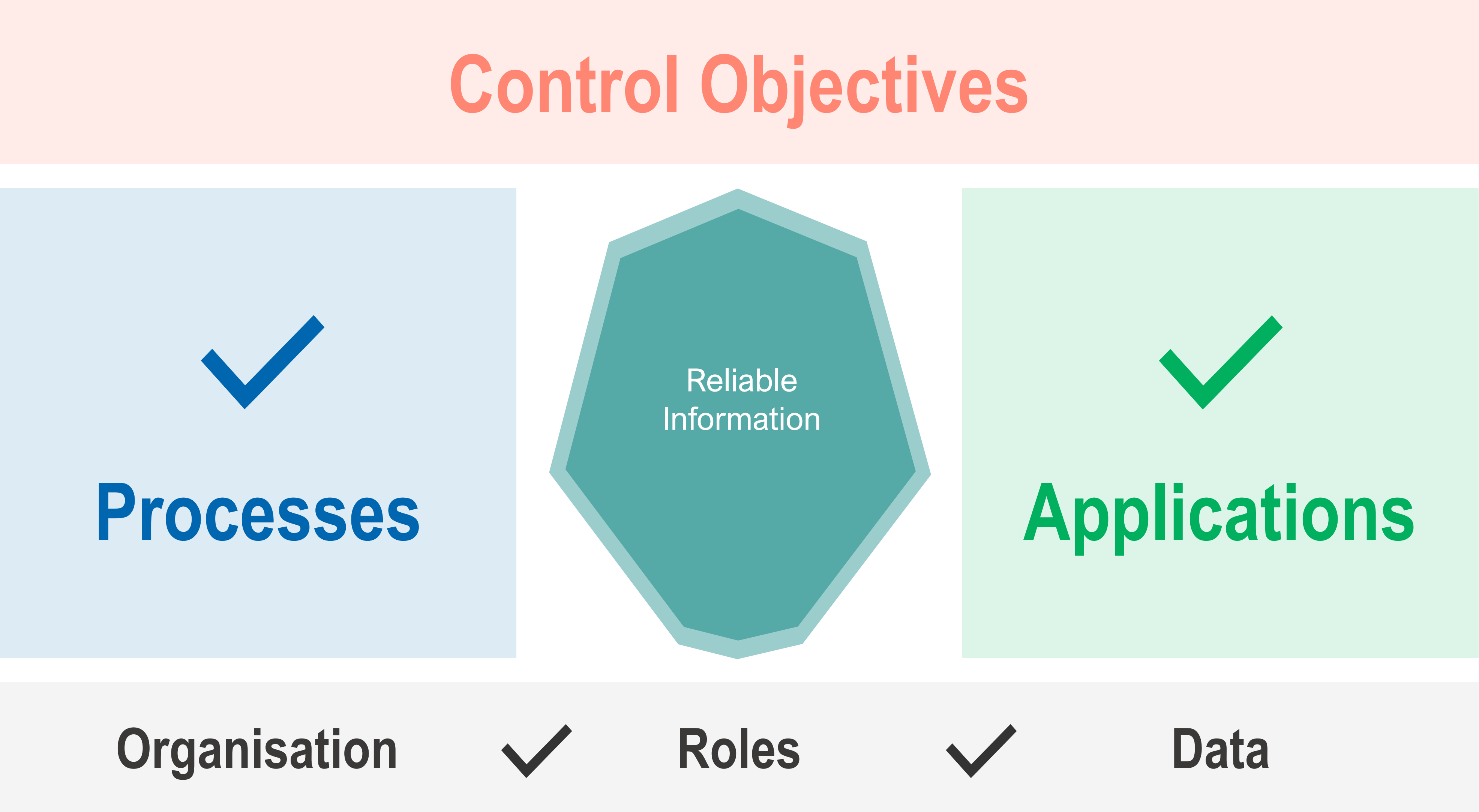
Leverage your existing data.



Leverage your existing data.



Leverage your existing data.



Control Objectives

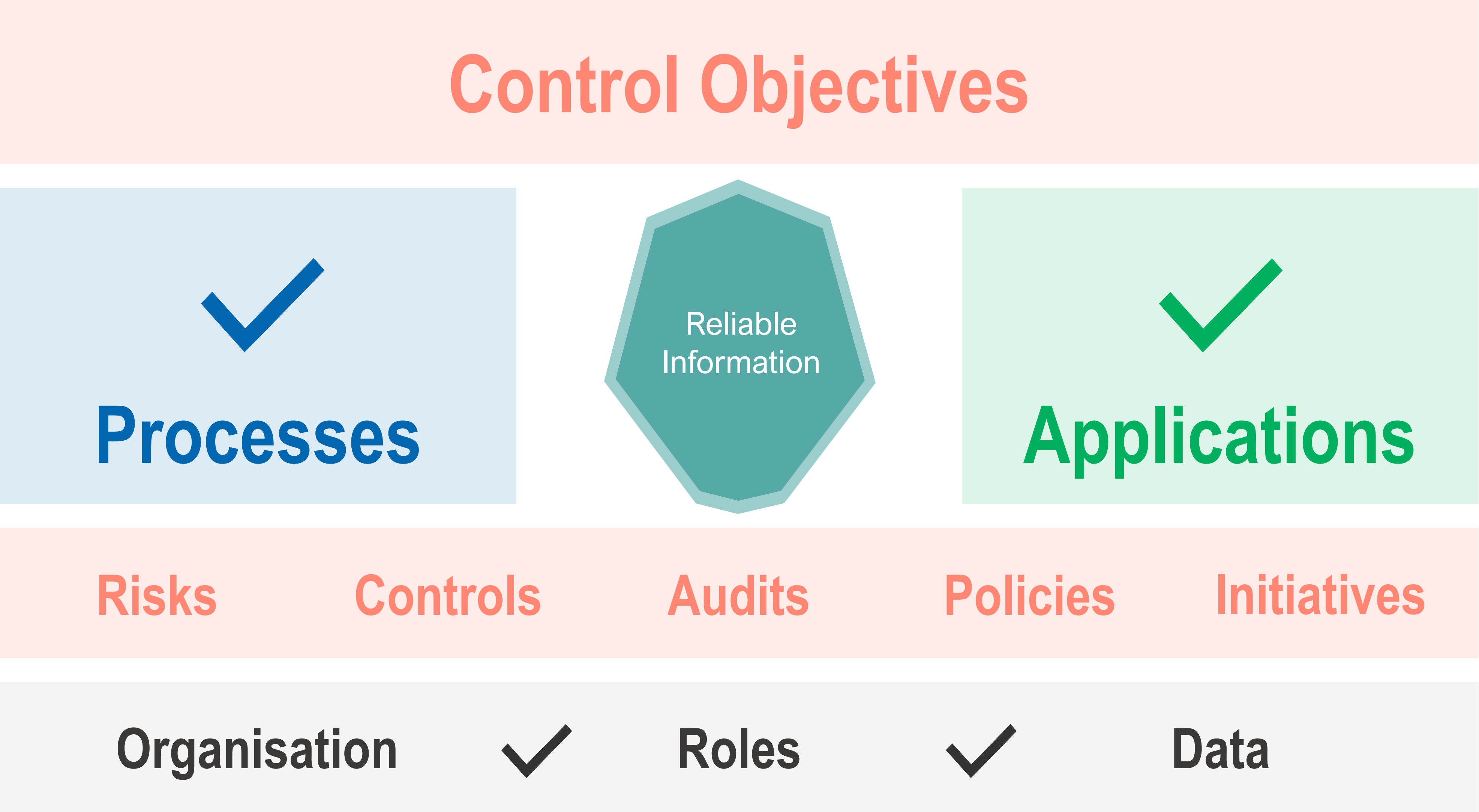
✓ Processes

Reliable Information

✓ Applications

Organisation ✓ Roles ✓ Data

Leverage your existing data.



