



**Cognition  
Shared  
Solutions LLC**

RESILIENCE OF OPERATIONS WORTH HAVING



# RESILIENCE BUILDING

FCA GUIDANCE AND RULES &  
THE SUPPORT SCHEME BY  
COGNITION SHARED SOLUTIONS LLC

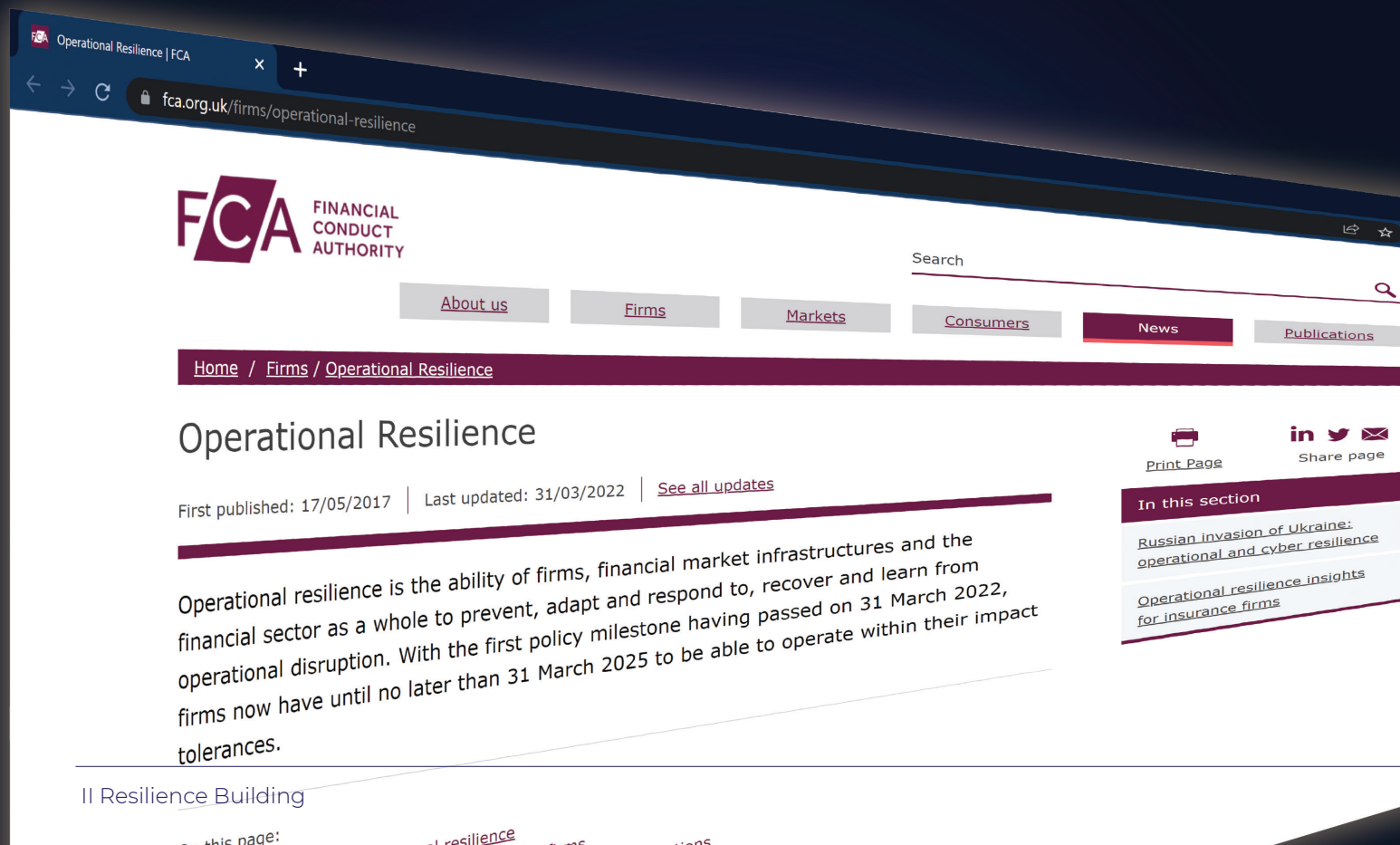
## RATIONALE

On 31 March 2022, the Financial Conduct Authority operational resilience guidance and rules were introduced.

Although they apply to only a subset of FCA-regulated firms, all financial institutions are advised to consider aligning with the guidance to strengthen their operational resilience.

