Site reliability engineering – driving digital transformation in BFSI

December 2025

Contents

Foreword

Digital transformation is reshaping industries worldwide, and the banking, financial services and insurance (BFSI) sector is also significantly impacted by this evolution. Rapid advancements in digital platforms, shifting customer expectations and a growing reliance on technology are changing the BFSI sector's operations significantly despite the challenges posed by legacy systems and regulatory constraints. As financial institutions (FIs) strive to meet the demands of this digital era, ensuring the robustness, reliability and scalability of their systems has become a priority.

In such a scenario, site reliability engineering (SRE) emerges as a strategic framework that integrates software development with IT operations to enhance system reliability and performance. Its relevance in the financial services landscape lies in its ability to address key challenges—from maintaining high system uptime and scalability to balancing innovation with operational stability. In a sector governed by stringent regulatory and security standards, SRE practices can complement broader compliance strategies by embedding reliability and observability into the development lifecycle, thereby helping mitigate risks and reinforce customer trust.

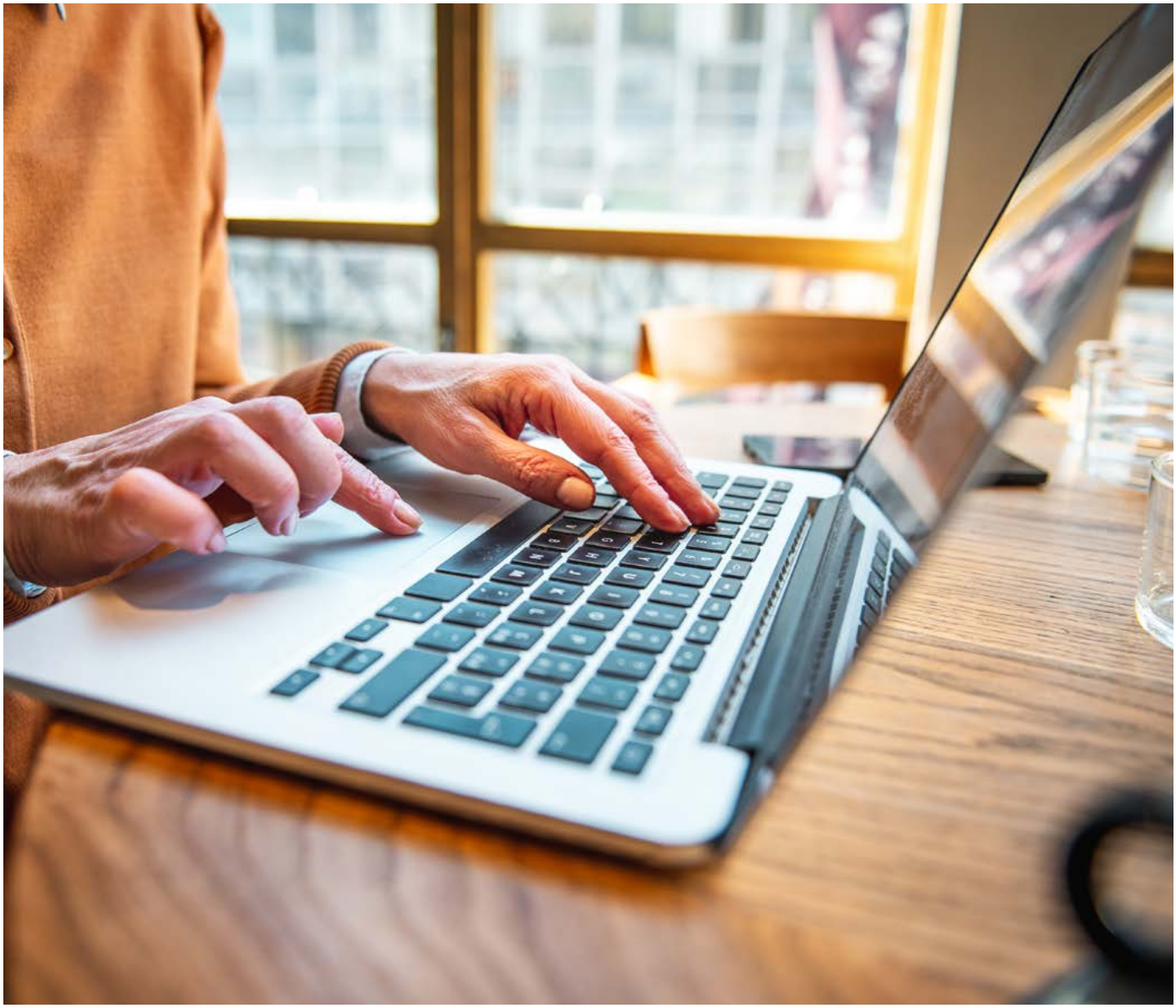
This paper explores the strategic role of SRE in the BFSI sector, highlighting how its adoption enhances operational resilience and positions FIs for sustained success. By embracing SRE, financial services organisations can achieve the dual goals of operational excellence and digital agility, equipping themselves to meet current demands while proactively preparing for future challenges.

01

Introduction

SRE is a discipline that merges software engineering principles with IT operations to address the challenges of building and maintaining scalable, reliable and secure systems. In the BFSI sector, where uptime, performance and trust are non-negotiable, SRE plays a critical role in ensuring system resilience and operational continuity. By applying engineering rigor to infrastructure and service management, SRE empowers FIs to meet evolving customer expectations while maintaining compliance and stability in an increasingly digital environment.

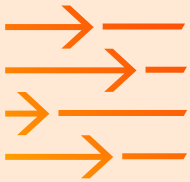
The intersection of finance and technology demands a robust and resilient infrastructure. SRE goes beyond traditional IT operations by applying software engineering principles to manage complex, high-volume systems. In the BFSI sector, where millions of transactions occur in real time and data sensitivity is paramount, SRE plays a critical role in ensuring performance, security and reliability. It emphasises automation, proactive monitoring and rapid incident resolution, enabling financial institutions to deliver seamless customer experiences while maintaining system integrity and compliance.



