ABS Consulting™
An ABS Group Company

NERC CIP-003-9: Security Management Controls

A Compliance Action Guide for Owners and Operators of Low Impact Bulk Electric System (BES) Cyber Systems

Contents

Overview: Bulk Electric System Cyber Risk in Power and Utilities

For years, the requirements for low impact BES cyber systems were less prescriptive, and the scrutiny less intense. Now, regulators and auditors have recognized that low impact does not translate into low risk. Distributed assets, remote access pathways and third-party vendor connections represent an expanding attack surface to manage, which the North American Energy Corporation Critical Infrastructure Protection, NERC CIP-003-9, specifically addresses.

NERC CIP-003-9 enforcement begins April 1, 2026, for registered entities that own or operate low impact assets connected to the BES that could affect grid reliability.

This compliance resource is for the transmission owners and operators responsible for low impact BES cyber systems who need to act now. Our OT cybersecurity consultants have done the hard part translating what CIP-003-9 requires for your operations by creating a starter framework for compliance. The following insights detail what it takes to build a truly resilient cyber risk management program that can hold up under audit scrutiny and, more importantly, under real-world, battle-tested threat conditions.

Solving for Invisible Risks in BES Cyber Systems

Reported scenarios represent how low impact BES cyber system operations have become a low threshold attack surface. This includes environments where vendors such as original equipment manufacturers (OEMs) and other service providers often maintain remote connections that can invite invisible or unforeseen cyber threats.

For example, a cybersecurity consultant walking the plant floor after a series of productive meetings about new security controls spotted an antenna protruding from a maintenance trailer. Inside was an unpatched Windows XP Embedded HMI, no firewall, with a cellular modem plugged into the back, patched directly into the control system network. The operations team had full monitoring visibility on their known network. **But they had no idea this connection existed.**

When asked by a cybersecurity consultant how often vendors were accessing their BES cyber systems, another utility's plant managers realized they had no idea how much third-party traffic was flowing through the environments they thought they controlled. To manage its vendor supply chain security, the utility asked its turbine control vendor to stop using a direct backdoor connection, instead routing through a managed, and monitored, channel with control room authentication.

NERC has recognized this risk at scale. In its 2019 Supply Chain Risk Assessment, the agency surveyed more than 1,000 registered entities and confirmed that vendor remote access to low impact BES cyber systems is a widespread, largely uncontrolled operational risk. That assessment is the reason CIP-003-9 was updated and as of April 1, 2026, the controls NERC and Federal Energy Regulatory Commission (FERC) require are enforceable.

Notable headlining incidents reinforce the urgency. Colonial Pipeline in 2021 demonstrated how a mixed trust environment with poor visibility between IT and OT boundaries can shut down critical operations. The 2020 SolarWinds attack involved sophisticated malware that was inserted into the software supply chain, ultimately exposing a significant portion of the electric utilities SolarWinds regulated to vulnerability. Reports of non-industrial control system (ICS)-specific malware reaching the ICS environment of a U.S.-based energy company showed that the barrier between enterprise networks and OT may be less resilient than most entities want to admit.

With remote access so widespread across generation, substations and control systems, a new cybersecurity standard was introduced that speaks to the need to secure vendor electronic remote access, specifically in low impact BES cyber systems.

CIP-003-9 Standard Requirements At-A-Glance

The threat model behind the NERC CIP-003-9 standard for supply chain security risk is a coordinated cyberattack. Risk to supply chain security rises if adversaries can exploit vendor access pathways across multiple low impact facilities, scaling a larger attack that could cascade into a regional reliability event.

Why low impact specifically? Before the CIP-003-9 standard was written, low impact assets might be overlooked. Consequently, that means the threshold is low for cyber risk. There are scores of low impact sites across the BES (substations, generation facilities, remote installations), many of which have no inventory requirements and are often the least defended.

The current reality is that risk tolerance is high across the low impact landscape, sometimes by design and sometimes by neglect. NERC's own Supply Chain Risk Assessment conducted in 2019 revealed that a large percentage of low impact sites allows third-party remote access, meaning non-asset-owner vendors often operate outside any enforceable security baseline. That means these entities are often tolerating unknown vendor connections, unmonitored access paths and minimal documentation because their individual sites do not carry enough megawatt impact to command the same attention and budget as medium and high impact programs.

Without a precise understanding of what you have that is susceptible to escalating cyber risk and how to protect these assets, there's no reliable way to evaluate whether your containment efforts are truly effective and where the gaps lie.

Key Terms for CIP-003-9 Compliance

It's important to note that several terms central to understanding the new CIP-003-9 standard requirements are not formally defined by NERC, leaving room for interpretation during audits. Getting your definitions documented according to your own unique operating environment is critical to compliance.