Control Objectives

✓ Processes

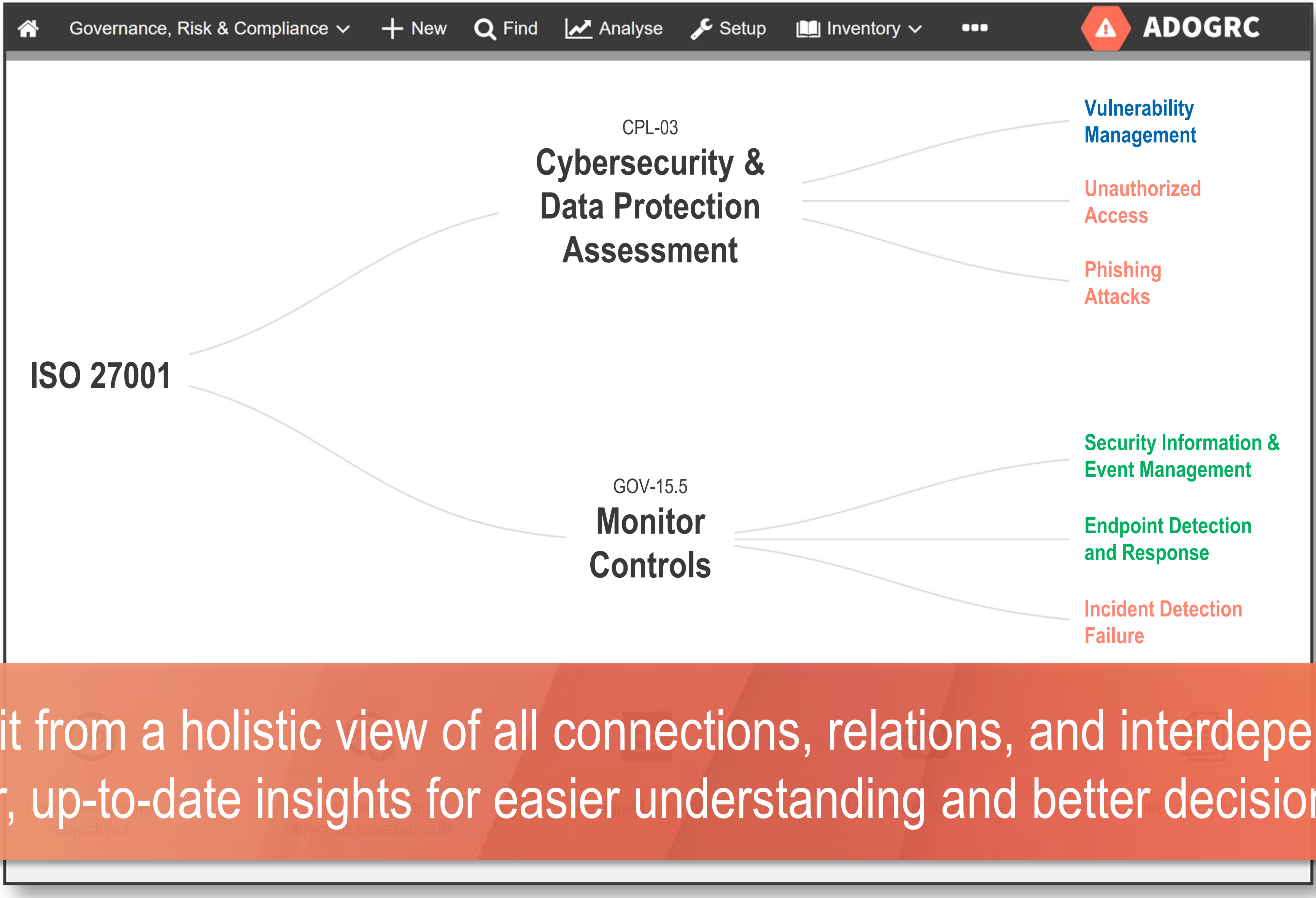
Reliable Information

✓ Applications

Risks Controls Audits Policies Initiatives

Organisation ✓ Roles ✓ Data

Leverage your existing data.



Governance, Risk & Compliance ⌄ + New Find Analyse Setup Inventory ⌄ ••• ADOGRC

ISO 27001

CPL-03
Cybersecurity & Data Protection Assessment

- Vulnerability Management
- Unauthorized Access
- Phishing Attacks

GOV-15.5
Monitor Controls

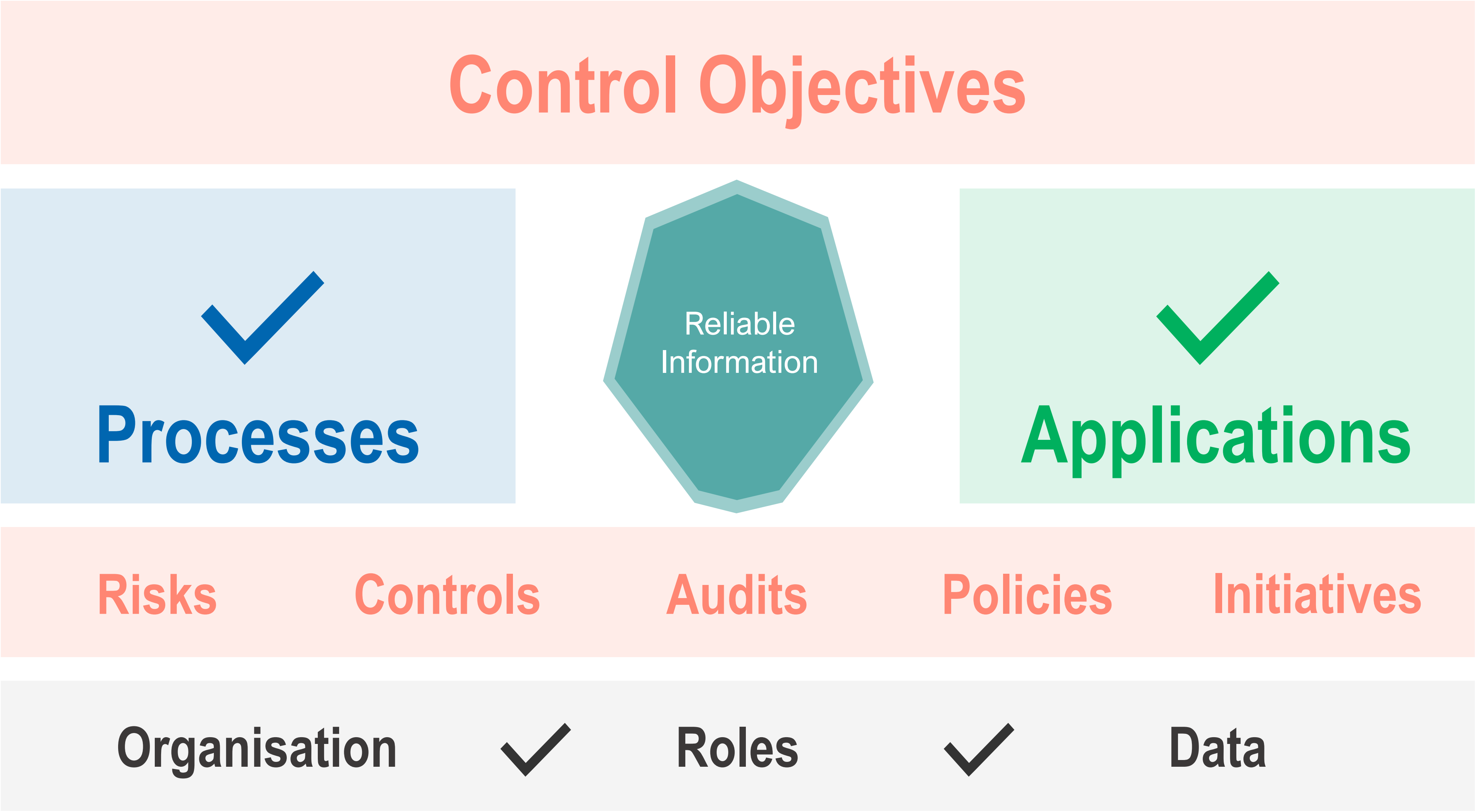
- Security Information & Event Management
- Endpoint Detection and Response
- Incident Detection Failure

Benefit from a holistic view of all connections, relations, and interdependencies.
Use clear, up-to-date insights for easier understanding and better decision-making.

