LTIMindtree

TrustMAPP®

# Five Steps to a Mature Cybersecurity Program and Achieve Resiliency:

# A Systems Perspective

Enhancing Cyber Resiliency through Mature Practices

# Contents

**Executive Summary** 3

**Why cybersecurity program management is critical** 3

**Understanding the challenges in security program management** 4

**How to achieve a mature cyber posture with GRC** 6

**How to align GRC metrics with cybersecurity maturity** 7

**Five steps to achieve a mature cybersecurity program** 8

1. Assess – Use maturity to evaluate effectiveness of the cybersecurity program 8
2. Report – Communicate cybersecurity maturity 9
3. Model – Build a comprehensive cybersecurity strategy 9
4. Remediate – Implement robust security measures 9
5. Communicate – Use Cybersecurity Maturity to Communicate Program Effectiveness 10

**Case in Point - Journey of an American veterinary service provider** 11

Customer Challenges: 11

Our Solution Highlights: 11

Benefits delivered: 11

**Cyber Maturity Assessment- Measuring Cyber Posture with Maturity Rating Scale** 12

**Benefits of a Mature Cybersecurity Program** 13

**Conclusion** 13

© 2023 LTIMindtree Limited

# Executive Summary

As cyber threats continue to evolve and surge, knowing your organization's security defenses and how you can defend against these threats is critical. In addition to the complex threat landscape, compliance and regulatory requirements need to be factored in. Anticipating threats before they happen and mitigating them when they do, is the priority of today's security leaders. One way to achieve this is by continuously evaluating the company's cybersecurity performance.

Cybersecurity program assessments have become difficult due to a growing attack surface, increased adoption of cloud technologies, and remote work culture. A strong and mature cybersecurity program enables organizations to defend against cyber-attacks and keep critical assets safe against them.

To protect sensitive information and maintain the customer's trust, security leaders must develop a mature cyber program - a comprehensive approach that encompasses prevention detection, response, and recovery from cyberattacks. This whitepaper will dig into the importance of a having mature cyber program for security leaders, the key challenges faced, the steps in achieving a robust cyber posture, and the benefits.

# Why cybersecurity program management is critical

With new and sophisticated attacks emerging constantly, organizations need to ensure that their security measures are up-to-date and effective in protecting sensitive data. Cybersecurity program management enables organizations to comply with industry regulations and statutory compliances to avoid costly fines or legal repercussions over and beyond the operational, reputational, and financial risks that are attached to any cyber breach.

For example, many industries have stringent data protection policies that companies must follow, such as HIPAA for healthcare or GDPR for businesses in the European Union. Having a robust security program in place ensures that all necessary measures are taken to comply with these regulations reducing the risk of non-compliance.

© 2023 LTIMindtree Limited

# Understanding the challenges in security program management

Today's security leaders are faced with several challenges due to the expanding threat landscape. They often fail to communicate effectively with board members, build an effective security program, and improve their cyber posture. The typical challenges include:

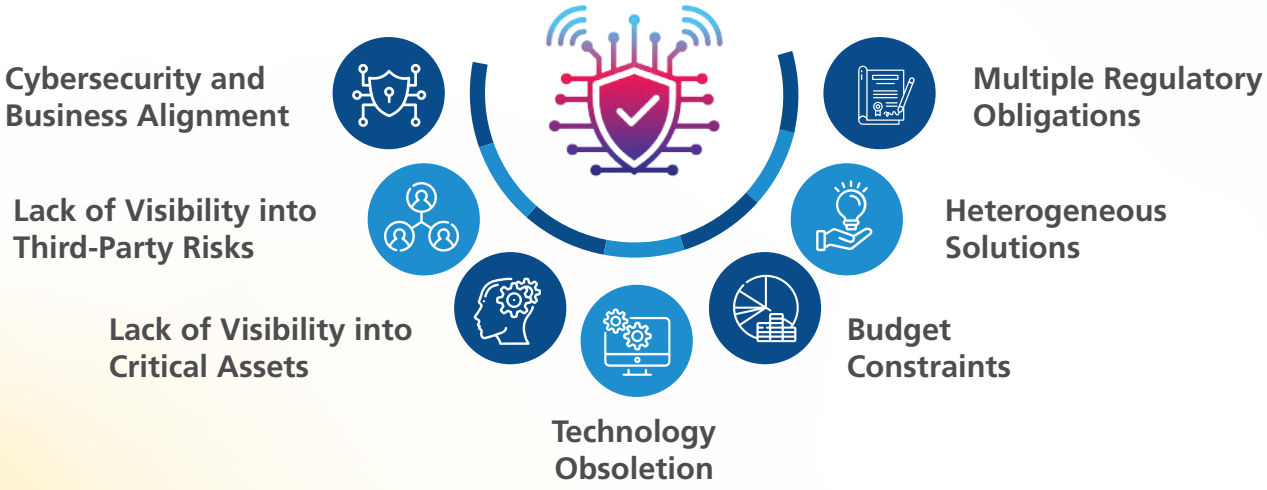


Figure 1: Challenges in security program management

**Cybersecurity and business alignment** - One of the primary challenges for security leaders is aligning cybersecurity with their organization's business objectives. Often, there is a disconnect between security practices and the goals of other departments within an organization. It becomes essential for security leaders to bridge this gap by establishing effective communication channels, educating stakeholders about security risks and opportunities, and demonstrating the importance of cybersecurity in achieving business success.

**Lack of visibility into third-party risks** - Modern-day organizations rely heavily on third-party vendors and partnerships as the business landscape becomes interconnected. However, this introduces significant risks as it becomes challenging to monitor and manage the security posture of external entities. Security leaders must establish a comprehensive vendor risk management program and implement regular assessments to ensure that their contracted third parties adhere to robust security standards.

© 2023 LTIMindtree Limited

**Lack of visibility into critical assets** - Identifying and prioritizing critical assets within an organization is critical for effective security program management. However, many organizations struggle with accurately assessing their tangible and intangible assets across various systems and networks. Security leaders must invest in asset management solutions that provide real-time visibility into critical assets. This will help them understand potential vulnerabilities better and allocate appropriate resources for protection.

**Technology obsolescence**: Technological advancements continue at a rapid pace, leading to the constant introduction of new tools and systems meant to enhance security measures. However, keeping up with evolving technologies can be a challenge for security leaders as they often face budget constraints or organizational resistance to change. It becomes essential for the security leader to stay updated on emerging trends, conduct regular technology assessments, and develop strategies to mitigate risks associated with outdated or unsupported solutions using compensating or alternate controls.

**Budget constraints:** Limited financial resources present a common challenge faced by many security leaders. Building a robust security posture requires investments in advanced technologies, skilled personnel, and ongoing training programs. Security leaders must effectively communicate the potential financial impact of inadequate security measures to the top management. They must also develop strong business cases for funding, and prioritize investments based on regular cybersecurity performance assessments.

**Heterogeneous solutions:** Organizations typically employ a variety of security tools and solutions from different vendors, resulting in a heterogeneous security architecture. Managing multiple systems can be complex for security leaders, leading to challenges like compatibility issues, data integration problems, and overlapping functionalities. It becomes crucial for security leaders to adopt holistic security frameworks that consolidate and streamline security operations across the organization.

**Multiple regulatory obligations:** Compliance with various industry-specific regulations and data protection laws is a significant challenge for security leaders. Ensuring adherence to these obligations requires continuous monitoring, reporting, and maintaining an up-to-date understanding of evolving regulatory landscapes. Security leaders must establish robust compliance programs and collaborate with legal teams to implement effective controls that address specific requirements.

By addressing these challenges, security leaders can strengthen their organization's security posture. With the need to report on cybersecurity performance to the board in real time, this critical function must be managed like any other part of the business. This requires adopting a performance management mindset and tools to manage an effective cybersecurity program.

© 2023 LTIMindtree Limited

# How to achieve a mature cyber posture with GRC

Governance, risk management, and compliance, or GRC in short, is described as the foundation upon which an organization builds its cyber posture. This is because GRC provides a structured approach to managing risk and ensuring compliance with regulatory requirements. Without a strong foundation in GRC, organizations can find themselves vulnerable to cyber threats and unable to respond to incidents effectively.

If you already have GRC as a foundation and want to unlock its value, security posture management turns the data locked in GRC into actionable insights.

