Supply & Support
Service Systems Co. Ltd

Providing industrial automation solutions, services and agency representations to numerous petrochemical facilities and industrial manufacturers since 2008, actively delivering cybersecurity solutions and services since 2015.

Supply and Support Service Systems Co. Ltd (4S) are certified ISA/IEC 62443 Experts offering professional cybersecurity services to conduct cybersecurity vulnerability assessments, risk assessments, cybersecurity program compliance evaluations, and provided of managed services.

A local Saudi organization, building on our legacy expertise in industrial automation, we believe in simplifying the complex; we deliver peace-of-mind to stakeholders by identifying, assessing, and mitigating risk while improving cyber resiliency.

We are expert cyber security advisors, focused on helping businesses protect their brand, customer information, and reputation against the constantly changing cyber threat landscape.

Key Cybersecurity Services

We Offer

- Aramco SACS-002 Compliance Evaluation
- Cybersecurity Risk and Vulnerability Assessments
- Security Posture and Gap Analysis
- Key **Local** Cybersecurity Services
- Countermeasure Designs, Gap Closure
- Programs, Policy and Procedure Development
- Security Program Consultation

Vulnerability Assessments	Penetration Testing	Program Development (Policy and Process Creation)
Managed Security Awareness Training and Phishing Emails	Managed Security Operations Center (SOC)	Program Assessments (SACS-002, ECC:2018, ISA62443, CIS, NIST, ISO)

4scompanyco

National Cybersecurity Authority (NCA) ECC:2018 Essential Cybersecurity Controls

These cybersecurity controls are linked to related national and international law and regulatory requirements. Set the minimum cybersecurity requirements for information and technology assets in organizations. These requirements are based on industry leading practices which will help organizations minimize the cybersecurity risks that originate from internal and external threats. The following key objectives must be focused on in order to protect the organization's information and technology assets:

- Confidentiality
- Integrity
- Availability

These controls take into consideration the following four main cybersecurity pillars:

- Strategy
- People
- Processes
- Technology

Third Party Cybersecurity Standard (TPCS) sets forth the minimum Cybersecurity requirements for Saudi Aramco Third Parties to protect Saudi Aramco from possible cyber threats and strengthen Third Parties' security posture. This Standard applies to All Third Parties engaging with Saudi Aramco through contractual agreements.

SACS-002

National Cybersecurity Authority (NCA) CCC:2020 Cloud Cybersecurity Controls

An extension to the ECC; to achieve higher levels of national cybersecurity goals by focusing on cloud computing services from the perspective of Cloud Service Providers (CSPs) and Cloud Service Tenants (CSTs). Also, the CCC aim to set the minimum requirements for cybersecurity of cloud computing, for both CSPs and CSTs, to contribute to enable the CSPs and the CSTs to provide and use secure cloud computing services and mitigating cyber risks against them.

The cybersecurity of cloud computing services, for both CSPs and CSTs, must be able to protect the confidentiality, integrity and availability of the data and information within the cloud environment. To that aim, CCC take into consideration the following four main cybersecurity pillars:

- Strategy
- People
- Procedures
- Technology

4S Supply & Support Service Systems Co. Ltd

NIST800.53

National Institute of Standards and Technology Cybersecurity Framework CSF presents the security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations.

The NIST SP 800-53 provides a catalog of controls that support the development of secure and resilient federal information systems.

These controls are the operational, technical, and management safeguards used by information systems to maintain the integrity, confidentiality, and security of federal information systems.

ISA/IEC6244

- Conduct cybersecurity vulnerability assessments/evaluations and risk assessments
- Determine current organizations cybersecurity posture
- Map assets to Zones and Conduits
- Consider existing countermeasures in assessments and risk ranking
- Identify risks, ranking according to an organizations risk tolerance
- Develop a cybersecurity requirements specification (CRS)
- Quantify and catalog unmitigated cybersecurity risks within an organization
- Determine where business resources are required to mitigate the highest risks
- Provide cost effective industrial cybersecurity solutions

ISO27001

It is a specification for an information security management system (ISMS) that is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

ISO27001 does not mandate specific information security controls, but it provides a checklist of controls that should be considered in the accompanying code of practice.