Cyber Resilience in Action

A Practical Guide

Contents

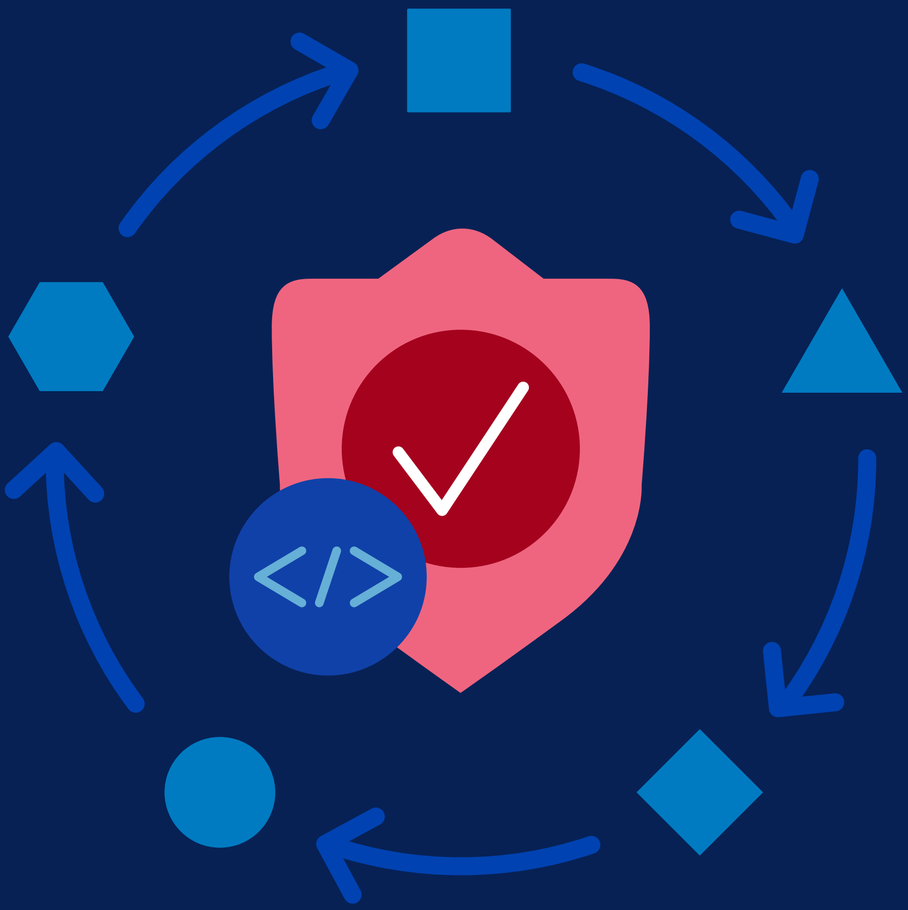
Introduction: 10-Step Playbook to Build Enterprise Cyber Resilience

Security leaders who proactively address evolving cyber threats enhance their organization's resilience and minimize risk exposure. This playbook outlines 10 steps to successfully build and maintain enterprise cyber resilience while optimizing security investments and operational excellence.

Key findings

- Organizations that align cyber resilience with business objectives effectively optimize investments and minimize risks.
- The ability to securely integrate emerging technologies while maintaining operational resilience is challenging for many security leaders.
- CXO support is essential for cyber resilience initiatives, but sufficient preparation and communication are also necessary to avoid missed opportunities.
- Building robust governance frameworks and fostering a security-first culture empowers organizations to successfully respond to and recover from cyber incidents.

Insights drawn from the collective wisdom and real-world experience of 47 industry leaders across three dynamic technology hubs in Asia.



Co-Creation

This playbook represents the collective wisdom and real-world experiences of 37 industry leaders across three dynamic technology hubs in Asia. The insights are drawn from executives representing diverse sectors—from financial services to technology—and roles spanning CISOs, CIOs, and security architects. This multi-regional collaboration brings together distinct perspectives on cyber resilience, enriched by each region's unique challenges and innovative approaches.