© 2023 LTIMindtree Limited

# How to align GRC metrics with cybersecurity maturity

GRC systems provide an excellent foundation for measuring and addressing cybersecurity risks and compliance gaps at an operational level. When communicating the business value of the cybersecurity function to executive stakeholders and board members, security leaders turn to cybersecurity performance management platforms, such as TrustMAPP. Using maturity as a key metric, these platforms identify, quantify, prioritize, and report on the effectiveness of controls and processes in support of the cybersecurity function. Maturity metrics correlate with risk and compliance metrics, thus enabling the security leader to tell a multi-faceted story about cybersecurity performance and its relationship with risk and compliance.

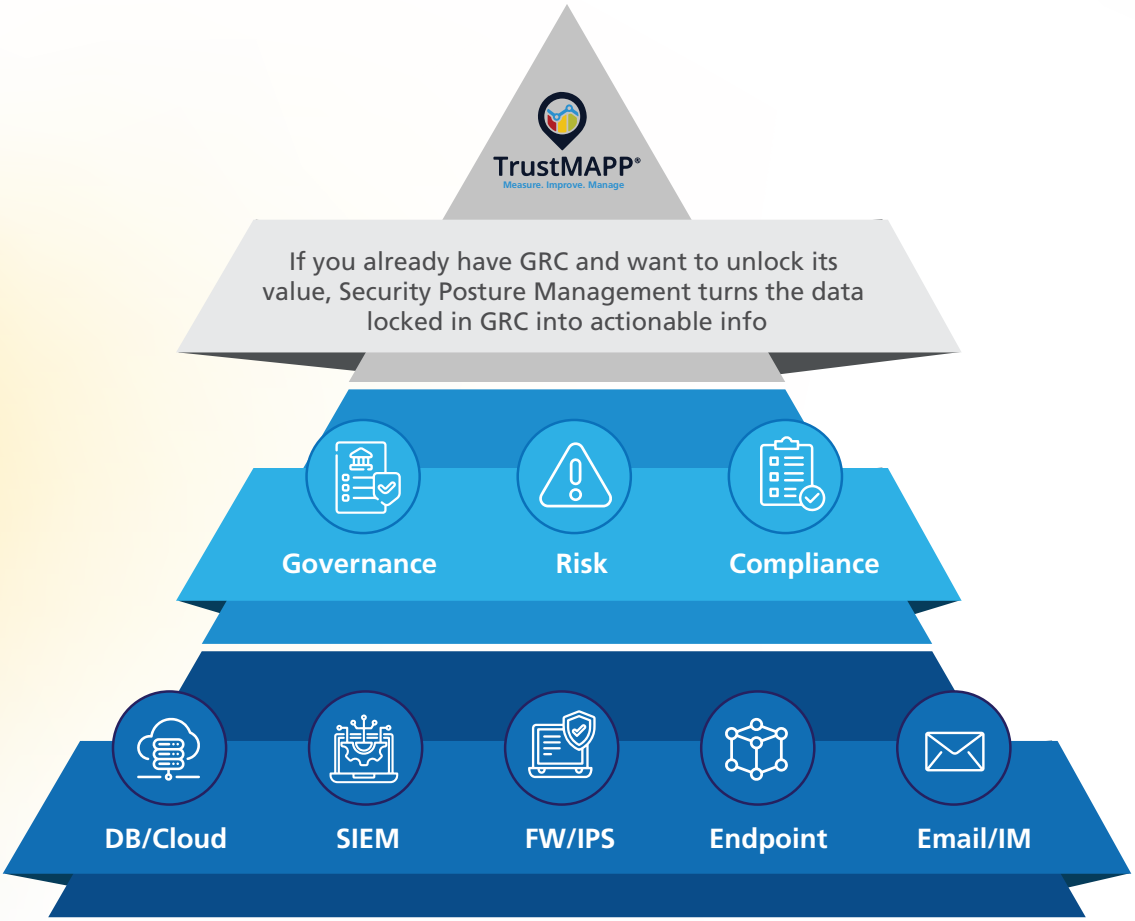


Figure 2: GRC key maturity metrics

Let us dive further to understand the different steps involved in achieving a mature cybersecurity program through a sound performance management strategy.

