# QUANTITATIVE CYBER RISK MANAGEMENT







### Overview

Diminishing enterprise perimeters have led to a substantial increase in the cyber risk associated with running digital businesses today. A major cybersecurity incident can potentially wipe out millions of dollars in assets and tarnish even the strongest of brands. It is therefore imperative that organizations should proactively measure and manage the financial exposure to cyber risks. By using manual cyber risk management processes organizations are left with disconnected efforts and ineffective controls. Furthermore, due to information silos, security teams not only have incomplete visibility of their security posture to make informed decisions but also have an inaccurate view of their risk exposure. The need of the hour is a robust Cyber Risk Quantification Solution that can help security teams quantify the cyber risk exposure across people, technology, and processes. Risks need to be identified, prioritized, and remediated at the earliest. Such a solution will enable organizations to identify the appropriate cybersecurity investments to be made, thereby building a more resilient business.

## Need for Quantitative Cyber Risk Management

Comprehensive risk assessment and management

Structured and unbiased approach to risk quantification Justified cyber security investment Complete trend analysis of risk over time

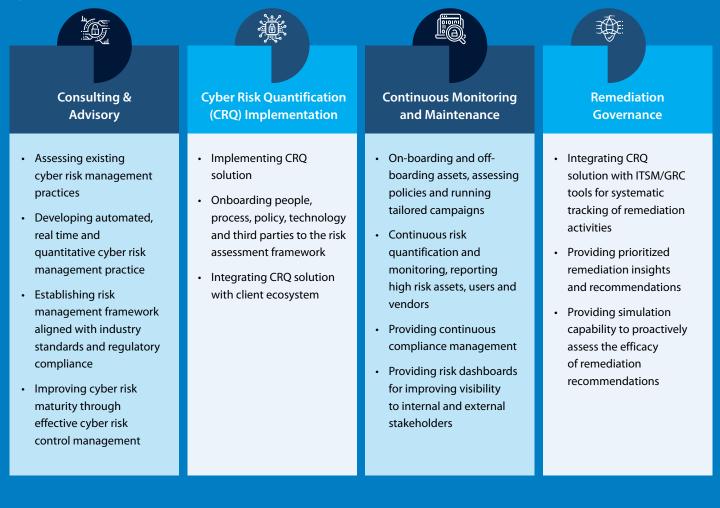
> Fair visibility on adequate cyber risk insurance coverage

## Infosys Cyber Risk Quantification Service powered by SAFE (Security Assessment Framework for Enterprise)

An enterprise-wide cyber risk quantification view allows an organization to measure and mitigate risks at each level, starting from a single asset or employee to the entire line of businesses, departments and locations. It provides people assessment on both macro and micro level, processes, and policies assessment along with technology – inside out and outside in along with third party risk assessment.

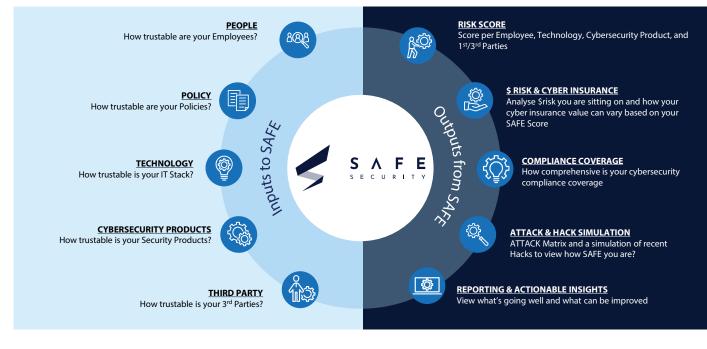


# Cyber Risk Quantification Solution & Services



DIAGNOSE	DESIGN	DELIVER	DEFEND
	Acti	vities	
<ul> <li>Share prerequisites and onboarding forms</li> <li>CRQ Server Provisioning &amp; providing privileged access</li> <li>Provisioning of SSL Certificate</li> <li>Updating the Asset Onboarding details</li> <li>Validate the Asset onboarding details</li> <li>Signoff from Customer team on the assets to be onboarded on our CRQ product</li> </ul>	<ul> <li>Provisioning Infrastructure, access &amp; SSL certificate for our CRQ product deployment</li> <li>Infrastructure team to provide asset inventory inline with pre-requisites</li> <li>Application team to share latest PT Reports for in-scope applications</li> <li>Access to the asset inventory &amp; applications PT report to be on-boarded onto our CRQ product</li> <li>Tools configuration to be shared for integration</li> </ul>	<ul> <li>CRQ tool Kick-off Workshop with all stakeholders</li> <li>Installation &amp; commissioning of CRQ solution</li> <li>CRQ server hardening as per Client's security policies</li> <li>User role creation</li> <li>Integration of our CRQ solution with Client tools based on the product support available</li> <li>Provide Phase wise approach for assets on-boarding</li> <li>For validation, on-boarding sample unique technology devices to CRQ product asset &amp; applications</li> </ul>	<ul> <li>Handover the post migration support activities to BAU team</li> <li>Creating Playbook based on learnings for team for on-boarding any new assets</li> <li>Supporting in risk prioritization and risk remediation by integrating with ITSM tools.</li> </ul>
	Out	come	
<ul> <li>CRQ Solution Requirements</li> <li>Specification Document</li> <li>CRQ Governance Model</li> <li>Detailed Project Plan</li> </ul>	<ul> <li>CRQ solution architecture and design</li> <li>Test plan and approach</li> <li>CRQ product configured</li> </ul>	<ul> <li>CRQ Test Results</li> <li>CRQ Operational Runbook</li> <li>Larger rollout plan and user and administrator training needs</li> </ul>	<ul> <li>CRQ solution rollout for the business units in scope in a phased manner</li> <li>CRQ solution is monitored on continuous basis</li> </ul>

## A panaromic view of Enterprise Cyber Risk Quantification solution



## **Key Business Benefits**

Real-time visibility of the cyber risk posture Support adherence to regulatory compliance requirements such as NIST CSF, ISO 27001, PCI DSS, HIPAA and SOX

#### To know more, please write to us at cybersecurity@infosys.com



For more information, contact askus@infosys.com

© 2021 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights to document.