Mumbai

These experts focused on aligning cyber resilience with strategic business objectives and integrating global compliance frameworks (ISO 27001, NIST CSF) into enterprise operations. This approach established foundational governance and risk management practices.

Bangalore

Regional thought leaders advocated for innovation and adaptability, highlighting secure integration of emerging technologies. This session introduced advanced practices like self-healing systems, zero trust architecture, and AI-powered predictive threat modeling.

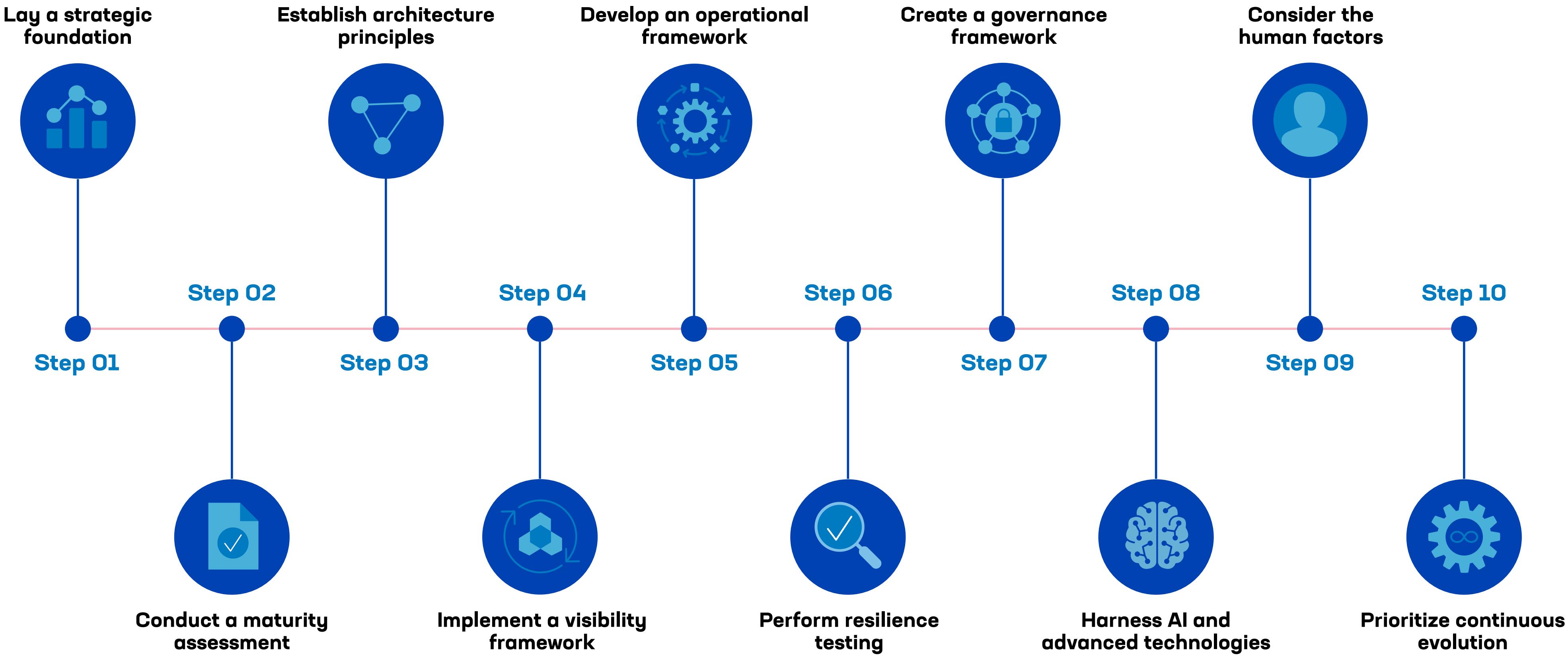
Kuala Lumpur

Participants emphasized operational excellence through proactive threat management and incident response. This roundtable prioritized real-time monitoring, AI-driven analytics, and cloud resilience for minimizing disruptions.