The four pillars of SRE

SRE plays a pivotal role in enhancing user experience which is an essential driver for the success of digital transformation initiatives in BFSI.

Figure 1: Four pillars of SRE

Scalability	Performance	High availability	Reliability
			
SRE focuses on designing systems that can scale effortlessly to meet growing demands. By forecasting capacity needs and optimising resource allocation and integrating service level indicators (SLI) organisations can ensure smooth operations even during peak traffic. Scalable infrastructure or platform can be achieved by vertical or horizontal scaling of system resources, serverless computing or microservice patterns using container architecture.	SRE teams collaborate with software developers, embed performance engineering in the development cycle, and use monitoring tools to optimise **application performance**, improve response times, and **minimise latency**. This ensures a smooth and seamless user experience, leading to higher retention rates and improved customer satisfaction.	By establishing **robust incident response** processes and ensuring disaster recovery plans including fail over strategies, SRE practices help organisations **minimise downtime**. Fast response times and efficient recovery mechanisms limit the impact of failures, reducing revenue loss and brand damage.	Reliable digital experiences powered by SRE translate into higher customer satisfaction and retention. With defined error budgets which balance innovation with stability and deep monitoring resulting in minimum downtime, customers can rely on seamless access to your digital **services by monitoring, measurement and incident response** and management.

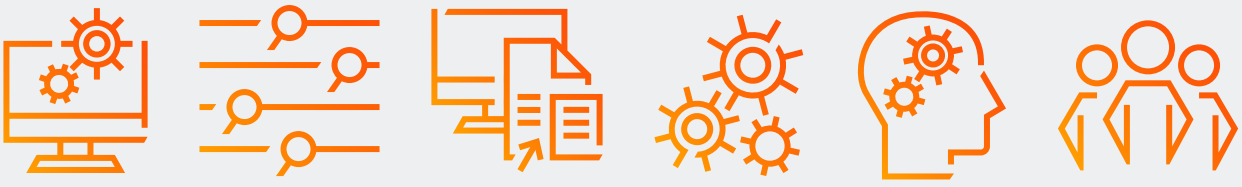
Developing the mindset for digital transformation with SRE

SRE represents a strategic mindset which focuses on collaboration, automation, and reliability. By adopting SRE principles, organisations can modernise their digital infrastructure, reduce operational risk, and deliver consistently high-performing services.

This transformation unlocks new levels of agility, scalability, and customer trust—key drivers of success in today's digital economy.

Collaboration	Automation	Reliability

The effectiveness of SRE implementation is closely tied to leveraging emerging technologies that drive automation, streamline operations, and enhance system visibility. By adopting modern tools for configuration management, collaboration, and observability, businesses can build resilient digital platforms that support innovation, reduce risk, and deliver consistent value to customers and partners.



Why SRE matters in BFSI

In BFSI, where reliability and scale are non-negotiables, SRE offers a disciplined approach to managing complex systems with engineering precision.

- **Reliability:** In BFSI, system downtime not only results in financial losses but also erodes customer trust. SRE introduces engineering practices such as monitoring, automation and proactive incident response to keep critical services available and performant even under extreme conditions.

- **Bridging development and operations:** Embeds software engineering in operations, facilitating seamless collaboration between Dev and Ops. This is vital for managing complex BFSI architectures that include payment gateways, core banking systems and risk management platforms.

- **Handling scale and complexity:** BFSI platforms must process millions of secure transactions daily. SRE principles like auto-scaling, capacity planning and orchestration tools allow these platforms to manage fluctuating workloads without sacrificing reliability.

Core benefits of SRE for BFSI

By embedding reliability into the fabric of operations, SRE delivers tangible advantages that align with the strategic priorities of FIs.

- **Enhanced resilience:** Practices like redundancy, fault tolerance and disaster recovery enable banks to minimise service disruptions and meet regulatory uptime requirements.

- **Operational efficiency:** Automation reduces manual intervention, lowers operational costs and increases consistency especially in repetitive or complex deployment scenarios.

- **Regulatory compliance:** SRE frameworks now include controls and separation of duties tailored to BFSI regulations, helping banks stay compliant while delivering innovation. Audit trails, immutable logs and clear SLOs make risk management and reporting easier.

02

Adoption trends of SRE in BFSI

The adoption of SRE in BFSI is increasingly being shaped by the industry's broader digital transformation agenda. As BFSI organisations modernise their operations through mobile banking, digital payments and FinTech integrations, the need for resilient, scalable and secure systems becomes paramount. The factors and trends which underscore the strategic importance of SRE are:

1. **Customer expectations:** Customers today expect seamless, always-on digital services. Any downtime or service disruptions can lead to significant dissatisfaction and reputational damage. SRE practices such as proactive monitoring, incident response and error budgeting help to ensure high availability and reliability of services.

2. **Regulatory compliance and agility:** The BFSI sector is subject to strict compliance requirements for data security, privacy and operational resilience. SRE can aid in meeting these standards by integrating best security practices into the software development lifecycle and enabling faster, more reliable deployments, thereby improving agility. This allows organisations to respond quickly to market demands and competitive pressures.

3. **Data-driven decision-making:** By making data accessible and actionable, SRE fosters a culture of informed decision-making enabling organisations to optimise their operations, improve system reliability and align service level objectives (SLOs) and service level indicators (SLIs) with business goals. This can enable banks to create a system boundary while trying to modernise legacy applications or increase the number of releases.

4. **Cost optimisation:** SRE focuses on automating manual tasks and improving operational efficiency, leading to cost savings. This is particularly important for BFSI institutions that are often constrained by tight IT budgets.

5. **Innovation:** SRE fosters a culture of experimentation and continuous improvement, enabling BFSI organisations to innovate and adapt quickly to the evolving technological landscape.