## CONTENTS

*	1	INTRODUCTION
*	2	OPERATIONAL RESILIENCE
*	3	REQUIREMENTS OF THE OPERATIONAL RESILIENCE
*	7	HOW CAN WE HELP?
*	12	SUMMARY



The screenshot shows the FCA website page for Operational Resilience. The browser address bar displays 'fca.org.uk/firms/operational-resilience'. The page features the FCA logo, a search bar, and navigation tabs for 'About us', 'Firms', 'Markets', 'Consumers', 'News', and 'Publications'. The 'News' tab is selected. The breadcrumb trail reads 'Home / Firms / Operational Resilience'. The main heading is 'Operational Resilience', with a sub-heading 'Operational Resilience Building'. The text states: 'Operational resilience is the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption. With the first policy milestone having passed on 31 March 2022, firms now have until no later than 31 March 2025 to be able to operate within their impact tolerances.' A 'Share page' section includes icons for Print, LinkedIn, Twitter, and Email. A 'In this section' box lists two articles: 'Russian invasion of Ukraine: operational and cyber resilience' and 'Operational resilience insights for insurance firms'. The footer contains the text 'this page: ... resilience ... firms ... tions'.

## INTRODUCTION

In early 2021, the Financial Conduct Authority (FCA), in partnership with the Bank of England (BoE) and the Prudential Regulation Authority (PRA), published new rules and guidance designed to strengthen the operational resilience of the UK financial services sector.

These rules apply to banks, building societies, PRA-designated investment firms, insurers, Recognised Investment Exchanges, Enhanced scope SM&CR firms, and entities authorized and registered under the Payment Services Regulations 2017 and Electronic Money Regulations 2011.

However, firms out of scope are nevertheless advised to consider aligning to the guidance as best practice to strengthen their operational resilience.

At Cognition Shared Solutions LLC, we have been helping our clients build a resilience framework for the last 15 years.

The second part of this document will present support measures designed to help you meet and exceed FCA's requirements.

# OPERATIONAL RESILIENCE

## THE WHAT AND WHY

### WHAT IS OPERATIONAL RESILIENCE?

FCA created the new rules to increase the oversight of resilience planning and management in the UK financial sector. Operational resilience is the ability of firms, financial market infrastructures, and the financial sector to absorb and adapt and recover and learn from operational disruption. It extends beyond business continuity and disaster recovery and is a strategic priority for regulators.

### WHY IS IT IMPORTANT?

Operational disruptions and the unavailability of essential business services can cause wide-reaching harm to consumers and/or risk to market integrity, threaten firms' viability, and cause instability in the financial system.

Like previous examples of disruptions, the coronavirus pandemic has again highlighted the interconnectedness of the financial sector across the globe. Disruptions can and are likely to happen and will likely take as yet unseen forms. While preparing for known threats is essential, true resilience means being ready to withstand impacts yet unknown.

# FCA REQUIREMENTS FOR OPERATIONAL RESILIENCE

WHILE PREPARING  
FOR KNOWN  
THREATS IS  
ESSENTIAL, TRUE  
RESILIENCE MEANS  
BEING READY  
TO WITHSTAND  
IMPACTS YET  
UNKNOWN.

## 1. ESSENTIAL BUSINESS PROCESSES MAPPING

As the first step, firms must identify and map their key business processes, which could cause 'intolerable levels of harm' to the firm, its clients, or the markets.

The mapping will vary across firms, depending on their size, scale, and complexity. However, it must be sufficiently granular to allow firms to enumerate and document the people, processes, data, and systems necessary to deliver the identified essential business services.

Firms must set impact tolerances for 'severe but plausible' disruptions to their essential business services. The impact tolerances, and the range of severe but plausible scenarios, must be monitored and should evolve to match the economic, technological, and socio-political conditions.

Payment service providers must also consider their obligations under the European Banking Authority (EBA) Guidelines on Information and Communication Technology (ICT) and Security Risk Management when defining their impact tolerances.



## 2. OPERATIONAL TOLERANCE



Firms must set impact tolerances for 'severe but plausible' disruptions to their essential business services. The impact tolerances, and the range of severe but plausible scenarios, must be monitored and should evolve to match the economic, technological, and socio-political conditions.

Payment service providers must also consider their obligations under the European Banking Authority (EBA) Guidelines on Information and Communication Technology (ICT) and Security Risk Management when defining their impact tolerances.

### 3. SCENARIO TESTING



Firms must carry out scenario testing to assess whether they can remain within the impact tolerances they have set for each of their essential business services in a severe but plausible disruption to their operations. Firms must identify an appropriate range of adverse circumstances of varying nature, severity, and duration relevant to their business and risk profile and consider the risks of delivering their essential business services. Potential sources of disruption could include cyber-attacks, telecommunications/power outages, third-party supplier failure, the unavailability of key people, or natural hazards such as fire, flood, or severe weather.

If any issues are identified through audits, after carrying out scenario testing, or after an operational disruption, firms must remedy any vulnerabilities which would prevent them from staying within the defined tolerances.

