DERISK UWA · UNDERWRITER · UNDERWRITING VERDICT

Underwriting Verdict

Generated by DeRISK UWA on the DeRISK™ Intelligence Platform.

Applicant: Aldermere Energy **Assessment date:** 2026-06-30 **Report generated:** 2026-11-05

Submission: Insurer questionnaire (116 items) plus three supporting audit documents

Classification: Sample report

The verdict, the reasons behind it, and the conditions that have to be met before it binds.

UNDERWRITING VERDICT

Quote with Conditions

18 conditions precedent · four void the policy ab initio if unmet

MODEL CONFIDENCE

0.78

High — IT and OT evidence weighed separately

INDICATIVE PREMIUM

USD 3.5M

Midpoint of USD 2.85M–4.2M · ~0.25% of revenue

Three critical prioritized recommendations

1. **IMMEDIATE** — Separate administrative from day-to-day credentials and change all default passwords across 14,000 ICS/OT assets within 30–45 days — failure voids the policy ab initio.
2. **IMMEDIATE** — Implement bi-directional deny-by-default firewall rules between all OT network zones and document all physical access points within 30 days — failure voids the policy ab initio.
3. **WITHIN 30 DAYS** — Establish 24/7 enterprise-level security alert notification, provide dedicated CSIRT incident response training, and re-establish the 35-day NERC CIP patch evaluation cycle.

I · EXECUTIVE SUMMARY

I.1 Applicant Overview

ATTRIBUTE	VALUE
Legal entity name	Aldermere Energy
Industry sector	Renewable and conventional power generation
Annual global revenue (USD)	$1,429,000,000
ICS/OT cyber assets discovered	14,000
Estimated equipment replacement value (USD)	$16,230,000,000
Revenue loss per hour of OT downtime (USD)	$13,059,360
Facility types referenced	Wind generation, natural gas-fired power (Example Facility 1, Example Facility 2, Example Facility 3)
Third-party IR hourly rate (USD)	$2,500 per person

Aldermere Energy operates a large and geographically distributed OT environment spanning wind turbine farms and natural gas-fired generation facilities. The scale of the asset base (14,000 discovered ICS/OT assets, $16.23B equipment replacement value) and the $13.06M/hour revenue exposure at risk from OT downtime place this submission in the highest tier of financial exposure for OT cyber insurance. The submission was evaluated fresh for this run against NIST SP 800-82 Rev.3 and IEC 62443 frameworks.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

I.2 Risk Profile Classification

Aldermere Energy is classified as **HIGH** risk (overall score 6.8/10). The organization demonstrates mature foundational controls — IT/OT Active Directory separation, DMZ architecture, application-layer (OSI Layer-7) ingress/egress filtering, MFA-enforced VPN remote access, jump-host architecture, dedicated ICS/OT incident response plan, and 6–24 hour detection/containment windows. However, critical operational gaps materially elevate the risk profile: administrative credentials are not separated from day-to-day credentials; default passwords have not been changed across 14,000 assets; bi-directional firewall rules between OT zones are absent; physical access points are undocumented; and NERC CIP audit evidence reveals 97-day patch delays, 3–5 day access revocation delays, and DCS configuration baselines not updated within the 30-day requirement. These gaps are remediable within 90 days under the conditions precedent framework.