This abbreviated list covers some of the basics to help you get started in assessing your site.

Asset: The word *asset* appears in lowercase throughout the standard and is not included in NERC's glossary as a standalone, defined term. This creates interpretive challenges. The indications from CIP-002 Requirement 1 suggest an asset can be physical (e.g. a generating station, substation or control center) or categorical (e.g. a special protection system or a group of networked devices). Entities should develop a documented methodology for defining what qualifies as an asset in their environment and apply it consistently.

Asset Boundary: Not a NERC-defined term but a practical concept used to describe the boundary around an asset containing low impact BES cyber systems. You must define where your boundary is, whether at the physical perimeter of the facility, at the electronic boundary defined by your firewall or at another defensible point, because Section 6 is aimed at what enters and leaves that boundary. Without a defined asset boundary, you cannot measure or control external routable communications.

BES Cyber System: One or more BES cyber assets logically grouped by a registered entity to perform one or more reliability tasks for a functional entity. These are categorized as high, medium or low impact based on the criteria in CIP-002.

Low Impact BES Cyber System (LIBCS): BES cyber systems that are not categorized as high or medium impact. Low impact does not require a discrete asset inventory, a significant distinction from medium and high programs, but CIP-003-9 now requires documented controls for vendor access to these systems.

Responsible Entity: A NERC-registered entity accountable for complying with applicable NERC CIP Reliability Standards. For CIP-003-9, this includes any entity registered as a generator operator, generator owner, reliability coordinator, transmission operator or transmission owner that has assets containing low impact BES cyber systems. The standard language consistently uses "the Responsible Entity shall," which limits the ability to transfer compliance accountability to third parties.

Vendor: Not defined by NERC, but for CIP purposes, a *vendor* is understood as any entity that provides services to a registered entity supporting reliable BES operation. This includes OEMs, software providers, integrators, contractors, managed service providers, on-site contractors handling day-to-day operations and maintenance and any other third parties providing systems or services. It does not include other NERC-registered entities providing reliability services.

Vendor Electronic Remote Access: Also not explicitly defined by NERC. This could refer to any non-physical method by which a vendor or third-party provider connects to the electronic systems of a NERC-regulated entity. This includes interactive user connections (VPN, remote desktop), system-to-system communications initiated by the vendor from outside the access control boundary, machine-to-machine connections authorized through firewall rules and other remote communication pathways. It is not limited to interactive remote access. Offsite generation health monitoring, automated data collection and any vendor-initiated data flow traversing your asset boundary are in scope.

What CIP-003-9 Requires for Your Operations

Section 6 of Attachment 1, added under Requirement R2, establishes three core obligations for any low impact BES cyber system that allows vendor electronic remote access:

6.1 — Determine that vendor electronic remote access exists. You should have one or more methods to identify where vendors are connecting, how they're connecting and what systems they can reach. This is not a one-time inventory exercise. New skids arrive, cell modems get installed and OEMs open connections during commissioning and never close them. You should have an ongoing process, not a snapshot.

6.2 — Disable vendor electronic remote access when necessary. You should have documented methods to shut down vendor access, not just a "rip cord" approach of physically disconnecting from the network. You should have granular control: the ability to disable access for Vendor A while keeping Vendor B online i.e., the ability to terminate a session mid-stream if operational or security conditions demand it.

6.3 — Detect known or suspected malicious communications during vendor remote access sessions. You should have one or more methods for identifying inbound and outbound malicious communications flowing through vendor access pathways. Manual log review satisfies the letter of the requirement, but it raises immediate follow-up questions: How do you define malicious? What's your repeatable process for making that determination? What happens when you find something? If you can't answer those questions with documented procedures, you are probably going to struggle in an audit.

Additionally, Requirement R1.2.6 now requires you to update your cybersecurity policies to explicitly address vendor electronic remote access security controls. If your policy documents haven't been revised since Section 6 was adopted, that's a gap auditors will identify immediately.

ABS Consulting™
An ABS Group Company

Starter Framework for CIP-003-9 Standard Compliance

If your entity owns, operates or controls low impact BES cyber systems with any form of vendor remote connectivity, you will be required to have documented and implemented controls in place that govern that access.

While ABS Consulting's Industrial Cybersecurity professionals can help tailor cyber risk frameworks according to specific operating environments, these initial steps include some best practices for compliance.

1. Know Where You Stand / Define Your Current State

Actions:

- Validate which BES cyber systems are subject to CIP-003-9.
- Define your asset boundaries.
- Compare your existing CIP policies, roles and controls with the new requirements.
- Determine which assets qualify.
- Walk down your facilities.
- Identify vulnerabilities in governance, low impact controls and vendor access.