© 2023 LTIMindtree Limited

# Five steps to achieve a mature cybersecurity program

Organizations can improve the maturity of their cybersecurity programs by implementing the following five steps:

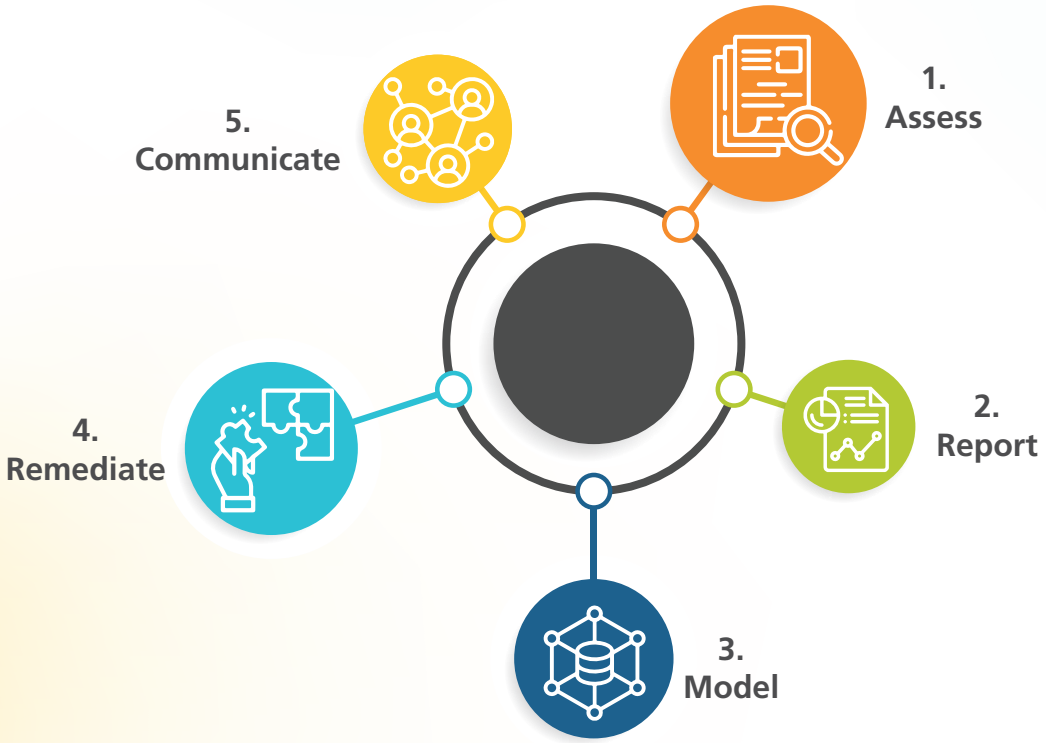


Figure 3 5 steps to maturity of cybersecurity program

## 1. Assess – Use maturity to evaluate effectiveness of the cybersecurity program

Assessing the effectiveness of controls and processes in support of cybersecurity is the first step. When combining the results of risk and compliance assessments with maturity metrics, security leaders benefit from a holistic, business-focused approach to measuring and communicating the value of the cybersecurity program with executive stakeholders and the board of directors.

© 2023 LTIMindtree Limited

## 2.Report – Communicate cybersecurity maturity

Once the assessment is complete, it is crucial to compile and analyze the findings into a detailed report. The reporting stage involves documenting the results of the cybersecurity maturity assessment and presenting them clearly and concisely. The report should include an overview of high and low-maturity processes, with recommendations and estimates for improving cybersecurity maturity over time via a planned and phased approach.

To ensure effective communication of cybersecurity findings, the report should be tailored to different stakeholders, such as senior management, IT teams, and other relevant departments. It is important to use non-technical language and provide context to help stakeholders understand the benefits of implementing and maintaining mature cybersecurity processes.

## 3.Model – Build a comprehensive cybersecurity strategy

Based on cybersecurity maturity assessment findings and recommendations from the report it is essential to develop (or model) a strategic plan. This plan should outline specific goals, objectives, and actionable steps necessary to improve the maturity of the organization's cybersecurity program. The plan should be tailored to address low-maturity processes, establish and/or refine cybersecurity measures, allocate resources effectively, and align with industry best practices.

