EDB™

The CIO's Guide to Operational Resiliency in Financial Services:

3-Step Approach to Strengthen Your Database

Julian Moffett
Field CTO, EDB

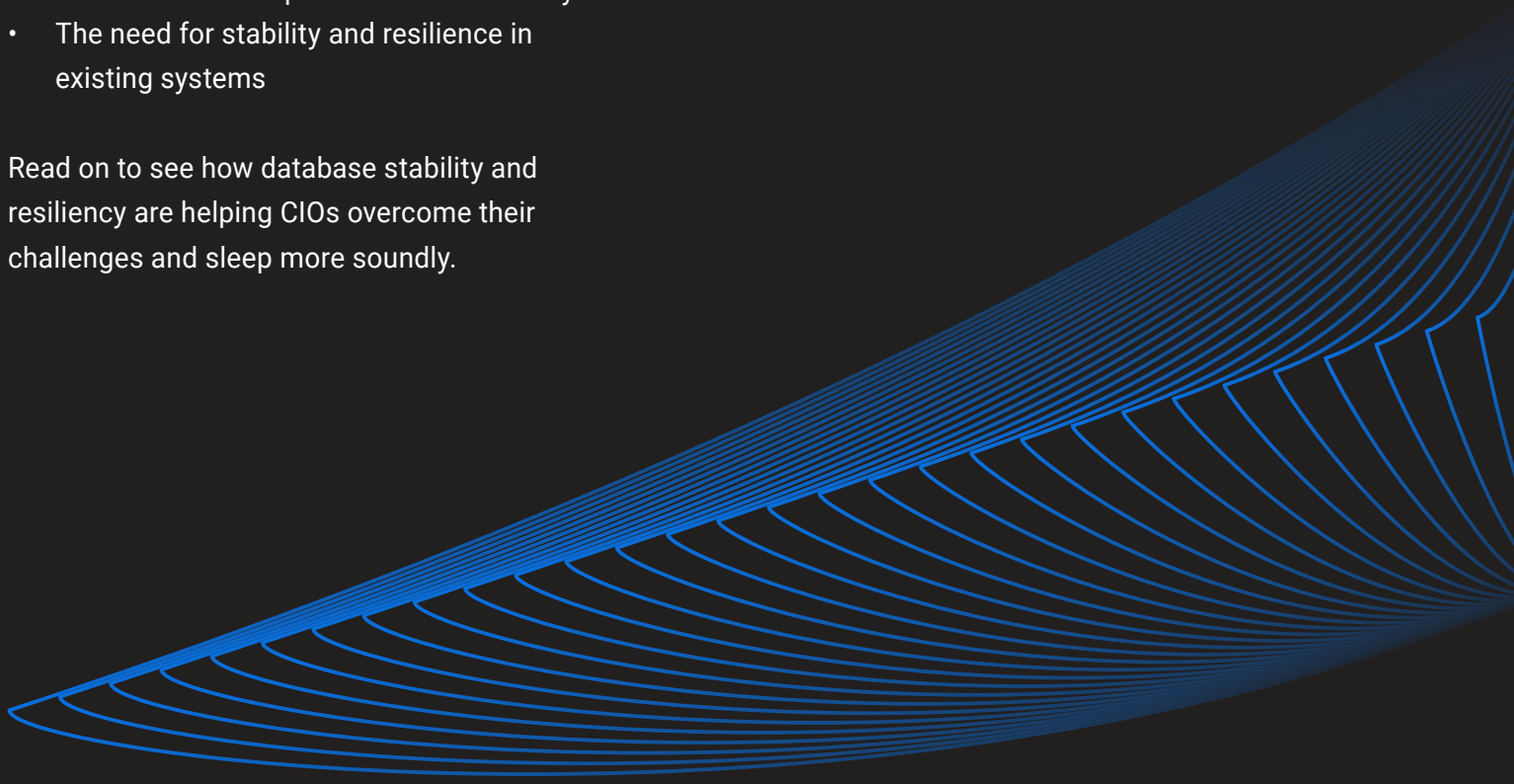
Jerry Hemenway
VP, Global Sales Engineer

POWER TO POSTGRES

In today's rapidly evolving, data-driven world, C-level executives in banking, financial services, and insurance (BFSI) are under tremendous pressure to ensure their database systems are operating as they should be. Some of the issues CIOs face are unique to their companies, but in our work with BFSI organizations, we've found that these 4 major challenges are the ones most likely to keep CIOs awake at night:

- The need for technological innovation and optimized user experience
- The need for performant systems
- The need for data protection and security
- The need for stability and resilience in existing systems

Read on to see how database stability and resiliency are helping CIOs overcome their challenges and sleep more soundly.