I.3 Key Risk Indicators

INDICATOR	STATUS	EVIDENCE SOURCE	RISK IMPACT
Admin/privileged credential separation	Critical Gap	Q2, Q60; NERC CIP audit (6 shared DCS accounts, 15+ month password age)	Privilege escalation across 35 personnel and 14,000 assets
Default password remediation	Critical Gap	Q23, Q81	Immediate unauthorized access risk across entire OT environment
Bi-directional OT zone firewall rules	Critical Gap	Q25, Q83	No lateral movement containment; full OT network blast radius
Physical access point documentation	Critical Gap	Q27, Q85; 2022 third-party assessment (unlocked telemetry building, non-functional motion detection)	Rogue/undocumented access points may exist undetected
Security patch evaluation cycle	High Gap	NERC CIP audit PNC-01 (97-day delay vs. 35-day requirement)	Exploitable vulnerability window; CIP-007-6 R2 violation
ICS/OT logging coverage	High Gap	Q55 (70% enabled), Q56 (75% centrally forwarded)	4,200 assets with no logging; 3,500 assets with local-only logs
Remote access security	Adequate	Q37, Q38, Q40, Q44, Q57	VPN + MFA + jump host + session management in place
Network segmentation / DMZ	Adequate	Q8, Q9, Q21, Q35, Q39	Layer-7 filtering; DMZ enforced; no bypass permitted

I.4 Underwriting Verdict

Binding recommendation: Quote with Conditions.

Critical concerns

Four policy-voiding conditions must be met within 30–45 days: (1) credential separation and shared account elimination; (2) default password changes across all 14,000 assets; (3) bi-directional OT zone firewall implementation; (4) physical access point documentation and physical security remediation. Multiple NERC CIP violations (PNC-01, PNC-02, PNC-03 — all High VRF) and material contradictions between questionnaire responses and audit evidence require senior underwriting review and written explanation from the insured before binding.

Recommended premium adjustment

Indicative annual premium range USD 2,850,000–4,200,000 (base factor 2.1 × risk adjustment 1.35 × conditions credit 0.75 applied to HIGH risk profile). Midpoint USD 3,500,000 represents approximately 0.25% of annual revenue.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

The binding decision is contingent on 18 conditions precedent with specific deadlines and impact-if-unmet provisions. Four conditions carry policy-void-ab-initio consequences. Quarterly compliance certification and an annual third-party security assessment are required throughout the policy period. Mitigation credits of up to 63% of premium are available upon full conditions precedent compliance, yielding an estimated total implementation cost of USD 1.57M against USD 2.21M in annual premium reduction.

II · CONDITIONS PRECEDENT TO BINDING

Eighteen conditions precedent govern binding; the four below void the policy ab initio if unmet and are listed with their deadlines. The remaining conditions, the quarterly compliance certification and the annual third-party security assessment are itemized in the Professional-tier underwriting report.

#	CONDITION PRECEDENT	DEADLINE	IMPACT IF UNMET
1	Separate administrative from day-to-day credentials; eliminate the six shared DCS accounts	30–45 days	Policy void ab initio
2	Change all default passwords across the 14,000 ICS/OT assets	30–45 days	Policy void ab initio
3	Implement bi-directional, deny-by-default firewall rules between all OT network zones	30 days	Policy void ab initio
4	Document all physical access points; remediate the unlocked telemetry building and non-functional motion detection	30 days	Policy void ab initio
5	Establish 24/7 enterprise-level security alert notification	30 days	Condition precedent
6	Provide dedicated CSIRT incident response training	30 days	Condition precedent
7	Re-establish the 35-day NERC CIP patch evaluation cycle (PNC-01)	30 days	Condition precedent
—	Quarterly compliance certification and annual third-party security assessment	Policy period	Ongoing requirement

II · COMPANY PROFILE & KEY METRICS

II.1 Risk Tier

TIER 3 — HIGH RISK. Overall OT risk score: 6.8 / 10. NIST CSF Protect maturity: 0.65. IEC 62443 SL2 compliance: 0.68. IEC 62443 SL3 compliance: 0.52.

II.2 Analysis or Rationale

The HIGH tier is driven by nine CRITICAL findings (credential management, default passwords, lateral movement containment, physical access documentation, patch delays, access revocation delays, DCS baseline management, shared account passwords, vendor remote access control) and nine HIGH findings. The $16.23B equipment replacement value and $13.06M/hour revenue exposure amplify the financial consequence of each gap. Foundational controls (segmentation, DMZ, Layer-7 filtering, MFA remote access, dedicated OT IR plan) prevent a CRITICAL tier classification and support binding with conditions rather than decline.