During this phase, security leaders perform the following activities:

- Perform maturity gap analysis
- Benchmark against peers
- Understand risk appetite and the relationship between risk and maturity
- Generate objective remediation priorities and budgets
- Plan remediation work

## 4.Remediate – Implement robust security measures

This step focuses on implementing the necessary controls and processes to improve cybersecurity maturity over time. Since cybersecurity performance management focuses primarily on process improvement, security leaders use maturity metrics to improve the effectiveness of controls and processes in support of cybersecurity. This may involve improving processes in support of cybersecurity operations, such as addressing vulnerabilities, upgrading systems or software, and strengthening overall defenses. Other operational improvements may include the following:

- Consistently applying patches and updates to fix known vulnerabilities in software and systems. This helps prevent potential exploitation by cyber attackers and reduces the potential attack surface.

© 2023 LTIMindtree Limited

- Implementing specific security controls that align with their cybersecurity goals and objectives. This may include measures such as access control policies, encryption mechanisms, intrusion detection systems, firewalls, and antivirus software.
- Ensuring that network infrastructure is securely configured and protected against potential attacks or breaches. This may involve setting up secure firewalls, network segmentation and micro-segmentation, monitoring network traffic for suspicious activities, and implementing strong authentication mechanisms.
- Prioritizing remediation efforts based on the potential impact of identified vulnerabilities or weaknesses on the organization's assets and sensitive data. By focusing on critical issues first, organizations can effectively allocate their resources and reduce their overall risk exposure.
- Leveraging automated workflows and task management systems ensure that remediation actions are tracked, assigned to appropriate personnel, completed within specified timelines, and documented for future reference.

The maturity of an organization's cybersecurity is improved on an ongoing basis. It must be continuously monitored for the effectiveness of the implemented security measures and any new issues must be promptly addressed. By continuously updating maturity scores in real-time, security leaders benefit from insights into improvement areas while dynamically adjusting priorities to ensure efficient resource allocation.

## 5. Communicate – Use Cybersecurity Maturity to Communicate Program Effectiveness

Effective communication is a crucial aspect of achieving and maintaining a mature cybersecurity program within an organization. It is important to regularly communicate updates about ongoing cybersecurity initiatives, incident response procedures, and training programs. The communication creates awareness among employees about their role in maintaining good security practices.

Clear and consistent communication fosters a culture of cybersecurity awareness throughout the organization. It ensures that employees are well-informed about potential threats, best practices, and any changes in security policies or procedures. This phase involves:

- Conduct regular training sessions to educate employees about the importance of cybersecurity
- Establish incident reporting channels
- Regularly update employees through internal newsletters and bulletins
- Maintain transparent communication with clients, partners, and stakeholders

By implementing a comprehensive communication strategy, organizations can improve employee engagement, reduce human error-related vulnerabilities, enhance incident response capabilities, and encourage a collective effort toward maintaining a strong cyber posture.

© 2023 LTIMindtree Limited

# Case in Point - Journey of an American veterinary service provider

Our client is one of the largest privately owned veterinary services providers in the US, operating several clinics across the country.

## Customer Challenges:

The client conducted a NIST CSF-aligned cybersecurity maturity assessment in 2020 and achieved a rating of 2.65 (on a scale of 1-5). Due to COVID, they could not measure their maturity while making investments to improve the security posture with a target of 3.

To continue the measurement of cybersecurity maturity, the client wanted fixed parameters to ensure the maturity is assessed every year with the same benchmark and help them plan future roadmap.

## Our Solution Highlights:

LTIMindtree onboarded the cloud-based TrustMAPP® Cybersecurity Performance Management platform for the customer. We performed operations such as:

- Configured TrustMAPP to match the client's requirements and future.
- Conducted TrustMAPP user training for self-assessment and launched assessment both through the tool and manual using LTIM IP.
- Completed NIST CSF-based maturity assessment both using the tool and the manual approach.
- Compared both the reports and fine-tuned the TrustMAPP configurations.
- Developed the reports both manual and auto-generated from TrustMAPP and submitted them to the client.

## Benefits delivered:

- The client got access to a robust library of assessment frameworks built into TrustMAPP. This enabled the client to use TrustMAPP for future cybersecurity maturity assessments, without engaging any third party.
- TrustMAPP provided common-sense recommendations and estimates to help security leaders improve cybersecurity maturity over time.
- TrustMAPP provided a roadmap and tools to create, assign, and track the progress of tasks in support of improving cybersecurity maturity.

