



Third-Party & Supplier Cybersecurity Compliance

Protecting Our Business Together

At Maaden, cybersecurity is a shared responsibility. To help protect our systems, data, and operations from cyber threats, all suppliers and third parties are required to comply with Maaden's cybersecurity requirements.

Purpose

The Third-Party & Supplier Cybersecurity Compliance Program ensures that suppliers meet the cybersecurity requirements defined in the Third-Party and Supplier Cybersecurity Standard and maintain appropriate security controls when doing business with Maaden.

Why Compliance Matters

By meeting cybersecurity requirements, suppliers help:

- Protect confidential information and business data.
- Reduce the risk of cyberattacks and security incidents.
- Ensure reliable and uninterrupted business operations.
- Comply with applicable cybersecurity and regulatory requirements.
- Strengthen trust between Maaden and its suppliers.
- Support a secure and resilient supply chain.

What Suppliers Need to Do

When requested by Maaden Cybersecurity, suppliers must:

1. Provide a Valid Cybersecurity Certification
2. Submit at least one of the following certifications: ISO 27001 SOC 2 Type II Aramco CCC , Aramco CCC+2.
3. Follow third-Party and Supplier Cybersecurity Standard , download and review [Third-Party and Supplier Cybersecurity Standard](#)
4. Complete and submit the Maaden Third-Party Cybersecurity Self-Assessment Questionnaire along with any supporting documentation requested by Maaden [Third-Party Cybersecurity Self-Assessment Questionnaire](#)

Frequently Asked Questions

What is the objective of this program?

The objective of the program is to ensure that suppliers and third parties comply with Maaden's cybersecurity requirements, helping to protect Maaden, its suppliers, and the broader supply chain from cybersecurity risks while supporting compliance with applicable regulations and standards.

What happens if my company does not comply?

Failure to meet cybersecurity requirements may result in:

- Increased cybersecurity risks and vulnerabilities.

- Delays in onboarding, qualification, or contract-related activities.

- Potential impact on ongoing business engagement with Maaden.

Increased exposure to operational, financial, and reputational risks.

Compliance helps ensure a secure and trusted business environment for all parties.

Contact Us

For questions regarding supplier cybersecurity compliance, please contact:

Cybersecurity Supplier Relations 

CybersecuritySupplierRelations@maaden.com.sa

Cybersecurity Incident Alerts 

CSIncidentAlerts@maaden.com.sa

TEAM MAADEN



من القلب
HEART



بدون أعذار
NO EXCUSES



الفريق أولاً
TEAM FIRST



النزاهة
INTEGRITY



العزم
DRIVE

