kyndryl

Kyndryl Cyber Resilience Maturity Assessment

Measure cyber readiness, identify gaps, and build a custom roadmap for cyber risk management

Highlights

- Measure the maturity level of your current cyber resilience capabilities
- Get prescriptive recommendations to improve cyber resilience
- Fine-tune your existing solutions through integration

Introduction

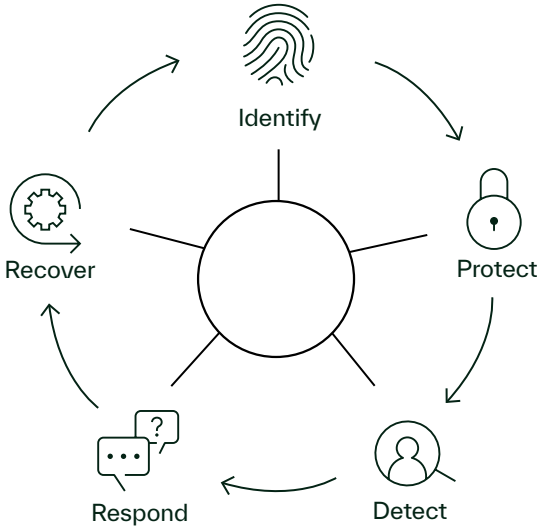
Ransomware increased 435% in 2020[1], while the average cost of a data breach today is 4.24 million[2]. With cyberattacks and threats to cyber resilience on the rise, it is more important than ever to ensure your organization can detect an attack when it occurs to resume operations as quickly as possible.

To protect your business and stakeholders, it is vital to examine the rapidly changing cyber resilience landscape and critically assess how prepared your enterprise is to withstand an attack and recover.

In a complex hybrid environment, achieving cyber resilience demands an integrated approach to detect and respond to threats, safeguard data, ensure high availability, and quickly recover critical business processes and systems after a cyberattack to minimize impact on the organization.

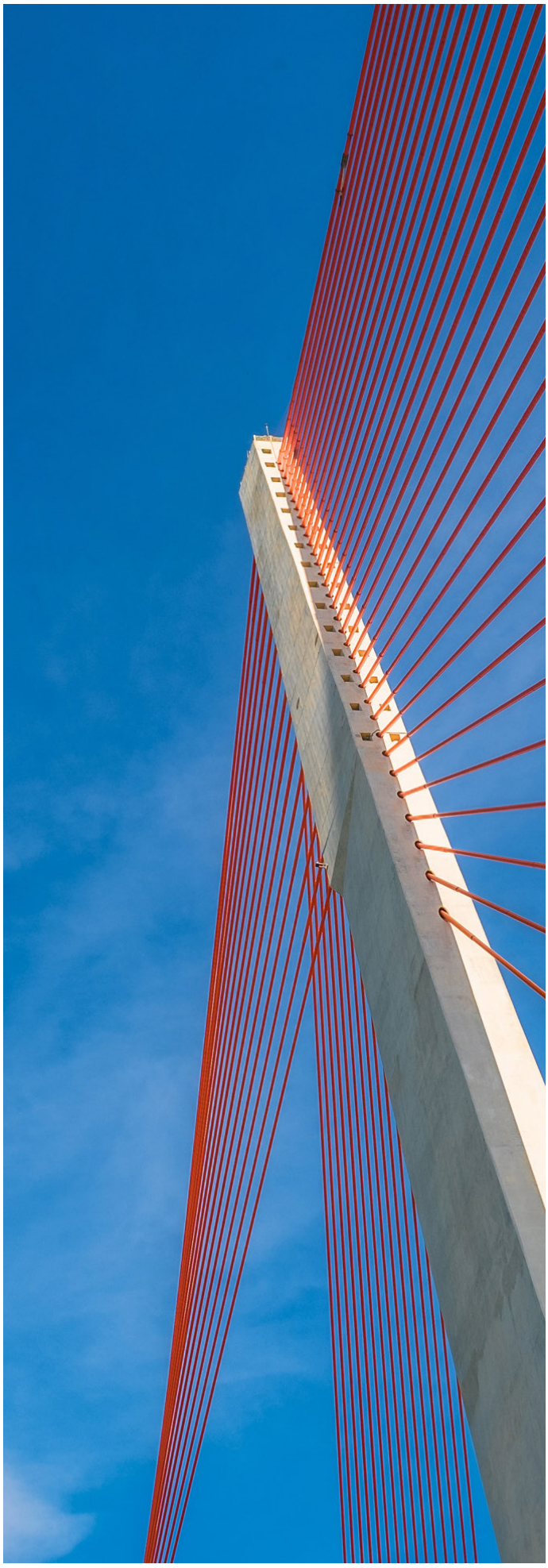
Kyndryl™ Cyber Resilience Maturity Assessment (CRMA), is a remotely facilitated, one-day assessment workshop to help determine your level of preparedness to respond to and recover from a cyber-related event. Suitable for any mix for technology, regardless of vendor, this assessment measures your organization's ability to process new cyber risks, identifying where existing resilience capabilities are sufficient and where there are gaps or weaknesses. With the results, we create a customized roadmap and action plan for improvement.