Outcome: Prioritized list of gaps and risks to address.

2. Align Policies, Roles and Governance

Actions:

- Update your cybersecurity policy to the CIP-003-9 standard.
- Include vendor electronic remote access security controls under R1.2.6.
- Map policies related to CIP standards.
- Confirm and maintain consistency across your compliance program.

Outcome: Comprehensive, defensible framework that matches how you actually operate.

3. Standardize Low Impact Controls

Actions:

- Define a standard minimum control set for all low impact sites.
- Review all firewall rules, not just vendor-related ones.
- Confirm deny-by-default is in place.
- Clearly document your rules.

Outcome: Proof of compliance across distributed assets.

4. Tighten Vendor and Remote Access

Actions:

- Assess your architecture.
- Document all network paths used for vendor access.
- Include paths you didn't authorize.
- Implement risk-based controls for approving, authenticating, monitoring, logging and disabling access.

Outcome: Lower risk of compromise through vendor channels and stronger audit defensibility.

5. Enhance Awareness and Audit Readiness

Actions:

- Reinforce cybersecurity awareness for personnel and contractors with BES access.
- Document training and awareness activities.
- Prepare by conducting periodic mock audits.
- Make sure operations teams understand what "vendor access" looks like.
- Document when and how to report anomalies.
- Build the culture: Cybersecurity is safety culture.
- Familiarize yourself with the Reliability Standard Audit Worksheets.

Outcome: Better practices and smoother audit interactions.

ABS Consulting – How We Can Help

Strengthen Your Power Operations Resilience

Meeting NERC CIP compliance deadlines demands operational capability as well as technical depth from a trusted advisor who understands both the industrial and regulatory sides of the conversation. ABS Consulting's Industrial Cybersecurity practice brings decades of hands-on experience in NERC CIP compliance, OT cybersecurity and critical infrastructure protection for both the public and private sectors.

Here's how we're helping BES cyber system owners and operators in their efforts to get compliant and stay resilient during this compliance transition through a managed cybersecurity approach.

Strategy, Assessment and Program Design

Understand your current posture and design a sustainable NERC CIP program.

- **NERC CIP Readiness and Gap Assessments** identify compliance gaps across all applicable CIP standards, including BES Cyber System categorization and impact rating.

- **Program and Policy Development** for policies, procedures and governance structures aligned with CIP requirements; these are built to match how your organization actually operates, not how a template assumes you operate.

- **CIP Applicability and Scoping Support** clarifies asset boundaries, Electronic Security Parameters (ESPs) and system categorizations to right-size your compliance efforts.

Managed OT Cybersecurity and Monitoring

Maintain continuous visibility and protection across your OT environment.

- **Network Visibility and Cyber Vulnerability Assessment (CVA)** provides a comprehensive view of your OT networks and vulnerabilities, aligned with NERC CIP cyber requirements.

- **Industrial Cybersecurity Operations Center (ISOC)** helps detect and respond to threats targeting BES cyber systems; on-premises and cloud deployment options allow you to choose the solution architecture that aligns with your security and regulatory requirements.

Implementation, Testing and New Facility Cybersecurity Design

Secure design, deployment and testing for both existing and new facilities.

- **New Facility and Major Upgrade Cybersecurity Design** supports vendor capability reviews, BES Cyber System categorization, risk assessments and NERC CIP applicability reviews for new builds and significant modifications — and factoring in Section 6 requirements from the design phase rather than bolted on after commissioning.

- **System Hardening and ESP Definition** helps define ESPs, implement network segmentation and apply baseline hardening to BES cyber systems.

- **Testing and Commissioning Support** covers Factory Acceptance Tests (FAT), Site Acceptance Tests (SAT), System Integration Testing (SIT) and commissioning activities with documentation that supports NERC CIP evidence requirements.

Supply Chain Cyber Risk and Physical Security Management

Manage risk across your supply chain and physical assets.

- **Supply Chain Cyber Risk Management (CIP-013)** by developing and implementing supplier risk management processes, contractual requirements and monitoring practices to address supply chain threats — the very threat vector that CIP-003-9 was designed to mitigate at the low impact level.

- **Physical Security Risk Management (CIP-014)** by conducting vulnerability analyses for transmission stations, substations and control centers, as well as designing and implementing physical security plans to mitigate identified threats.