Firms must develop internal and external communication strategies to enable acting “quickly and effectively” to reduce the anticipated harm caused by operational disruptions. For example, the regulators expect firms to consider how they would promptly provide important warnings or advice to clients and other stakeholders and gather information about the cause, extent, and impact of operational incidents.

Firms should also consider their reporting obligations to the FCA (under Principle 11), the PRA (where dual-regulated), Action Fraud (if the incident is criminal), the Information Commissioner’s Office (if the incident involves a data breach), and the National Cyber Security Centre and the Cyber Security Information Sharing Partnership (for cyber incidents).



## ARE YOU WITHIN SCOPE?

### WHICH FIRMS ARE WITHIN THE SCOPE OF THE RULES?

The new rules apply to the UK authorized financial services firms - banks, building societies, investment firms, insurers, recognized investment exchanges, enhanced scope firms in the senior manager and certification regime, payment services firms, electronic money firms, and registered account information services providers.

### WHAT IS THE IMPLEMENTATION DEADLINE?

The operational resilience requirements came into force on 31 March 2022. As a result, firms must consistently remain within their impact tolerances for each critical business service as soon as practicable after 31 March 2022 and no later than **31 March 2025**.



## HOW CAN WE HELP?

### OUR FRAMEWORK

WE ASSIST IN ACHIEVING FULL COMPLIANCE.  
WE HELP BUILDING BUSINESS RESILIENCE.


Given the events of the last few years, it is clear that operational resilience is key to looking after the firm's clients, its reputation, and the orderly functioning of financial markets. The speed and interconnectedness of today's markets require all participants to be in top readiness condition, and resilience is clearly at the top of the regulators' agenda. Any issues or shortcomings in this area could translate into intolerable losses and regulatory censure. At the same time, well-prepared firms will dominate the market, turning negative scenarios into opportunities to help their clients, and therefore increase their market share.



**RESILIENCE IS MORE  
THAN A LEGAL  
REQUIREMENT.**

**IT'S A BUSINESS  
NECESSITY.**





**Operational resilience** implementation will vary across firms, depending on their size, scale, and complexity. All firms must be able to demonstrate, e.g. through scenario testing, that they would be able to withstand “severe but plausible” scenarios.

---

01

---

## CRITICAL SYSTEM IDENTIFICATION

The first stage of our process involves mapping the firm’s environment (clients, systems, and suppliers) and major internal stakeholders.

We perform the mapping with our clients using our tried and tested **Trilayer Business Process Analysis™**. It analyses the process on three levels: process execution, supporting data, and risk management. This way, we capture the potential impacts of disruptions in a broad spectrum of scenarios.

Based on the resulting map, the first FCA requirement can be met, namely the identification of important business processes.

02

---

## OPERATIONAL TOLERANCE CALIBRATION

Once the critical processes are identified, the FCA requires the firms to set operational tolerances, i.e., maximum tolerable disruption for these services. Although FCA expects time/duration to be the primary metric used across the processes, they also allow some flexibility in using additional appropriate metrics, depending on the specifics of the firms’ processes.

We work with our clients to define appropriate metrics and calibrate tolerable disruption levels, considering clients’ requirements, the orderly operation of financial markets, and the firm’s overall tolerable risk levels and reputation.

## 03

---

### SCENARIO DEFINITION AND TESTING

FCA mandates testing based on severe but plausible scenarios to ensure that the calibrated operational tolerances are met. The level of testing will depend on the sophistication level of the firm and the risk level of the service.

