Compliance readiness — Acme Manufacturing (Demo)

Acme Manufacturing (Demo) · Period 2026-10-09 to 2026-11-08 · Generated 2026-11-08 15:30 UTC by superadmin@acme-demo.test

How to read this report

SecOwl measured each control below from live data on this installation. "met" and "partial" rows cite the evidence; "manual" rows need documents or records kept outside SecOwl. This is readiness evidence for your auditor, not a certification.

Summary

Framework	Met	Partial	Not met	Manual
ISO/IEC 27001:2022 Annex A	10	11	2	2
SOC 2 — Trust Services Criteria (2017)	4	8	2	0
NIST Cybersecurity Framework 2.0	6	9	4	0
NIST SP 800-207 Zero Trust tenets	3	4	0	0
India DPDP Act 2023 / DPDP Rules 2025 (security obligations)	4	2	1	0
CERT-In Directions (28 April 2022)	2	0	1	1
RBI Cyber Security Framework / IT Governance (2023) — baseline controls	2	7	2	1

ISO/IEC 27001:2022 Annex A

Control	Requirement	Status	SecOwl evidence
A.5.15	Access control	partial	70 per-request zero-trust decisions in 30 days (allow 29, deny 20, quarantine 1, step_up 20). 3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person.
A.5.16	Identity management	partial	1/1 guests have a sponsor and an end date (limit 30 days). 1 Super Admins (2–5 recommended: break-glass without over-privilege); 3 privileged accounts in total.
A.5.17	Authentication information	partial	20% of 10 active accounts have a second factor; 0 passkeys registered. Account locks after 5 failed sign-ins for 15 min; brute-force and password-spray detections active.
A.5.18	Access rights (provision, review, removal)	met	0 access requests decided in 90 days; 0 pending longer than 7 days; 0 grants without an end date.
A.5.19	Information security in supplier relationships	met	Vendor access only through signed, Super-Admin-approved, time-bound support windows (1 requested, 0 active now); every request audited. 0 signed adapters imported, 0 enabled with approved scopes; disabled by default.
A.5.24	Incident management planning and preparation	met	2 response playbooks enabled; risky steps need human approval.
A.5.25	Assessment and decision on information security events	met	Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days.
A.5.26	Response to information security incidents	met	1 incidents in 12 months, 0 closed; timelines and AI summaries recorded. Device isolation available to Security Admins and playbooks; 0 isolations completed.
A.5.28	Collection of evidence	met	Hash-chained audit ledger: 36 entries verified, chain intact.
A.5.30	ICT readiness for business continuity	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.

Control	Requirement	Status	SecOwl evidence
A.8.1	User endpoint devices	partial	6 managed devices enrolled, 5 reporting now; software inventory from 4. 2/6 devices compliant (33%). 5/6 devices report full-disk encryption.
A.8.2	Privileged access rights	partial	0/3 privileged accounts use an authenticator app or passkey. 1 Super Admins (2–5 recommended: break-glass without over-privilege); 3 privileged accounts in total.
A.8.5	Secure authentication	partial	20% of 10 active accounts have a second factor; 0 passkeys registered. Idle timeout 30 min, maximum session 12 h, step-up for sensitive admin actions on (10 min).
A.8.7	Protection against malware	partial	5/6 devices report active antivirus; malware detections raise alerts.
A.8.8	Management of technical vulnerabilities	partial	5/6 devices have recent OS updates.
A.8.13	Information backup	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.
A.8.15	Logging	met	Hash-chained audit ledger: 36 entries verified, chain intact. Retention: sign-ins 365 d, device events 180 d, access log 365 d (CERT-In: 180 days, kept in India on this server).
A.8.16	Monitoring activities	partial	Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days. SIEM forwarding not enabled (SecOwl alerts and audit remain available locally). Endpoint security events collected (cleared logs, new admins/accounts/services, failed logons, malware).
A.8.17	Clock synchronisation	met	0 devices currently out of time sync (agent rejects > 4 min skew at enrolment; server flags > 5 min).
A.8.19	Installation of software on operational systems	met	Software policy "blocklist" with 1 rules; unapproved installs raise alerts.
A.8.20	Networks security	partial	3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person. Internet egress mode "allowlist"; outbound connections checked against the allow-list.
A.8.22	Segregation of networks	met	Trusted company networks defined: 10.20.0.0/16. Device isolation available to Security Admins and playbooks; 0 isolations completed.
A.8.24	Use of cryptography	partial	Console address http://localhost:5077; agents sign every request (HMAC) and verify server commands (Ed25519). 5/6 devices report full-disk encryption.
A.5.1	Policies for information security	manual	Show: approved information security policy document (outside SecOwl)
A.6.3	Information security awareness, education and training	manual	Show: training records (outside SecOwl)