Training, Audit Readiness and Continuous Improvement

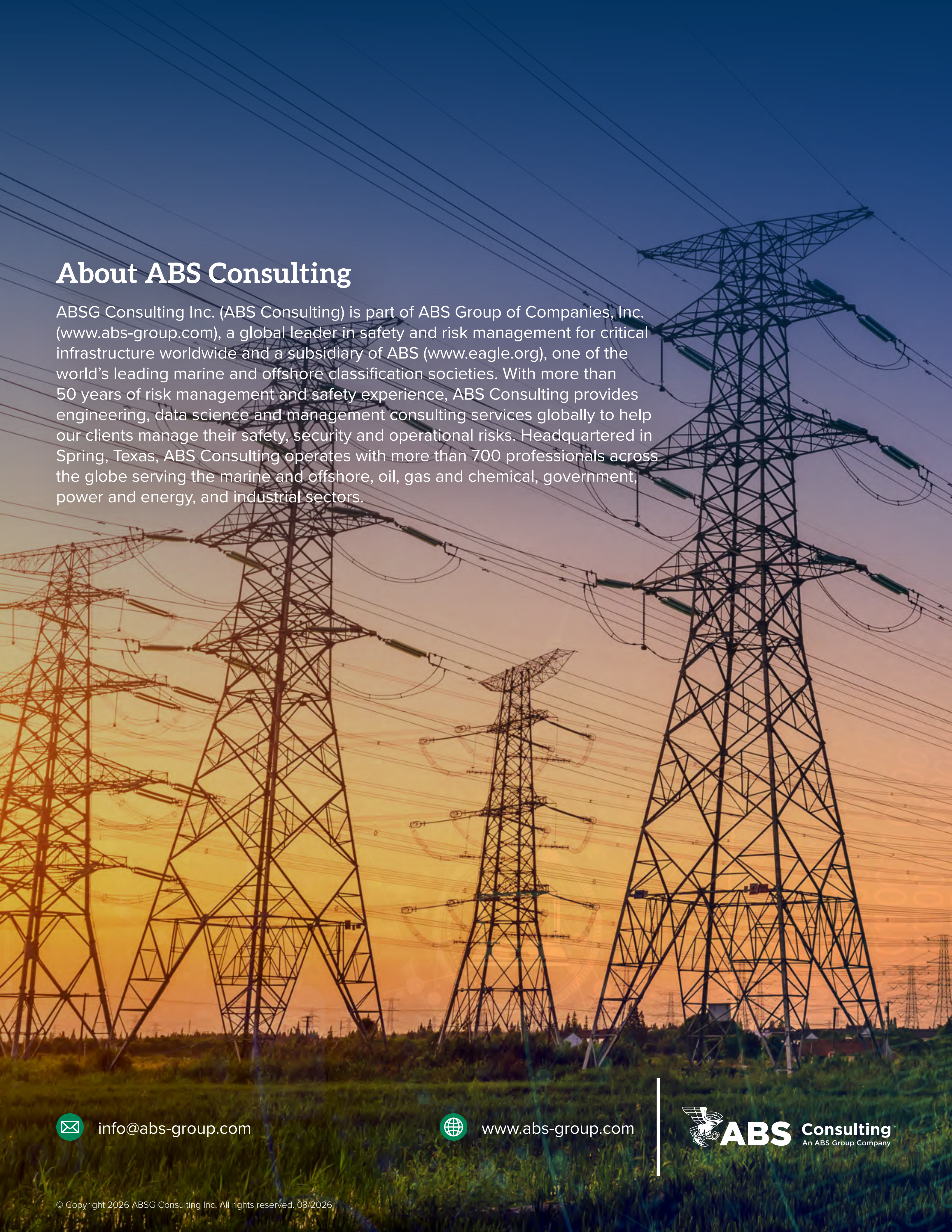
Build internal capabilities and prepare for regulatory scrutiny.

- **NERC CIP Compliance Training Programs** deliver role-based, standard-specific training on-site or virtually to technical, operational and management audiences.

- **Audit Preparation and Evidence Management** supports pre-audit assessments, evidence collection, documentation review and mock audits.

- **Remediation and Lessons Learned** assist in closing findings, improving processes and integrating lessons learned back into your NERC CIP program.

Level up your compliance and request an assessment tailored to your OT environment.



About ABS Consulting

ABSG Consulting Inc. (ABS Consulting) is part of ABS Group of Companies, Inc. (www.abs-group.com), a global leader in safety and risk management for critical infrastructure worldwide and a subsidiary of ABS (www.eagle.org), one of the world's leading marine and offshore classification societies. With more than 50 years of risk management and safety experience, ABS Consulting provides engineering, data science and management consulting services globally to help our clients manage their safety, security and operational risks. Headquartered in Spring, Texas, ABS Consulting operates with more than 700 professionals across the globe serving the marine and offshore, oil, gas and chemical, government, power and energy, and industrial sectors.

✉ info@abs-group.com

🌐 www.abs-group.com

ABS Consulting™
An ABS Group Company