Tokyo

Addressed AI-driven security challenges, emphasizing governance, compliance, and false positives. Discussions highlighted automation, AI validation frameworks, and risk committees as key strategies to strengthen resilience and bridge workforce gaps.

The 10 Steps for Cyber Resilience Success



Step 01
Lay a strategic foundation

Step 02
Conduct a maturity assessment

Step 03
Establish architecture principles

Step 04
Implement a visibility framework

Step 05
Develop an operational framework

Step 06
Perform resilience testing

Step 07
Create a governance framework

Step 08
Harness AI and advanced technologies

Step 09
Consider the human factors

Step 10
Prioritize continuous evolution

Step 01
Strategic Foundation

Objective

Begin your resilience journey by mapping your security landscape to business priorities. This groundwork is essential for success.

Rationale

This foundation ensures security investments are strategic drivers rather than isolated decisions.

Outcome

Your security program transforms from a reactive defense framework to a proactive driver of business strategy.

1.1 Conduct a business impact analysis

- Prioritize critical systems and evaluate dependencies.
- Map security investments to business objectives with measurable ROI metrics.
- Regularly revisit alignment as business goals evolve.
- Document interdependencies between business processes and security controls.

1.2 Define a risk appetite framework

- Establish clear risk thresholds tied to SLAs.
- Create financial loss models for risk communication.
- Set industry-aligned acceptable risk levels.
- Review and update risk appetite quarterly.

1.3 Integrate compliance requirements

- Embed global standards (ISO 27001, NIST CSF) into operations.
- Leverage compliance as a strategic advantage.
- Implement continuous monitoring systems.
- Maintain updated compliance documentation.

Step 02
Maturity Assessment

Objective

Conduct a comprehensive evaluation of your security posture to identify strengths, gaps, and opportunities. This assessment creates your transformation baseline.

Rationale

By measuring current capabilities, organizations ensure aligned investments and achieve comprehensive security coverage.

Outcome

A clear, data-driven roadmap that evolves your security program from current to target state.

2.1 Analyze current state

- Review existing security controls and capabilities.
- Assess organizational security culture.
- Evaluate third-party security risks.
- Document technology stack and security tools.

2.2 Identify capability gaps

- Compare current state against industry benchmarks.
- Prioritize gaps based on risk exposure.
- Create capability enhancement roadmap.
- Define success metrics for each capability.

2.3 Define target state

- Set realistic maturity goals.
- Align targets with business objectives.
- Create phased improvement plan.
- Establish a measurement framework.

Step 03
Architecture Principles

Objective

Establish a zero-trust, adaptive security architecture that forms your resilience backbone. This framework must evolve with emerging threats.

Rationale

Traditional perimeter-based security fails against modern threats. Your architecture must enable both protection and rapid recovery.

Outcome

A future-ready security infrastructure that automatically detects, responds, and adapts to threats while enabling business agility.

3.1 Implement zero trust architecture

- Deploy role-based access controls with continuous verification.
- Implement micro-segmentation for critical assets.
- Enable strong authentication mechanisms.
- Design network architecture with a security-first approach.

3.2 Build adaptive resilience

- Implement automated recovery mechanisms.
- Deploy active-active configurations.
- Enable cloud-based redundancy.
- Leverage microservices architecture.

3.3 Integrate advanced technologies

- Deploy AI-powered SIEM solutions.
- Implement a vendor-neutral cloud architecture.
- Standardize API security controls.
- Secure IoT and edge computing infrastructure.

Step 04
Visibility Framework

Objective

Implement comprehensive visibility across all assets, threats, and risks. You cannot protect what you cannot see.