CONTENTS

01

03 What is operational resiliency and why is it important?

02

04 Safety and operational resiliency: two sides of the same coin

03

07 3 steps to achieving operational resiliency:

08 Step #1: Enhance data security and protection

08 Step #2 Safeguard against planned and unplanned outages

08 Step #3 Support and maintain database performance and efficiency

04

13 Operational resilience is the key to business sustainability

1. What is operational resiliency and why is it important?

What is operational resiliency and why is it important?

The digital landscape is rapidly changing, and all organizations need to change with it to succeed. Not only are new threats—such as bad actors and malware—evolving on a daily basis, but your users' expectations are constantly growing. With all of the transformative options at their disposal, customers expect you to handle their financial and personal data efficiently, store it securely and provide them with applications, solutions and services that effectively meet their needs.

That's why your business needs to prioritize **operational resiliency** in every single one of your endeavors and initiatives; and the responsibility for this rests on the shoulders of your CIO.

Operational resiliency is defined as the ability to prevent, identify, respond to and overcome adverse circumstances during operation to avoid financial loss and a disruption of business services. Having a strategy for operational resiliency enables you to safeguard against unplanned outages, maintain system health and ensure seamless continuity of operations.

For BFSI firms dealing with sensitive financial data on a daily basis, operational resiliency is non negotiable.

2. Safety and operational resiliency: two sides of the same coin

Safety and operational resiliency: Two sides of the same coin

Security is always top of mind, as the safety of financial information is critical to individual firms and to the stability of the financial system as a whole. Financial service providers can't risk the reputational damage or loss of revenue that comes with a sustained outage. Yet, operational resiliency is equally important—even though it gets less air time—as it's a de facto expectation today.

Your database is where these two crucial concerns merge.

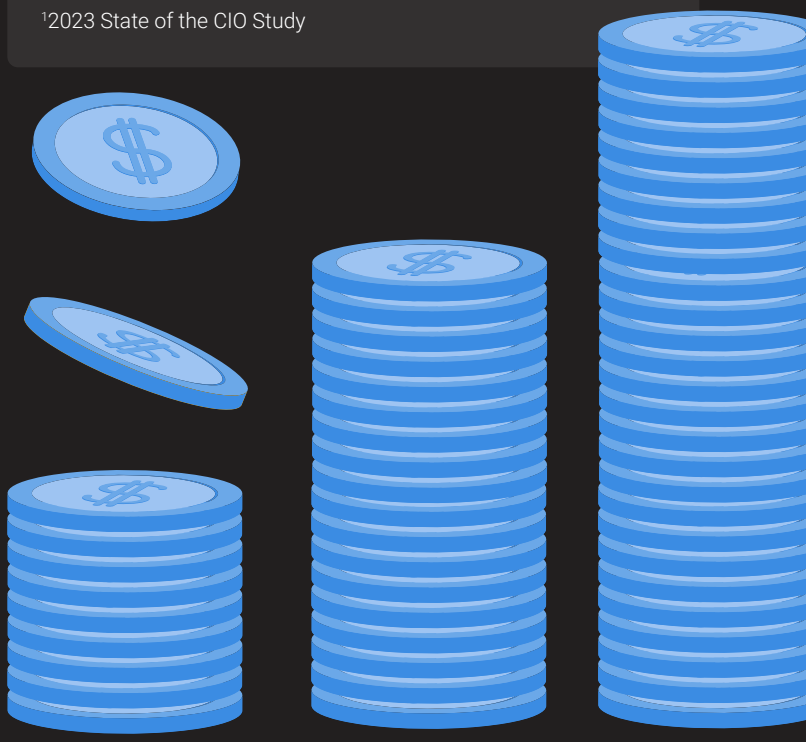
In the last few years, Postgres has established itself as the leading Database Management System (DBMS) for those looking to innovate at a low cost, while adhering to diverse regulatory practices and leveraging their applications and assets to the fullest degree. The extreme high availability solution for Postgres keeps business- and mission-critical applications running and protects against planned and unplanned outages

Read on to learn how to harness the total power of Postgres to ensure you achieve full operational resiliency in **3 steps:**

1. Enhance data security and protection
2. Safeguard against planned and unplanned outages
3. Support and maintain database performance and efficiency