- ✓ Understand your compliance challenges better.
- ✓ **Leverage your existing data.**
- Assess what matters.

- ✓ Understand your compliance challenges better.
- ✓ Leverage your existing data.
- **Assess what matters.**

Assess what matters.



Control Objectives

✓ Processes

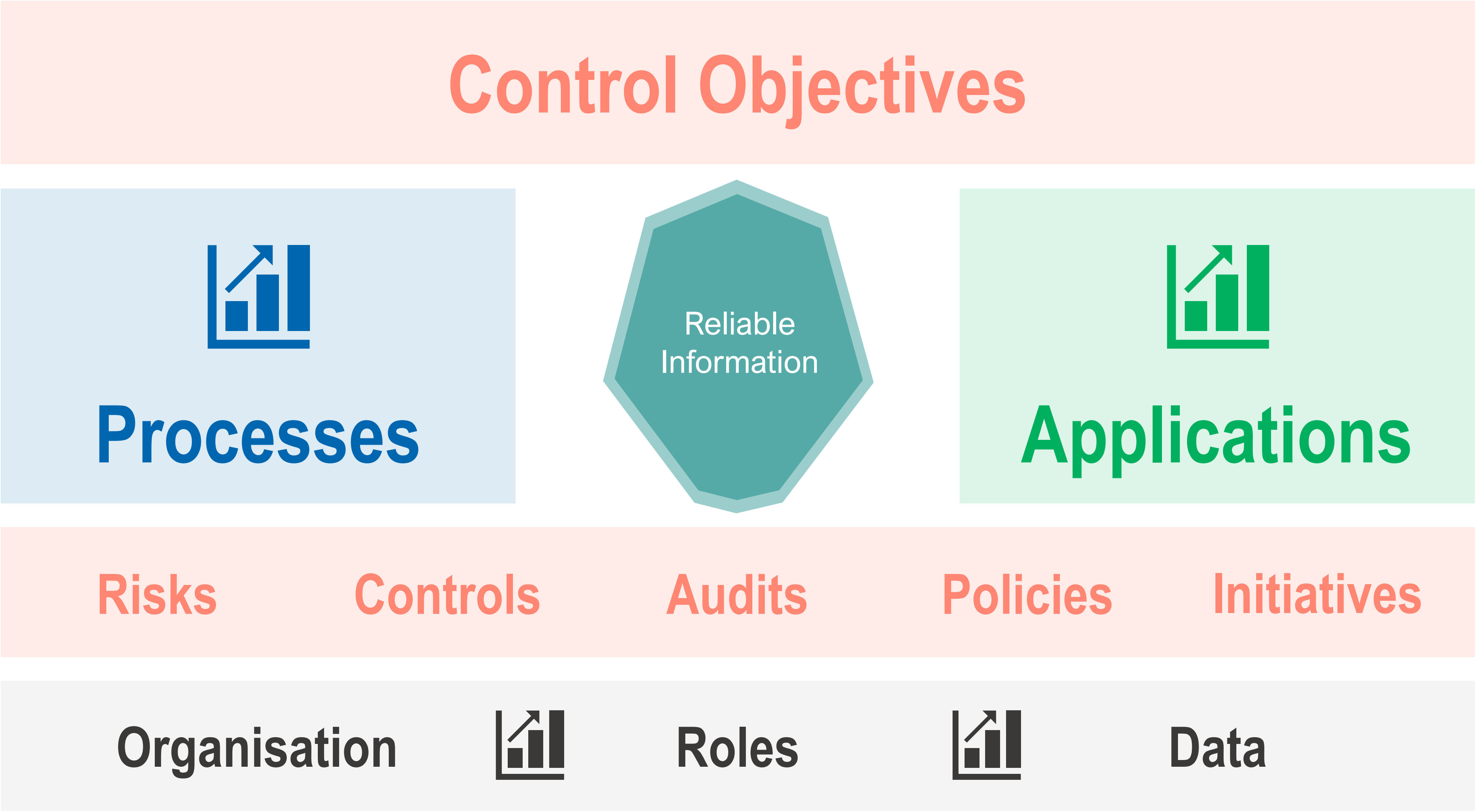
Reliable Information

✓ Applications

Risks Controls Audits Policies Initiatives

Organisation ✓ Roles ✓ Data

Assess what matters.



Control Objectives

Processes

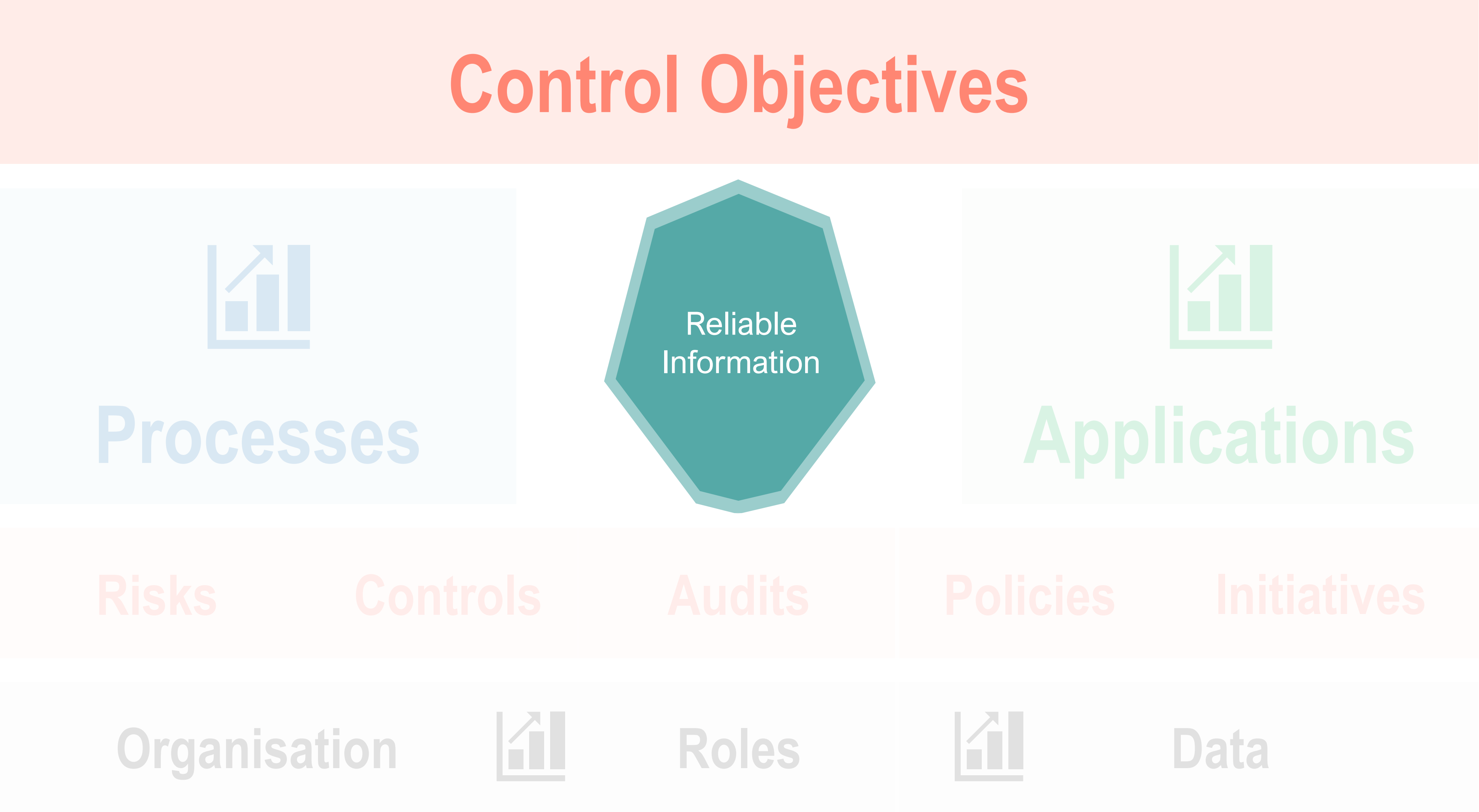
Reliable Information

Applications

Risks Controls Audits Policies Initiatives

Organisation Roles Data

Assess what matters.