6. **Tools and technologies:** The implementation of SRE in FinTech firms often involves using monitoring tools like Prometheus, Grafana, Dynatrace, and Datadog, and infrastructure-as-code solutions like Terraform, Azure ARM, chef, AWS CloudFormation and containerisation platforms like Kubernetes, AKS (Azure Kubernetes Service), EKS (Elastic Kubernetes Service), GKE (Google Kubernetes Engine). These tools enhance system monitoring, consistency and scalability.

7. **Key strategies:** Successful SRE implementation in finance adopting a DevOps culture, implementing fault tolerance and redundancy, ensuring load balancing and scalability, and proactive monitoring. It also requires rigorous testing and disaster recovery planning to ensure business continuity.

Adoption challenges

- **Legacy systems and integration:** Outdated core systems are common and may resist full automation or orchestration, requiring hybrid strategies to mix old and modern technologies.

- **Cybersecurity and data privacy:** Managing sensitive financial data elevates the need for stringent security practices, automated vulnerability testing and compliance with data privacy act.

- **Regulatory constraints:** Stringent regulations demand segregation of responsibilities, limiting 'you build it, you run it' models and mandating meticulous documentation and controls to avoid systemic risks.

- **Cultural shifts:** The transition to SRE requires mindset changes across the organisation which helps them embrace automation.

Left shift approach—reliability by design

It is essential to prioritise reliability from the very beginning of the design and development process. Doing so ensures that best practices, guiding principles and effective tools are thoughtfully integrated from the outset. In the BFSI sector, the following principles, applied across various layers, help build an ecosystem which is inherently dependable, secure and resilient by design.

Core systems

- **Design for high availability:** Using redundant servers, failover mechanisms and distributed architectures to ensure that core banking systems are always available—even during maintenance or outages.

- **Disaster recovery planning:** Implementing with real-time data replication strategy and geographically separated backup sites to recover quickly from disasters.

Digital channels (mobile and web apps)

- **Load balancing and scalability:** Well architected frameworks are followed to manage peak loads (e.g. during salary credit days or IPO launches) without crashing.

- **Secure authentication:** Multi-factor authentication (MFA), biometric login and tokenisation are built into the design to prevent unauthorised access.

Payment systems, unified payment interface (UPI), national electronic fund transfer (NEFT), real-time gross settlement (RTGS))

- **Transaction integrity:** Systems are designed to ensure atomicity where either a transaction completes fully or not at all, avoiding partial failures.

- **Real-time monitoring:** Continuous monitoring and alerting systems are embedded to detect and respond to anomalies instantly.

Middleware or API management platform

- **Robust contract:** Coordination between upstream and downstream solutions are bound by well-defined contracts.

- **Maintenance:** Proper monitoring of transaction per second (TPS), logging of transactions, error rate and quick detection of errors leveraging the codes mapped at both ends.

Fraud detection systems

- **AI/ML integration:** Algorithms are designed to learn and adapt to new fraud patterns, improving detection accuracy over time.

- **Behavioural analytics:** Systems are built to analyse user behaviour and flag deviations that may indicate fraud.

Regulatory compliance systems

- **Automated reporting:** Compliance systems are designed to automatically generate reports for regulators (e.g. RBI, SEBI, IRDA) with minimal manual intervention.

- **Audit trails:** Every action is logged and traceable, ensuring accountability and transparency.

Customer support systems

- **Omnichannel reliability:** Chatbots, IVR and live support systems are designed to work seamlessly across platforms (mobile, web, phone, etc.).

- **Fallback mechanisms:** If one channel fails, customers are automatically routed to another available support option.

03

Emerging practices in SRE

While traditional design principles still serve as a foundation for architects and SRE professionals, the shift to cloud-native environments introduces new complexities, and new opportunities.

Ensuring system reliability, high availability, scalability and performance in these dynamic ecosystems requires more than just conventional approaches. Fortunately, the rise of emerging technologies, coupled with increasingly advanced skillsets, is equipping SRE teams to meet these challenges head-on. From automated observability to intelligent incident response, modern tools are reshaping how reliability is built and maintained in today's digital infrastructure.

Table 1: Emerging technologies and site reliability

Emerging technologies	Relevance with site reliability
Serverless computing	SRE teams are finding new ways to manage serverless systems, which don't rely on traditional servers and change quickly. They're focusing more on tracking performance and fixing issues using tools for measuring, logging and tracing. Since serverless systems work differently, older methods of monitoring and troubleshooting aren't as effective and need to be updated. Key considerations for serverless SRE include: • implementing **distributed tracing** across function invocations. • optimising cold start times • managing **concurrency** and **scalability** • ensure **high availability**.
Container orchestration platforms	As containerisation platforms become the standard for container orchestration, SRE adapts to manage and scale clusters with greater efficiency. This includes developing expertise in: • Cluster **autoscaling** • Service mesh implementation • **Native monitoring** and logging solutions.
Observability, tracing and monitoring	Recent advancements in observability are unlocking deeper, real-time visibility into system behaviour, empowering SREs to detect and resolve issues faster across increasingly complex and distributed environments. With richer telemetry data and more intelligent tooling, teams can now trace problems across services, pinpoint root causes and maintain reliability at scale more effectively than ever before.
Log analytics	Modern log analysis is being transformed by powerful search and correlation capabilities, allowing teams to troubleshoot issues faster and optimise systems more effectively. Today's log analytics platforms offer features such as real-time indexing and searching along with automated correlation of logs with metrics and traces.