> "Banks have made progress in enhancing operational resilience in recent years, including through their response to the challenges posed by the COVID-19 pandemic… However, more work remains to be done to ensure that banks are resilient to potential operational disruptions from all hazards, including severe but plausible cybersecurity incidents, which could pose risks to the wider financial system."
>
> – Board of Governors of the FInancial Reserve System

> CIOs anticipate their involvement to increase in the following areas: cybersecurity (70%), data analysis (55%), data privacy (55%), AI/machine learning (55%), and customer experience (53%).[1]
>
> [1]2023 State of the CIO Study



3. 3 steps to achieving operational resiliency

3 steps to achieving operational resiliency:

Step #1: Enhance data security and protection

In a world where bad actors are constantly finding new ways to infiltrate the databases of even the most secure organizations—whether they be banks or government agencies—security and data protection is the highest priority.

Not only does your ability to secure your data govern the efficacy of your applications, it determines your reputation with your users. How enterprises manage and share cyber security risks and maintain the highest levels of operational resiliency has been the impetus for a range of new regulations, including the EU's **Digital Operational Resilience Act** (DORA), passed in 2022.

DORA 101

The UK's new Digital Operational Resilience Act (DORA) aims to ensure that the financial sector in Europe is able to stay resilient through a severe operational disruption. This new Regulation requires financial institutions to manage all components of operational resilience and follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. With plans for enforcement starting in 2025, EU financial services firms need to work to ensure their systems are operationally resilient now.

"The suggested transparency and robustness of vendor's risk management processes might be a differentiator for consumers. DORA makes 3rd party providers answerable to the EU, but Protiviti sees vendors with transparent and robust risk management as potentially more favorable to financial services consumers. What standards a vendor may need to uphold are not clear, but there is work ongoing in the UK to build a framework on this."

– Laura Moore, Director, Protiviti UK

"In our modern world of cyber attacks, we're in a war zone."

– Martin Buckley, CIO, Barclays Europe

That's why so many organizations choose Postgres, bolstered and supported by **EDB**. With EDB, businesses have a range of options to build out their database security with break/fix support and **Transparent Data Encryption (TDE)**.

TDE encrypts:

- Files underlying tables, sequences and indexes, including TOAST tables and system catalogs—including all forks. These files are known as data files.
- Write-ahead log (WAL) files
- Temporary files for query processing and database system operation

With TDE you can prevent unauthorized viewing of data in operating system files on the database server and on backup storage. Data becomes unintelligible for unauthorized users if it's stolen or misplaced, which is critical when it's highly sensitive financial data.

Data encryption and decryption are managed by the database and do not require application changes or updated client drivers.

EDB Postgres Advanced Server and EDB Postgres Extended Server provide SQL injection protection, data redaction, enhanced auditing and enhanced RBAC granularity with VPD in EPAS.

3 steps to achieving operational resiliency:

Step #2: Safeguard against planned and unplanned outages

For a number of years, Postgres has offered some resiliency in the event of failures, but over the last five years, the definition of High Availability (HA) has changed. HA used to refer to technology protecting users from hardware failures, network glitches, and software faults. Today, HA technology makes sure that software services are always on—365 days a year, 24 hours a day. HA products still protect users from failures, but as hardware, networks, power supplies, and storage devices have become much more reliable, near-zero downtime maintenance and management have moved to the forefront of the HA debate. Near-zero downtime, or "Always On," has become a must-have for successful digital transformation in a global economy.

Planned vs unplanned downtime: Are you ready for both?

Downtime can occur because of a planned database migration, major version upgrade or database maintenance operations. And it can also occur unexpectedly, due to a lack of database maintenance, configuration changes that require a restart, or a cyber attack. Either way, the end result is the same. Critical and non critical data isn't available, which can seriously impact BFSI processes and customers.

Seeing these sea changes, EDB wanted to take HA to the next level, above and beyond. Why settle for high availability when you can have **extreme high availability**.

We define extreme high availability as five 9's of uptime—i.e. your database is online 99.999% of the time. As we've discussed in previous blogs, this amounts to less than five and a half minutes of downtime a year. Put another way, that is just 864 milliseconds a day.

That's the promise of EDB Postgres Distributed (PGD). With its "Always On" architecture, PGD is the industry leading solution for Postgres high availability. EDB Postgres Distributed's "Always On" architecture enables customers for the first time to use Postgres for 99.999% EHA availability solutions—a domain that was traditionally reserved for a few select commercial database products.