Rationale

Without end-to-end visibility, threats go undetected and risks remain hidden, creating dangerous security blind spots.

Outcome

A real-time view of your entire security landscape that enables proactive threat detection and informed decision making.

4.1 Enhance asset management

- Deploy automated asset discovery tools.
- Maintain real-time asset inventory.
- Monitor shadow IT activities.
- Track asset dependencies and relationships.

4.2 Implement threat detection

- Deploy AI-driven threat analytics.
- Enable real-time threat monitoring.
- Integrate threat intelligence feeds.
- Establish an alert prioritization framework.

4.3 Create risk dashboards

- Build executive-level risk visualizations.
- Track key risk indicators.
- Monitor compliance status.
- Implement predictive risk analytics.

Step 05
Operational Framework

Objective
Transform security operations from reactive to proactive through integrated tools, automated workflows, and empowered teams.

Rationale
Siloed operations and manual processes create delays in threat response and strain security resources.

Outcome
A streamlined security operation that responds faster, scales better, and empowers teams to focus on strategic priorities.

5.1 Develop response plans

- Create detailed incident playbooks.
- Align with business continuity plans.
- Define clear escalation procedures.
- Establish communication protocols.

5.2 Integrate security tools

- Consolidate security platforms.
- Automate security workflows.
- Enable cross-platform integration.
- Implement centralized logging.

5.3 Empower security teams

- Provide role-based security tools.
- Deploy automation for routine tasks.
- Enable collaborative response capabilities.
- Implement knowledge management systems.

Step 06

Resilience Testing

Objective

Validate your security resilience through rigorous testing and continuous measurement. Assumptions must be proven through action.

Rationale

Untested security measures often fail when needed most. Regular testing reveals gaps before attackers do.

Outcome

A battle-tested security program that demonstrably protects and recovers under real-world conditions.

6.1 Conduct regular assessments

- Schedule penetration testing.
- Perform vulnerability assessments.
- Execute disaster recovery drills.
- Test business continuity plans.

6.2 Measure response effectiveness

- Track mean time to detect.
- Monitor mean time to respond.
- Assess recovery time objectives.
- Validate recovery point objectives.

6.3 Implement continuous improvement

- Document lessons learned.
- Update response playbooks.
- Refine testing procedures.
- Share best practices.

Step 07

Governance Framework

Objective

Establish a structured governance system that drives accountability and ethical decision-making across your security program.

Rationale

Strong governance ensures security initiatives are focused, accountable, and executed with consistency.

Outcome

A well-orchestrated security program that balances innovation with control through clear policies and leadership.

7.1 Establish oversight structure

- Create a security steering committee.
- Define reporting hierarchies.
- Establish decision-making authorities.
- Implement review cycles.

7.2 Develop AI governance

- Create AI risk frameworks.
- Establish ethical guidelines.
- Monitor AI system effectiveness.
- Define accountability measures.

7.3 Maintain a policy framework

- Update security policies regularly.
- Align with industry standards.
- Monitor compliance requirements.
- Document governance procedures.

Step 08

AI and Advanced Technologies

Objective

Harness AI and emerging technologies to augment your security capabilities while ensuring responsible implementation.

Rationale

Traditional security approaches cannot scale to meet modern threats. AI and advanced technologies are essential.

Outcome

A future-ready security program that leverages automation and AI to detect, prevent, and respond to threats at machine speed.

8.1 Deploy AI security solutions

- Implement AI-driven XDR.
- Enable automated threat response.
- Deploy predictive analytics.
- Monitor AI model effectiveness.

8.2 Secure emerging technologies

- Establish innovation frameworks.
- Implement security-by-design.
- Enable secure cloud adoption.
- Deploy IoT security controls.

8.3 Maintain technology governance

- Monitor technology risks.
- Update security controls.
- Track technology dependencies.
- Assess security impact.

