

# Cybersecurity in solutions

A journey of turning ideas into reality

protiviti®  
Global Business Consulting

 solutions  
by stc

# > Content

About	3
Prologue	4
1- Introduction	5
2- Snapshot of solutions' cybersecurity transformation journey	6
2.1- Establishing Business Context	6
2.2- Understanding the Current State	9
2.3- Defining SAFE Cybersecurity Strategy	12
2.4- Executing "SAFE" Cybersecurity Strategy	14
2.5- Values Realized & Key Accomplishments	20
2.6- Sustaining the Momentum	22
3- Conclusion	24



# Abstract

A Whitepaper on how solutions by stc transformed its Cybersecurity program for a sustainable digital future in partnership with Protiviti Member Firm for the Middle East Region.



## About solutions by stc

Arabian Internet and Communications Services Company, doing business as solutions by stc, provides holistic, end-to-end technology services to help transform entities across the Kingdom. solutions<sup>1</sup> has been operating in the Kingdom for over 25 years, providing innovative, integrated technology solutions to enterprises and consumers alike. Over the years, solutions by stc, have evolved to become the Kingdom's leading provider of Information and Communications Technology services, enabling the public and private sectors to meet the new trends and ongoing demands of the digital age.

## About Protiviti

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For<sup>®</sup> list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Digitization and Digital Transformation have become key enablers in improving the efficiency of people and organizations. Government and business leaders, globally acknowledge Digital Transformation (DX) as a strategic enabler for meeting their people's and stakeholders' expectations. However, there is a pressing question that gets discussed in stakeholder meetings - "How do we ensure our digital transformation is reliable, resilient, and sustainable<sup>1</sup>?" . Deliberations highlight diverse aspects such as business alignment, culture change, technology selection, and ROI, among many other factors. Well, are those enough?

Cyber threats are growing at a rapid pace<sup>2</sup> and leaders across nations and organizations face challenges hindering the pace of digital innovation. Adversaries and cyberattacks have become increasingly complex, severely impacting the goals of a resilient digital transformation. Therefore, Cybersecurity<sup>1</sup> is also acknowledged as a key element in the recipe for a successful digital journey.

An effective cybersecurity program with evolving strategy is essential to strike the right balance between managing cyber risks and enabling the business. Cybersecurity must be treated as a business risk with a shared responsibility model that integrates cybersecurity into the business processes. Thus, the participation from business leaders and executives in managing cyber threats and risks are crucial towards building resilient business culture. This forms the central theme for this whitepaper and annotates the vision of Arabian Internet and Communication Services Company's ("solutions by stc" or "solutions") cybersecurity transformation program. solutions' cybersecurity transformation program was aimed at enabling the business to leap forward through successful digital transformations and to be a center of excellence in fulfilling the prestigious 2030 Vision of the Kingdom of Saudi Arabia.



Cybersecurity plays a crucial role in maintaining solutions' brand and reputation as a trusted business enabler to our customers. Ensuring robust cybersecurity measures is pivotal aspect facilitating the Kingdom's vision 2030 and its digital transformation journey.

**Ahmed N. Bajnaid, Chief Governance Officer,  
solutions by stc**

---

<sup>1</sup>Forbes Article – why cybersecurity is the springboard for successful digital transformation; URL: - <https://www.forbes.com/sites/forbestechcouncil/2022/06/09/why-cybersecurity-is-the-springboard-for-successful-digital-transformation/?sh=292c047262cb>

<sup>2</sup>2019 Cyber Security Statistics; URL: -<https://purplesec.us/resources/cyber-security-statistics/#Start>



# 1. Introduction

In 2018, stc group (solutions' parent company) launched the "DARE" business strategy that aims to make stc a globally recognized best-in-class digital leader and innovative service provider. This drives solutions' to launch "LEAP" business strategy aiming to spearhead the B2B ICT and digital agenda to support stc group by offering segment focused digital products and services.

Lead,  
Expand,  
Advance,  
Promote.  
- solutions' Strategy

Digitization,  
Accelerate performance,  
Reinvent experience,  
Expand scale and scope.  
- stc Group Strategy

The business leadership quickly recognized the impact and importance of cybersecurity as a key enabler in achieving its business strategies and digital vision. Thus, in 2019, stc launched "GUARD"; and in 2020, solutions' established "SAFE" cybersecurity strategies to effectively manage cybersecurity risks and support the business in their digital transformation agenda.

This whitepaper summarizes solutions' 6-staged cybersecurity transformation journey and its experiences driven by its visionary leadership in partnership with Protiviti Member Firms for the Middle East Region through the launch and execution of its "SAFE" cybersecurity strategy. The key stages are as below:

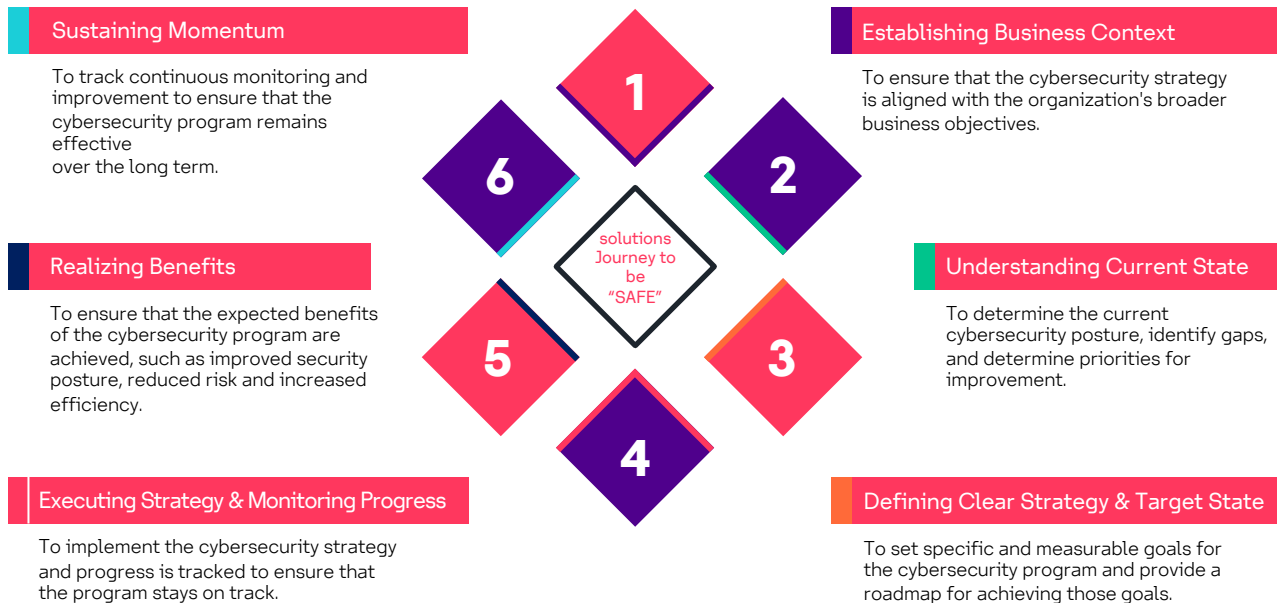


Exhibit 1: solutions' Journey to be 'SAFE'

---

## 2. Snapshot of solutions' cybersecurity transformation journey

"Well begun is half done" (Aristotle)

Having the right start to our cybersecurity transformation journey was necessary and equally challenging. The overwhelming ambitions and expectations, challenging the status quo and breaking silos with minimal conflicts, being less disruptive to the existing ecosystem, building trust, and adapting to the culture were crucial factors that needed to be managed effectively. Collective and strenuous brainstorming sessions with the business, coupled with constant guidance and support from the solutions' management, positively impacted and helped shape the transformation journey. The sections below summarize the key challenges, actions, and lessons learned during the 6-stage cybersecurity transformation journey.

