CORA · CYBER OPERATIONAL RISK ASSESSMENT

FrontRange Energy & Gas (FREG) — Cyber Operational Risk Assessment (Notional Demo)

FrontRange Energy & Gas (FREG)

MISSION AREAS	THREATS IN SCOPE	SCENARIOS ANALYZED	GROSS ANNUAL RISK
4	6	18	$4,310,000
in scope	threat sources	risk scenarios	expected annual loss

REPORT DETAILS

Prepared By	CyberRAM CORA Demo Team
Report Date	February 15, 2026
Report ID	—
Version	1.0
Classification	Internal

INTENDED AUDIENCE

— Leadership

DOCUMENT CONTROL

Document Control

Document Title	FrontRange Energy & Gas (FREG) — Cyber Operational Risk Assessment (Notional Demo)
Version	1.0
Classification	Internal
Date	February 15, 2026
Prepared By	CyberRAM CORA Demo Team
Approved By	—
Review Date	—
Report ID	—

Distribution List

No distribution list specified.

ℹ This document contains sensitive risk assessment findings. Handle in accordance with the classification marking on the cover page.

NAVIGATION

Table of Contents

1

Executive Summary

FrontRange Energy & Gas (FREG) delivers high-consequence electric and natural gas services. This notional CORA demo summarizes where cyber events could most impact safe operations, service reliability, customer trust, and regulatory outcomes. The highest drivers of risk are (1) disruption of OT-adjacent access and restoration workflows, (2) gas SCADA integrity/safety scenarios, and (3) customer data exposure and payment fraud. The recommended plan prioritizes hardening privileged access and vendor remote access, improving resilience (backup/restore and segmentation), and strengthening detection and verification for critical operations.

GROSS ANNUAL RISK	NET ANNUAL RISK	RISK REDUCED	SCENARIOS	MISSION AREAS	THREATS IN SCOPE
$4,310,000	$1,715,000	$2,595,000	18	4	6

Risk & Response Overview

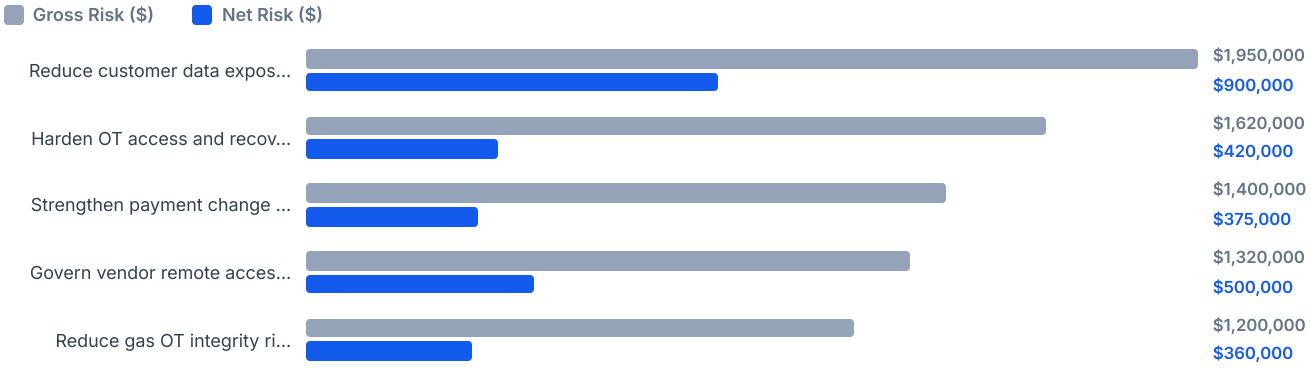
Top Risk Scenarios

THREAT	MISSION AREA	EFFECT	ANNUAL RISK ($)
Financial Fraud / Phishing Group	Customer Operations	Disclose	**$1,957,906**
Ransomware Affiliate / Broker	Electric Operations (OT)	Deny	**$684,169**
Financial Fraud / Phishing Group	Enterprise IT + Governance	Deceive	**$646,516**
Negligent User	Enterprise IT + Governance	Disclose	**$525,452**
Financial Fraud / Phishing Group	Enterprise IT + Governance	Deny	**$371,589**
Negligent User	Enterprise IT + Governance	Deny	**$239,375**
Ransomware Affiliate / Broker	Customer Operations	Disclose	**$211,181**
Contractor / Temp Worker	Gas Operations (OT)	Deceive	**$188,655**

