Loft Company

Report: CRA

Loft Company CRA + Core Questions + Secure Development + Requirements effective from 11 September 2026 + Requirements effective from 11 December 2027 + Advanced + Supply Chain Extended + Audit + Core Security + Release Controls + Incident Handling + Lifecycle End + Assurance

v1.0.2026-11-14

Created: 2026-11-13 23:12
Closed: 2026-11-13 23:27
Answered: 99%

Compliance Score:

98%

(489/498)

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

Top Risks:

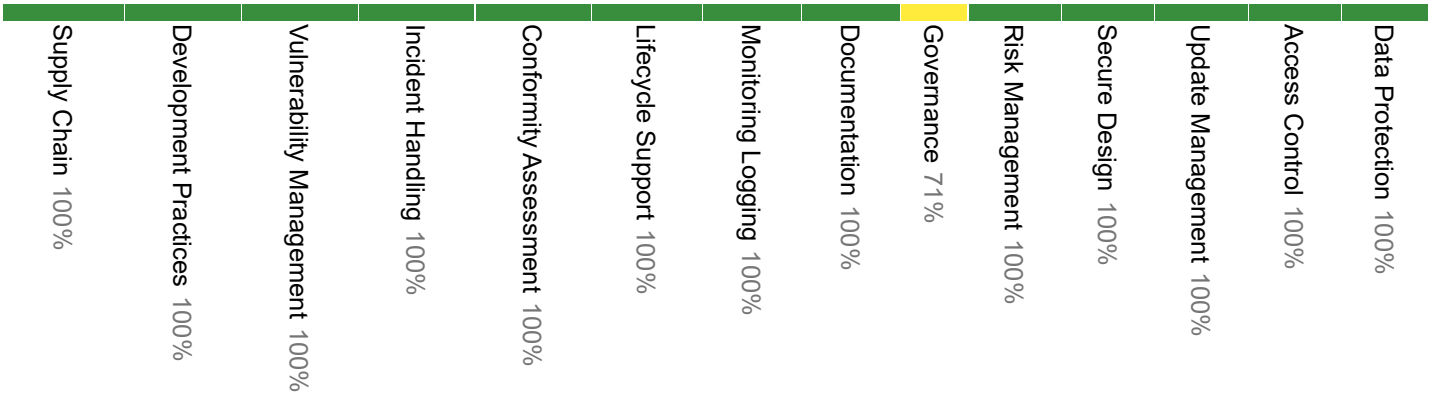
Governance – 25% Compliant
1. Are cybersecurity policies maintained and updated for all in-scope products? Unanswered
Criticality: High
2. Does the organization define and maintain clear responsibility for CRA cybersecurity compliance? Partially
Criticality: High

Report: CRA
Loft Company CRA + Core Questions + Secure Development + Requirements effective from 11 September 2026 + Requirements effective from 11 December 2027 + Advanced + Supply Chain Extended + Audit + Core Security + Release Controls + Incident Handling + Lifecycle End + Assurance
v1.0.2026-11-14

Compliance By Section:

Governance	71%	Risk Management	100%	Secure Design	100%
Development Practices	100%	Supply Chain	100%	Vulnerability Management	100%
Incident Handling	100%	Update Management	100%	Data Protection	100%
Access Control	100%	Monitoring Logging	100%	Documentation	100%
Conformity Assessment	100%	Lifecycle Support	100%		

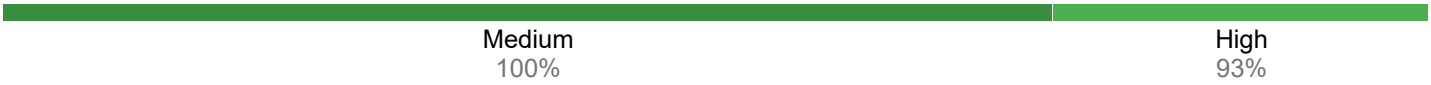
Sections, Weighted



Compliance by Criticality

Criticality	Measurement Points	Yes	Partially	No	Missing	Compliance %
High	23	21	1	0	1	93 %
Medium	90	90	0	0	0	100 %
Total	**113**	**111**	**1**	**0**	**1**	**98 %**

Criticalities, Weighted



Access Control

Authentication, authorization, and privilege management mechanisms.

Are authentication mechanisms enforced? **Yes**

Criticality: High

Is least privilege enforced? **Yes**

Criticality: High

Are privileges reviewed? **Yes**

Criticality: Medium

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

Recommendations:

Governance

Organizational governance, accountability, and management responsibility for product cybersecurity and compliance.

1. Establish and formally assign responsibility for CRA cybersecurity compliance, including documented ownership, escalation paths, and accountability across relevant roles.

Criticality: High

2. Establish, maintain, and regularly update cybersecurity policies covering all in-scope products, ensuring alignment with regulatory and internal requirements.

Criticality: High

Compliance Score: 98% (489/498)
Almost all requirements met; very low risk.