SOC 2 — Trust Services Criteria (2017)

Control	Requirement	Status	SecOwl evidence
CC6.1	Logical access security over protected information assets	partial	70 per-request zero-trust decisions in 30 days (allow 29, deny 20, quarantine 1, step_up 20). 20% of 10 active accounts have a second factor; 0 passkeys registered. 3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person.
CC6.2	User registration and de-registration	met	1/1 guests have a sponsor and an end date (limit 30 days). 0 access requests decided in 90 days; 0 pending longer than 7 days; 0 grants without an end date.

Control	Requirement	Status	SecOwl evidence
CC6.3	Role-based access; removal of access	partial	0 access requests decided in 90 days; 0 pending longer than 7 days; 0 grants without an end date. 1 Super Admins (2–5 recommended: break-glass without over-privilege); 3 privileged accounts in total.
CC6.6	Boundary protection against threats from outside	partial	3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person. Internet egress mode "allowlist"; outbound connections checked against the allow-list. Trusted company networks defined: 10.20.0.0/16.
CC6.7	Restriction of transmission and movement of information	partial	Console address http://localhost:5077; agents sign every request (HMAC) and verify server commands (Ed25519). Internet egress mode "allowlist"; outbound connections checked against the allow-list.
CC6.8	Prevention or detection of unauthorised or malicious software	partial	5/6 devices report active antivirus; malware detections raise alerts. Software policy "blocklist" with 1 rules; unapproved installs raise alerts.
CC7.1	Detection of configuration changes and vulnerabilities	partial	5/6 devices have recent OS updates. 2/6 devices compliant (33%). Endpoint security events collected (cleared logs, new admins/accounts/services, failed logons, malware).
CC7.2	Monitoring of system components for anomalies	partial	Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days. SIEM forwarding not enabled (SecOwl alerts and audit remain available locally).
CC7.3	Evaluation of security events	met	1 incidents in 12 months, 0 closed; timelines and AI summaries recorded.
CC7.4	Incident response	met	2 response playbooks enabled; risky steps need human approval. Device isolation available to Security Admins and playbooks; 0 isolations completed.
CC7.5	Recovery from incidents	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.
CC8.1	Change management	partial	Built-in policy only; policy changes require four-eyes approval when made. 3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person.
CC9.2	Vendor and business partner risk	met	Vendor access only through signed, Super-Admin-approved, time-bound support windows (1 requested, 0 active now); every request audited. 0 signed adapters imported, 0 enabled with approved scopes; disabled by default.
A1.2	Backup and recovery infrastructure	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.

NIST Cybersecurity Framework 2.0

Control	Requirement	Status	SecOwl evidence
GV.SC-07	Supplier risks understood, recorded and monitored	met	Vendor access only through signed, Super-Admin-approved, time-bound support windows (1 requested, 0 active now); every request audited.
ID.AM-01	Inventories of hardware are maintained	partial	6 managed devices enrolled, 5 reporting now; software inventory from 4.
ID.AM-02	Inventories of software and services are maintained	partial	6 managed devices enrolled, 5 reporting now; software inventory from 4. Software policy "blocklist" with 1 rules; unapproved installs raise alerts.
PR.AA-01	Identities and credentials are managed	partial	1/1 guests have a sponsor and an end date (limit 30 days). 1 Super Admins (2–5 recommended: break-glass without over-privilege); 3 privileged accounts in total.