Control Objectives

Processes

Reliable Information

Applications

Risks

Controls

Audits

Policies

Initiatives

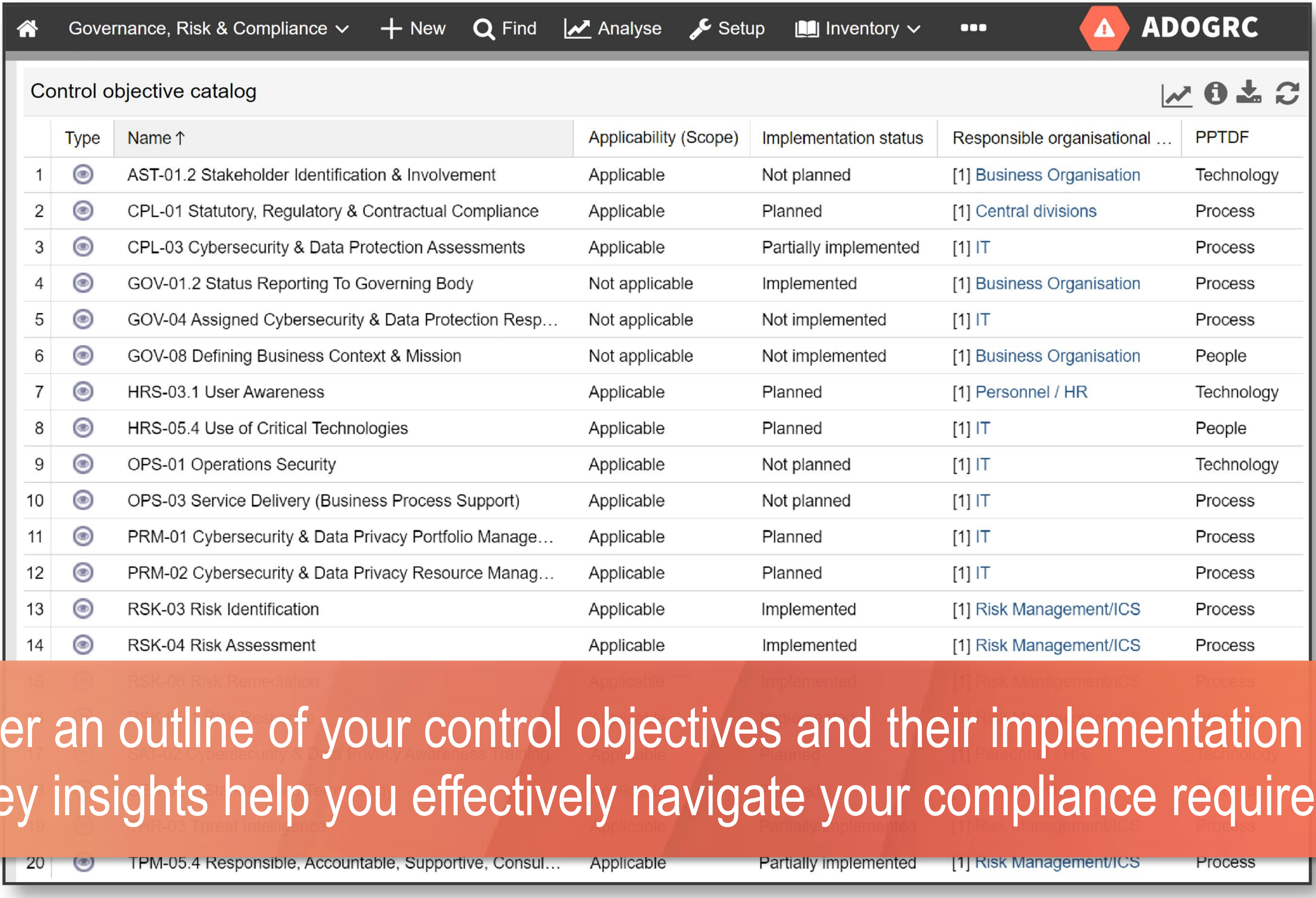
Organisation

Roles

Data

Assess what matters. Control Objectives.

