TRACE3

OFFERING OVERVIEW

CYBERSECURITY PROGRAM ASSESSMENT

Trace3's Governance, Risk, and Compliance (GRC) team understands that cybersecurity assessments play a crucial role in protecting the organization. By identifying vulnerabilities, assessing risks, and ensuring the overall security posture, these assessments help in safeguarding sensitive data, intellectual property, and infrastructure from potential threats such as cyber-attacks and data breaches.

With combined industry experience and subject matter expertise in Technology, AI, Privacy, Cybersecurity, and Governance, Risk, and Compliance and a deep understanding of industry standards, frameworks, best practices, and technology solutions, Trace's GRC team can not only mitigate risks within the organization but also support strategic decision-making related to cybersecurity investments and improvements.

OVERVIEW

Trace3's Cybersecurity Program Assessment enables informed decision-making and proactive mitigation strategies for safeguarding against adverse events. Our assessment provides a detailed understanding of the organization's security maturity, identifies potential gaps, and offers prioritized recommendations.

OFFERING DETAILS

Trace3 assessment methodology typically consists of the following:

- Review and assess appropriate artifacts (policies, procedures, tooling, etc.) relating to the security domains and control categories
- Leverage information and data points from internal risk and GRC tooling
- Review and map the current controls to the required framework and compliance requirements
- Interview and deep dives across core stakeholders (technology and security-centric groups)
- Interview with the ancillary teams (e.g., human resources, compliance, internal audit)