### 2.1 Establishing Business Context

The starting point for solutions' cybersecurity transformation journey was to establish a context aligned with the business to gain a holistic view of the organization's cybersecurity threats, vulnerabilities, and associated risks and opportunities. The internal and external contexts, such as regulatory requirements, threat landscape, and stakeholder expectations, were assessed to establish the business context to set the drivers and boundaries as depicted in the diagram below.

"The solutions Cybersecurity Journey is testament of how innovation and effective collaboration are core values for a successful transformation program. We are proud of having contributed to this journey."

- Adnan Zakariya, Country Managing Director, Protiviti Member Firm for the Kingdom of Saudi Arabia

#### Regulatory Context

Understanding the regulatory requirements



#### Stakeholder Expectations

Identifying the business needs and concerns



#### Threat Landscape

Understand the potential threats

Exhibit 2: Establishing the Context

Context  
#1:

Cybersecurity Regulatory Agencies in KSA :

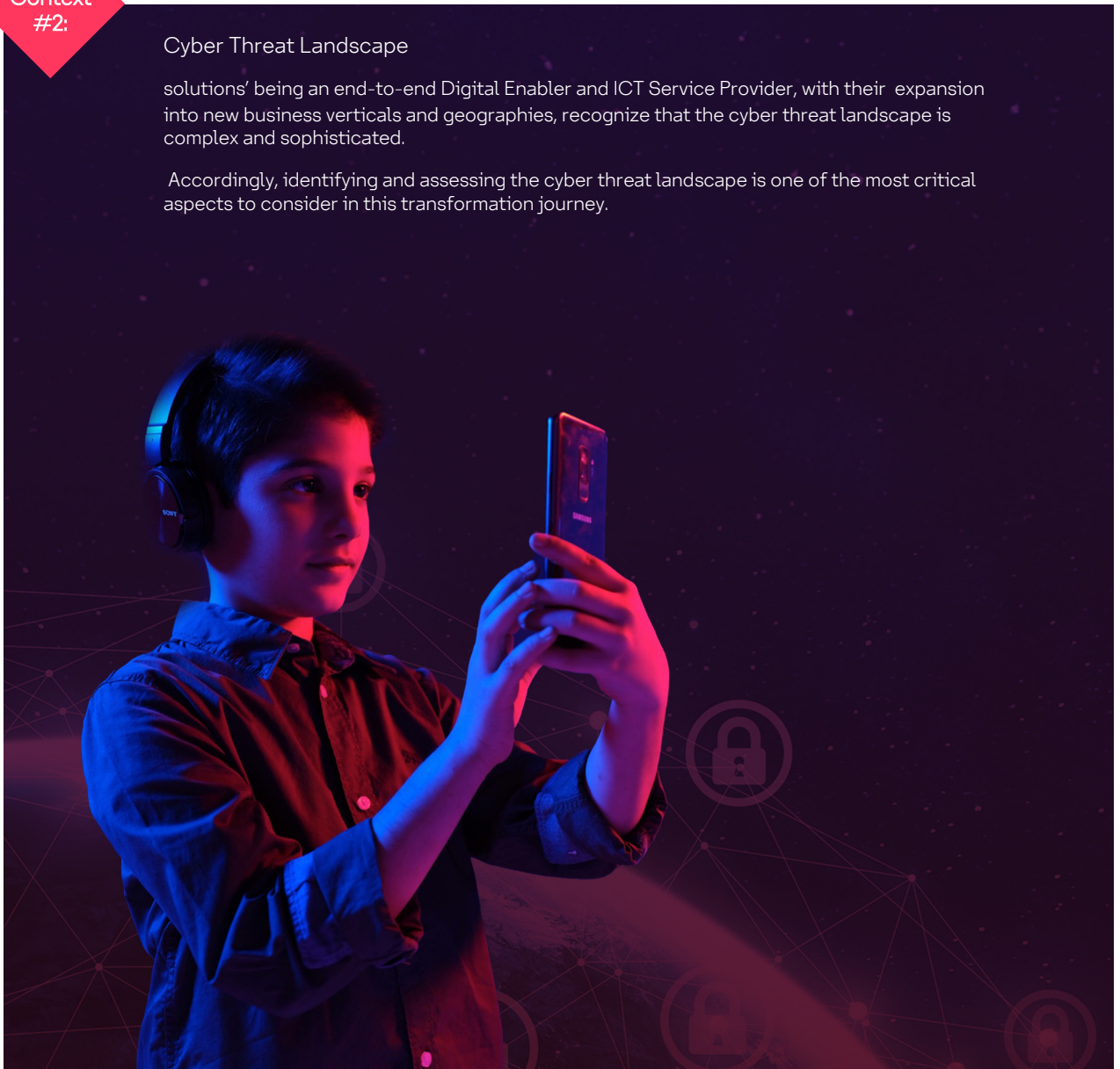
The regulatory agencies in the Kingdom, such as the National Cybersecurity Authority (NCA), Communications, Space and Technology Commission (CST), Saudi Authority for Data and Artificial Intelligence (SDAIA), Saudi Arabian Monetary Authority (SAMA), and Capital Markets Authority (CMA), have published numerous cybersecurity standards and frameworks to foster best in class adoption of cybersecurity within the region. solutions' aspire to maintain the highest levels of regulatory compliance against those cybersecurity standards and frameworks

Context  
#2:

Cyber Threat Landscape

solutions' being an end-to-end Digital Enabler and ICT Service Provider, with their expansion into new business verticals and geographies, recognize that the cyber threat landscape is complex and sophisticated.

Accordingly, identifying and assessing the cyber threat landscape is one of the most critical aspects to consider in this transformation journey.







**\$4.35M**

Average cost of data breach in Middle East region



**\$4.24M**

Cost of data breach on private cloud in 2022

**\$5.02M**

Cost of data breach on public cloud in 2022



**277 Days**

Average time to identify and contain a data breach in 2022



**\$ 1.93Bn**

Attempts to compromise using exploitation techniques in KSA



**Technology**

4<sup>th</sup> most targeted sector in data breach



**21%**

of breaches in 2022 were attributed to Human errors

**5**

Underground forums selling or sharing the leaked data

**256**

Actors behind the data breaches

**1057**

Total number breaches on the dark web

Exhibit 3: Statistics of Data Breaches in 2022<sup>3</sup>

Context  
#3:

Stakeholder Expectations:

Driven by Kingdom's Vision 2030, stc group's DARE and solutions' LEAP business strategies triggered its business and revenue diversification through organic and inorganic initiatives. Recognizing the impact and influence of cybersecurity, the committed business leadership has set their key expectations on this cybersecurity transformation journey, as demonstrated in the exhibit below:



Exhibit 4: Stakeholder Expectations

## 2.2 Understanding the Current State

The current-state assessment of the solutions' cybersecurity capabilities is carried out to identify their current maturity posture, strengths, weaknesses, and areas for improvement. Thus, a baseline of the current state and strategic focus areas to steer the cybersecurity transformation program are determined. The current state assessment approach is summarized in the exhibit and explanation below:

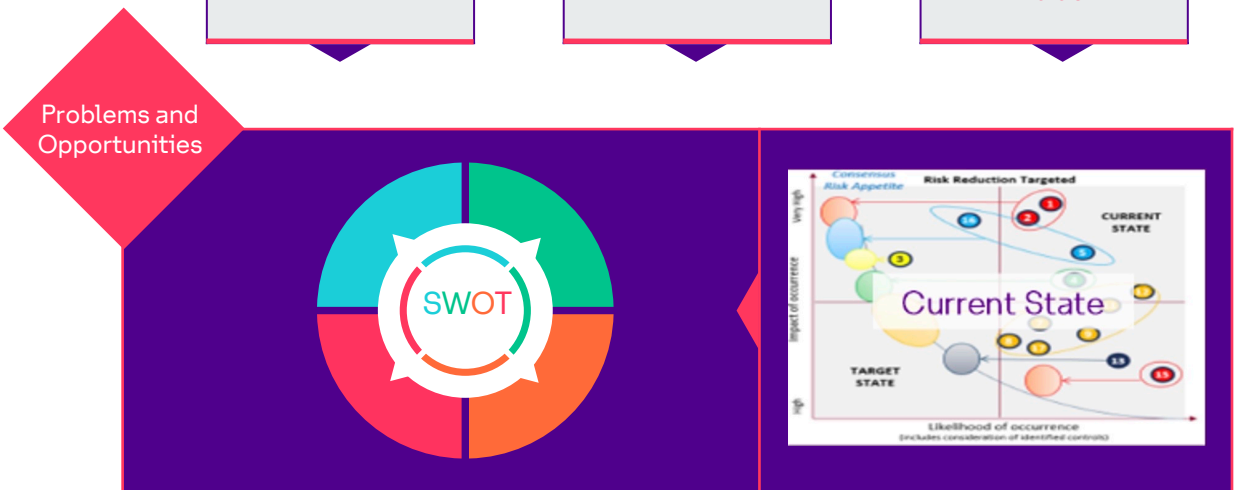
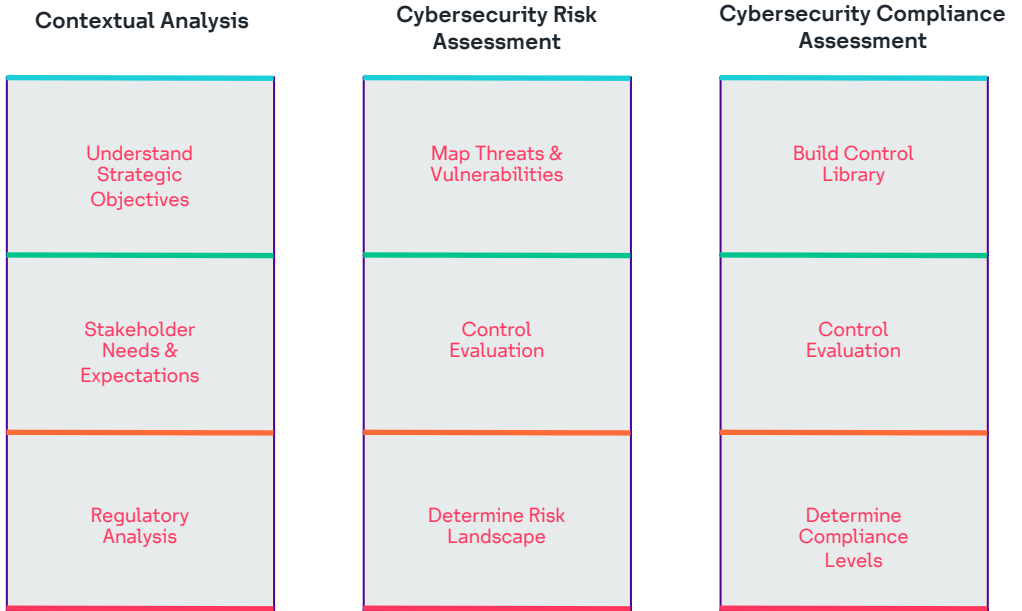
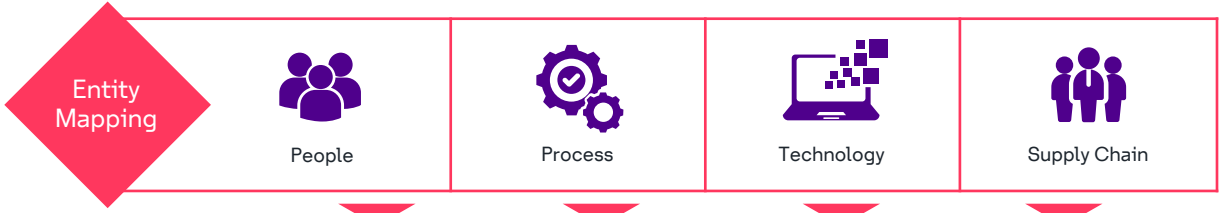
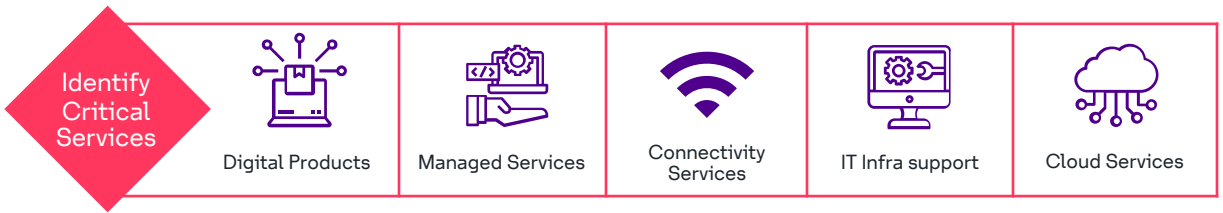


Exhibit 5: CS Current-State Assessment Approach



- **Contextual analysis** enabled solutions to understand the business context and its expectations from the Cybersecurity program.
- **Cybersecurity Risk Assessment** enabled solutions to gain visibility over the potential Cybersecurity risks impacting organizations.
- **Cybersecurity Compliance Assessment** enabled solutions to determine the regulations/standards applicable to solutions and the current state of compliance.

Accordingly, the results were aggregated to define the as-is cybersecurity posture and conduct a SWOT analysis. As an outcome of the current state assessment enabled solutions to determine the following key focus areas to support the transformation of its cybersecurity program:

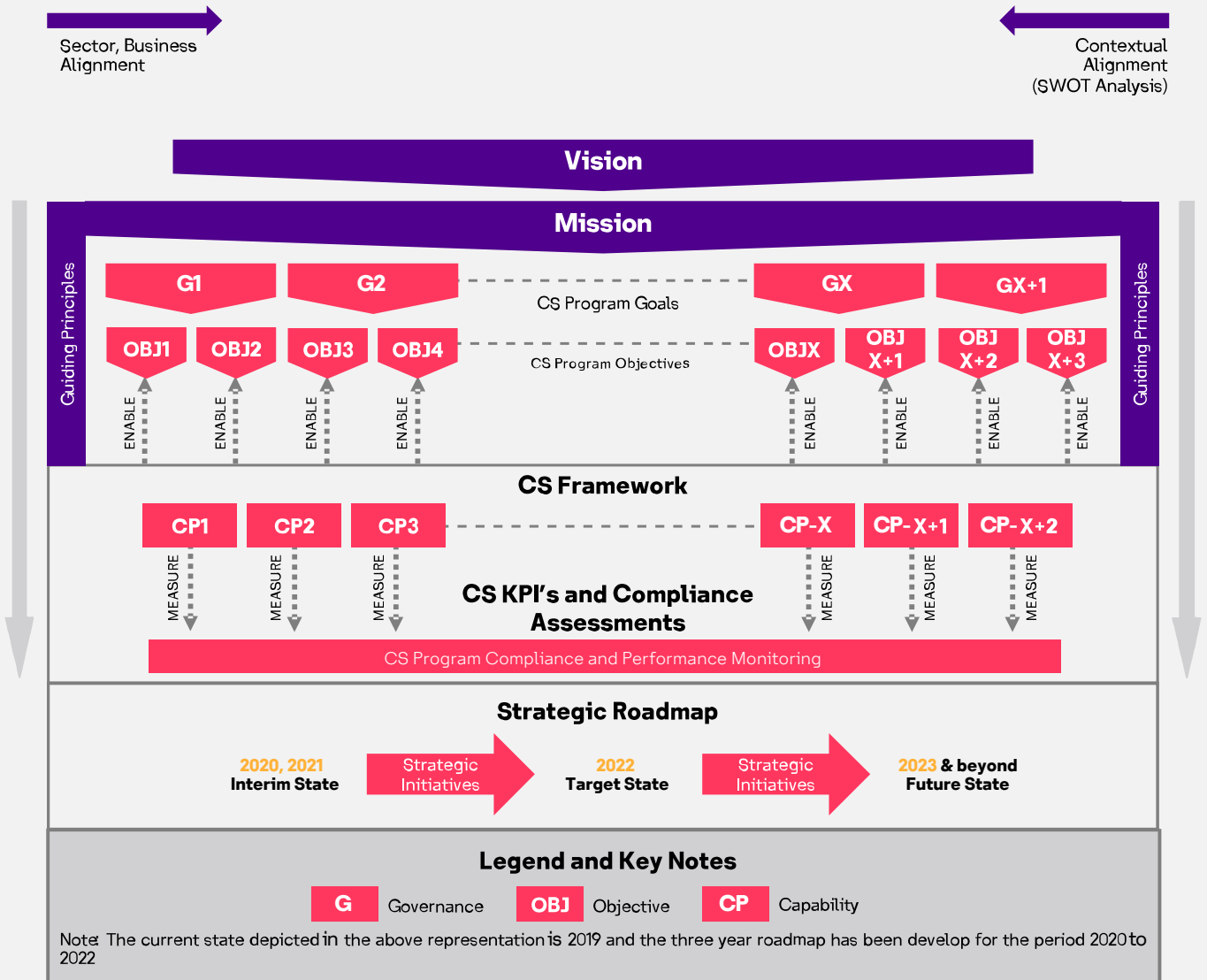
- To strengthen the overall governance of the program.
- To clearly define the accountability model, roles, and responsibilities to govern, manage, implement, and operate the cybersecurity program.
- 4. ▪ To improve the overall cybersecurity culture of the organization.
- To enhance cybersecurity defense and resilience capabilities.
- To improve cybersecurity maturity and compliance levels.

To achieve the key focus areas, solutions established the 'SAFE' cybersecurity strategy. Below sections explain how solutions operationalized the 'SAFE' cybersecurity strategy.



## 2.3 Defining SAFE Cybersecurity Strategy

solutions' cybersecurity strategy "SAFE" is defined by its vision, mission, goals, objectives, and 30+ capabilities; towards achieving its core objective of business enablement with cyber resilience. The overall skeleton of the SAFE strategy is depicted in the exhibit below.



هيئة الاتصالات والفضاء والتقنية  
Communications, Space & Technology Commission



الهيئة الوطنية للأمن السيبراني  
National Cybersecurity Authority

Exhibit 6: Skeleton of the SAFE Cybersecurity Strategy

Further, "SAFE" define a 3-year strategic initiatives roadmap with the target maturity achieved for each of its cybersecurity program capabilities during 2020-2022. The CS compliance and KPI program executed by stc group CS division have greatly supported and influenced solutions' roadmap execution. CS SAFE's aggregated cybersecurity capability maturity projections are exhibited below:



Exhibit 7: SAFE's Capability Maturity Projections (aggregated)



## 2.4. Executing “SAFE” Cybersecurity Strategy

The cybersecurity Target Operating Model (TOM) aligned with “SAFE” capabilities is defined to operationalize the strategic program and its initiatives.

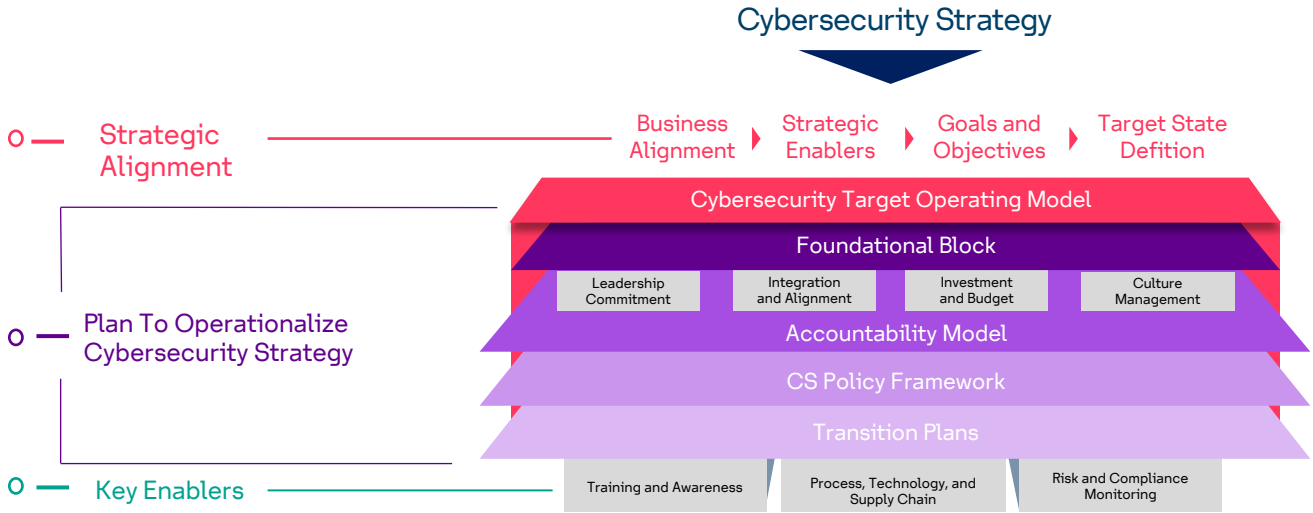


Exhibit 8: SAFE’s Target Operating Model (TOM)

### 2.4.1 Foundational Block

The key ingredient in TOM that sustained the successful transformation journey of “SAFE” is its ‘Foundational Block’ elements, which are explained in the exhibit below:



Exhibit 9: TOM: Foundational Block

## 2.4.2 Accountability Model

The TOM included an accountability model aligned with the Three Lines Model prescribed by the Institute of Internal Auditors<sup>4</sup> as summarized in the exhibit and explanation below:

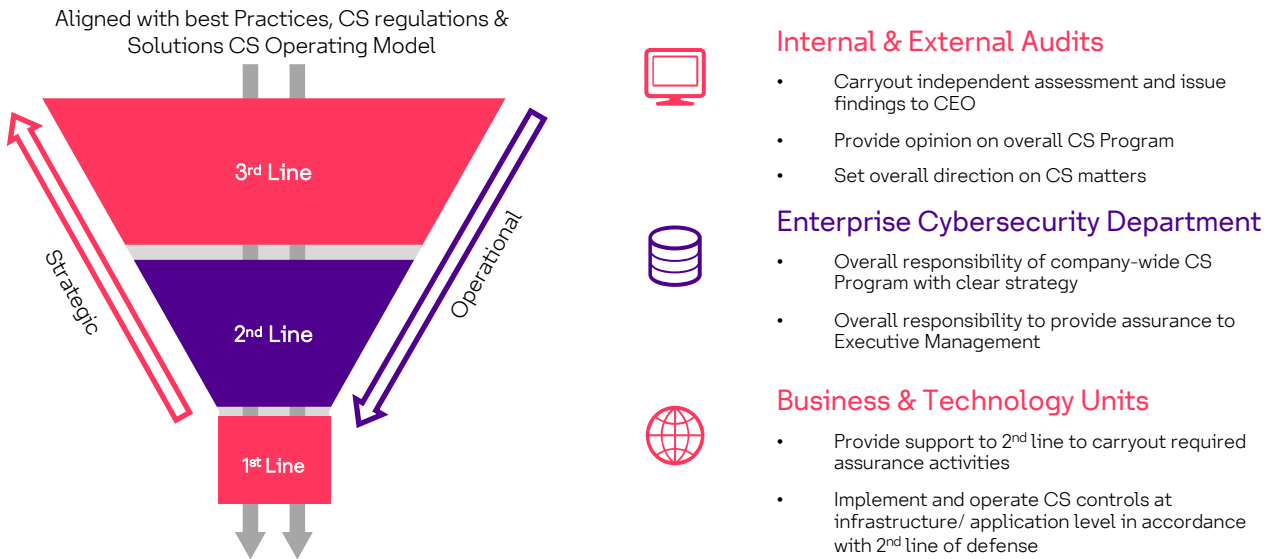


Exhibit 10: TOM: Accountability Model

The Three Lines of Defense alignment and integration were achieved as below:

- **First Line of Defense:** Each business and technology unit remains responsible and accountable mainly for the implementing, operating, and maintaining cyber defense and resilience capabilities.
- **Second Line of Defense:** The Enterprise Cybersecurity department remains accountable mainly for the cybersecurity strategic directions, governance, assurance, and orchestration capabilities to effectively integrate and interoperate across the 3-lines of defense in alignment with the Legal, Enterprise Governance, Risk and Compliance (GRC), and Enterprise Architecture (EA) departments.
- **Third Line of Defense:** solutions' Internal Audit (IA) department played the third line of defense role. And, IA's Combined Assurance program adds significant value from an independent and objective assurance standpoint to effectively achieve SAFE's cybersecurity objectives.

The cybersecurity competency matrix was developed in alignment with the NICE<sup>5</sup> and SCyWF<sup>6</sup> cybersecurity workforce frameworks. The competency matrix defined the cybersecurity roles along with the required competency levels in terms of knowledge, and skills needed to perform cybersecurity tasks and responsibilities that best fit the operating context of solutions'.

<sup>4</sup>The IIA's Three Lines Model: An update of the Three Lines of Defense, URL: <https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/>

<sup>5</sup>NIST Special Publication 800-181, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", 2017. <https://doi.org/10.6028/NIST.SP.800-181>

<sup>6</sup>The Saudi Cybersecurity Workforce Framework (SCyWF) SCyWF - 1: 2020

## 2.4.3 Cybersecurity Policy Framework

The TOM included solutions' Cybersecurity Policy Framework, the governance documentation pyramid is comprised of policies, standards, frameworks, guidelines, and processes/procedures. The policy framework was kept up-to-date to ensure that the changing needs of the organization, industry, and regulatory environment were met; and the emerging threats, new technologies, and best practices in cybersecurity were addressed.

## 2.4.4 Cybersecurity Transition Plans

The TOM also included Cybersecurity Transition Plans. The transition plan(s) translated the SAFE strategy's capability maturity roadmap into tangible, actionable items; and guided solutions' stakeholders to transition from the current state to the envisioned target maturity state. The transition plans defined initiatives and milestones at strategic, tactical, and operational levels aligned with TOM's accountability model. Thus, the transition plans helped to unify the initiatives to achieve SAFE's cybersecurity objectives with optimum cybersecurity investments. Nevertheless, effective change management's significance in managing changes to business processes, technologies, and organizational cultural shifts, along with an effective program governance with continuous monitoring and periodic reporting across all focus groups, was crucial. The exhibit below illustrates solutions' approach to developing the cybersecurity transition plans.

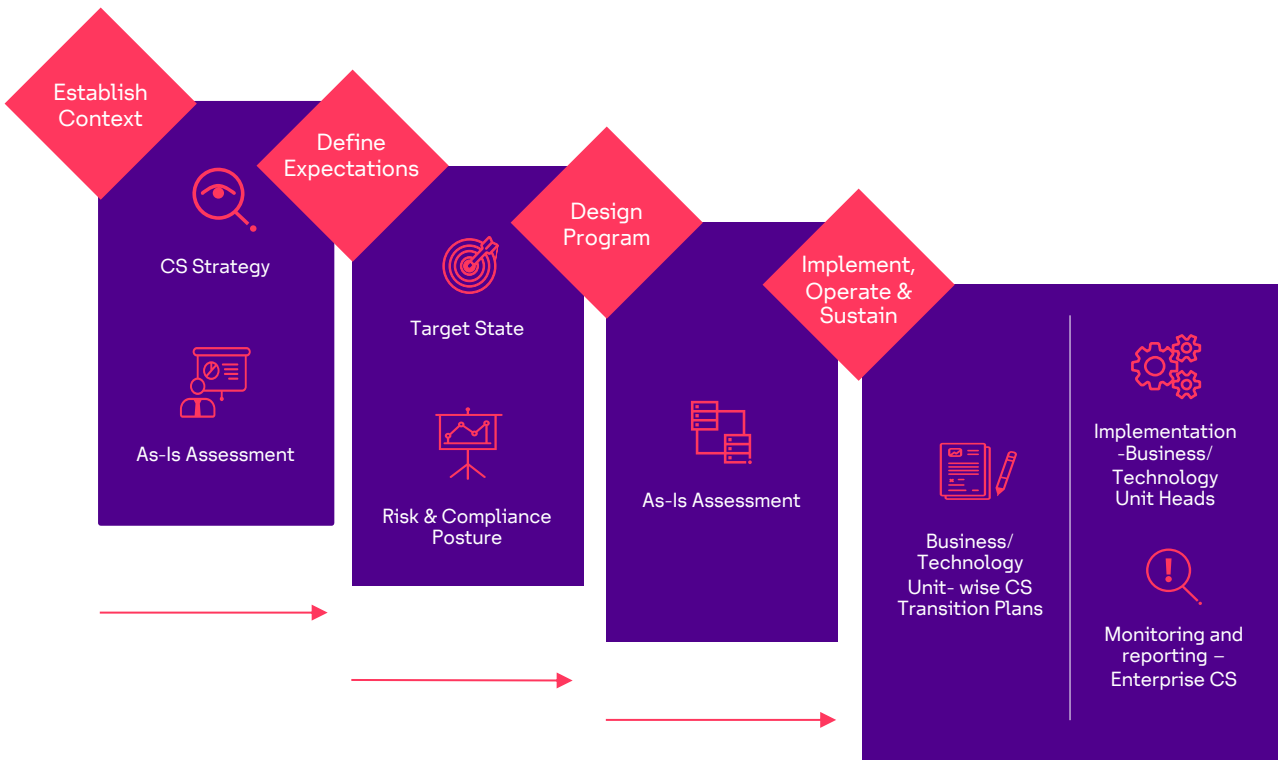
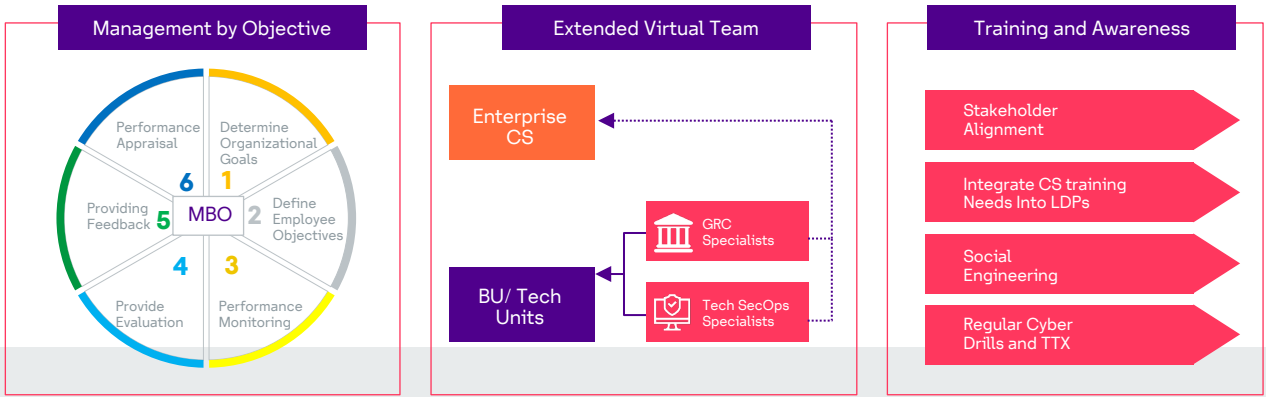