Step 09

Human Factors

Objective

Transform your workforce into your strongest security asset through culture, skill development, and continuous learning.

Rationale

Technology alone cannot ensure security. Human behavior and expertise are crucial elements of cyber resilience.

Outcome

A security-conscious organization where every employee is empowered to actively contribute to cyber resilience.

9.1 Build a security culture

- Deploy security awareness programs.
- Implement gamified training.
- Establish security champions.
- Create reward mechanisms.

9.2 Develop security talent

- Create career development paths.
- Enable certification programs.
- Establish mentorship initiatives.
- Support skill development.

9.3 Enable continuous learning

- Provide training resources.
- Share threat intelligence.
- Enable knowledge sharing.
- Create learning communities.

Step 10
Continuous Evolution

Objective

Establish a dynamic framework that enhances cyber resilience through systematic assessment and adaptation.

Rationale

Evolving threats require dynamic security measures, making continuous adaptation essential for cyber resilience.

Outcome

An adaptive security program that evolves through learning, evolving threats, and emerging best practices.

10.1 Conduct holistic assessments

- Measure control effectiveness and maturity.
- Analyze threat intelligence and incident patterns.
- Assess business impact and alignment.
- Review compliance and risk posture.

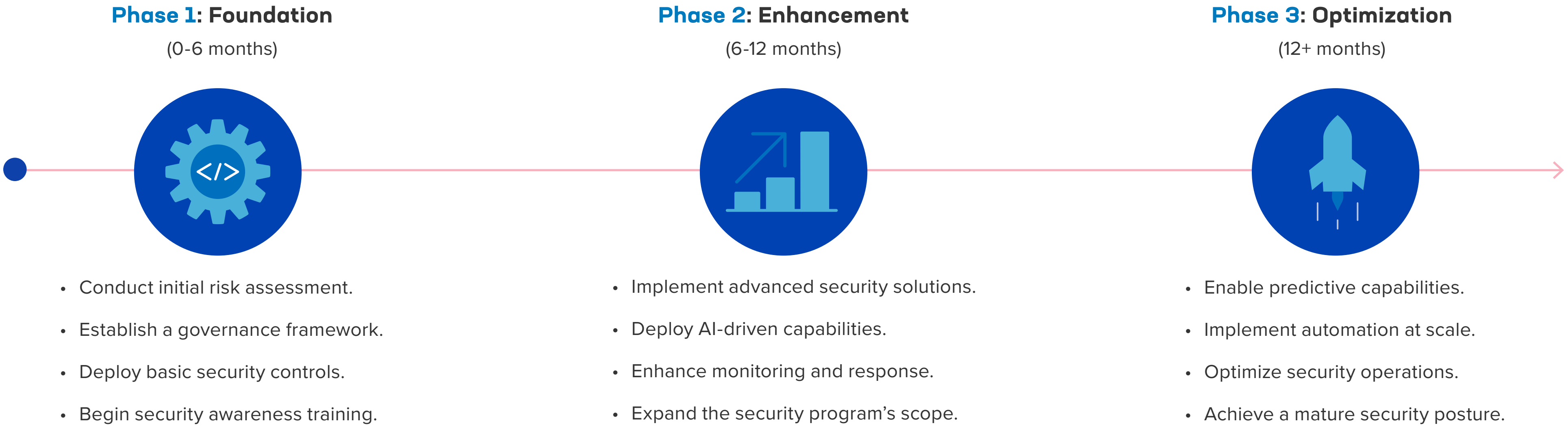
10.2 Focus on capability enhancement

- Strengthen detection and response mechanisms.
- Advance technological capabilities.
- Improve team competencies.
- Optimize security operations.

10.3 Prioritize strategic adaptation

- Update security strategies and roadmaps.
- Realign resources and investments.
- Refine policies and procedures.
- Bridge insights into the next cycle.

