Loft Company

Report: NIST CSF
Loft Company NIST CSF + Core Questions + Process Maturity + Audit + Critical Infrastructure

v1.0.2026-11-14

Created: 2026-11-14 00:10
Closed: 2026-11-14 00:25
Answered: 99%

Compliance Score:

98%

(493/500)

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

Top Risks:

Identify – 30% Compliant
1. Are risk assessments performed periodically to identify threats and vulnerabilities? Unanswered
Criticality: Medium
2. Are all organizational assets inventoried and classified according to risk and criticality? Partially
Criticality: High

Compliance By Section:

Identify	92%	Protect	100%	Detect	100%
Respond	100%	Recover	100%		

Sections, Weighted

Compliance by Criticality

Criticality	Measurement Points	Yes	Partially	No	Missing	Compliance %
High	50	49	1	0	0	99 %
Medium	50	49	0	0	1	98 %
Total	**100**	**98**	**1**	**0**	**1**	**98 %**

Criticalities, Weighted

Detect

Detect establishes the processes and activities to identify cybersecurity events in a timely manner, including monitoring and anomaly detection.

Are anomalies and security events detected through automated monitoring systems? **Yes**

Criticality: High

Are security logs collected, correlated, and reviewed regularly for unusual activity? **Yes**

Criticality: Medium

Are monitoring tools deployed for industrial control systems to detect security events? **Yes**

Criticality: High

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

Recommendations:

Identify

Identify focuses on understanding the organization's assets, risks, and environment to develop an effective cybersecurity strategy and risk management approach.

1. Inventory and classify all organizational assets according to risk and criticality.

Criticality: High

2. Perform periodic risk assessments to identify threats and vulnerabilities.

Criticality: Medium

Compliance Score: 98% (493/500)
Almost all requirements met; very low risk.