security®
quotient.

DIFFERENTIATING

GAP & RISK ASSESSMENTS

IN CYBERSECURITY COMPLIANCE

1

Focus areas

Gap assessment identifies differences between current processes and future goals to find areas for improvement.

Risk assessment focuses on finding and evaluating potential risks that could affect the organization’s operations, including its data and systems.

2
Purpose

Gap assessments assess an organization’s readiness to meet specific cybersecurity compliance objectives.

Risk assessments evaluate an organization’s exposure to potential threats and vulnerabilities.

3

When to use

Gap assessments are beneficial during regulatory changes, the introduction of new industry standards, or internal restructuring.

Risk assessments are helpful in scenarios such as the emergence of new threats, operational changes, or when implementing new technologies.

“

Make your workforce cyber resilient

security® quotient.

Singapore | India | Malaysia