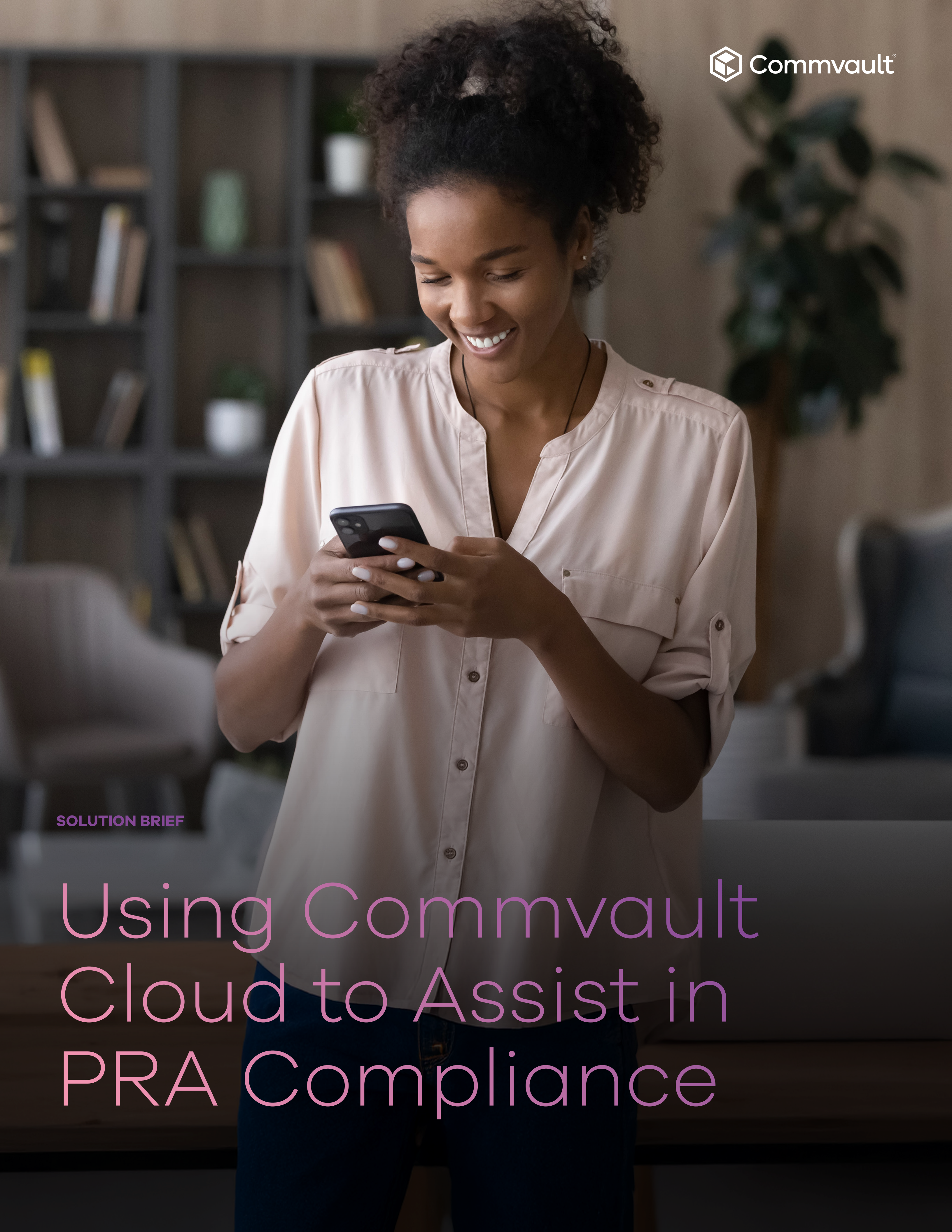

SOLUTION BRIEF

Using Commvault Cloud to Assist in PRA Compliance

In November 2024, the Bank of England's Prudential Regulation Authority (PRA) released an updated Statement of Policy (SoP) on Operational Resilience, revising its previous March 2021 version. This statement of policy aims to ensure that financial firms can withstand disruptions and continue to provide important business services. For the PRA, this means that covered entities:

- Prevent disruptions as much as possible.
- Adapt systems to maintain essential services during incidents.
- Return to normal operations swiftly.

This policy applies to all UK banks, building societies, and PRA-designated investment firms, as well as UK Solvency II firms, the Society of Lloyd's, and its managing agents.

The SoP also extends to outsourcing and third-party providers supporting firms, offering clarity on how the PRA's operational resilience policy influences the regulatory framework.

Firms are expected to be fully compliant with the operational resilience requirements by March 31, 2025.

WHAT IS RESILIENCE?

Resilience is organization's ability to bounce back from cyberattacks and other security incidents. Preventing attacks and defending against threat actors are key elements of any cyber strategy, but being prepared to respond and recover effectively is arguably more important. This is especially true as the reality of business today is that it's not a matter of if you're going to be attacked, but when, and how bad it will be.

Resilience can be a differentiator for any organization due to the large number of both targeted and opportunistic attacks waged daily by cyber criminals. Building processes and using technology that helps maintain continuous business and minimize downtime and data loss can help build the trust of your customers and capture the business of those who were not so prepared.

But it's not just good business practices to build resilience. Many organizations deliver vital, critical services to people, including healthcare, social services, utilities, and financial services. Because of this, governments and regulatory bodies around the world have codified what is required for organizations to remain a going concern and protect markets from the adverse effects of cyberattacks.

