Operational Resilience
ClusterSeven by Mitratech
White Paper

MITRATECH

RAISING THE BAR: OPERATIONAL RESILIENCE AND SHADOW IT

ClusterSeven

INTRODUCTION

The past decade has seen the banking regulators focus on improving the financial resilience of banks and other institutions. Those efforts have paid off: the risk of any individual organization threatening the stability of the wider financial system has reduced significantly, as banks especially hold more capital and liquidity than ever before.

Now the UK regulators are turning their attention to building the Operational Resilience of the UK financial system as a whole, and the individual firms within it.

A discussion paper on the topic, issued jointly by the Bank of England, the Prudential Regulation Authority (PRA), and the Financial Conduct Authority (FCA) in July 2018, describes a resilient financial system as one that can 'absorb shocks rather than contribute to them.' This goes well beyond the traditional understanding of operational risk and recovery capabilities by focusing on preserving the continuity of the provision of critical economic functions, both to an institution's clients and to the UK economy as a whole.

In this white paper, we look at the likely implications of any future Operational Resilience regulation on the way an institution manages non-IT supported applications and processes (Shadow IT) such as spreadsheets or other end-user computing (EUC) applications; and outline the steps you could start taking now, to be ready to comply when regulation comes into effect.

RESILIENCE IN THE FACE OF DISRUPTION

Operational disruption can impact on financial stability, threaten the viability of individual businesses, or cause harm to consumers and other market participants in the financial system. Institutions will need to consider all these risks when assessing appropriate levels of Operational Resilience within their businesses.

Operational Resilience, as defined in the discussion paper, is the ability of individual companies — and the financial sector as a whole — to prevent, respond to, recover from, and learn from operational disruptions.

Prevent. Institutions must understand their critical services and the processes, systems, and the people that underpin them. They also need frameworks for managing operational risk, so that they understand and control their risk environment.

Respond. They must be able to quickly identify the scale of the impact of an operational disruption, and communicate effectively with those affected, in order to manage expectations and restore confidence.

Recover. Organizations must be able to recover from a disruptive incident. They need to have contingency plans in place that enable resumption of critical functions within agreed tolerance levels.

Learn. Institutions should ensure that they learn from both incidents and near misses, to limit the chances of a recurrence.

Continuity of business services is the outcome of Operational Resilience, and this is what institutions will be required to focus on. The paper advises organizations to assume that individual systems and processes that support business services will inevitably suffer disruption at some point. They should therefore concentrate their efforts on backup plans, responses, and recovery options.

The paper acknowledges that ensuring Operational Resilience has become a more challenging undertaking in today's landscape of growing cyber risk, large-scale technological change, and increased outsourcing. However, organizations are advised to adopt an approach that allows them to maintain continuity of the services they provide, regardless of the cause of the disruption.

Who will own Operational Resilience?

As institutions weigh up the implications of the discussion paper, an intriguing question is emerging: Who will own Operational Resilience at a business? Is it IT and the associated Business Continuity Management (BCM) team, who may apply ISO 25999 to their existing business processes, and who will have a tight control of the IT business processes? Or is this an area best covered by the Operational Risk Management function, which will have a detailed grasp of the core business processes?

Each function may interpret the requirements differently, and have differing priorities which can impact the spirit and language of Operational Resilience differently. How will businesses best design, implement, and manage Operational Resilience, when it finally becomes mandated?

An additional consideration is how will regulators interpret Operational Resilience? Where will they focus their efforts, at least initially?

WHY SHADOW IT RISK MANAGEMENT WILL MATTER IN OPERATIONAL RESILIENCE

While many institutions will be familiar with the fundamentals of Operational Resilience, both technically and operationally, Shadow IT risk will present a new challenge for them under Operational Resilience. In many financial firms, Shadow IT is core to a wide range of processes and services, including business and financial modeling, business management and reporting, portfolio management, analysis, decision-making, as well as compliance.

Operational Resilience means that these institutions will need to understand and document how Shadow IT features in these business processes, and how they are managed to ensure they meet Operational Resilience. A further potential outcome for institutions is that once they have surfaced these mission critical Shadow IT applications, they will likely be of greater interest to regulators and auditors, as well as senior management, who will likely be interested in how these Shadow IT applications are managed, controlled, and documented.

To understand their significance and value, it is worth exploring why Shadow IT is used extensively in institutions in the first place.

Shadow IT applications provide business users significant flexibility and capacity to innovate. It can encompass development environments, databases, and business intelligence tools for example. Spreadsheet-based applications form a significant part of an organization's Shadow IT environment.

Spreadsheets are the familiar, go-to tool used by many people to answer a question or solve a problem much faster than is generally possible using a more formalized IT system. Spreadsheets are powerful enough to run complex calculations and models, and it's easy to connect them together so that data can flow between them. A spreadsheet may have an officially sanctioned role in a process. Equally, a spreadsheet may start out as a tactical fix, and soon become too embedded in a process to be easily removed.