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

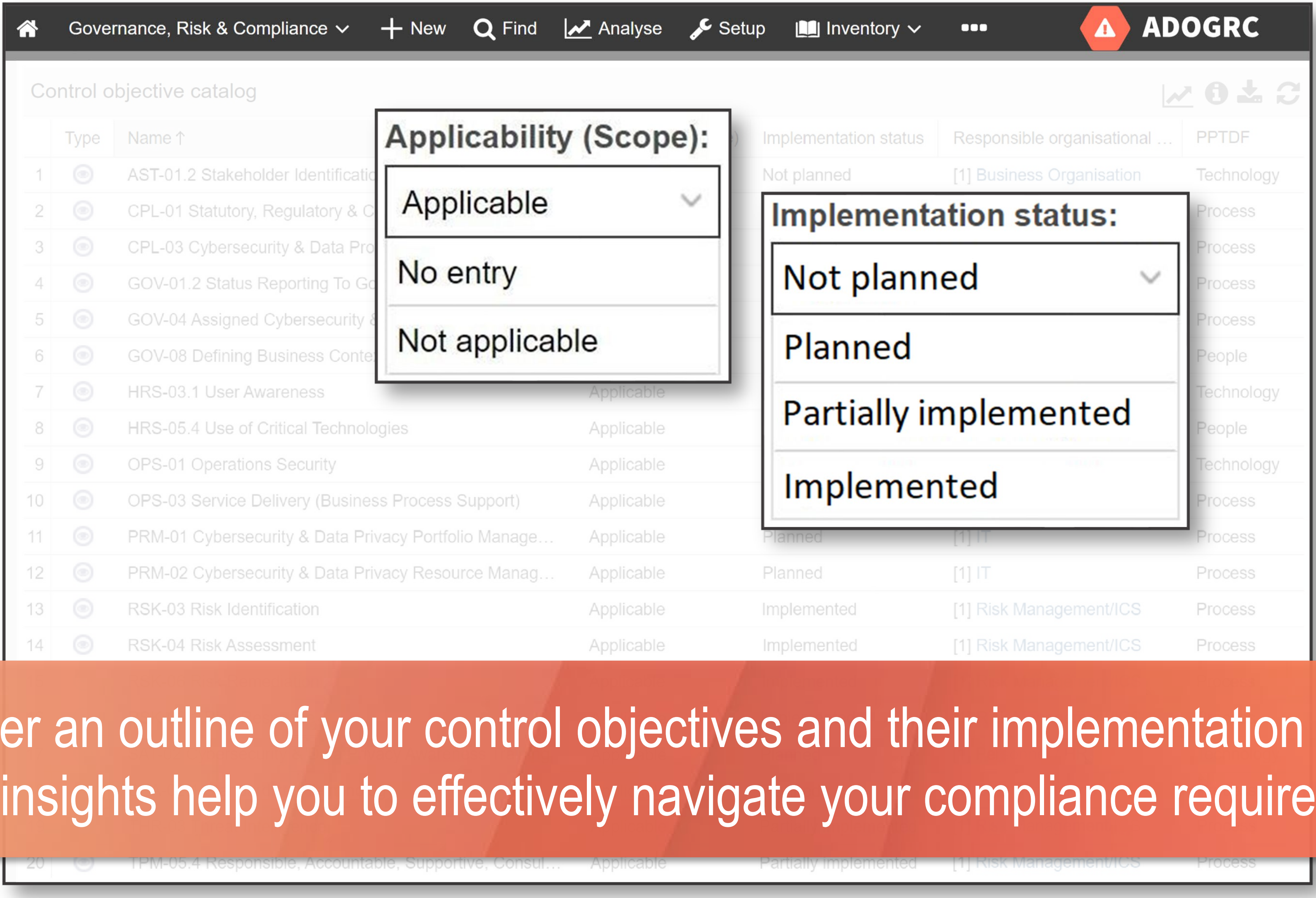


Control objective catalog

	Type	Name ↑	Applicability (Scope)	Implementation status	Responsible organisational …	PPTDF
1	◉	AST-01.2 Stakeholder Identification & Involvement	Applicable	Not planned	[1] Business Organisation	Technology
2	◉	CPL-01 Statutory, Regulatory & Contractual Compliance	Applicable	Planned	[1] Central divisions	Process
3	◉	CPL-03 Cybersecurity & Data Protection Assessments	Applicable	Partially implemented	[1] IT	Process
4	◉	GOV-01.2 Status Reporting To Governing Body	Not applicable	Implemented	[1] Business Organisation	Process
5	◉	GOV-04 Assigned Cybersecurity & Data Protection Resp…	Not applicable	Not implemented	[1] IT	Process
6	◉	GOV-08 Defining Business Context & Mission	Not applicable	Not implemented	[1] Business Organisation	People
7	◉	HRS-03.1 User Awareness	Applicable	Planned	[1] Personnel / HR	Technology
8	◉	HRS-05.4 Use of Critical Technologies	Applicable	Planned	[1] IT	People
9	◉	OPS-01 Operations Security	Applicable	Not planned	[1] IT	Technology
10	◉	OPS-03 Service Delivery (Business Process Support)	Applicable	Not planned	[1] IT	Process
11	◉	PRM-01 Cybersecurity & Data Privacy Portfolio Manage…	Applicable	Planned	[1] IT	Process
12	◉	PRM-02 Cybersecurity & Data Privacy Resource Manag…	Applicable	Planned	[1] IT	Process
13	◉	RSK-03 Risk Identification	Applicable	Implemented	[1] Risk Management/ICS	Process
14	◉	RSK-04 Risk Assessment	Applicable	Implemented	[1] Risk Management/ICS	Process
15	◉	RSK-06 Risk Remediation	Applicable	Implemented	[1] Risk Management/ICS	Process
16	◉	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
17	◉	SAT-02 Cybersecurity & Data Privacy Awareness Training	Applicable	Planned	[1] Personnel / HR	Technology
18	◉	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
19	◉	THR-03 Threat Intelligence	Applicable	Partially implemented	[1] Risk Management/ICS	Process
20	◉	TPM-05.4 Responsible, Accountable, Supportive, Consul…	Applicable	Partially implemented	[1] Risk Management/ICS	Process

Discover an outline of your control objectives and their implementation status.
Key insights help you effectively navigate your compliance requirements.

Assess what matters. Control Objectives.

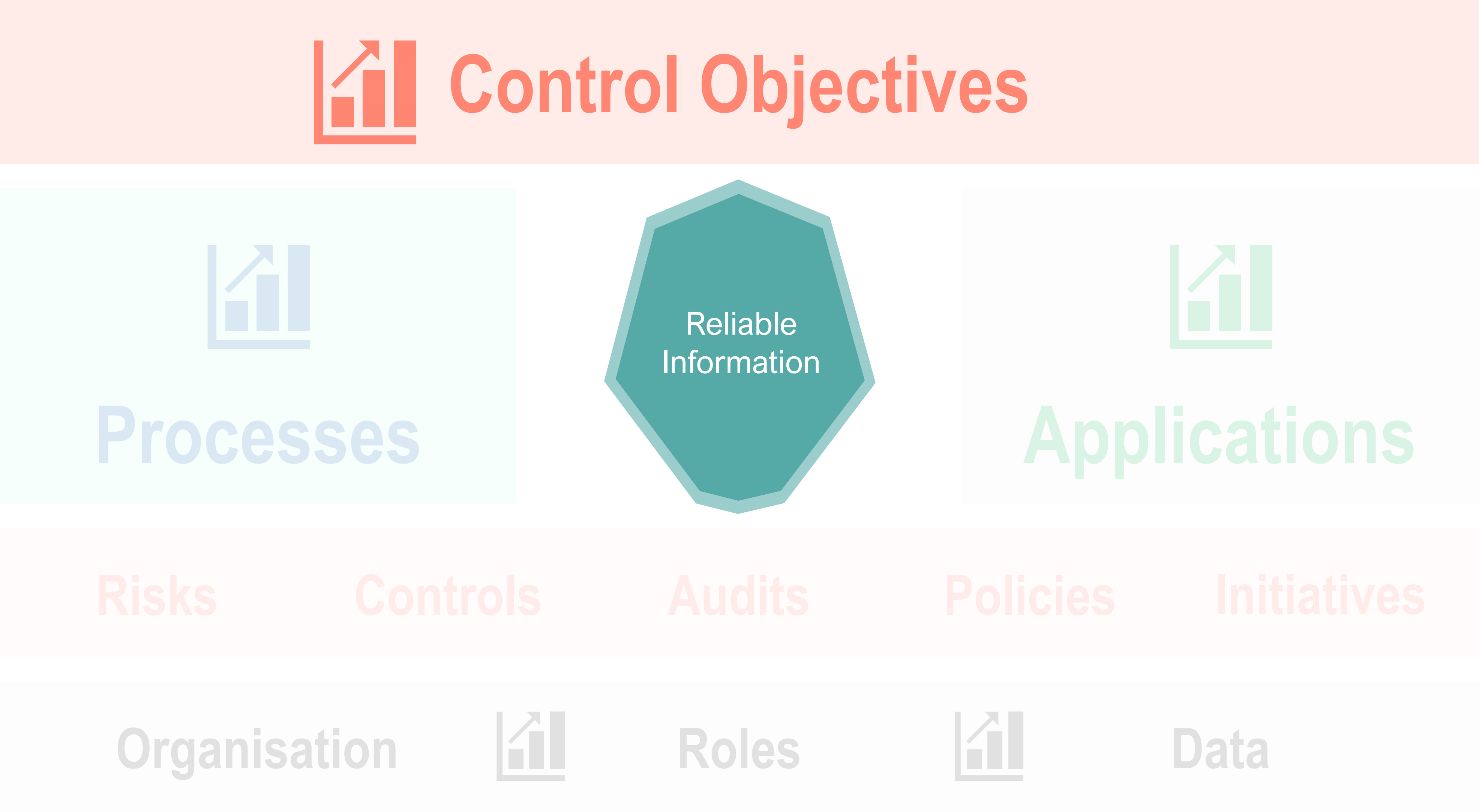


Control objective catalog

	Type	Name ↑	)	Implementation status	Responsible organisational …	PPTDF
1	○	AST-01.2 Stakeholder Identificatio		Not planned	[1] Business Organisation	Technology
2	○	CPL-01 Statutory, Regulatory & C				Process
3	○	CPL-03 Cybersecurity & Data Pro				Process
4	○	GOV-01.2 Status Reporting To Go				Process
5	○	GOV-04 Assigned Cybersecurity &				Process
6	○	GOV-08 Defining Business Conte				People
7	○	HRS-03.1 User Awareness	Applicable			Technology
8	○	HRS-05.4 Use of Critical Technologies	Applicable			People
9	○	OPS-01 Operations Security	Applicable			Technology
10	○	OPS-03 Service Delivery (Business Process Support)	Applicable			Process
11	○	PRM-01 Cybersecurity & Data Privacy Portfolio Manage…	Applicable	Planned	[1] IT	Process
12	○	PRM-02 Cybersecurity & Data Privacy Resource Manag…	Applicable	Planned	[1] IT	Process
13	○	RSK-03 Risk Identification	Applicable	Implemented	[1] Risk Management/ICS	Process
14	○	RSK-04 Risk Assessment	Applicable	Implemented	[1] Risk Management/ICS	Process
20	○	TPM-05.4 Responsible, Accountable, Supportive, Consul…	Applicable	Partially implemented	[1] Risk Management/ICS	Process

Discover an outline of your control objectives and their implementation status.
Key insights help you to effectively navigate your compliance requirements.