Implementation Roadmap



Phase 1: Foundation

(0-6 months)

- Conduct initial risk assessment.
- Establish a governance framework.
- Deploy basic security controls.
- Begin security awareness training.

Phase 2: Enhancement

(6-12 months)

- Implement advanced security solutions.
- Deploy AI-driven capabilities.
- Enhance monitoring and response.
- Expand the security program’s scope.

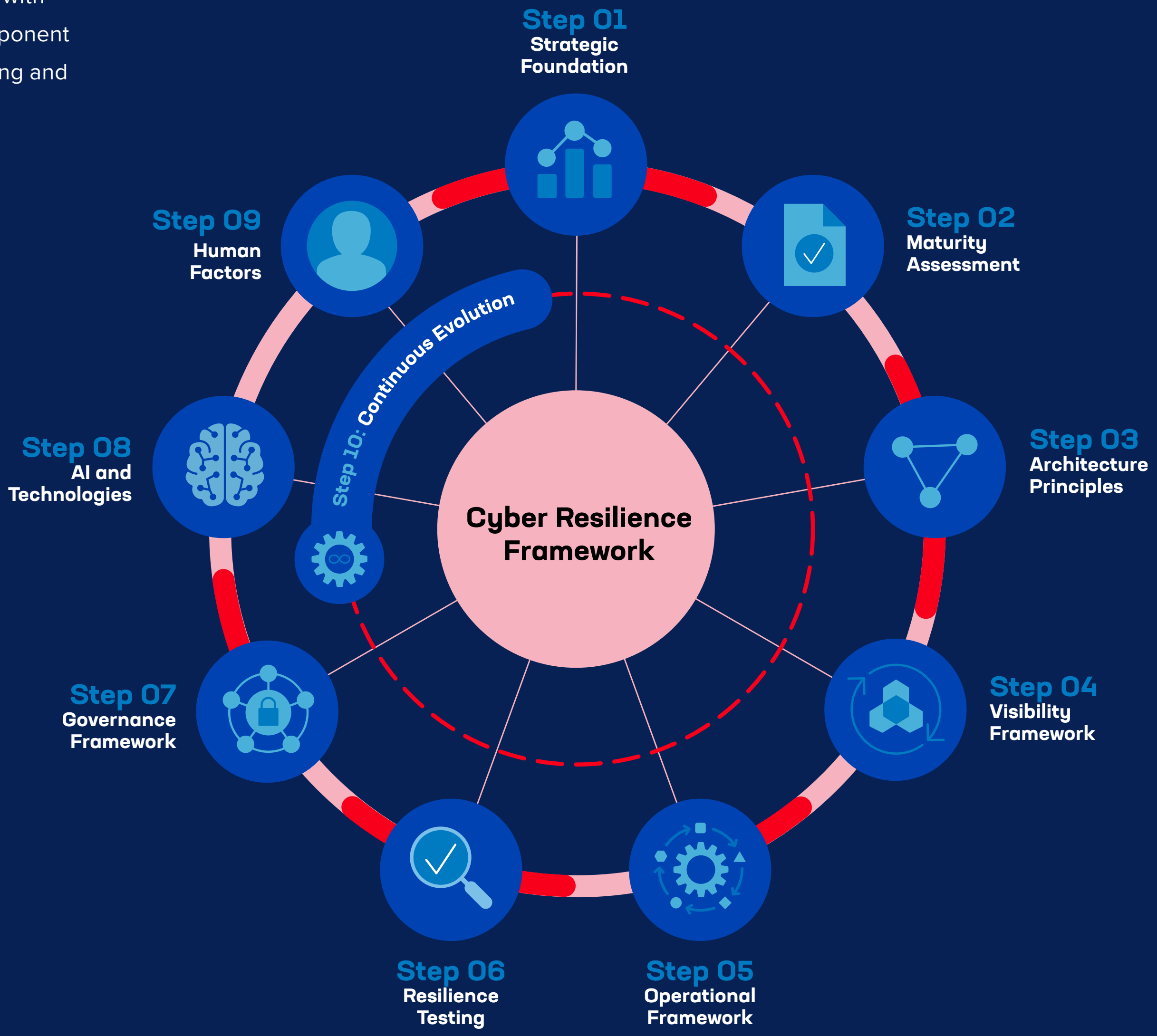
Phase 3: Optimization

(12+ months)

- Enable predictive capabilities.
- Implement automation at scale.
- Optimize security operations.
- Achieve a mature security posture.