WHY SHADOW IT RISK MANAGEMENT WILL MATTER IN OPERATIONAL RESILIENCE

Ensuring effective spreadsheet risk management will be a critical element of Operational Resilience. Spreadsheet-related operational disruption could have many causes, such as:

- A server, network, or data center outage, preventing access to a critical spreadsheet
- A data entry error caused by, for example, fat finger, that isn't immediately identified
- Poor-quality data, entered directly or acquired from a linked spreadsheet impacting a model or calculation, which can affect the availability or performance of a business service or offering.
- Uncontrolled or unauthorized changes, leading to unintended calculation errors that can impact core services.
- Lack of version control, resulting in use of multiple versions of the same spreadsheet, or updates being made to an out-of-date version, which can impact decision-making or reporting
- Lack of clarity about the links between spreadsheets, impacting on a business transformation activity such as a merger, demerger, or outsourcing agreement, which can affect the availability of a service.

Once Operational Resilience becomes a regulatory requirement, as seems likely, spreadsheets will be subject to close inspection. Institutions will need to bring their spreadsheet environment into line with Operational Resilience requirements, or identify and migrate their most critical spreadsheets to enterprise applications.

GET READY FOR COMPLIANCE

So what can you do to prepare your spreadsheet estate for compliance with any future Operational Resilience regulation? We recommend building a framework for spreadsheet risk management, which will enable you to:

- Understand which spreadsheets support critical processes and business services
- Define the risks of spreadsheet complexity to your institution's operations
- Appreciate the financial, operational, regulatory, and reputational impact of spreadsheet errors
- Ensure clarity of spreadsheet ownership
- Set up processes to govern how changes are made to spreadsheets

You'll also have the information you need to support the eventual migration of spreadsheets to a formalized enterprise IT application.

Step 1. Establish your spreadsheet estate

Creating an inventory of your critical spreadsheets is the first step to getting them under control.

Step 2. Carry out a risk check

Once you know what spreadsheets exist, you can carry out a risk analysis on critical files — assessing their materiality and the associated operational risks.

Step 3. Reveal the connections

Revealing the connections between spreadsheets — exposing the data lineage — will help you understand the relationships between them, and which ones underpin the delivery of critical business services. You'll also gain insight into the associated risks around data and input quality.

Step 4. Manage and monitor key spreadsheets

Knowing what spreadsheets you have and how they're connected will help you better manage spreadsheet-dependent processes, and reduce the risk of errors and the ensuing operational disruption. You'll be able to:

- Identify the differences between versions of the same spreadsheet
- Implement change control and ensure that changes to a spreadsheet are documented for others to see
- Establish a review and approval process that records details of the approval steps. This effectively becomes a continuous audit process that will be critical for compliance with future Operational Resilience regulation

THE BENEFITS OF AUTOMATION

If your institution relies on more than a handful of important spreadsheets, a manual framework for spreadsheet risk management will soon become untenable. In contrast, an automated software-based process will help you realize the benefits of spreadsheet risk management more quickly, without it becoming a drain on resources;

- An automated solution will scan your IT infrastructure to locate the spreadsheets in use across the institution. It will provide you with accurate information about how many there are, where they reside, and when they were created and modified
- The data lineage will be clearly exposed, with a dependency tree that shows data sources and relationships between files in a visual way
- Risk-checking critical files is faster and simpler with an automated solution. You'll be able to apply rules that matter to your business, such as formula or macro-code complexity, or the presence of hidden worksheets.

With an automated approach to monitoring and management, you'll find it quicker and easier to:

- Compare multiple versions of a file to identify what changes were made when, and by whom
- Manage the review and approval process for critical cells in high-risk spreadsheets
- Apply a control framework to your spreadsheets that increases transparency by creating an audit trail of changes and showing how each spreadsheet evolves over time
- Automate the production of documentary evidence for regulatory reporting

You'll also be able to maintain a secure and up-to-date inventory of your spreadsheets (that meets your own as well as regulatory reporting requirements) by capturing data about each spreadsheet such as the owner, the business areas that use it, and the business services it supports.

CONCLUSION

The UK regulators haven't yet defined or scheduled any regulation relating to Operational Resilience, but there's no doubt that it's on the horizon. The discussion paper issued in July 2018 provides plenty of guidance on the areas the regulation is likely to cover, and how institutions should approach the matter.

Given the critical role spreadsheets play in many banking processes, it's never too soon to improve spreadsheet risk management. Starting now means your institution will be ready in good time to demonstrate that its spreadsheet environment complies with any new Operational Resilience regulation. In the meantime, implementing effective spreadsheet risk management means you'll be able to continue taking advantage of the benefits spreadsheets offer, while reducing the scale and scope of regulatory, reputational, and other risks to your business.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk, and compliance professionals seeking to maximize productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, enterprises worldwide are able to implement best practices and standardize processes throughout their organizations and realize fast time-to-value.

Serving 1,200 organizations of all sizes worldwide, Mitratech works with almost 40% of the Fortune 500 and over 500,000 users in over 160 countries.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com