LEXCLAW

Framework Gap Analysis Report

NIST CSF 2.0 vs **ISO 27001:2022**

Generated: March 17, 2026

Executive Summary

45

Total Controls Analyzed

0%

Overall Coverage

0

Fully Covered

0

Partial Coverage

45

Gaps Identified

45

Control Mappings

Control Mapping Detail

NIST CSF 2.0 Control	Title	ISO 27001:2022 Control	Mapped To	Relationship	Confidence
DE.AE-02	Event Analysis	*No mapping*	—	none	—
ID.AM-03	Network Representation	*No mapping*	—	none	—
DE.AE-04	Impact Estimation	*No mapping*	—	none	—
GV.OC-03	Legal Requirements	*No mapping*	—	none	—
RC.RP-03	Restoration Integrity	*No mapping*	—	none	—
PR.AA-04	Identity Assertions	*No mapping*	—	none	—
ID.AM-04	External Systems	*No mapping*	—	none	—
RC.RP-04	Critical Services Restoration	*No mapping*	—	none	—
GV.OC-04	Critical Objectives	*No mapping*	—	none	—
DE.AE-06	Incident Alerting	*No mapping*	—	none	—
RS.MA-05	Incident Termination	*No mapping*	—	none	—
RC.RP-05	Recovery Completion	*No mapping*	—	none	—
DE.AE-07	Cyber Intelligence	*No mapping*	—	none	—
GV.OC-05	Outcomes and Dependencies	*No mapping*	—	none	—
ID.AM-07	Data Inventory	*No mapping*	—	none	—
RS.AN-03	Analysis Tasks	*No mapping*	—	none	—
DE.AE-08	Incident Declaration	*No mapping*	—	none	—
RC.RP-06	Incident Closure	*No mapping*	—	none	—
RS.AN-06	Actions Cataloged	*No mapping*	—	none	—
RC.CO-03	Recovery Communications	*No mapping*	—	none	—
RS.AN-07	Incident Scope	*No mapping*	—	none	—

NIST CSF 2.0 Control	Title	ISO 27001:2022 Control	Mapped To	Relationship	Confidence
DE.CM-02	Physical Environment Monitoring	*No mapping*	—	none	—
RC.CO-04	Public Communications	*No mapping*	—	none	—
GV.RM-03	Cybersecurity Risk Management	*No mapping*	—	none	—
ID.RA-02	Cyber Threat Intelligence	*No mapping*	—	none	—
DE.CM-03	Personnel Activity Monitoring	*No mapping*	—	none	—
GV.RM-06	Policies and Procedures	*No mapping*	—	none	—
ID.RA-03	Threat Identification	*No mapping*	—	none	—
RS.AN-08	Notifications	*No mapping*	—	none	—
DE.CM-06	External Service Provider Monitoring	*No mapping*	—	none	—
PR.DS-10	Data-in-Use Protection	*No mapping*	—	none	—
ID.RA-05	Risk Assessment	*No mapping*	—	none	—
RS.CO-02	Internal Reporting	*No mapping*	—	none	—
GV.RM-07	Cybersecurity Program	*No mapping*	—	none	—
PR.IR-01	Network Integrity	*No mapping*	—	none	—
DE.CM-09	Computing Hardware and Software Monitoring	*No mapping*	—	none	—
ID.RA-06	Risk Response	*No mapping*	—	none	—
RS.CO-03	External Reporting	*No mapping*	—	none	—
ID.IM-01	Improvement Plan	*No mapping*	—	none	—
GV.RR-02	Cybersecurity Roles	*No mapping*	—	none	—
RS.MI-01	Incident Containment	*No mapping*	—	none	—
PR.IR-02	Secure Development	*No mapping*	—	none	—

NIST CSF 2.0 Control	Title	ISO 27001:2022 Control	Mapped To	Relationship	Confidence
RS.MI-02	Incident Eradication	*No mapping*	—	**none**	—
PR.IR-03	Hardware and Software Integrity	*No mapping*	—	**none**	—
PR.IR-04	Adequate Capacity	*No mapping*	—	**none**	—

Recommendations

Based on the gap analysis, the following priority actions are recommended:

- **Address Critical Gaps:** Focus remediation efforts on the 45 control areas with no coverage in ISO 27001:2022.
- **Strengthen Partial Coverage:** Review the 0 partially covered controls to determine if additional implementation is required.
- **Leverage Existing Controls:** The 0 fully covered controls represent existing investments that satisfy both frameworks.
- **Prioritize by Risk:** Rank gap remediation by the risk impact and regulatory consequence of each uncovered control area.

Generated by LexClaw — Cybersecurity Legal Intelligence Platform | March 17, 2026 | **Disclaimer:** This report is for informational purposes only and does not constitute legal advice. Always consult qualified legal counsel for compliance decisions.