Control	Requirement	Status	SecOwl evidence
PR.AA-03	Users, services and hardware are authenticated	not met	20% of 10 active accounts have a second factor; 0 passkeys registered. Console address http://localhost:5077; agents sign every request (HMAC) and verify server commands (Ed25519).
PR.AA-05	Access permissions are managed with least privilege	met	0 access requests decided in 90 days; 0 pending longer than 7 days; 0 grants without an end date. 70 per-request zero-trust decisions in 30 days (allow 29, deny 20, quarantine 1, step_up 20).
PR.DS-01	Data-at-rest is protected	partial	5/6 devices report full-disk encryption.
PR.DS-02	Data-in-transit is protected	not met	Console address http://localhost:5077; agents sign every request (HMAC) and verify server commands (Ed25519).
PR.DS-11	Backups are created, protected, maintained and tested	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.
PR.PS-02	Software is maintained, replaced and removed	partial	5/6 devices have recent OS updates. Software policy "blocklist" with 1 rules; unapproved installs raise alerts.
PR.PS-04	Log records are generated and made available	partial	Hash-chained audit ledger: 36 entries verified, chain intact. SIEM forwarding not enabled (SecOwl alerts and audit remain available locally).
PR.IR-01	Networks are protected from unauthorised access	partial	3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person. Trusted company networks defined: 10.20.0.0/16.
DE.CM-01	Networks and network services are monitored	met	Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days.
DE.CM-09	Computing hardware, software and their data are monitored	partial	Endpoint security events collected (cleared logs, new admins/accounts/services, failed logons, malware). 5/6 devices report active antivirus; malware detections raise alerts.
DE.AE-02	Adverse events are analysed	met	Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days. 1 incidents in 12 months, 0 closed; timelines and AI summaries recorded.
RS.MA-01	Incident response plan is executed	met	2 response playbooks enabled; risky steps need human approval.
RS.MI-01	Incidents are contained	met	Device isolation available to Security Admins and playbooks; 0 isolations completed.
RS.CO-02	Internal and external stakeholders are notified	partial	0/1 reportable incidents reported to CERT-In within 6 hours. No personal-data breaches recorded; 72-hour Board report clock ready.
RC.RP-01	Recovery portion of the plan is executed	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.

NIST SP 800-207 Zero Trust tenets

Control	Requirement	Status	SecOwl evidence
ZT-1	All data sources and computing services are resources	partial	3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person.
ZT-2	All communication is secured regardless of network location	partial	Console address http://localhost:5077; agents sign every request (HMAC) and verify server commands (Ed25519). Trusted company networks defined: 10.20.0.0/16.
ZT-3	Access is granted per session	met	70 per-request zero-trust decisions in 30 days (allow 29, deny 20, quarantine 1, step_up 20).

Control	Requirement	Status	SecOwl evidence
ZT-4	Access is determined by dynamic policy (identity, device, behaviour)	met	Built-in policy only; policy changes require four-eyes approval when made. 70 per-request zero-trust decisions in 30 days (allow 29, deny 20, quarantine 1, step_up 20).
ZT-5	The integrity and posture of all assets is monitored	partial	2/6 devices compliant (33%). Endpoint security events collected (cleared logs, new admins/accounts/services, failed logons, malware).
ZT-6	Authentication and authorisation are dynamic and strictly enforced	partial	20% of 10 active accounts have a second factor; 0 passkeys registered. Idle timeout 30 min, maximum session 12 h, step-up for sensitive admin actions on (10 min).
ZT-7	Information is collected to improve security posture	met	Hash-chained audit ledger: 36 entries verified, chain intact. Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days.