Emerging technologies	Relevance with site reliability
Distributed tracing	Distributed tracing has become an essential tool for enhancing visibility in modern, distributed systems. By mapping the journey of requests across multiple services, it enables SREs to pinpoint performance bottlenecks and gain a clearer understanding of system interactions, making troubleshooting faster and more precise. Key benefits include: • end-to-end visibility of request lifecycles • **latency analysis** across service boundaries • **correlation of traces** with logs and metrics for comprehensive debugging.
Performance enhancement	**Application performance** is an important success factor in SRE. Unlike performance engineering, SRE is not only responsible for RCA and event correlations at the time of delivery but also for tuning, patching and fixing issues of application and platform in production. This includes expertise in the following: • in memory caching • database indexing • asynchronous event driven process implementation.
Chaos engineering	Chaos engineering enables organisations to proactively test system limits, uncover hidden flaws and strengthen reliability before failures occur. Automating chaos experiments increase efficiency and repeatability, allowing for more frequent and comprehensive testing. This approach, known as 'chaos engineering as code', involves: • defining experiments in version-controlled configuration files • integrating **chaos experiments into continuous integration and deployment** pipelines
Infrastructure automation	Infrastructure as Code (IaC) is rapidly advancing to support the growing complexity of modern infrastructure. By using declarative configuration files, SRE teams can define and manage infrastructure in a consistent, repeatable way, treating provisioning and operations as part of the software development lifecycle. This approach reduces manual errors, improves reliability, and accelerates deployment workflows. Key benefits of IaC in SRE include: • **Version control:** Infrastructure configurations can be version-controlled, allowing for easy rollbacks and changing tracking. • **Reproducibility:** Environments are easily replicated across non prod and production environments. • **Scalability:** Infrastructure can be scaled up or down programmatically based on demand. • **Compliance and security:** Security policies and compliance requirements can be codified and consistently applied.

Emerging technologies	Relevance with site reliability
Synthetic monitoring	SRE teams are designing more sophisticated synthetic monitoring tests that closely mimic real user interactions. These proactive tests help uncover issues from the user's perspective before they impact actual experience, making monitoring more realistic and effective. This approach involves: • simulating user interactions with the system • testing from **multiple geographic locations**.
Adoption of GitOps for configuration management	By embracing GitOps principles for declarative configuration and deployment, SRE workflows are becoming more efficient. GitOps leverages Git repositories as the sole source of truth, extending Git-based practices to manage both infrastructure and application deployments in a consistent and automated manner. Key aspects of GitOps in SRE include: • **Declarative configurations:** System configurations are defined in a declarative manner and version-controlled in Git repositories. • **Version control:** Changes to infrastructure and applications are tracked through Git commits. • **Automated synchronisation:** Tools automatically synchronise the desired state in Git with the actual state in the production environment. • **Pull-based deployment:** Changes are pulled from Git repositories rather than pushed to the environment, improving security and control.
AI-driven task automation for incident response, anomaly detection, capacity planning and self-healing	Robust automation platforms are being built to support complete SRE workflows from monitoring and alerting to incident management. These platforms aim to unify diverse SRE functions into a seamless, automated ecosystem, minimising manual effort and enhancing system reliability. Key features of modern SRE automation platforms include: • **Automated incident response:** Triggering predefined runbooks or playbooks in response to detected issues. • **Self-healing systems:** Automated remediation of common issues without human intervention. • **Capacity planning:** AI-driven forecasting and automated scaling of resources
Cloud native security	Security is being more deeply embedded into the SRE lifecycle, with specialised tools for vulnerability scanning, threat detection, and incident response designed for cloud-native environments. The move to DevSecOps integrates security into every stage of development and operations, ensuring risks are addressed early and continuously. Key areas of focus include: • Runtime application self-protection (RASP) • Container image scanning • Network policy enforcement. • Secrets management.

Core metrices of SRE

1. **Service-level objectives (SLOs):** Specific and quantifiable goals that the software can achieve at a reasonable cost to other application health metrics, e.g. application up time should be 99.95%.

2. **Service-level indicators (SLIs):** The actual measurements of the metric. This value will be different from SLO. Application is up and running 99.92% of the time, which is lower than the SLO. SLI can be captured by four fundamental or golden signals of application or health services.

   Resource saturation: CPU, memory, storage, network bandwidth – the fraction of resources that are utilised vs. available. Whether those have sufficient capacity to manage the traffic and load.

   Traffic: Growth trends of users, abnormal fluctuation of traffic, be it exceptionally high or remarkably low, can signal underlying issues

   Error: Service outage, system unavailable, Http 4xx, 5xx errors

   Latency: Service or application response time

3. **Error budgets:** As an example, the non-compliance tolerance for the SLO, an uptime of 99.95% in the SLO means that the allowed downtime is 0.05%.

4. **Service level agreements (SLAs):** Formal contracts that define the consequences when one or more SLOs are not achieved.

Note: If the **delta between SLO and SLI is too high**, an organisation cannot make any statement about the reliability of a service. The requirements for costs and development speed of the service can then also be derived from the SLO. Excessive system availability generates unnecessary costs and effort. Too low availability will result in not achieving the business goals.

04

Setting up site reliability CoE

Our proposed maturity assessment model can help organisations adopt SRE through a comprehensive 360-degree build-operate-run approach. This suggested model is anchored in key principles such as maturity dimensions, empathy, psychological safety, embracing failure and fostering cross-functional collaboration.

Establishing an SRE CoE requires strong change management and a focus on cultural and operational transformation. Core enablers in this process are:

- **Service ownership:** Developers take full responsibility for system performance and reliability.
- **Automation:** Streamlines operations and frees teams for strategic work.
- **Data-driven decisions:** Metrics guide architecture, resource use, and incident response.
- **Psychological safety:** Open communication fosters innovation and continuous improvement.

Conducting a maturity assessment is the first step in establishing an SRE CoE. The assessment model follows a standardised methodology, leveraging a structured questionnaire and scoring system that feeds into a maturity radar chart for quick and intuitive visualisation.

Maturity assessment model for site reliability is based on a common methodology driven by a questionnaire and scoring pattern that maps to a maturity radar chart for quick visualisation

SRE assessment playbook

SRE assessment playbook is a compliance check of reference parameters associated with a scorecard that gets updated in real time about the readiness of fantastic four of system design i.e. availability, resilience, performance and scalability

Why playbook?