Aldermere Energy is a U.S.-based power generation company operating renewable (wind) and conventional (natural gas) generation assets. Referenced facilities include Example Facility 1, Example Facility 2 (natural gas, assessed by an independent security firm in April 2022), and Example Facility 3 (1,720 MW medium-impact BES facility, subject to a NERC CIP mock audit in 2026). The company has a Director of Cybersecurity and a VP/CIO. An internal audit of security incident response (IA-24-01, October 2024) was conducted with external audit-firm involvement. The company is subject to NERC CIP, FERC, and applicable state regulatory requirements. Annual global revenue is USD 1,429,000,000.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

III · OT CYBERSECURITY RISK POSTURE

III.1 NIST CSF 2.0 / Control Domains



NIST CSF FUNCTION	MATURITY SCORE	KEY STRENGTH	KEY GAP
Identify	0.72	Crown Jewels assessment completed; 14,000 assets in dynamic weekly discovery	Physical access points not documented (Q27); data flow diagrams not created (2022 assessment)
Protect	0.65	Layer-7 ACLs; DMZ; MFA remote access; IT/OT AD separation	Admin credentials not separated (Q2); default passwords not changed (Q23); no OT zone firewall rules (Q25)
Detect	0.68	Industrial protocol monitoring; rogue device detection; EDR deployed	30% of assets lack logging (Q55); log retention <6 months (Q58); no enterprise 24/7 alert notification (IA-24-01)
Respond	0.58	Dedicated ICS/OT IR plan; 6–24 hour detection/containment windows	CSIRT lacks dedicated training (IA-24-01); no MTTR metrics; no formal risk acceptance process
Recover	0.55	Baseline/last-known-good configuration tracked; OT network containment procedure documented	Backup restoration testing only bi-annual (Q34); DCS recovery untested operationally since 2022 (NERC audit)

NIST SP 800-82 Rev.3 assessment was generated fresh for this run. The lowest maturity scores are in Recover (0.55) and Respond (0.58), driven by inadequate backup restoration testing frequency and CSIRT training gaps. Protect (0.65) is constrained by the three policy-voiding credential and firewall gaps. Identify (0.72) benefits from comprehensive dynamic asset discovery but is limited by undocumented physical access points.

