

7 MYTHS

ABOUT OPERATIONAL
RESILIENCE COMPLIANCE

& HOW TO CONVERT INTO
BUSINESS BENEFIT

Antony Bream

Advisor, Gieom

GET THE EBOOK



gieom

Agenda

- **7 Alarming Myths** about Operational Resilience Compliance
- **Risks of Believing** These Myths
- **The Benefits of** Getting it Right





- 12 Years specialising 100% in Operational Resilience technology
- Over 120 FSI clients globally
- Unique combination of technical, industry SME and complementary partner skills
- Experience delivering SOX and Solvency II projects where lessons learned informed our solutions





Jimi Hinchliffe

Geom Advisory Board Member

MYTH 1

We coped with COVID, so job done on resilience

THE REALITY

- In hindsight, COVID was a **slow burn event** – most operational disruptions don't offer advance notice
- COVID was **systemic** – due to its market-wide impact the world was accepting and tolerant

Disrupted or poor service in more 'normal' times could significantly impact client experience, harm reputation and lead to enforcement fines



Jimi Hinchliffe

Geom Advisory Board Member

MYTH 1

We coped with COVID, so job done on resilience

RISKS OF BELIEVING – OPERATIONAL RESILIENCE AT A STANDSTILL

- Regulators have given plenty of runway and expect to see operational resilience improvements
- Regulators are already assessing the readiness of financial entities and will hold senior managers accountable

Firms should seize the opportunity to embrace new tech, including AI, and apply best practices to improve OpRes continuously and gain holistic oversight



Bhavana Mallesh

Chief Technology Officer, Gieom

MYTH 2

DORA is a cybersecurity regulation, so IT and Info Security have it covered

THE REALITY

- Your technology platform should encompass the broad scope of the upcoming regulations – ICT risk management, incident reporting, resilience testing, third-party risk and governance
- Modern tech & AI can help overcome challenges around third-party contract analysis, risk-based testing & threat detection and standard procedures

A multi-departmental approach is needed to assess, implement and monitor OpRes effectively

gieom



Bhavana Mallesh

Chief Technology Officer, Gieom

MYTH 2

DORA is a cybersecurity regulation, so IT and Info Security have it covered

RISKS OF BELIEVING – LATE & INCOMPLETE COMPLIANCE

- Many risks will be overlooked – CrowdStrike was a critical third-party software update not a cyber attack
- Lack of accountability across the business
- Employees disengaged with resilience-building initiatives

Operational risks may be overlooked including: human error, supply chain and system failures



Andrew Sheen

Geom Advisory Board Member

MYTH 3

The DORA deadline may change and, even then, we're under the regulator's radar

THE REALITY

- 'Deadline deniers' and 'low fliers' have had 4 years to prepare
- Compliance by the deadlines is feasible utilising a technology-enabled approach that takes on the heavy lifting
- Manual processes and traditional GRC won't cut it

Impressive progress has been made by those applying best practices and adopting AI-powered tech to accelerate and embed OpRes across the firm



Andrew Sheen

Gieom Advisory Board Member

MYTH 3

The DORA deadline may change and, even then, we're under the regulator's radar

RISKS OF BELIEVING – PENALTIES & REPUTATIONAL HARM

- Firms risk sanctions if they experience operational disruptions after the deadline that highlight DORA non-compliance
- Fines and penalties for both financial institutions and their ICT service providers will follow

Firms failing to comply are putting their reputations and business continuity at risk



Gary Penolver

Chief Technology Officer, Quod Orbis

MYTH 4

We can run our operational resilience controls off a spreadsheet

THE REALITY

- Continual monitoring is required in Articles spanning all 5 Pillars
- Business is no longer linear – a multi-faceted, proactive approach to managing compliance is needed
- Using spreadsheets to monitor compliance and controls continuously has become unsustainable

Smart tech & intelligent automations connect your entire infrastructure, deliver accurate data & reporting



gieom



Gary Penolver

Chief Technology Officer, Quod Orbis

MYTH 4

We can run our operational resilience controls off a spreadsheet

RISKS OF BELIEVING – INDEFENSIBLE COMPLIANCE

- Age-old issues will remain – resource intensive, error-prone, unscalable, weak security, inefficient, static, data siloes
- Firms will lack a holistic, continuous view of OpRes
- Inadequate reporting & failure to meet response times

Inadequate reporting and oversight will impact your ability to evidence compliance to regulators