Maturity parameters

- Scalability
- Performance
- Availability
- Resilience
- Observability
- Incident management
- Infrastructure
- Toil reduction
- SLO/SLI
- Deployment
- Culture
- Tech modernisation
- Capacity planning

Playbook sample

Playbook for SRE maturity assessment

As-is score = Bronze 200
Target score = Platinum 350

Bronze level (Score = 200)

Basic level of uptime monitoring dashboard
+No defined SLI, SLO, SLA and Error budgets
+Manual deployment + No DevOps research and assessment (DORA)metrics

Silver level (Score = 250)

SLIs provide measurable insight on SLO
+ Toils to be automated
+ CI/CD pipeline introduced
+ no single point of failure

Gold level (Score = 320)

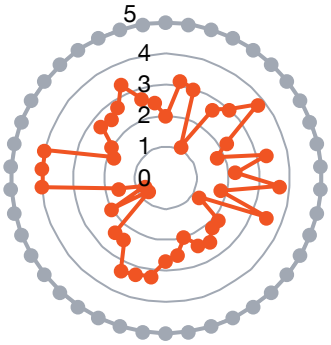
DORA captured
+ Forecasting future usage
+ infra auto scales horizontally

Blameless post-mortem of incidents
+ data driven decision can be taken easily
+ High infra-automation rate
+360-degree observability

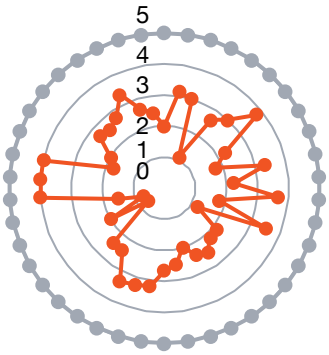
Platinum level Score = 350 (Final stage)

Chaos engineering introduced
+ Max burn rate and time to error budget exhaustion is calculated
+ Reduced time to market
+ Managed SLO

Cumulative score and as-is state mapping



GAP analysis



Target state mapping

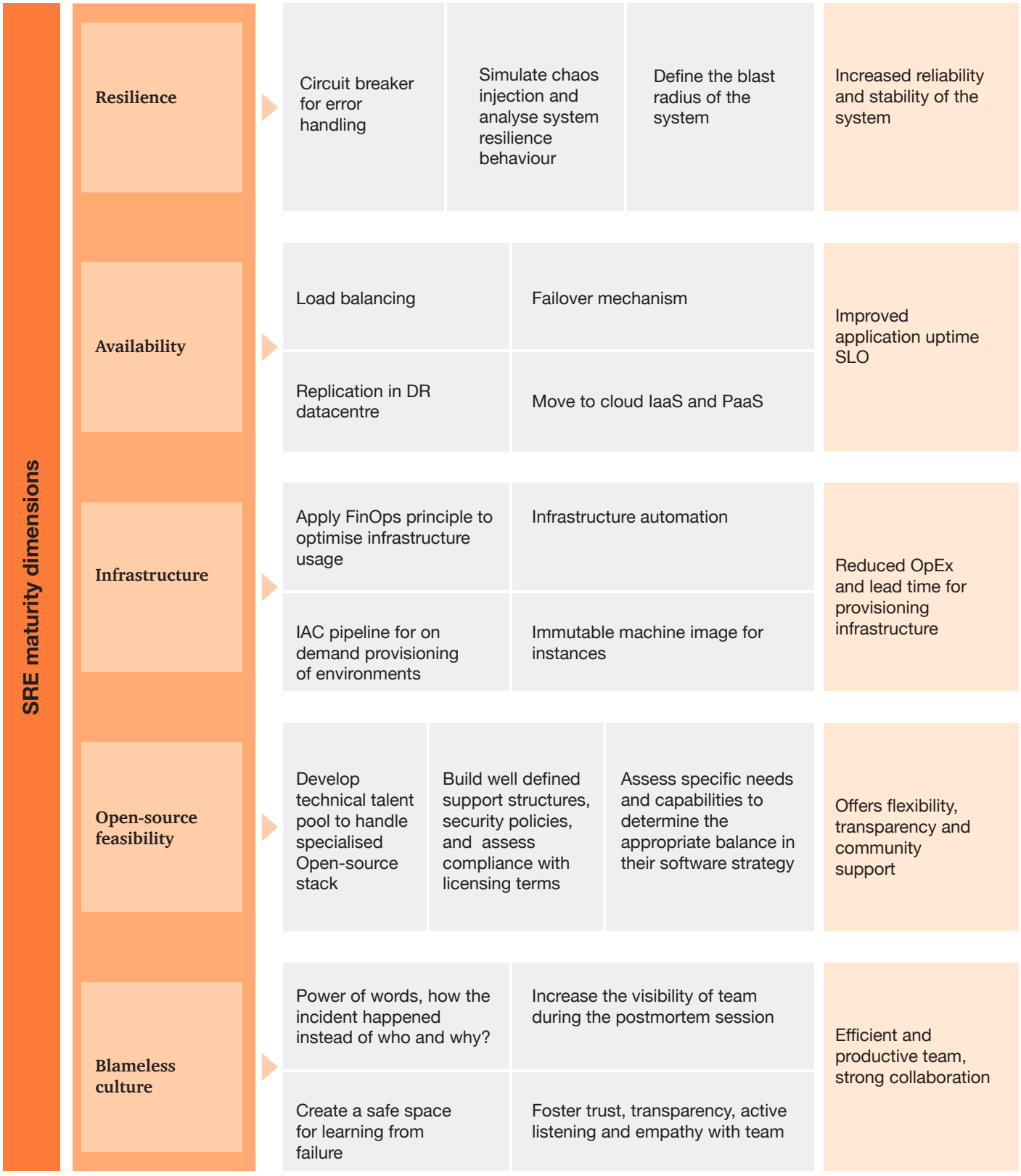
SRE adoption roadmap

Once the 'to be' state is designed the focus shifts to corresponding dimensions and the required tasks to achieve the state envisioned.