The 10 Steps for Cyber Resilience Success

Effective cyber defense requires a dynamic, ever-evolving framework that seamlessly integrates active implementation with continuous evaluation. Each component plays a crucial role in strengthening and sustaining cyber resilience.



🟥	Continuous phase
🟥	Active phase

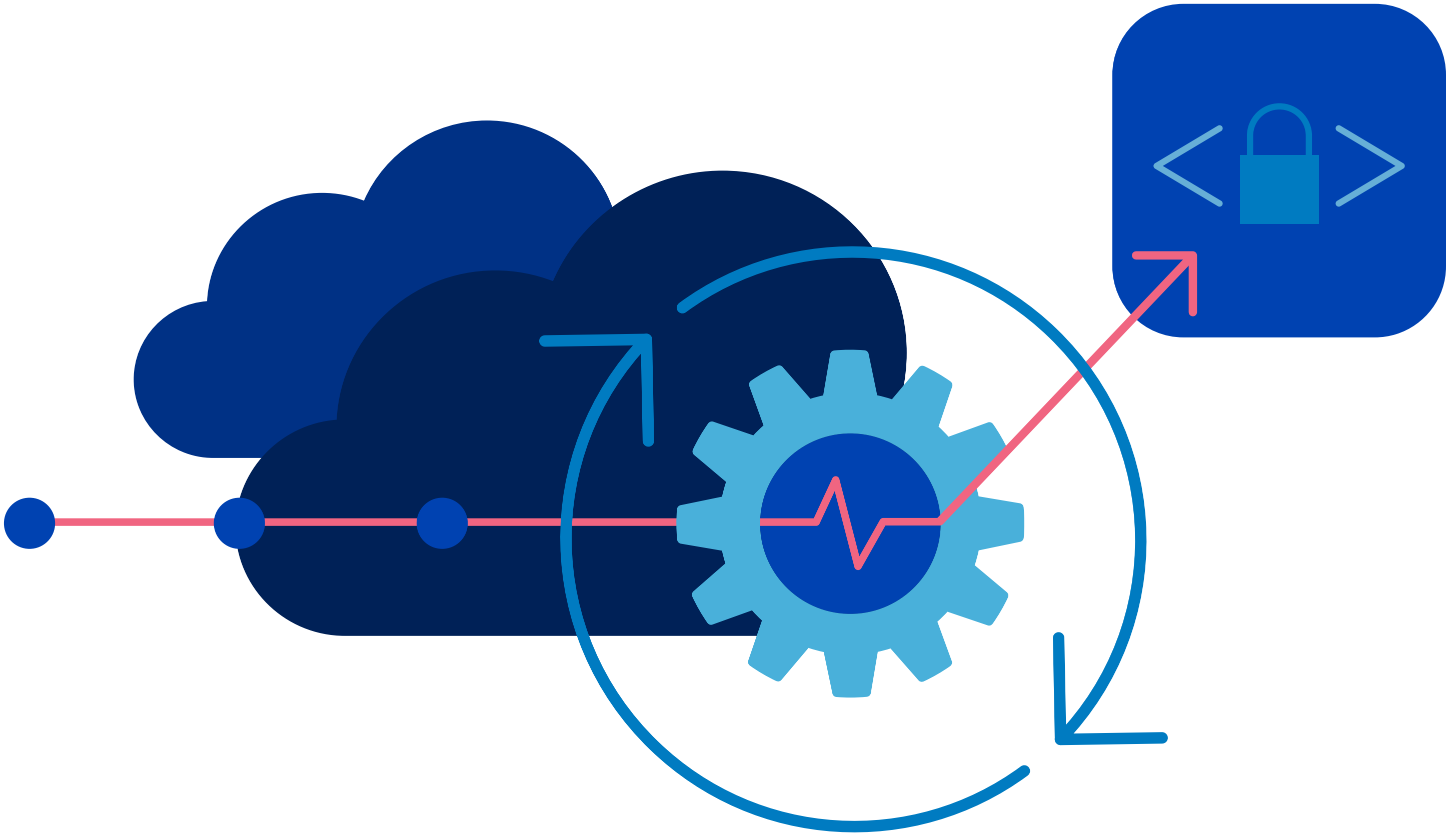
Conclusion

Building cyber resilience is a continuous journey that requires alignment of technology, people, and processes. This playbook provides a structured approach to enhance organizational security posture while enabling business growth and innovation. Regular review and updates of this framework ensure continued effectiveness against evolving threats.

Effective cyber defense requires a dynamic, ever-evolving framework where each component plays a crucial role in sustaining cyber resilience.

Learn more

Get more information on how to strengthen enterprise cyber resilience while optimizing security investments and operational efficiency.



Contributors

Abhijit Chakravarthy
Executive Vice President, Kotak Bank

Abhishek Jha
Chief Information Security Officer, Citi Global Markets India

Amitabh Sharan
Head of Domain, System Integration, Express Solution, DHL IT Services

Amogh Zade
Deputy Chief Technology Officer, ECGC

Arif Bhatkar
Head of Information Technology Security, Godrej Infotech

Ashutosh Pathak
Head of IT, Manipal Global Education

Azril Rahim
Head of Cyber Threat Intelligence Management, Tenaga Nasional Berhad

G Saravanan
Group Chief Information Officer, Thomson Hospital

Hilal Ahmad Lone
Chief Information Security Officer, Razorpay

James Thang