Antony Bream

DORA Lead, Gieom

MYTH 5

We have all the data we need to conduct DORA scenario testing

THE REALITY

- DORA Pillar 1 covers ICT Risk Management requiring extensive third-party risk scenario testing
- ICT service providers must also evidence OpRes compliance, requiring diligent testing of compliance status, financial health...
- Timely replacement of ICT service providers is expected

Data changes daily. Live, dynamic data embedded within your tech platform is needed for realistic scenario testing



gieom



Antony Bream

DORA Lead, Gieom

MYTH 5

We have all the data we need to conduct DORA scenario testing

RISKS OF BELIEVING – INADEQUATE SUPPLY CHAIN ACCOUNTABILITY

- Incomplete, inaccurate and meaningless scenario testing
- Regulatory enforcement fines
- Reputational damage causing loss of trust, client attrition and a decline in new business

Punitive sanctions for accountable senior managers





Nicola Cowburn

RegTech Lead, Gieom

MYTH 6

We are ISO 27001 certified, so we are DORA compliant

THE REALITY

- ISO 27001 is optional – DORA & UK OpRes are mandatory
- ISO 27001 will give you a head start – systems, processes, controls, focus on risk management
- ISO 27002 encompasses “key cybersecurity aspects” too

ISO 27001 gives you headwind but lacks the breadth needed to achieve compliance



gieom



Nicola Cowburn

RegTech Lead, Gieom

MYTH 6

We are ISO 27001 certified, so we are DORA compliant

RISKS OF BELIEVING – INADEQUATE COMPLIANCE & INDEFENSIBLE GAPS

- Firms will be exposed on:
 - Continuous compliance and monitoring vs. periodic reviews
 - Security & threat-led testing vs vulnerability management
 - Third-party (supply chain) risk management
 - Incident management & time-critical reporting
 - Senior manager accountability emphasised by new regs

Failure to implement complete, robust & defensible compliance measures could lead to personal sanctions



gieom



Vinod Menon

Chief Product Officer, Gieom

MYTH 7

ICT Service providers not named on the regulator's DORA critical suppliers list don't have to comply

THE REALITY

- DORA has unprecedented focus on ICT Service providers
- A third party that is critical to your operational resilience must be monitored and replaced quickly if need be
- The location of the financial services client is key

Ongoing, near-real-time supply chain risk management is an ideal use case for Artificial Intelligence



gieom



Vinod Menon

Chief Product Officer, Gieom

MYTH 7

ICT Service providers not named on the regulator's DORA critical suppliers list don't have to comply

RISKS OF BELIEVING – INCOMPLETE COMPLIANCE & REPUTATIONAL HARM

- Lack of appreciation of the extent of regulatory obligations
- ICT firms losing contracts with financial entities & being replaced by DORA compliant competitors
- Enforcement fines for non-compliance

Impact on reputation, revenues and long-term viability

The issues of today vs. benefits possible



A firm-wide, connected approach that enables re-use / incremental change to demonstrate compliance to new regulations

VS



Continuing to chase the ball around the playground

Updates to business documentation embedded as part of day-to-day operations making them a living document

VS

Competing priorities, diverse approaches and duplication of effort (often leading to gaps or inaccuracies)

Effortlessly link static (e.g. roles/vendor contracts) and transactional information (e.g. incidents/RCSA) from across the firm needed for operational resilience and to demonstrate regulatory compliance

VS

Slog of updating silos of unlinked documentation, reactively pulling together evidence and chasing departments across the firm

Benefits for a UK Financial Services firm with European clients

CHALLENGES

- No drill-down **consolidated reports**
- Excel-oriented; **time-consuming** and error-prone
- **Reactive** versus **proactive** decision-making
- Lack of **clarity** on RACI (Responsible, Accountable, Consulted, Informed) responsibility matrix
- **Evidencing** regulatory compliance
- Limited **scalability** hindering business growth and ability to cope with exponential rise in regulations
- Inadequate **user interface** and poor **client experience**

OUTCOMES

Single source of truth

Defensible compliance status

Versatility & agility

Extendability & scalability

Alerts & notifications

Management reporting

100%
UK OpRes compliant

75%
Fewer data errors

50%
Greater reporting accuracy

90%
User adoption within 3 months

50%
Less time to rollout new modules

70%
Less time needed for reporting

ABOUT GIEOM

Founded 2012 | 100% focus on operational resilience
120+ financial services clients | Global reach, local presence | Specialist partner ecosystem
ISO 27001 & ISO 9001 certified

CONTACT ME

Antony Bream Advisor
antony.bream@gieom.com
+44 (0)7880 796 403

WWW.GIEOM.COM
WWW.DORA360.AI



GET THE EBOOK