Exhibit 11: TOM: Cybersecurity Transition Plan(s)

The exhibit and the narrative table below provide a holistic overview of SAFE strategy's key transition plan initiatives from four layers - people, process, technology, and CS partnerships.



People



Process and Technology




CS Partnership



Exhibit 12: Key Transition Plan(s) and Initiatives





Initiative Type	Initiatives	Description
 <p><b>People</b></p>	<p>Management by Objective</p>	<p>To assign accountability for achieving the Cybersecurity objectives, Cybersecurity KPIs with annual target scores were assigned to relevant stakeholders. Executive Management level had a specific KPI and target to improve cybersecurity maturity, cascading to operational and tactical layers to ensure cybersecurity maturity is achieved as per cybersecurity strategic roadmap &amp; objectives. The progress of the KPIs was monitored periodically to verify if solutions' were on track to achieving the defined targets.</p>
	<p>Extended Virtual Team</p>	<p>To operationalize the cybersecurity operating model through management support, representatives were nominated from relevant departments ("Cybersecurity Champions"). The departments were further supported through the supply chain initiative (CORS), which created a specialized virtual team to help effectively execute the cybersecurity initiatives.</p>
	<p>Training and Awareness</p>	<p>To improve solutions' cybersecurity culture across the organization, a robust training and awareness program was rolled-out which included awareness during employee/contractor on-boarding, periodic role-based training, periodic phishing/ social engineering simulation campaigns, and encouraging a culture of specialized cybersecurity training/certifications.</p>
 <p><b>Process</b></p>	<p>Develop Cybersecurity Procedures and SOPs</p>	<p>To identify and embed cybersecurity requirements into business and technology processes, and standard operating procedures (SOPs) were defined, and checkpoints/ tailgates were introduced to integrate the Cybersecurity requirements for those business/ technology processes.</p>
	<p>Templates &amp; Toolkit Development</p>	<p>To standardize the cybersecurity practices, toolkits/templates/ implementation guidelines were developed. This helped in the repeatability of cybersecurity operations and ensured the consistency of cybersecurity capabilities across the organization.</p>
	<p>Cybersecurity Assurance on Products &amp; Services</p>	<p>To ensure cybersecurity requirements are considered throughout the Product Development Lifecycle (PDLC), cybersecurity standards requirements toolkits were embedded into the design and development phases, with layers of testing applied at relevant toll gates of the PDLC. A final cybersecurity endorsement is mandated, where the products/services should successfully complete a comprehensive security assessment prior to the product/service launch</p>



Initiative Type	Initiatives	Description
 <p><b>Technology</b></p>	<p>Enhance Cybersecurity Technologies</p>	<p>To assess and baseline the current cybersecurity technologies, security architecture reviews were carried out to focus on enhancements in capabilities and coverage of security technologies such as identify and access management (IDAM), privilege access management (PAM), Mobile device management (MDM), endpoint protection, malware prevention, application whitelisting, Advance Persistent Threat solutions (APT), network security, cloud security, and data protection technologies.</p>
	<p>Enhance Cybersecurity Response &amp; Resilience</p>	<p>To enhance Security Operations Center and Incident Response (SOC &amp; IR) capabilities with coverage/availability, custom use cases were designed, coupled with the automation of incident response processes. Further, solutions worked on integrating the cybersecurity incident management processes into business continuity and crisis management processes, carried out tabletop exercises/ cyber drills, and incorporated the lessons learned into the corrective/preventive action (CAPA) register to increase organization's resilience capabilities.</p>
 <p><b>CS Partnership</b></p>	<p>Cybersecurity Operational &amp; Resource Support (CORS)</p>	<p>To support resourcing needs, solutions' engaged skilled and experienced cybersecurity professionals specialized in cybersecurity GRC, VAPT and Security Operations etc. These SMEs were assigned to various business and functional units to support the cybersecurity program initiatives.</p>
	<p>Cybersecurity Technology Solutions/Partners</p>	<p>To identify technology solution partners, comprehensive technical evaluations and POCs were carried out to onboard the right-fit service providers and technologies that have the capability and flexibility to tailor solutions as per solutions' needs and operating context.</p>

## 2.5 Values Realized & Key Accomplishments

**“Protiviti’s agile partnership model, driven by deep expertise and innovation coupled with focus and leadership from solutions were key factors in this successful cybersecurity transformation journey.”**

- Niraj Mathur, Regional Leader for Security & Privacy Services, Protiviti Member Firm for the Middle East Region

By the end of 2022, internal evaluations and external independent reviews of the solutions’ Cybersecurity program recognized that the solutions’ SAFE cybersecurity strategy execution overachieved on its targets defined during 2019-2022. Where, the intended maturity was to improve from the current state of 2019 (2 – Reactive) to 2022 (4-Integrated); the achieved maturity in 2022 improved to **(5- Best in Class)**. The success of solutions’ cybersecurity transformation journey is showcased in the exhibit below.