> Operational resiliency is paramount for businesses today—especially those in banking and financial services. Downtime and data loss can lead to significant business disruption, and enterprises simply cannot afford that. EDB Postgres Distributed delivers extreme high availability to minimize downtime so customers can always access their data and applications –even through major version upgrades and during maintenance operations."
>
> – Marc Linster, Chief Technology Officer, EDB

3 steps to achieving operational resiliency:

Step #3: Support and maintain database performance and efficiency

The final component of true operational resiliency is the agility of your database. In highly regulated industries like financial services, you need expert 24/7 support with defined SLOs. Community and user group support can be helpful, but doesn't come with Production Tier 1 and Tier 2 application level Support response times.

EDB is proud to provide independent technical support services and operational staff augmentation designed to help businesses of all sizes fill the gaps in their support infrastructure and embark on a new journey with reduced risk, lower costs and a focus on what matters most to their business.

Offerings like EDB's **Remote DBA Service** (RDBA) helps businesses of all sizes complete or expand their support team when expert, certified Postgres DBAs can't be found or are too expensive to afford. Plus RDBA provides 24/7 monitoring of your systems so issues can be resolved before problems actually occur. **Technical Support** like **EDB Community 360** offers 24/7 Follow-the-Sun for Severity-1 and 2 issues, with response times as quick as 15 minutes for critical issues. Leveraging Postgres experts is a much more efficient and cost-effective approach than self-support to get the Postgres expertise and coverage you need while enabling the reallocation of current resources to more strategic projects.

In addition to these robust support options, EDB offers **Postgres Enterprise Manager (PEM)**, a browser-based console that combines managing, monitoring, and tuning Postgres clusters. PEM provides you with all the tools you need to expand, scale and optimize your Postgres database, ensuring that–no matter your data volume or operational needs–the DBMS that both you and your users rely on is up, is fast, is working to your standards.

4. Operational resilience is the key to business sustainability

Operational resiliency is the key to business sustainability

Operational resiliency and extreme high availability is business-critical to highly transactional databases. It ensures that your users can access what they need when they need it, and that you can leverage your data as efficiently as possible. And it's important for staying compliant with BFSI regulations for protecting customer data.

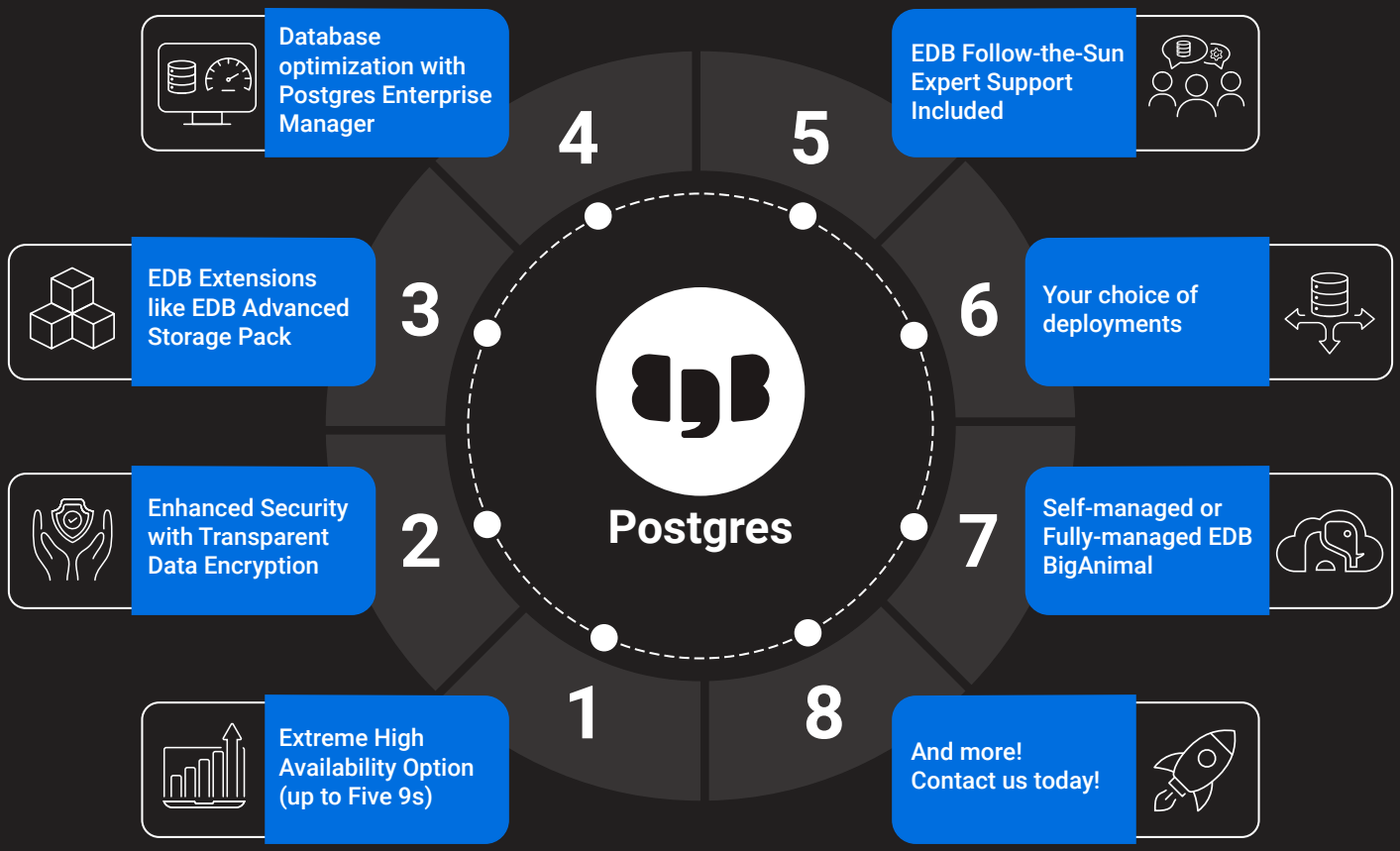
Throughout these pages, you've seen the many ways in which Postgres facilitates the fundamentals of operational resiliency, as well as the ways in which EDB builds upon Postgres' remarkable capabilities to create an even more flexible, agile and secure DBMS experience.