India DPDP Act 2023 / DPDP Rules 2025 (security obligations)

Control	Requirement	Status	SecOwl evidence
S.8(5) / R.6(a)	Reasonable security safeguards: encryption, obfuscation or masking	partial	5/6 devices report full-disk encryption. Console address http://localhost:5077; agents sign every request (HMAC) and verify server commands (Ed25519).
R.6(b)	Access control to computer resources processing personal data	partial	70 per-request zero-trust decisions in 30 days (allow 29, deny 20, quarantine 1, step_up 20). 20% of 10 active accounts have a second factor; 0 passkeys registered.
R.6(c)	Visibility of access through logs, monitoring and review	met	Hash-chained audit ledger: 36 entries verified, chain intact. Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days.
R.6(d)	Continued processing on compromise (backups)	not met	Last good backup never; encrypted no; daily at 2:00, 14 kept.
R.6(e)	Logs retained for at least one year	met	Access log 365 d and sign-ins 365 d (DPDP Rules: at least one year).
R.6(f)	Safeguards in contracts with Data Processors	met	Vendor access only through signed, Super-Admin-approved, time-bound support windows (1 requested, 0 active now); every request audited.
S.8(6) / R.7	Breach intimation to the Board and affected persons (detailed report within 72 h)	met	No personal-data breaches recorded; 72-hour Board report clock ready.

CERT-In Directions (28 April 2022)

Control	Requirement	Status	SecOwl evidence
Dir. (i)	Synchronise ICT clocks with NIC/NPL NTP	met	0 devices currently out of time sync (agent rejects > 4 min skew at enrolment; server flags > 5 min).
Dir. (ii)	Report specified incidents within 6 hours	not met	0/1 reportable incidents reported to CERT-In within 6 hours.
Dir. (iii)	Designate a Point of Contact	manual	Show: POC name, designation and contact in Settings -> Organisation
Dir. (iv)	Maintain ICT system logs for 180 days within India	met	Retention: sign-ins 365 d, device events 180 d, access log 365 d (CERT-In: 180 days, kept in India on this server).

RBI Cyber Security Framework / IT Governance (2023) — baseline controls

Control	Requirement	Status	SecOwl evidence
RBI-1	Inventory management of business IT assets	partial	6 managed devices enrolled, 5 reporting now; software inventory from 4.
RBI-2	Preventing execution of unauthorised software	met	Software policy "blocklist" with 1 rules; unapproved installs raise alerts.
RBI-4	Network management and security	partial	3/5 high/critical applications are reached only through SecOwl Gate or from managed devices; 4/5 approved by a second person. Trusted company networks defined: 10.20.0.0/16.
RBI-5	Secure configuration	not met	2/6 devices compliant (33%).
RBI-7	Patch / vulnerability and change management	partial	5/6 devices have recent OS updates. Built-in policy only; policy changes require four-eyes approval when made.
RBI-8	User access control / management	partial	0 access requests decided in 90 days; 0 pending longer than 7 days; 0 grants without an end date. 1 Super Admins (2–5 recommended: break-glass without over-privilege); 3 privileged accounts in total.
RBI-9	Authentication framework for customers / users	not met	20% of 10 active accounts have a second factor; 0 passkeys registered.
RBI-13	Advanced real-time threat defence and management	partial	Behavioural detections active (sign-in, endpoint, access, integrity); 10 distinct rules fired in 90 days. 5/6 devices report active antivirus; malware detections raise alerts.
RBI-15	Data leak prevention strategy	manual	Show: DLP tooling (outside SecOwl; adapter possible)
RBI-17	Audit log settings	partial	Hash-chained audit ledger: 36 entries verified, chain intact. SIEM forwarding not enabled (SecOwl alerts and audit remain available locally).
RBI-19	Incident response and management (report to RBI within 6 hours)	partial	1 incidents in 12 months, 0 closed; timelines and AI summaries recorded. 0/1 reportable incidents reported to CERT-In within 6 hours.
RBI-21	Vendor risk management	met	Vendor access only through signed, Super-Admin-approved, time-bound support windows (1 requested, 0 active now); every request audited.