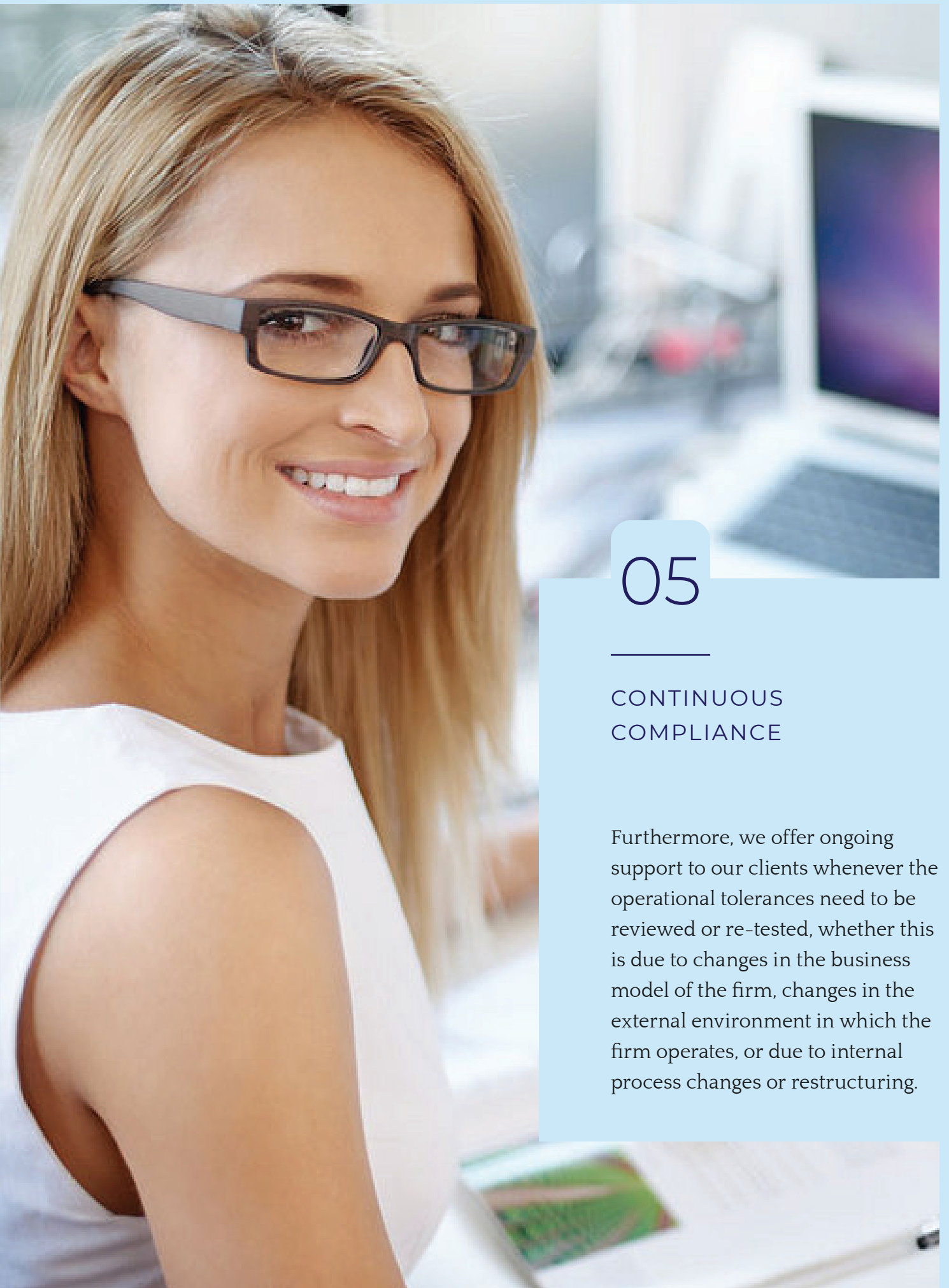
We offer our clients several approaches to testing, depending on the identified requirements, including theoretical scenario analysis, interactive reviews and walkthroughs, and full-scale simulations. These are applied depending on the client's requirements, such as risk levels, systems availability, and specific scenarios.

## 04

---

### REMEDIATION ROADMAP

All the steps up to this point should provide the client's board with a clear understanding of the operational resilience readiness of their firm. We assist our clients with specialist knowledge to perform gap analysis and design a remediation plan for any issues identified during the testing. We also work closely with our clients to support their teams' plan implementation until full compliance is achieved.



## 05

---

### CONTINUOUS COMPLIANCE

Furthermore, we offer ongoing support to our clients whenever the operational tolerances need to be reviewed or re-tested, whether this is due to changes in the business model of the firm, changes in the external environment in which the firm operates, or due to internal process changes or restructuring.

## SUMMARY

### ACT NOW!

On 31 March 2022, new Financial Conduct Authority operational resilience requirements were introduced, applying to specific subsets of UK authorized financial firms. Nevertheless, all firms are advised to consider applying all or some of the guidance to strengthen their operational resilience.

The interim period for these rules ends on 31 March 2025, and after this date, firms are expected to be continuously compliant with their operational resilience tolerance levels.

In response to the introduction of these requirements, we have worked with our clients to prepare them to meet and exceed the requirements by:

- » reviewing and mapping their businesses to identify critical processes,
- » defining and documenting operational tolerance levels,
- » designing and executing tolerance level tests
- » road-mapping and implementing remediation programs for any identified gaps.

Our clients can choose to work with us either on the end-to-end process or selected stages, depending on where they need us the most.

If you would like to discuss your firm's requirements regarding implementation or testing of operational resilience, please contact our expert team, and we will be happy to discuss your needs and provide support to achieve full compliance.



***Cognition Shared Solutions LLC***

16192 Coastal Highway  
Lewes 19958, DE, USA  
[contact@cog-shared.com](mailto:contact@cog-shared.com)  
[www.cog-shared.com](http://www.cog-shared.com)