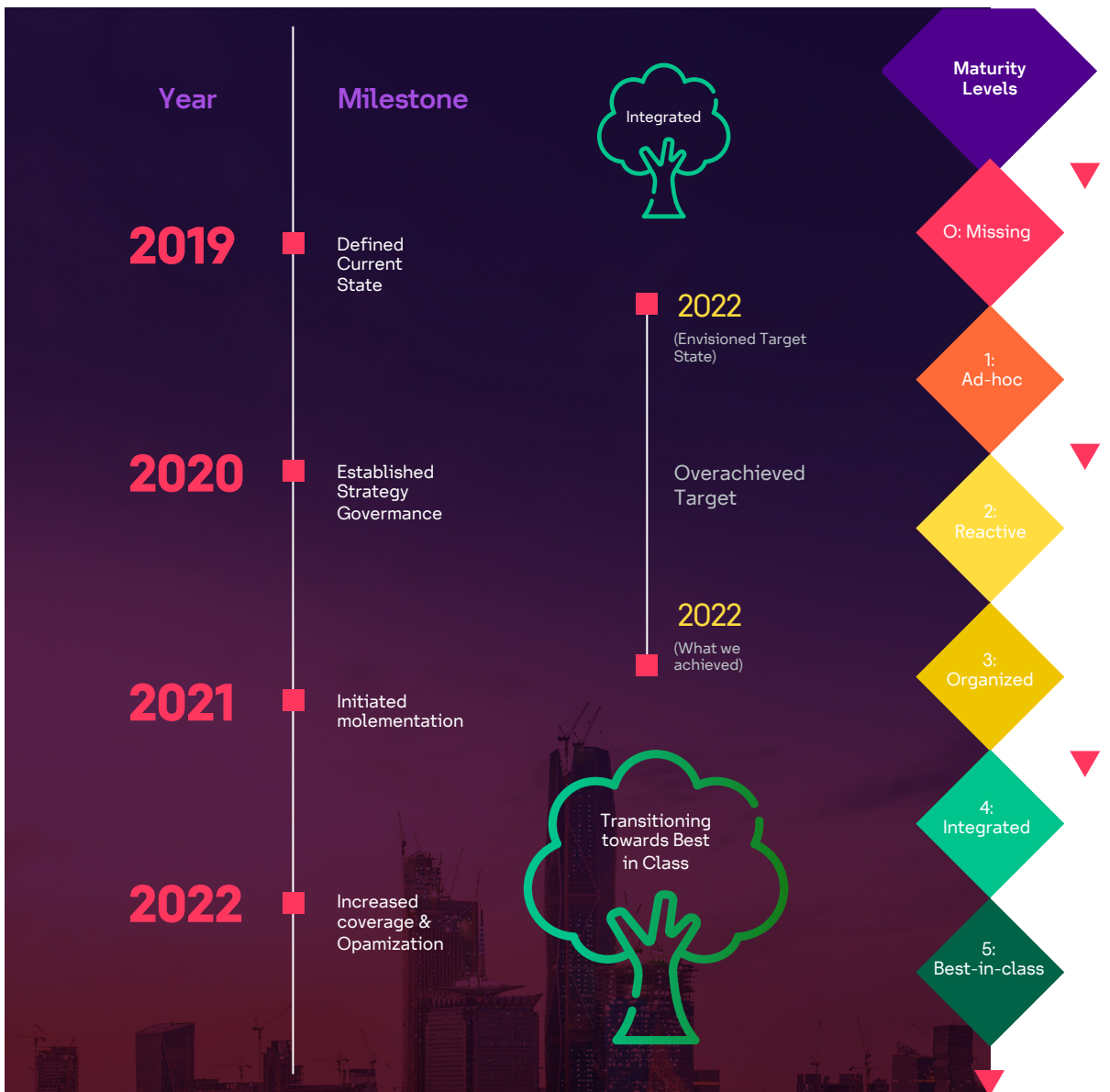


Exhibit 13: solution’s CS Maturity Landscape 2019-2022

The key benefits realized to solutions' through SAFE cybersecurity strategy's successful transformation journey summarized in the exhibit below.

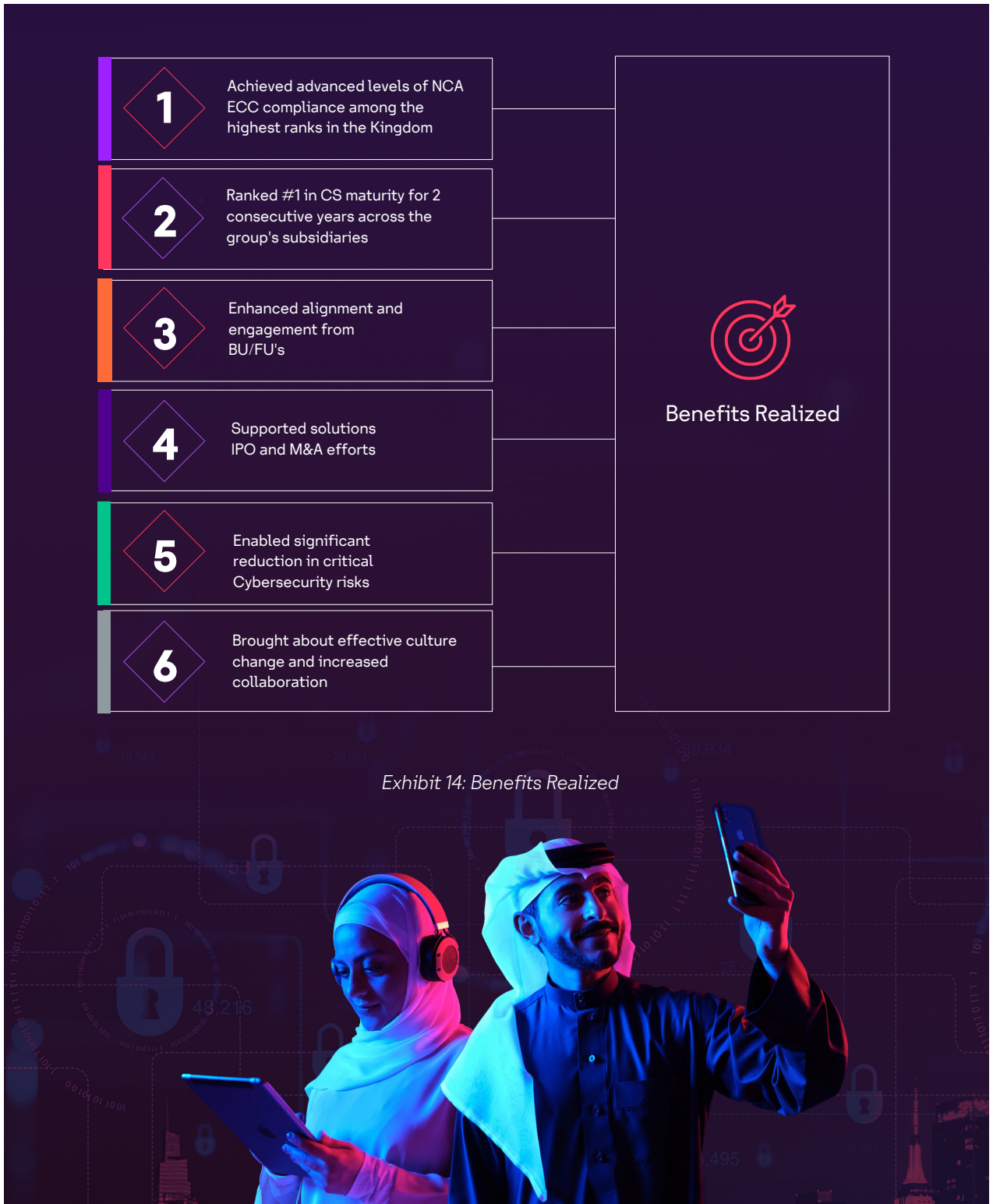


Exhibit 14: Benefits Realized



---

## 2.6 Sustaining the Momentum

### 2.6.1 Continual Improvement

The achieved success of solutions' SAFE strategy's cybersecurity transformation journey shall not define an end state. SAFE continues its journey as an iterative process, adapting to the contemporary changes in its internal and external context. The four key focus areas to drive the continual improvement in solutions' cybersecurity posture are shown in the exhibit below.



