Loft Company

Report: IEC 62443
Loft Company IEC 62443 + Core Questions + Training + Optional Advanced + Audit Verification + Supply Chain

v1.0.2026-11-14

Created: 2026-11-13 23:39
Closed: 2026-11-13 23:54
Answered: 99%

Compliance Score:

98%

(573/582)

Almost all requirements met; very low risk.
A very little uncertainty due to small fraction of measuring points not addressed.

Top Risks:

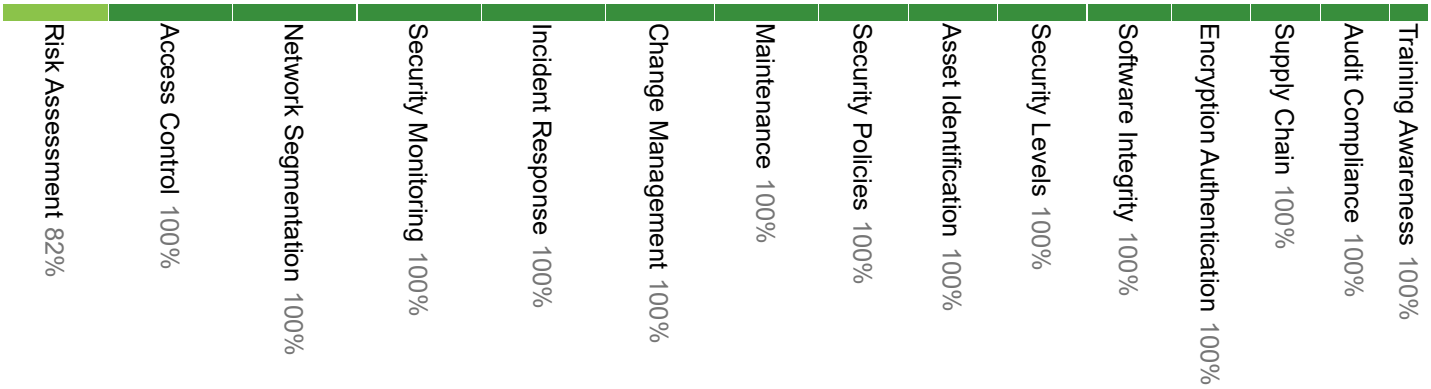
Risk Assessment – 25% Compliant
1. Are relevant cyber and physical threats to each IACS asset identified and documented?
Unanswered
Criticality: High

Risk Assessment – 25% Compliant
2. Has the organization defined and documented a risk assessment process specific to IACS?
Partially
Criticality: High

Compliance By Section:

Risk Assessment	82%	Security Policies	100%	Asset Identification	100%
Access Control	100%	Security Levels	100%		
Security Monitoring	100%	Change Management	100%	Network Segmentation	100%
Incident Response	100%	Training Awareness	100%	Maintenance	100%
Encryption Authentication	100%			Supply Chain	100%
		Software Integrity	100%	Audit Compliance	100%

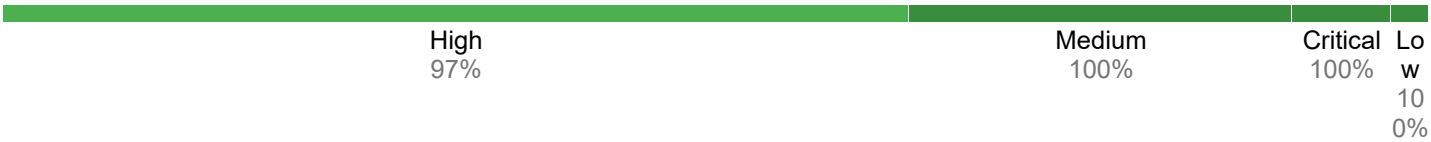
Sections, Weighted



Compliance by Criticality

Criticality	Measurement Points	Yes	Partially	No	Missing	Compliance %
Critical	4	4	0	0	0	100 %
High	63	61	1	0	1	97 %
Medium	39	39	0	0	0	100 %
Low	4	4	0	0	0	100 %
Total	**110**	**108**	**1**	**0**	**1**	**98 %**

Criticalities, Weighted



Access Control

Defines requirements for managing user and system access to IACS components, including authentication, authorization, and account management.

Does a formal access control policy exist for IACS access management? **Yes**

Criticality: High

Are strong authentication mechanisms required and enforced for all user and system access to critical IACS components? **Yes**

Criticality: Critical

Are privileged accounts strictly controlled, logged, and reviewed regularly? **Yes**

Criticality: High

<< The rest of this section is left out in this sample/preview >>

Recommendations:

Risk Assessment

Focuses on identifying and evaluating risks to industrial automation and control systems (IACS), including threats, vulnerabilities, and potential impacts.

1. Establish and document a formal risk assessment process specific to IACS to identify, evaluate, and mitigate risks.

Criticality: High

2. Identify and document all relevant cyber and physical threats to each IACS asset.

Criticality: High

Compliance Score: 98% (573/582)
Almost all requirements met; very low risk.