Assess what matters.



Control Objectives

Processes

Reliable Information

Applications

Risks

Controls

Audits

Policies

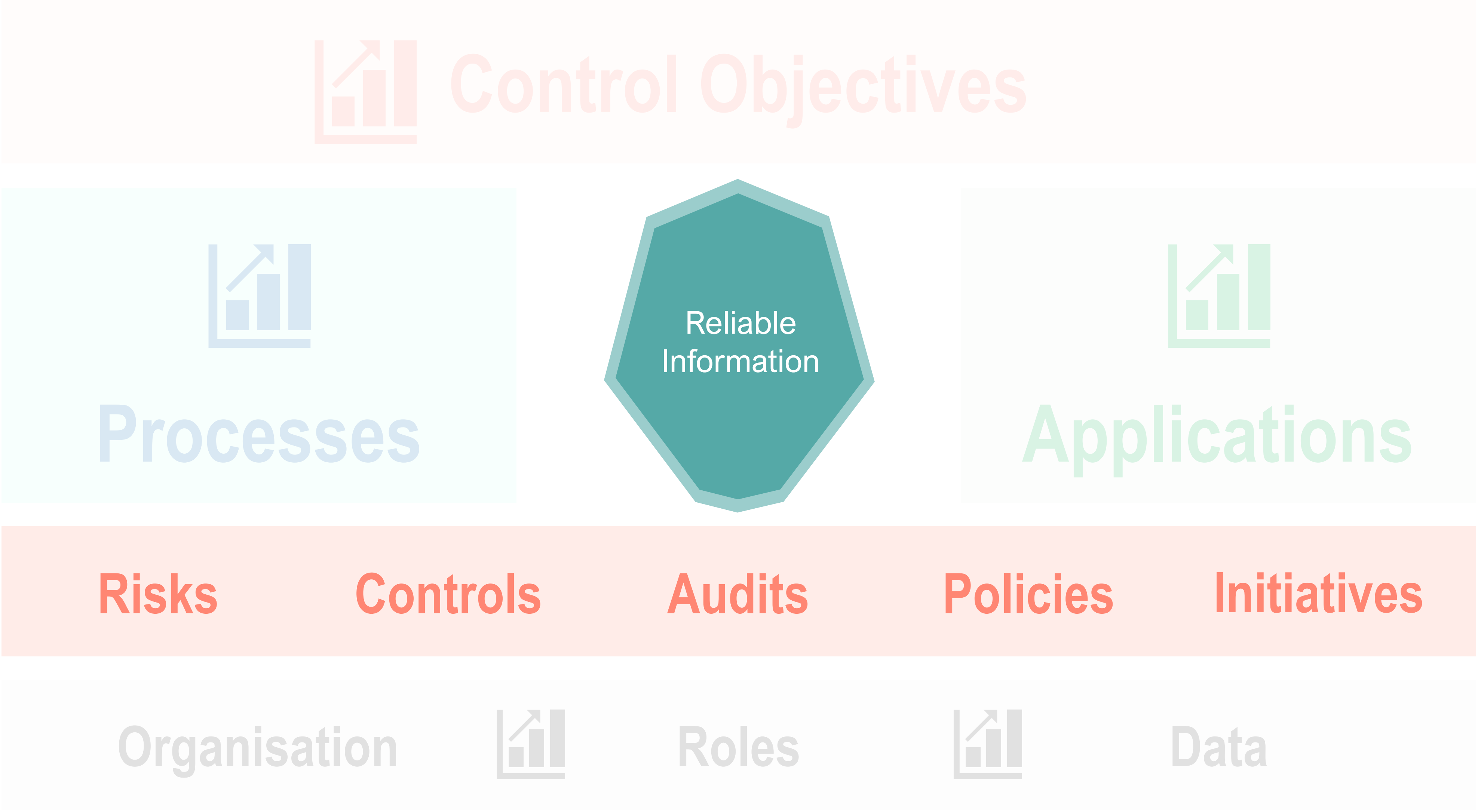
Initiatives

Organisation

Roles

Data

Assess what matters.