Group Chief Information Officer, HELP Education Group

Lalit Trivedi
Head of Information Security, FlexM

Maz Mirza
Chief Digital Officer, KWAP

Mohd Hanapi Bin Bisni
Head of Group IT, Petra Energy Berhad

Munish Blaggan
Head of Technology, Infrastructure Group, ICICI Bank

Nehal Shah
Deputy Chief Technology Officer, IDBI Bank

Dr. Naresh Kumar Harale
Chief Information Security Officer and Vertical Head of Cyber Security, Reserve Bank Information Technology (ReBIT)

Dr. Pawan K Sharma
Chief Information Security Officer, Tata Motors

Philip Varughese
Global Head of Applied Intelligence, Platforms, and Engineering, DXC Security, DXC Technology

Praveen Samariya
Chief Technology Officer, Medi Assist

Raghu P
Chief Technology Officer, Canbank Factors Limited

Rahul Malhotra
Senior Vice President, Global IT, Intertrust Group- CSC

Sanbir Singh Keer
Executive Director of Cyber Strategy and Transformation | Third-Party Risk Management, Deloitte

Sazul Samsuri
Chief Technology Officer, Digital Banking, KAF Investment Bank

Dr. Sekar Jaganathan
Chief Business Officer, Kenanga Investment Bank

Shinichiro Ikebe
Director, Cyber Security Office, Jupiter Shop Channel Co., Ltd

Srinivas Jaggumantri
Chief Technology Officer, Financial Services, Infosys

Srikanta Sahoo
Senior Director of IT, LTIMindtree

Vasudev Puranik
Managing Director and Chief Information Officer, Global IT, Sales Excellence, Accenture

ABOUT F5

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world’s largest, most advanced organizations to secure and optimize apps and APIs anywhere—on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats. For more information, go to f5.com. (NASDAQ: FFIV).