This is why we created the **EDB Standard Plan**. The Standard plan offers open source Postgres with enterprise-grade tools to strengthen and extend PostgreSQL security, resilience and reliability. CIOs can feel confident that their database is optimized for growth and minimizing disruption.They can assure their CEO that their DBMS can operate at scale and ensure high availability.

But the benefits don't stop there. With the EDB Standard Plan, you get the best of the open source Postgres community and the best of EDB innovation. Your organization can leverage the power of open source Postgres, open source tools and the community knowledge base while getting EDB-enhanced enterprise tools, extensions, and expert support. In fact, you get everything we discussed in this eBook, with:

- **Extreme high availability (up to Five 9s) with EDB Postgres Distributed**
- **EDB 24/7 Follow-the-Sun expert support**
- **Enhanced security with Transparent Data Encryption (TDE)**
- **Self-managed Postgres with your choice of deployment or fully-managed in the cloud with EDB BigAnimal**
- **EDB extensions like EDB Advanced Storage Pack**
- **Integration with various cloud architectures and configurations**
- **A comprehensive database design and tuning system with Postgres Enterprise Manager (PEM)**
- **Auto tune and storage packs with EDB Extensions**

EDB Standard Plan



EDB offers a spectrum of options to implement and maintain operational resiliency, and we're here to help you find the right solution for your needs.

For CIOs looking to ensure the longevity of their business and user-base, operational resiliency must be top of mind. And, the best way to ensure that is with a database and a database partner that understands the value of innovation, security, high availability and ongoing growth.

That's why BFSI leaders choose Postgres and EDB.

Learn how the EDB Standard Plan helps BFSI organizations like yours achieve operational resiliency.

About EDB

EDB provides enterprise-class software and services that enable businesses and governments to harness the full power of Postgres, the world's leading open source database. With offices worldwide, EDB serves more than 1,500 customers, including leading financial services, government, media and communications and information technology organizations. As one of the leading contributors to the vibrant and fast-growing Postgres community, EDB is committed to driving technology innovation. With deep database expertise, EDB ensures extreme high availability, reliability, security, 24x7 global support and advanced professional services, both on premises and in the cloud. This empowers enterprises to control risk, manage costs and scale efficiently. For more information, visit **www.enterprisedb.com.**

The CIO's Guide to Operational Resiliency in Financial Services: 3-Step Approach to Strengthen Your Database

Updated on August 23, 2023
EnterpriseDB Corporation
34 Crosby Drive
Suite 201
Bedford, MA 01730

POWER TO POSTGRES