Control Objectives

Processes

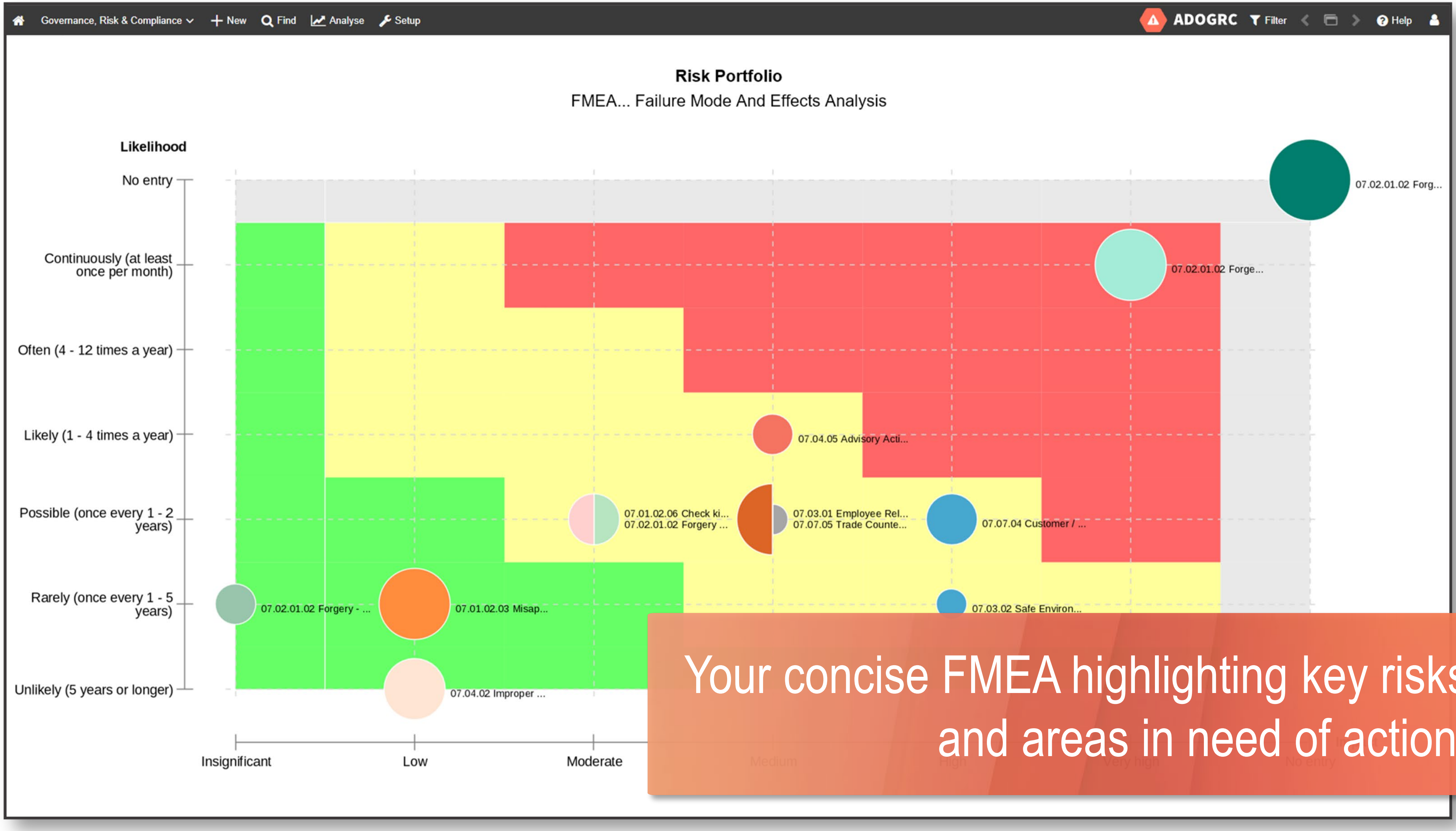
Reliable Information

Applications

Risks Controls Audits Policies Initiatives

Organisation Roles Data

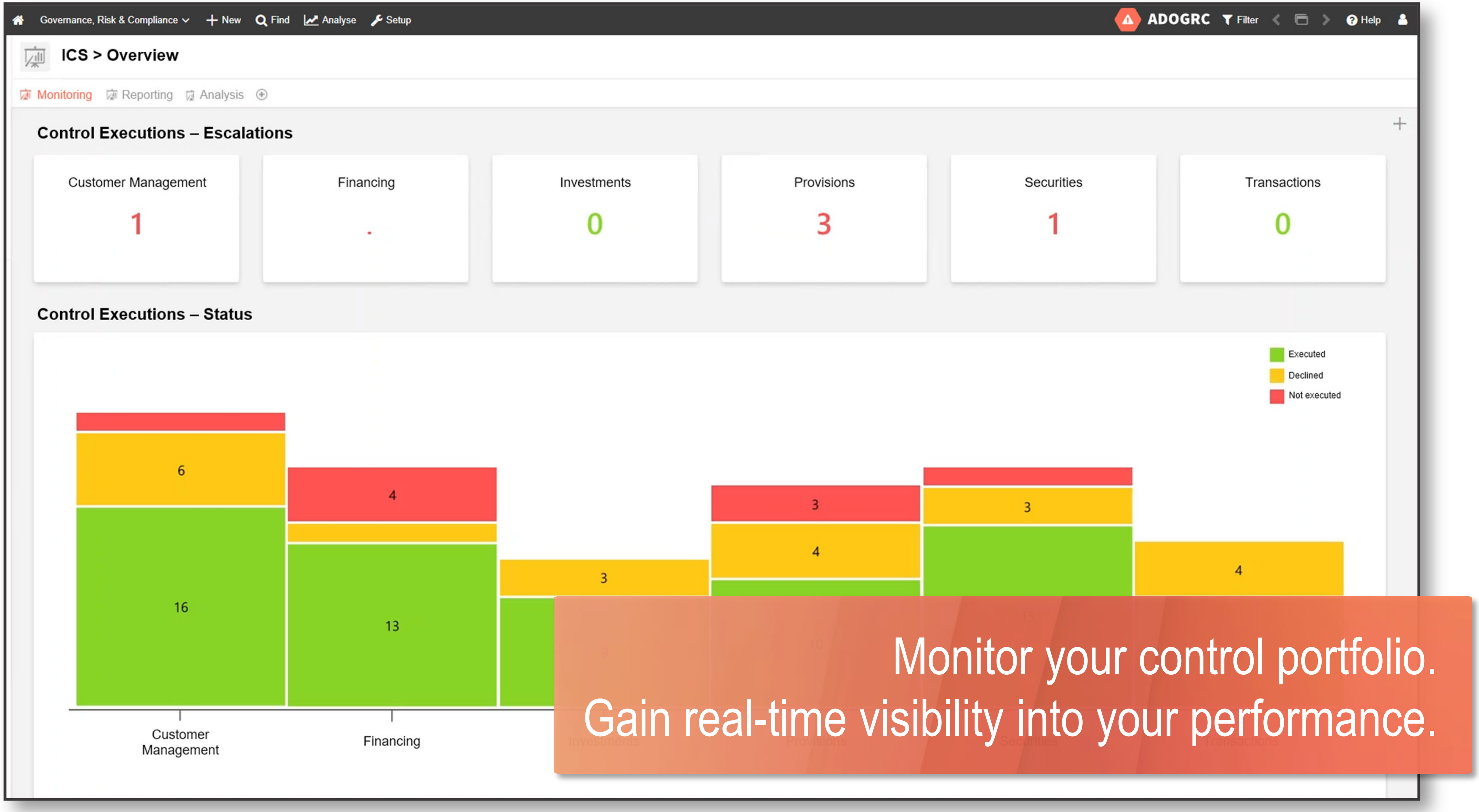
Assess what matters. Risks.



Your concise FMEA highlighting key risks and areas in need of action.

Assess what matters. Controls.

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



ICS > Overview

Monitoring | Reporting | Analysis

Control Executions – Escalations

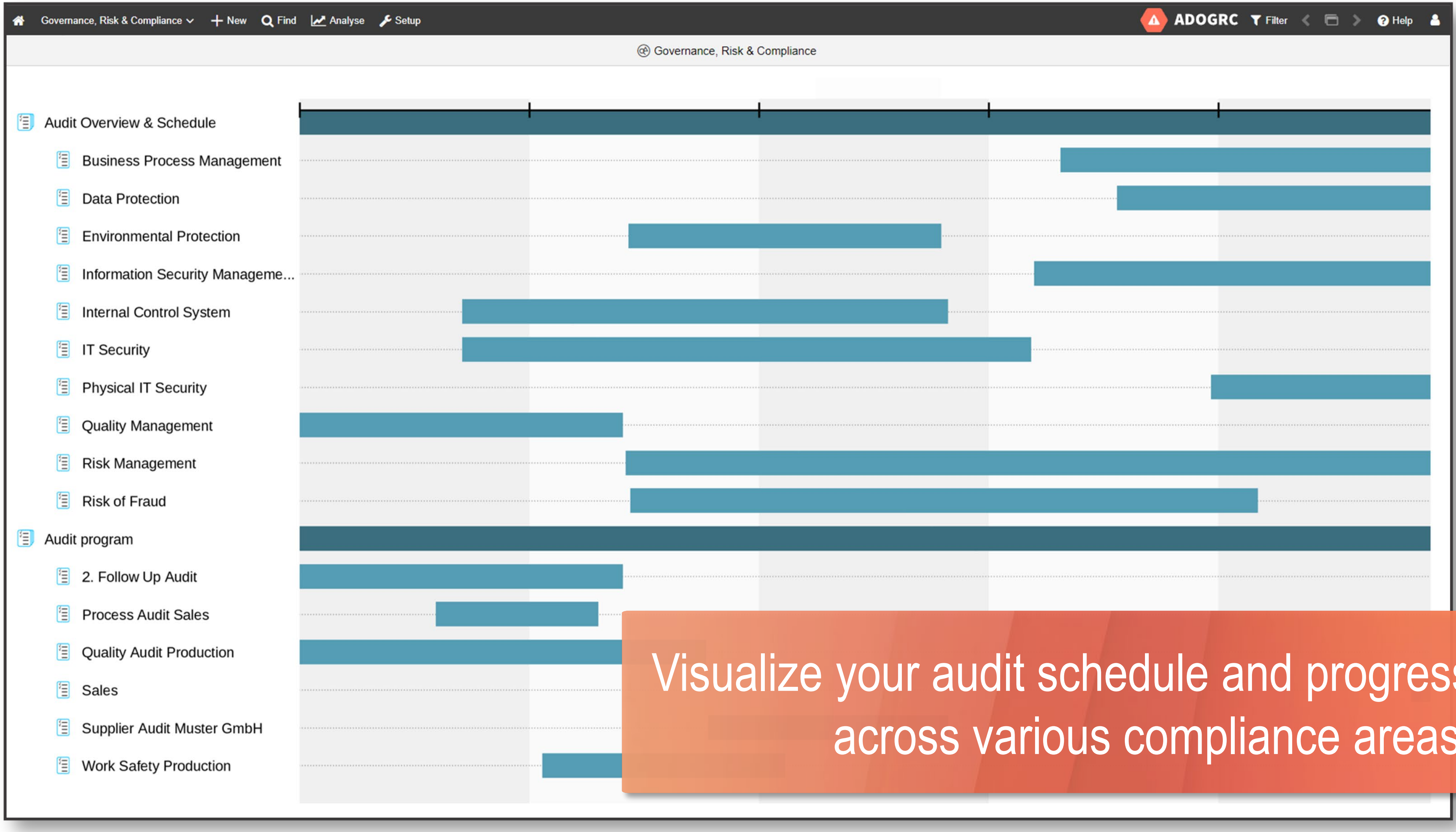
Customer Management	Financing	Investments	Provisions	Securities	Transactions
1	.	0	3	1	0

Control Executions – Status

Monitor your control portfolio.
Gain real-time visibility into your performance.