WHAT DOES PRA REQUIRE?

In the face of disruptive cyberattacks and outages, organizations need to implement strategies and controls to help reduce the likelihood of incidents and disruptions from occurring, and in the event that they *do occur*, show that they've made efforts to mitigate the impact of incidents and operational risks.

OPERATIONAL RISK MANAGEMENT: MAP & TEST IMPORTANT BUSINESS PROCESSES

An important element of any resilience plan begins with identifying the business components, services, and technology that, if disrupted, would cause significant harm to clients or the financial system. This also requires an analysis of the impact of disruptions on different parts of the organization and setting the minimum viable threshold of availability, or impact tolerance, that the business can withstand in terms of downtime in the face of an incident.

Once the important business services are understood and prioritized based on the impact tolerance, the organization must test those services against scenarios which may affect them, including system outages, disasters, and cyberattacks.

BUSINESS CONTINUITY PLANNING

Understanding the role that certain systems, apps, and data play in the daily operation of your business helps to establish which of those are most critical and must be fastest to recover. The mapping process in operational risk management can help fulfill this.

Business continuity planning involves people, processes, and technology in order to be executed properly.

Critical business roles need to have primary and secondary individuals assigned to them. This involves executive leadership, operational leadership, and the roles necessary to re-establish the business functions deemed critical for the business to operate. For most organizations, this will include individuals in IT and security roles to rebuild and restore digital architecture, systems, and data that power business and customer processes.

Planning for business continuity is only helpful if you can test the plans to validate whether they work. Running exercises, including tabletop simulations and full-scale cyber recovery tests, can help reveal gaps in your plan so you can close them, enable teams to know what is required of them to recover, offer insight into expected timelines and impacts, as well as build company leadership's confidence that recovery and continuous business is possible.

COMMVAULT CLOUD FOR CYBER RESILIENCE

Commvault helps organizations improve their cyber resilience and reduce risk, minimize downtime, and control costs. It's the only cyber resilience platform built for the hybrid world, offering the best data security for all workloads, anywhere, combined with rapid, enterprise-scale recovery.

UNDERSTAND YOUR DATA ASSETS, APPS, & DEPENDENCIES TO REDUCE RISKS

Commvault can help organizations meet the PRA requirements by using a variety of capabilities aimed at discovery, risk and configuration assessment, and continuous monitoring.

With Commvault Risk Analysis, organizations can effortlessly secure and defend sensitive data across their entire infrastructure. They gain visibility into data risks to easily identify and categorize sensitive data to collaborate with ease and mitigate potential data breaches, all while saving costs through smart, proactive data management strategies.

Commvault Threat Scan scans unstructured data, allowing operations teams to take control and defend their data by proactively identifying malware threats to reduce the likelihood of spread and prevent reinfection during a cyber recovery. Threat Scan analyzes backup data to find encrypted or corrupted files so users can quickly recover trusted versions of their data.

For cloud assets, Commvault Cloud Rewind can help map application data and dependencies to better understand the interconnectedness between systems, apps, infrastructure, and critical data. In the event of an attack or outage.

DETECT THREATS AND ANOMALIES TO YOUR ENVIRONMENT

Because Commvault Cloud already backs up your data, we can intelligently detect threats to it. The Commvault Cloud platform can look for early warnings of suspicious activity using machine learning, analyze event timelines, and establishing baseline behavior for each machine. By comparing file characteristic changes against established baselines, we can identify and alert you to abnormal behaviors. This empowers administrators to take immediate action, mitigate risks, and respond to threats.

IMPLEMENT & TEST YOUR RECOVERY & RESILIENCE

Commvault® Cloud Cleanroom™ Recovery provides an affordable, clean, secure, isolated recovery environment on demand for testing cyber recovery plans, conducting secure forensic analysis, and uninterrupted continuous business.

Every organization needs to be able to recover data cleanly after an outage or cyberattack. Practicing can help refine your processes to recover and help mitigate the risk of ransomware, data corruption, and disasters. These exercises may involve tabletop simulations that may corrupt or take down the systems, or random tests of recoverability of certain workloads, environments, clouds, or applications. These tests can help cyber recovery teams to understand what is necessary to restore the affected systems to operation. Cleanroom Recovery enables these types of tests.

Commvault Cloud Cleanroom Recovery offers the ability to recover data, apps, and infrastructure from AWS, Azure, GCP, OCI, and on-prem environments to a safe, on demand cloud-isolated cleanroom. This comprehensive recovery platform lessens the complexity and cost of using disparate tools and instead delivers reliable cyber resilience and readiness.

In addition to application and dependency mapping that was mentioned earlier, Cloud Rewind can also automate the process to rebuild those apps and their data quickly, helping mitigate the risk of extended downtime.

TRY COMMVAULT CLOUD TODAY

Commvault Cloud can help your organization achieve better resilience and comply with several elements of PRA. Commvault helps implement your risk management program by automating risk monitoring, providing real-time anomaly and threat detection, and enabling teams to test their recovery in the face of cyberattacks and disasters. Incident management can be streamlined with cyber recovery planning. And now, you can use cleanroom technology to test and execute your resilience strategies in an efficient, proactive, and cost-effective way. Get a live demo of Commvault Cloud today.

To learn more, visit **commvault.com**

Commvault®

commvault.com | 888.746.3849