Kyndryl CRMA is a high-level assessment across multiple domains to determine the level of maturity in your environment, as well as your state of readiness to respond to and recover from a cyber-related event.



Our approach is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

1. **Identify:** Define a roadmap and action plan to build or improve the current cyber resilience plan
2. **Protect:** Protect against attacks by discovering vulnerabilities before they are exploited
3. **Detect:** Detect unknown threats with advanced analytics
4. **Respond:** Respond effectively to cyberattacks and other outbreaks
5. **Recover:** Recover access to critical applications and data



During the one-day assessment workshop, our experts evaluate controls across 23 key categories to determine maturity level. We also examine more than 100 controls based on the current and target state and explore how to better align with NIST's five phases of an effective cyber resilience preparedness and response program—as well as other relevant standards and frameworks, like the International Organization for Standardization (ISO), Control Objectives for Information and Related Technologies (COBIT), the International Society of Automation (ISA), and the Council on Cyber Security.

After the workshop, we analyze the results and generate an executive report, providing recommendations and a roadmap to build or improve your cyber resilience capabilities.

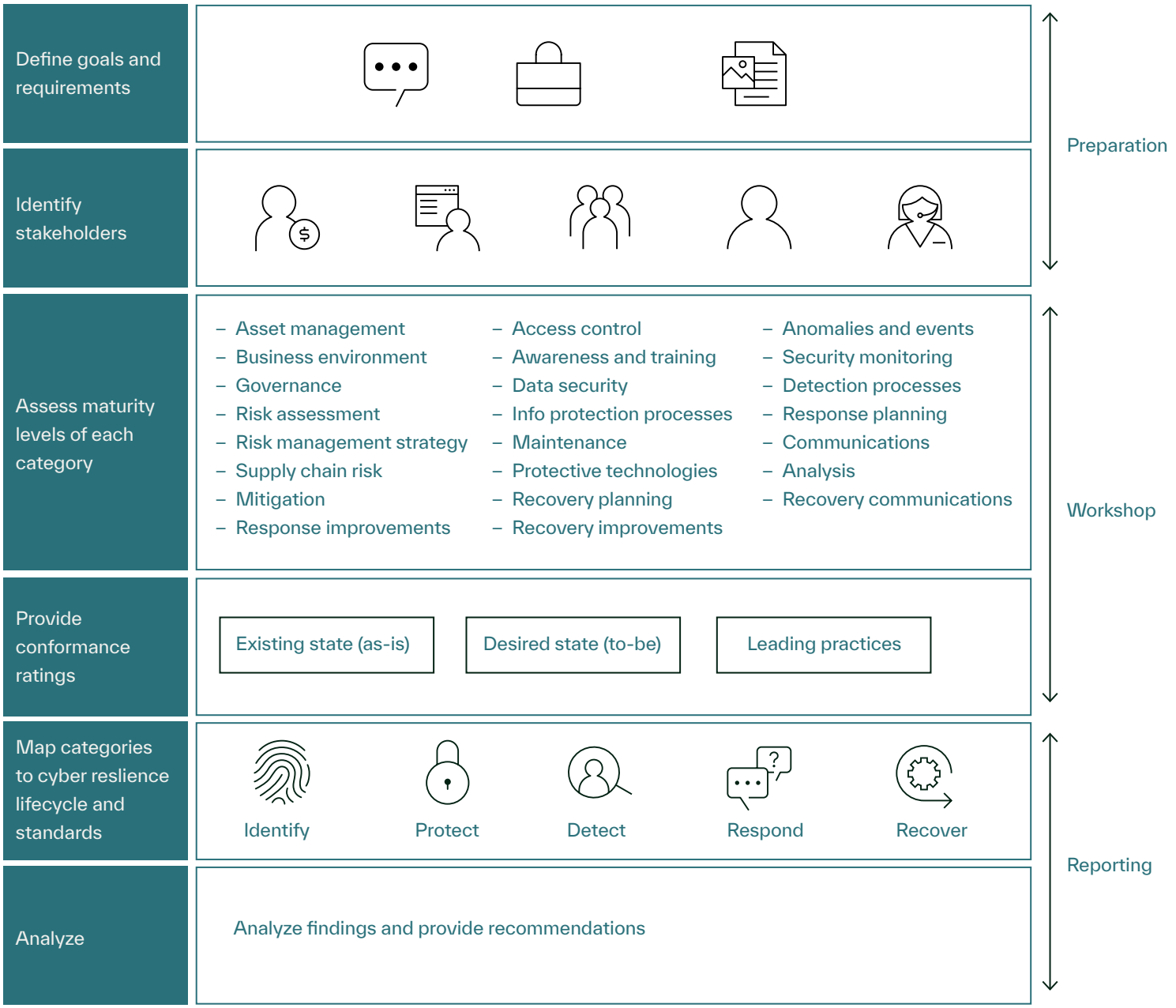


Figure 1. Kyndryl Cyber Resilience Maturity Assessment

Once the assessment is complete, we generate a report that includes:

- Accurate view of current cyber readiness, measured against industry standards
- Comprehensive, controls-based assessment for each stage of the NIST Cybersecurity Framework
- Identification of unknown gaps and vulnerabilities to enable improvements in security and resilience
- Objective ratings against industry best practices
- A high-level, custom roadmap for required actions to improve cyber resilience
- Ready-to-deliver remediation projects and platforms, based on intelligent automation and orchestration to enable rapid delivery of services for effective cyber resilience risk management