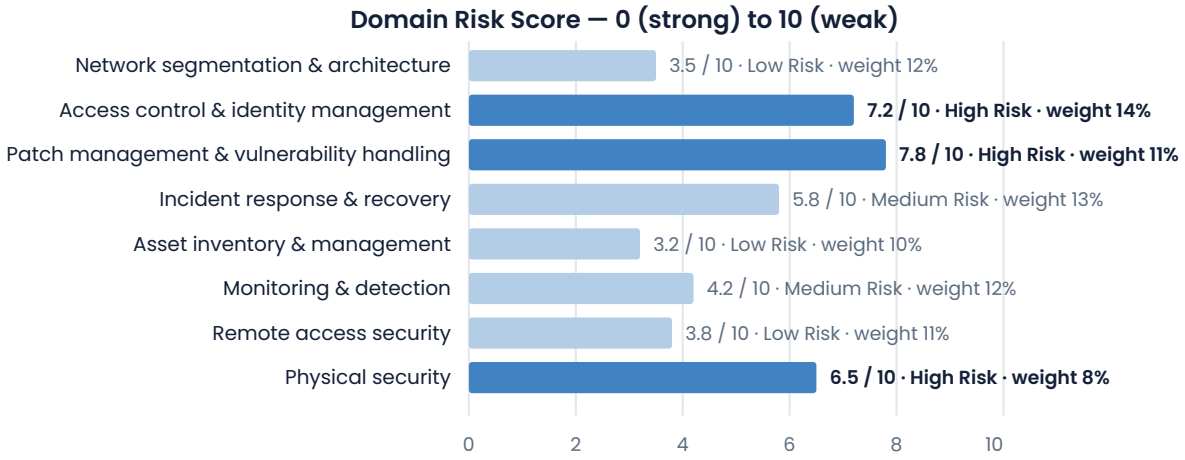
III.2 IEC 62443 / Security Levels

IEC 62443 LEVEL	COMPLIANCE SCORE	STATUS	PRIMARY GAP
SL1 — Basic	0.85	Largely met	Default passwords not changed (Q23); shared accounts in use (Q33)
SL2 — Medium	0.68	Partially met	Admin credential separation absent (Q2); no JIT privilege escalation (Q18); account audit >1 year (Q29)
SL3 — High	0.52	Partially met	No bi-directional OT zone firewall rules (Q25); vendor remote access not controllable on demand (NERC audit)
SL4 — Very high	0.38	Not met	No JIT/PAM solution (Q18); no biometric/FIDO MFA for remote access (Q57); DCS recovery untested (NERC audit)

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

IEC 62443 evaluation was generated fresh for this run. SL1 is largely met, confirming basic OT security hygiene is present. SL2 compliance (0.68) is constrained by credential management failures. SL3 (0.52) is limited by the absence of zone-to-zone firewall rules and uncontrollable vendor remote access. SL4 (0.38) is not achievable without JIT/PAM, stronger MFA, and validated recovery procedures.

III.3 Maturity Assessment (Current vs Peers)



Access Control & Identity Management (7.2) and Patch Management (7.8) are the highest-risk domains, driven by credential separation failures and documented NERC CIP patch delays. Remote Access Security (3.8) and Asset Inventory (3.2) are the strongest domains, reflecting mature VPN/MFA/jump-host architecture and dynamic weekly asset discovery. The weighted overall score of 6.8/10 reflects the disproportionate impact of credential and firewall gaps on an otherwise competent foundational posture.

IV · CONCLUSION & RISK OPINION

Final professional judgment

Aldermere Energy presents an insurable risk profile at the HIGH tier, supported by mature foundational OT security controls that are partially offset by critical operational gaps in credential management, network segmentation, physical security, and regulatory compliance. The organization's scale ($16.23B equipment value, $13.06M/hour revenue exposure, 14,000 OT assets) and active NERC CIP violations create elevated but quantifiable risk. The recommended Quote with Conditions decision is appropriate provided the four policy-voiding conditions are met within 30–45 days and all 18 conditions precedent are satisfied within their respective deadlines.

Acceptability assessment

ACCEPTABLE WITH CONDITIONS. Risk is insurable at the recommended premium range of USD 2,850,000–4,200,000 annually (indicative) subject to 18 conditions precedent, quarterly compliance certification, and annual third-party security assessment. Policy void ab initio if any of the four CRITICAL conditions are not met by their deadlines. Senior underwriting review and written explanation of questionnaire-audit contradictions required before binding.

This evaluation was generated fresh for this run (both OT risk evaluation and UW policy evaluation). The confidence score of 0.78 reflects high confidence in findings with explicit questionnaire evidence and supporting audit documentation, partially offset by material contradictions between self-reported questionnaire responses and third-party audit evidence. Third-party validation of all material representations is recommended prior to binding. The next scheduled review point is the WECC NERC CIP audit (Q1 2027), which should trigger a mid-term policy review.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.

Attribution and review

This assessment was produced by DeRISK UWA from the submission as received — the questionnaire and three supporting audit documents — with no contact with the applicant. Every finding traces to its questionnaire item or document, pipeline step and model version. It is decision support for a licensed underwriter: underwriter review is mandatory before any quote is issued or bound. Submission data was processed session-only and purged after this report was generated.

© 2026 DeNexus, Inc. · DeNexus and DeRISK are trademarks of DeNexus, Inc.