Assess what matters. Audits.

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



- Audit Overview & Schedule
  - Business Process Management
  - Data Protection
  - Environmental Protection
  - Information Security Manageme...
  - Internal Control System
  - IT Security
  - Physical IT Security
  - Quality Management
  - Risk Management
  - Risk of Fraud
- Audit program
  - 2. Follow Up Audit
  - Process Audit Sales
  - Quality Audit Production
  - Sales
  - Supplier Audit Muster GmbH
  - Work Safety Production

Visualize your audit schedule and progress across various compliance areas.

- ✓ Understand your compliance challenges better.
- ✓ Leverage your existing data.
- ✓ **Assess what matters.**

- ✓ Understand your compliance challenges better.
- ✓ Leverage your existing data.
- ✓ Assess what matters.

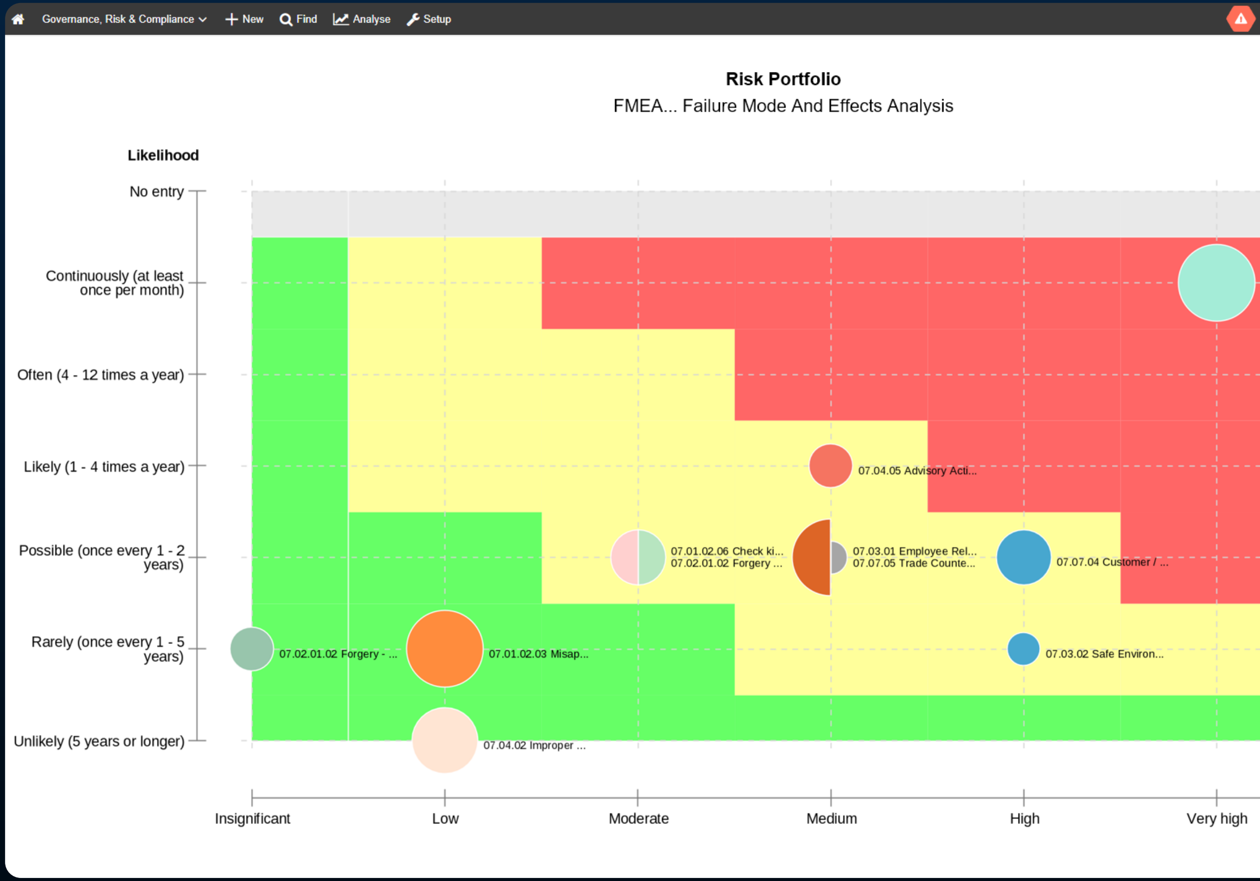
www.boc-group.com

Make your Compliance run better.

ADOGRC

Governance, Risk & Compliance

by boc-group.com


Governance, Risk & Compliance
New
Find
Analyse
Setup

Risk Portfolio

FMEA... Failure Mode And Effects Analysis

Likelihood
No entry
Continuously (at least once per month)
Often (4 - 12 times a year)
Likely (1 - 4 times a year)
Possible (once every 1 - 2 years)
Rarely (once every 1 - 5 years)
Unlikely (5 years or longer)
07.04.05 Advisory Acti...
07.01.02.06 Check ki...
07.02.01.02 Forgery ...
07.03.01 Employee Rel...
07.07.05 Trade Counte...
07.07.04 Customer / ...
07.02.01.02 Forgery - ...
07.01.02.03 Misap...
07.03.02 Safe Environ...
07.04.02 Improper ...
Insignificant
Low
Moderate
Medium
High
Very high

Fragen

Special-Offer: Proof of Value (PoV)

Make your Compliance run better
with ADOGRC

4’900* (statt 8’900*)
45% OFF

Angebotsumfang:

- 4 Workshops mit GRC-Experten
- 3 Monate Nutzung der ADOGRC-Software (Projektumgebung)
- Proof of Value Abschlussbericht

Ihre Vorteile:

- ADOGRC erleben und die Vorteile für ihr GRC-Management einschätzen
- Ermittlung eines Kosten-Nutzen-Verhältnisses mit minimalem Aufwand
- Unverbindlich! Keine Lizenzkaufentscheidung erforderlich.

Special-Offer: Proof of Value (PoV)

Make your Compliance run better
with ADOGRC

Phasen des Proof of Value (PoV) Angebots:

Einführung

- Kurzeinführung in GRC
- Aufbau der ADOGRC-Umgebung
- Identifikation relevanter Stakeholder
- Bestimmung relevanter Richtlinien und Vorgaben

Inventarisierung

- Analyse der vorhandenen Dokumentation
- Identifikation geschäftskritischer Prozesse
- Inventarisierung und Bewertung ausgewählter Risiken und Kontrollen

Operationalisierung

- Grobkonzeption des operativen Betriebs
- Identifikation der Reporting-Anforderungen

Abschluss PoV

- Erstellung eines Proof of Value Abschlussberichts
- Projektumfang für die Implemen-tierung von ADOGRC definieren