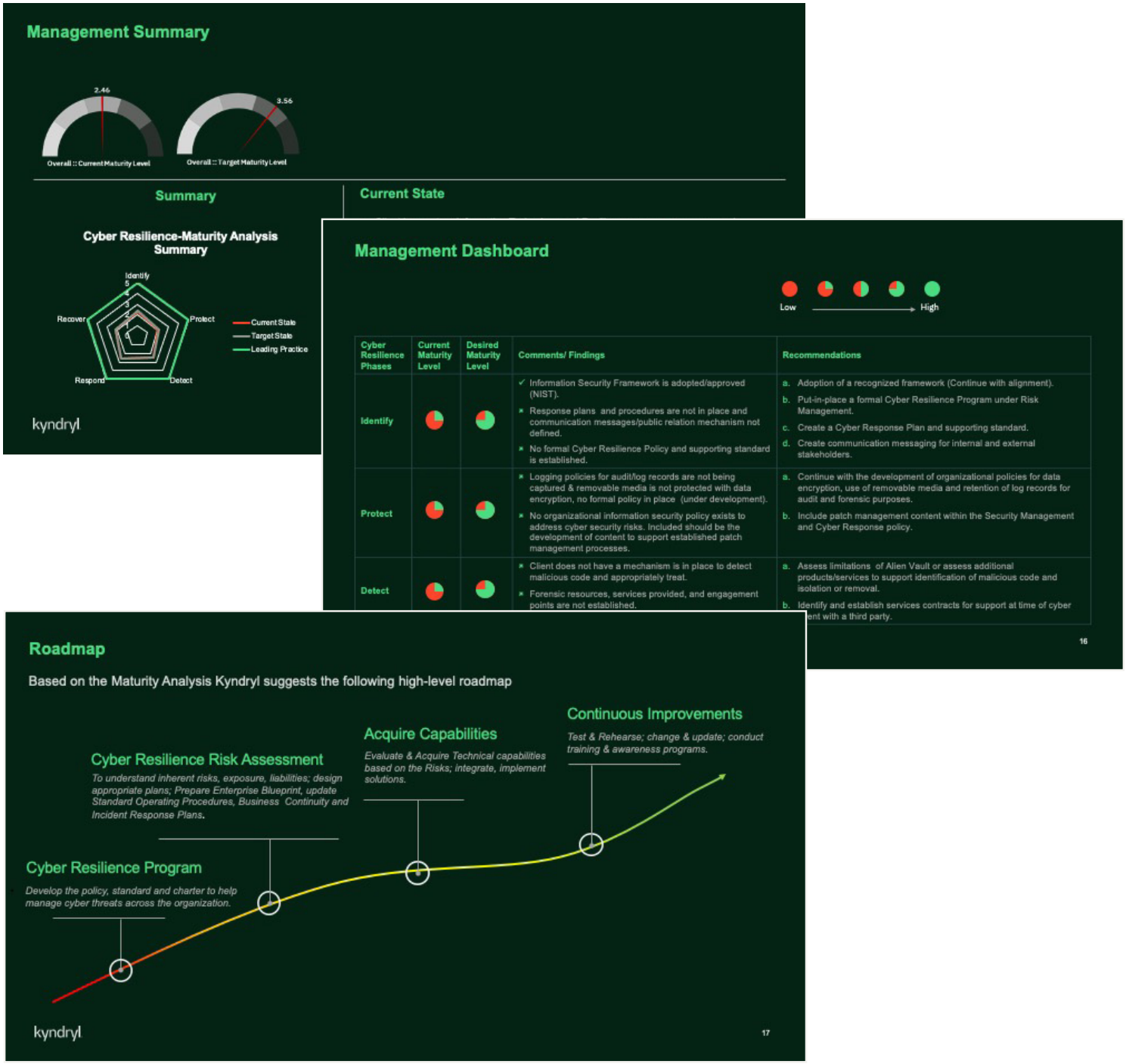


Figure 2. Cyber Resilience Assessment report examples

The engagement process

1. Begin engagement and identify workshop participants
2. Conduct data collection workshop and maturity assessment
3. Analyze findings, conclusions, and recommendations
4. Identify remediation projects
5. Define corresponding roadmap
6. Submit report and present results

Roles we commonly see in our workshops

- VP/Director of IT and Enterprise Architecture
- Security Lead
- CISO
- Director of Applications
- Director IT Operations
- Director Disaster Recovery
- Enterprise Architect, IT Architect
- Security Lead
- Application Lead

Why Kyndryl?

According to World Economic Forum, there is a gap of about three million people in cyber professionals needed worldwide by 2022.[1] At Kyndryl, we understand the pros and cons of various cyber resilience strategy options and can help you navigate and select a strategy that is most capable of meeting your requirements and assumptions.

Skills
With decades of experience, our experts stay current on the latest cyber resilience improvements and continue to apply that knowledge even after the engagement has ended.

Methodology
Our solutions are backed by the collective knowledge we share through intellectual capital assets.

Efficiency
With clear action plans and next steps, our experts save you time identifying which cyber resilience solution is the best one for your business.

Effectiveness
Our services and solutions are designed to be comprehensive, based on accurate requirements assumptions.

Kyndryl has deep expertise in designing, running, and managing the most modern, efficient, and reliable technology infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We are building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side by side with our customers to unlock potential.

For more information

To learn more about the Kyndryl Cyber Resilience Maturity Assessment (CRMA), please contact your Kyndryl representative or Kyndryl Business Partner, or visit www.kyndryl.com

Learn more →

kyndryl

Citations

1 Global Risks Report 2022, World Economic Forum, January 2022

2 Cost of a Data Breach Report 2021, Ponemon Institute, July 2021