Tasks which are required for each dimensions in the journey of reaching the desired state

SRE maturity dimensions

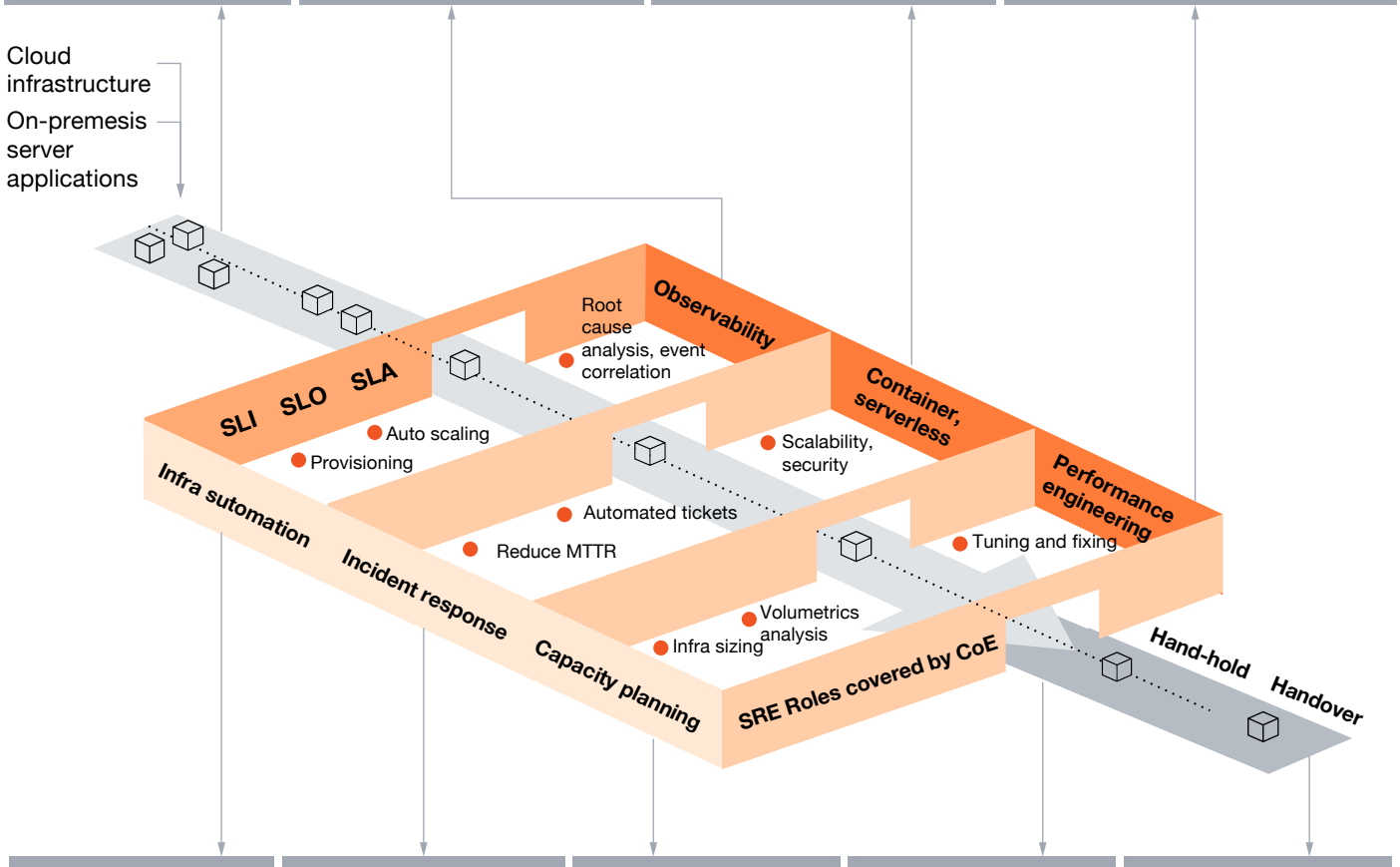
Technology modernisation	Microservices deployment App image Container registry HA Kubernetes cluster	Multi cloud architecture	 Serverless VM VM	Cost optimisation, TCO reduction, speed up in innovation
Observability	360-degree view dashboard of system	Proactive insight and detection	Faster detection, RCA and resolution	Full visibility into Ops, faster remediation and save revenue
	Supervised machine learning for pattern detection and predictive analysis	Distributed tracing and open telemetry		
SLI/SLO/error budget	Balance error budgets between reliability and innovation	Data driven decision is being taken	Calculate current burn rate, max burn rate and time to error budget exhaustion	Happy customer base, room for innovation
MTTX and toil reduction	Develop step-by-step instructions for handling alarms with efficient monitoring and alerting system	Automate simple resolutions for recurring issues with known fixes for speedy recovery		Prevent possible downtime, reduced manual effort
	Invest in redundancy and back up system	AIOps for anomaly self healing		
Deployment	Automated artifact repository management	Continuous integration, build and deployment pipeline as code)		Faster time to market, change failure rate Increased deployment frequency
	Automated defects tracking	Automated build and deployment process to push the fix		


SRE maturity dimensions
Resilience
Circuit breaker for error handling
Simulate chaos injection and analyse system resilience behaviour
Define the blast radius of the system
Increased reliability and stability of the system
Availability
Load balancing
Failover mechanism
Replication in DR datacentre
Move to cloud IaaS and PaaS
Improved application uptime SLO
Infrastructure
Apply FinOps principle to optimise infrastructure usage
Infrastructure automation
IAC pipeline for on demand provisioning of environments
Immutable machine image for instances
Reduced OpEx and lead time for provisioning infrastructure
Open-source feasibility
Develop technical talent pool to handle specialised Open-source stack
Build well defined support structures, security policies, and assess compliance with licensing terms
Assess specific needs and capabilities to determine the appropriate balance in their software strategy
Offers flexibility, transparency and community support
Blameless culture
Power of words, how the incident happened instead of who and why?
Increase the visibility of team during the postmortem session
Create a safe space for learning from failure
Foster trust, transparency, active listening and empathy with team
Efficient and productive team, strong collaboration

SRE maturity dimensions					
	Scalability	Vertical scaling	Horizontal scaling		Adheres to increasing business needs
		Automatic scaling of applications	Microservices architecture		
	Performance	Caching	Database indexing	Asynchronous processing of requests	Faster application, less end user attrition
	Incident management	Establish clear incident escalation and notification procedures	Implement effective categorisation and prioritisation methods		Improved customer experience
		Conduct post incident analysis for lesson learning	Utilise IM tools and software for streamlined process		
	Capacity planning	Monitor IT infrastructure continuously and collect resource utilisation data	Assess current infrastructure component and benchmark the current capacity	Forecast future resource demand	Supported strategic business growth and scalability

Once the foundational protocols are established, the workforce is upskilled, roles are clearly defined, and operational processes are designed, the SRE CoE framework—complete with governance and policy structures—will be transitioned to the organisation for sustained ownership and execution.