© 2023 LTIMindtree Limited

# Cyber Maturity Assessment- Measuring Cyber Posture with Maturity Rating Scale

Cybersecurity maturity assessments help organizations measure their capacity to address cybersecurity risks and compliance failures. The table below shows different cybersecurity maturity levels, their control strength, criteria, and appropriate explanations.

| Control Strength | Cybersecurity Maturity Levels | Description |
|---|---|---|
| 0 | Absent | Supporting processes absent with no known plans to address |
| 1 | Initial | Supporting processes perceived as unpredictable, poorly controlled, and reactive |
| 2 | Managed | Supporting processes are characterized by projects and are frequently reactive. |
| 3 | Defined | Supporting processes are well-characterized and well-understood. Well-established standards are in place and the organization is proactive. |
| 4 | Quantitatively Managed | Supporting processes are measured and controlled. Organization uses quantitative data for decision making and to implement predictable processes that meet organizational goals. |
| 5 | Optimized | Supporting processes are stable and flexible. With a stable environment, the organization is focusing on continuous improvement processes and change management. |

Figure 4 Cybersecurity Maturity Levels

© 2023 LTIMindtree Limited

# Benefits of a Mature Cybersecurity Program

A mature cybersecurity program is an invaluable asset to any organization, as it empowers security leaders to protect organizations from sophisticated cyber threats in many ways.

- Security leaders can proactively identify and mitigate potential risks before they can be exploited by attacks. By continuously monitoring the systems and networks for vulnerabilities the security leader can prevent costly data breaches and avoid reputational damage.
- Security leaders can manage compliance requirements and navigate evolving regulatory landscapes. With robust processes for risk assessment, incident response, and ongoing monitoring, organizations are better positioned to meet regulatory standards such as GDPR or HIPAA.
- A mature cybersecurity program empowers the security leader with actional intelligence that supports informed decision-making across the entire organization. With comprehensive visibility of the threats and vulnerabilities across organizations, security leaders can prioritize resources efficiently and target areas of improvement effectively.

Developing a mature security posture equips a security leader with invaluable tools required for success in today's cyber landscape. From proactive risk mitigation to enhanced compliance management and informed decision-making capabilities, these benefits highlight how crucial it is for an organization to invest in cybersecurity program maturity as a part of their overall GRC strategy.

# Conclusion

Cybersecurity maturity is an indicator of an organization's overall cybersecurity strengths and resilience. The complexities of new-age cyber threats are making cybersecurity performance management even more challenging. It's become difficult for organizations to protect their sensitive data, adhere to stringent regulatory compliances, and stay vigilant all the time. To be cyber resilient, security leaders need to have a clear vision of their organization's security maturity, so that they can be aware of possible threats, and mitigate them on time.

LTIMindtree and the team supporting TrustMAPP have joined forces to empower security leaders with a clear vision of their organization's cybersecurity maturity, including trending analysis, planning, and budgeting, and built-in support for multiple frameworks. Together, we provide continuous cybersecurity performance management, giving security leaders a real-time view of their cybersecurity maturity.

© 2023 LTIMindtree Limited

# About the Authors

## Dilip Panjwani

Global Head of the Cybersecurity Technology Office and CoE, LTIMindtree

Dilip has over two decades of experience in leading some of the best cybersecurity practices for large Indian corporations and multinationals. As the Global Head of Cybersecurity Practice and CoE at LTIMindtree, his role involves building state-of-the-art and innovative cybersecurity solutions to transform customers' cybersecurity journey.

## Chad Boeckmann

Founder/CEO, TrustMAPP

Chad is the founder/CEO of TrustMAPP, a B2B Cybersecurity Performance Management platform providing businesses with a clear understanding of control performance, investment estimates, and reporting capabilities to communicate with non-technical audiences. In addition to TrustMAPP, Chad currently manages an active podcast titled "Business of Security Podcast Series" and is a Vice Chair for the IEEE working group for Next Generation Connectivity.

© 2023 LTIMindtree Limited

**LTIMindtree** is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 82,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit **www.ltimindtree.com.**

© 2023 LTIMindtree Limited