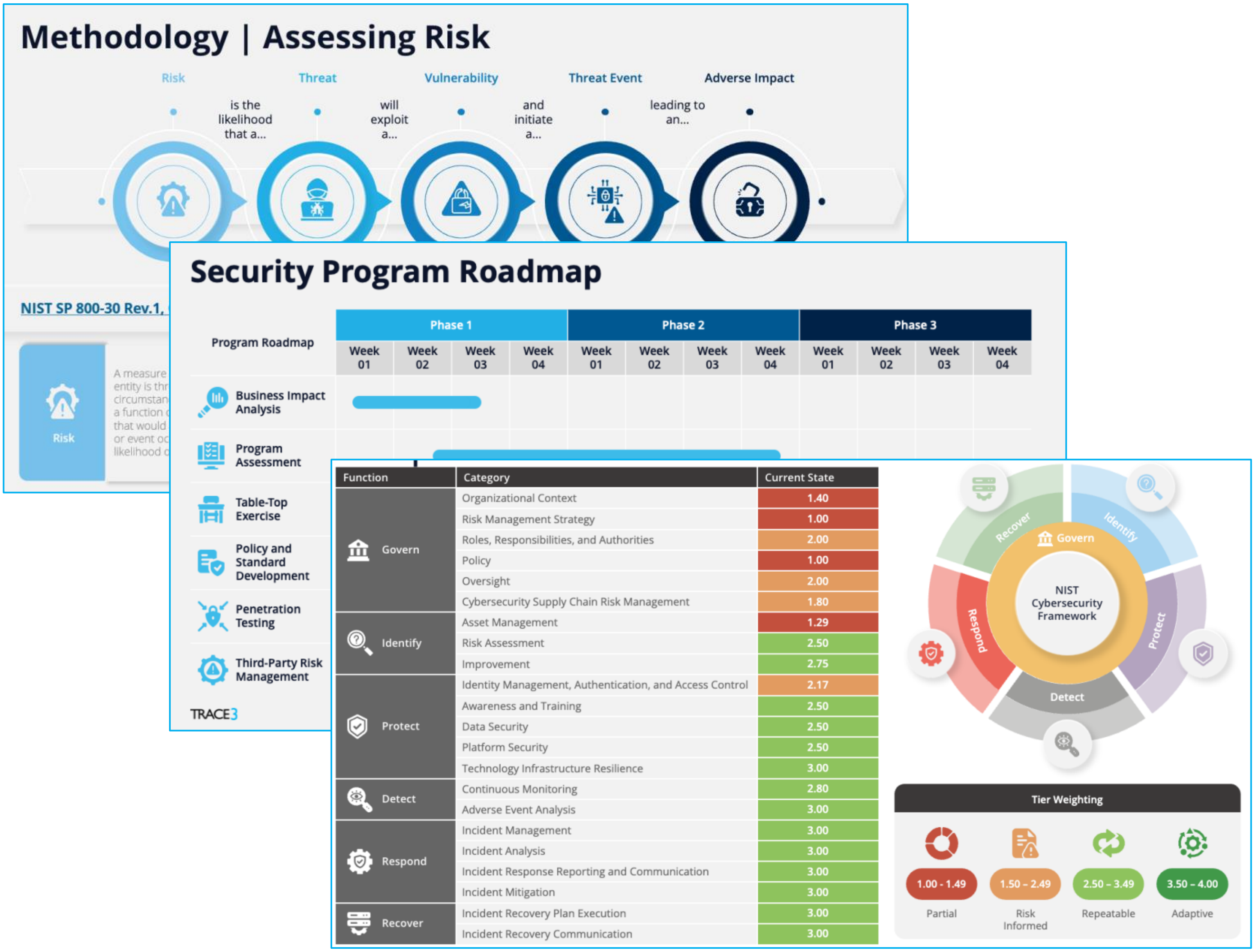
OUTCOMES & DELIVERABLES

Trace3's cybersecurity program assessment produces a detailed and objective understanding of the organization's security program health, compliance gaps, maturity, and risks. Deliverables can consist of the following:

- Cybersecurity Program Assessment Report with Roadmap – Detailed report highlighting strengths and weaknesses, current maturity, target maturity, and remediation recommendations.
- Assessment Worksheet - Technical details and methodology for each framework with controls assessed.
- Executive Summary – Executive-friendly presentation with prioritized remediation recommendations and improvement areas.

TRACE3

CYBERSECURITY PROGRAM ASSESSMENT



Methodology | Assessing Risk

NIST SP 800-30 Rev.1,

A measure
entity is thr
circumstan
a function o
that would
or event oc
likelihood o

Security Program Roadmap

Program Roadmap	Phase 1				Phase 2				Phase 3			
	Week 01	Week 02	Week 03	Week 04	Week 01	Week 02	Week 03	Week 04	Week 01	Week 02	Week 03	Week 04
Business Impact Analysis												
Program Assessment												
Table-Top Exercise												
Policy and Standard Development												
Penetration Testing												
Third-Party Risk Management												

TRACE3

Function	Category	Current State
Govern	Organizational Context	1.40
	Risk Management Strategy	1.00
	Roles, Responsibilities, and Authorities	2.00
	Policy	1.00
	Oversight	2.00
	Cybersecurity Supply Chain Risk Management	1.80
Identify	Asset Management	1.29
	Risk Assessment	2.50
	Improvement	2.75
Protect	Identity Management, Authentication, and Access Control	2.17
	Awareness and Training	2.50
	Data Security	2.50
	Platform Security	2.50
	Technology Infrastructure Resilience	3.00
Detect	Continuous Monitoring	2.80
	Adverse Event Analysis	3.00
Respond	Incident Management	3.00
	Incident Analysis	3.00
	Incident Response Reporting and Communication	3.00
	Incident Mitigation	3.00
Recover	Incident Recovery Plan Execution	3.00
	Incident Recovery Communication	3.00

Tier Weighting

1.00 - 1.49	1.50 - 2.49	2.50 - 3.49	3.50 - 4.00
Partial	Risk Informed	Repeatable	Adaptive

VALUE

Our robust cybersecurity assessment process is pivotal in safeguarding organizational integrity and resilience. By meticulously planning and executing assessments, including comprehensive risk evaluations, vulnerability analyses, and compliance checks, the team ensures a proactive defense against evolving threats. Through clear communication of findings and strategic recommendations, they empower stakeholders to make informed decisions that improve cybersecurity maturity and align with regulatory standards.

TO LEARN MORE, CONTACT YOUR TRACE3 SECURITY REPRESENTATIVE OR VISIT US AT TRACE3.COM.