Determine risk tolerance level	Observability	Serverless	Performance engineering
Understanding of key SRE metrics such as SLO, SLI and error budget and determine system stability to accept new builds or innovation	Observability framework set up for distributed log tracing and metrics analysis to detect abnormal behaviour of the live applications	Serverless architecture and containers enables concurrency and scaling along with distributed tracing	Ensure optimum performance, scalability, resilience, high availability and stability even under high traffic volume by enabling auto scaling, self healing infrastructure and tune the system configuration



Infra automation	Incident response	Capacity planning	Hand-hold and transition	Handover
Streamline infrastructure-as-code (IaC) that uses a declarative configuration language to define and provision infrastructure for cloud and on prem data centres	Establish incident response procedures, including incident detection, escalation, communication and resolution. Post analysis for preventive measure	Plan for future growth and ensure that infrastructure can handle increased traffic volumes Calculate scaling factor based on transaction growth	Create knowledge assets Provide knowledge transfer and training to client Ops team	Provide SRE assets to client teams Successfully transition the framework

Service-level objectives (SLOs) are specific and quantifiable goals that the software can achieve at a reasonable cost to other metrics – uptime, system throughput, system output, application loading time, etc.

Service-level indicators (SLIs) are the actual measurements of the metric. In real-life situations, it might give values that match or differ from the SLO. Application is up and running 99.92% of the time, which is lower than the SLO.

The service-level agreements (SLAs) are legal documents that state what would happen when one or more SLOs are not met.

Error budgets are the noncompliance tolerance for the SLO, an uptime of 99.95% in the SLO means that the allowed downtime is 0.05%

Leveraging the CoE framework could help in addressing challenges such as:

Cultural resistance

- **Detail:** Transitioning to an SRE model often requires a cultural shift towards collaboration, blameless postmortems and shared responsibility between development and operations teams. Resistance to change can hinder adoption.
- **Our approach:** Facilitate cultural transformation by conducting workshops and training sessions that emphasise the benefits of SRE principles. They can also help establish and foster a culture of collaboration, essential for successful SRE implementation.

Skill gaps

- **Detail:** SRE requires a unique blend of skills in software engineering, operations and automation. Organisations may face challenges in finding or developing talent with the necessary expertise.
- **Our approach:** Assist in identifying skill gaps and designing tailored training programmes to upskill existing staff. They can also provide recruitment support to help organisations find qualified SRE professionals.

Tooling and technology integration

- **Detail:** Implementing SRE involves integrating various tools for monitoring, automation, and incident management, which can be complex and resource intensive.
- **Our approach:** Share our expertise in selecting and integrating the right tools and technologies that align with the organisation's goals. They can provide guidance on best practices for tool implementation and configuration.

Defining and measuring SLOs and SLIs

- **Detail:** Though establishing meaningful SLOs and SLIs is crucial for SRE success, it can be challenging to define and measure them accurately.
- **Our approach:** Develop a framework for defining and measuring SLOs and SLIs, ensuring they align with business objectives. They can also assist in setting up monitoring systems to track these metrics effectively.

Cybersecurity and data privacy

- **Detail:** Managing sensitive financial data demands robust security, automated vulnerability testing and strict compliance with data privacy laws (e.g. Digital Personal Data Protection(DPDP) Act). Regulations often require segregation of duties, detailed documentation and strict controls—limiting the 'you build it, you run it' model.
- **Our approach:** Help in enforcing encryption at rest and in transit and applying identity and access management(IAM) policies to restrict access based on region and roles and strategic guidance on involving risk, compliance and legal teams early in the SRE adoption process to ensure alignment with regulatory mandates.

Balancing innovation with reliability

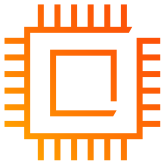
- **Detail:** Organisations may struggle to balance the need for rapid innovation with the requirement for system reliability and stability.
- **Our approach:** Provide strategic guidance on implementing SRE practices that support both innovation and reliability. They can help establish processes for continuous improvement and risk management, ensuring that new features are delivered without compromising system stability.

05

Future trends and opportunities of SRE in BFSI sector

SRE is poised to evolve with emerging trends, opportunities, increased regulatory requirements and evolving customer expectations. As digital transformation continues to reshape the BFSI sector, SRE practices will adapt to meet new challenges and leverage technological advancements. Some future trends and opportunities for SRE in the sector are:

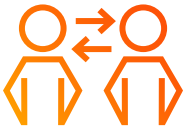
1. AI and machine learning integration: The integration of AI and ML into SRE processes will become increasingly prevalent. These technologies can be used to predict infrastructure failures, automate incident responses and enhance monitoring capabilities. Predictive analytics can help BFSI companies anticipate issues before they impact operations, contributing to more proactive reliability management.



2. Edge computing: As BFSI services extend to more diverse and distributed environments, edge computing will play a crucial role in managing reliability and performance at the network edge, ensuring seamless user experiences regardless of where the service is accessed.

3. Enhanced observability: Advanced observability tools will enable deeper insights into system performance and user behaviour. SRE teams will use these tools to gain real-time visibility into complex, distributed systems, allowing for quicker identification and resolution of issues as BFSI companies embrace multi-cloud strategies.

4. Continuous compliance: Since BFSI sector is heavily regulated, SRE practices will focus on automated compliance checks and reporting, enabling organisations to meet regulatory requirements more efficiently and with fewer errors.