Exhibit 15: Key Focus Areas

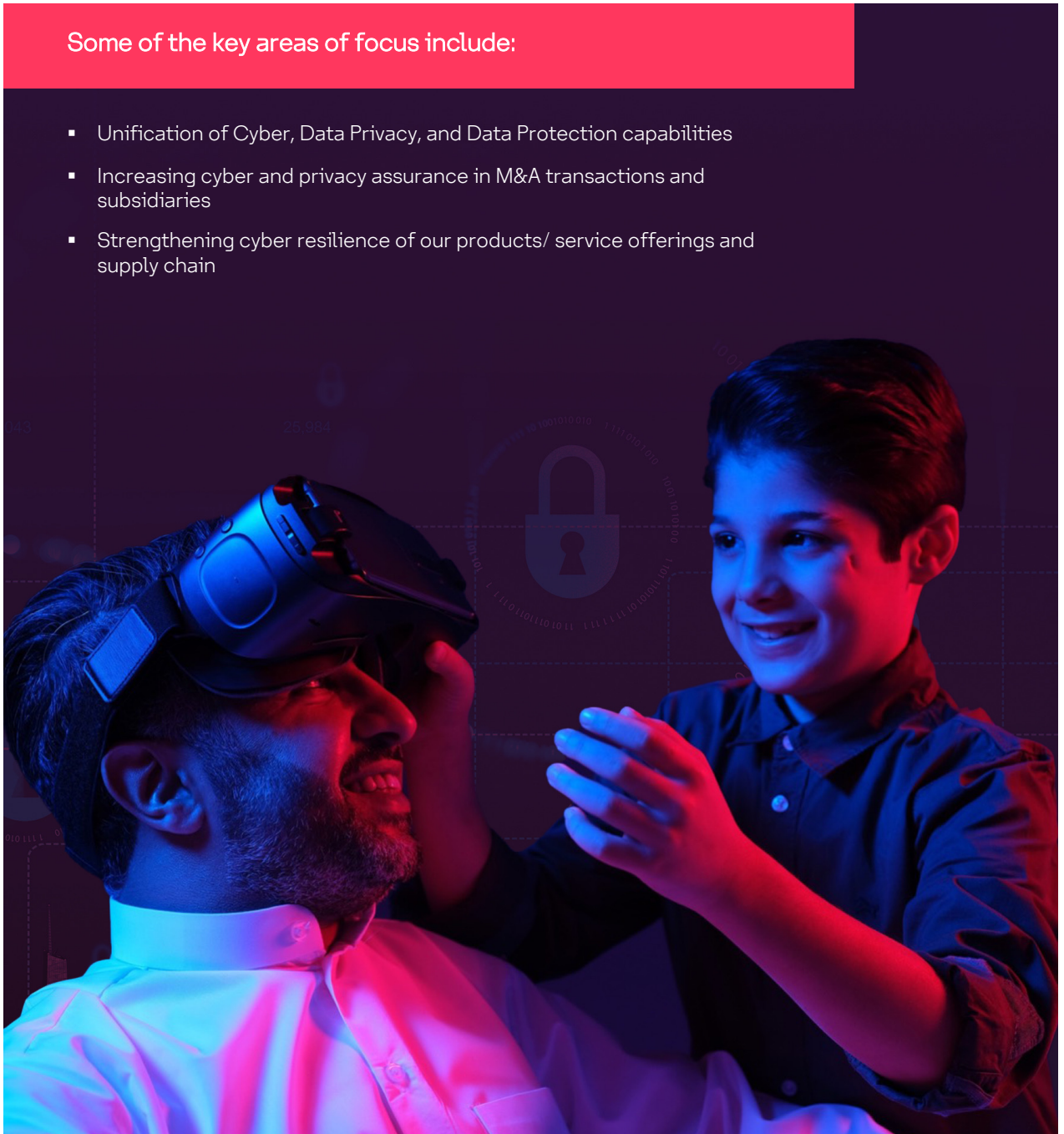
In addition to the above improvement initiatives, solutions' SAFE cybersecurity strategy has also embarked upon its journey to various areas such as supply chain cyber risk management, cyber resilience, cyber threat intelligence, advanced data protection, adoption of AI/ML etc. to name a few, to further expand and strengthen its cybersecurity program.

## 2.6.2 Keeping the Momentum Going

While the transformation program enabled solutions to mature the cybersecurity program, the renewed vision towards the next phase is "Keeping solutions' systems and data SAFE and enabling EASE for Business to achieve defined objectives, ensure compliance, and uphold Customer TRUST. To achieve our full potential and make our dreams a reality, we must DARE to take risks and LEAP forward with confidence and determination".

Some of the key areas of focus include:

- Unification of Cyber, Data Privacy, and Data Protection capabilities
- Increasing cyber and privacy assurance in M&A transactions and subsidiaries
- Strengthening cyber resilience of our products/ service offerings and supply chain



---

### 3. Conclusion

By 2023, 30% of Chief Information Security Officers' (CISOs') effectiveness will be directly measured by their ability to create value for the business<sup>7</sup>. Cybersecurity leaders must craft and implement a cybersecurity vision that supports creating digital value at scale and pragmatic management of security risks while driving core business needs. An effective cybersecurity program should be consistent, adaptable, scalable, and protect information assets.

A few key takeaways from our cybersecurity transformation journey attempted to outline in this whitepaper are:

- Successful cybersecurity transformation program has significant benefits to the overall organization. It can lead to a more robust and effective cybersecurity posture that effectively safeguards the organization's information assets and supports its business objectives.
- Cybersecurity is no longer one team's responsibility; instead, it is a way of collaborating and operating collectively.
- You are as strong as your weakest link; the success of a cybersecurity transformation program is defined by its influence and impact on the business and how quickly it wins business support and a cultural adoption.
- Culture does not change because we desire to change it. Culture changes when the organization is transformed, reflecting the realities of people working together daily.
- Prioritize initiatives based on their impact and urgency rather than taking an extensive approach to implementation.
- Don't think of governance as more paperwork and hassle; instead, it's simply about running your program in the best way possible, which can improve its reputation, attract investment, and increase its chances of long-term success.
- Focus on business outcomes to treat cybersecurity as a business priority, not a set of technologies and tactics.

solutions' embarked on this transformation journey to build cybersecurity resilience through a robust cybersecurity strategy, framework, transparent operating model, proactive risk management, compliance management, performance management and automation of GRC activities. solutions' shall continue to invest in transforming its cybersecurity program and scaling to greater heights with the objective of supporting the organization's mission to "provide innovative technology solutions that enable its customers to succeed in evolving market needs."

#### solutions by stc contributing authors:

Khalid Binahmad  
Mohammed Alomari  
Shahid Shamsudeen

#### Protiviti contributing authors:

Niraj Mathur  
Siva S  
Rahul Ramesh

---

<sup>7</sup><https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing-information-security>

protiviti®  
Global Business Consulting

 solutions  
by stc



[solutions.com.sa](https://solutions.com.sa)