5. Cross-functional teams: The trend towards blurring the lines between development, operations, and security will continue, leading to more cross-functional SRE teams. This will enhance collaboration and innovation, allowing BFSI companies to respond more swiftly to market demands.

6. Focus on customer experience: SRE will play a crucial role in optimising customer experiences by ensuring that digital services are fast, reliable and available. As BFSI institutions focus on digital-first strategies, SRE will help maintain an elevated level of service quality to meet the customers' expectations.

7. Sustainability and green computing: As environmental concerns grow, BFSI companies will increasingly look to SRE to help reduce their carbon footprint by optimising resource usage, reducing data centre energy consumption and leveraging sustainable technologies.

8. Quantum computing: Although still in its initial stages, quantum computing has the potential to revolutionise certain BFSI applications. SRE teams will need to explore how they can ensure reliability and performance in environments that leverage quantum technologies.

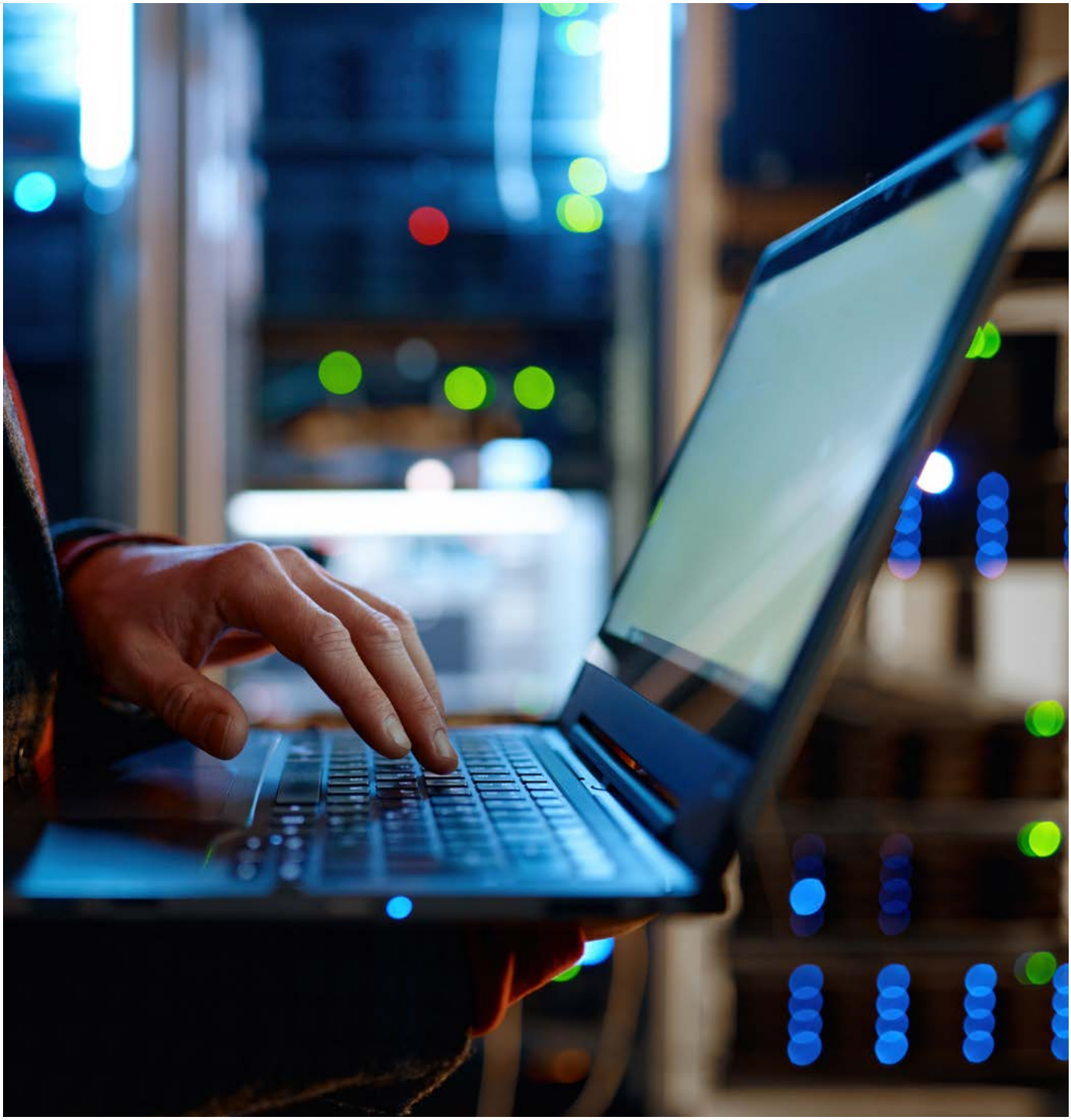
9. Cultural transformation: The shift towards a DevOps and SRE culture will continue to gain momentum, emphasising shared responsibility for system reliability and continuous improvement. This cultural change will be essential for fostering innovation and agility within BFSI organisations.

By embracing these trends, organisations in the BFSI sector can enhance their operational efficiency, security and ability to innovate while maintaining a competitive edge.

06

Way forward

SRE is pivotal in driving digital transformation within the BFSI sector, enabling FIs to build resilient, scalable, and secure systems. By embedding reliability into core operations and aligning teams around shared goals, organisations can accelerate digitisation, improve service quality, and stay ahead in a rapidly evolving landscape.



About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.
Please see www.pwc.com/structure for further details.

Contact us

Vivek Belgavi
Partner, Financial Services Advisory Leader
vivek.belgavi@pwc.com

Sayandeb Mitra
Partner, FS Digital Strategy and Platform Transformation
sayandeb.mitra@pwc.com

Authors:
Bikramjit Pal, Somsubhra Chakraborty, Saumil Shah

Contributors:
Mihir Karoor, Sreyoshi Mukherjee, Sayan Dhara

Editor:
Rubina Malhotra

Design:
Harshpal Singh

pwc.in

HS/December 2025 - M&C 50465