Key Recommendations

#	RECOMMENDATION	NET RISK ($)	ROI
1	Harden OT access and recovery to reduce ransomware disruption risk	**$1,200,000**	**-4%**
2	Reduce customer data exposure via access controls and detection on CIS/MDM	**$1,050,000**	**88%**
3	Strengthen payment change controls to reduce BEC fraud risk	**$1,025,000**	**583%**
4	Reduce gas OT integrity risk with segmentation and change monitoring	**$840,000**	**-13%**
5	Govern vendor remote access to OT using PAM, approvals, and monitoring	**$820,000**	**110%**

Risk Reduction Impact (Top 5 Treatments)



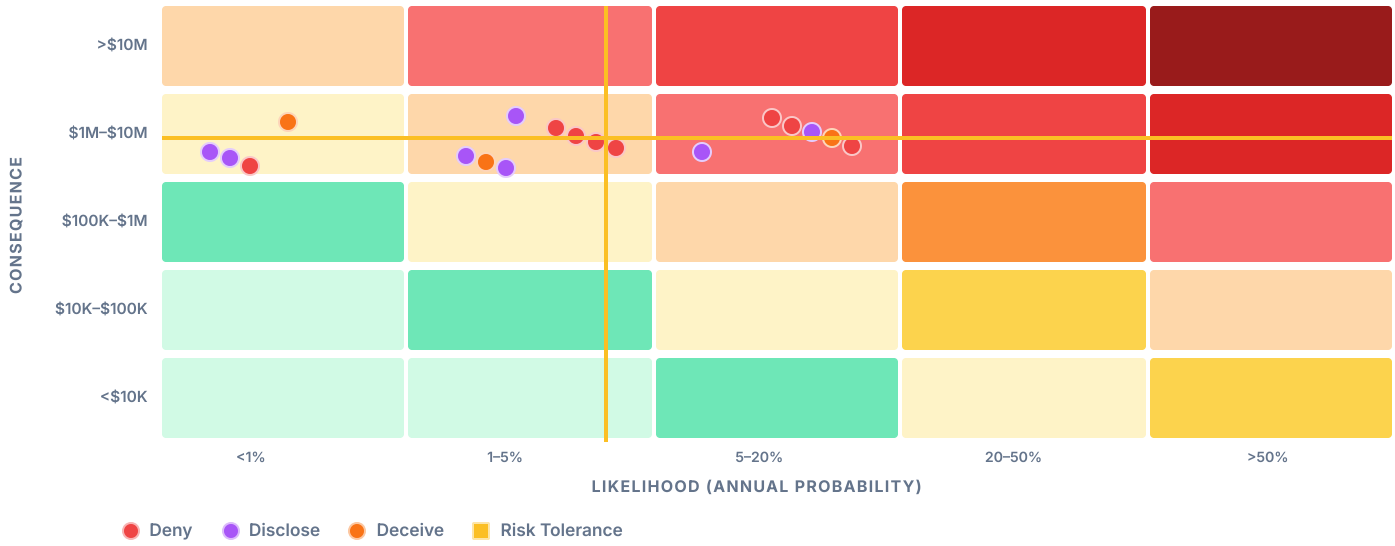
✓ Implementing the recommended risk treatments would reduce gross annual risk by $2,595,000 (60% reduction).

2

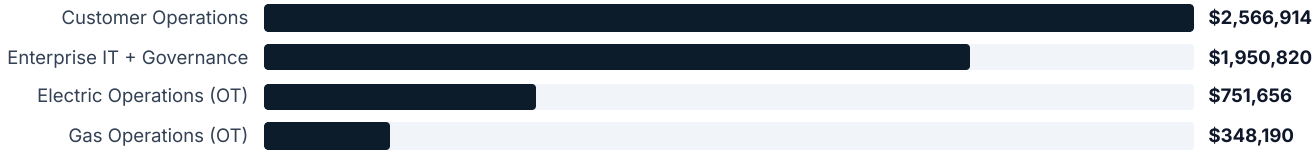
Portfolio Risk Posture

GROSS ANNUAL RISK	NET ANNUAL RISK	RISK REDUCED	SCENARIOS	MISSION AREAS	THREATS
$4,310,000	$1,715,000	$2,595,000	18	4	6

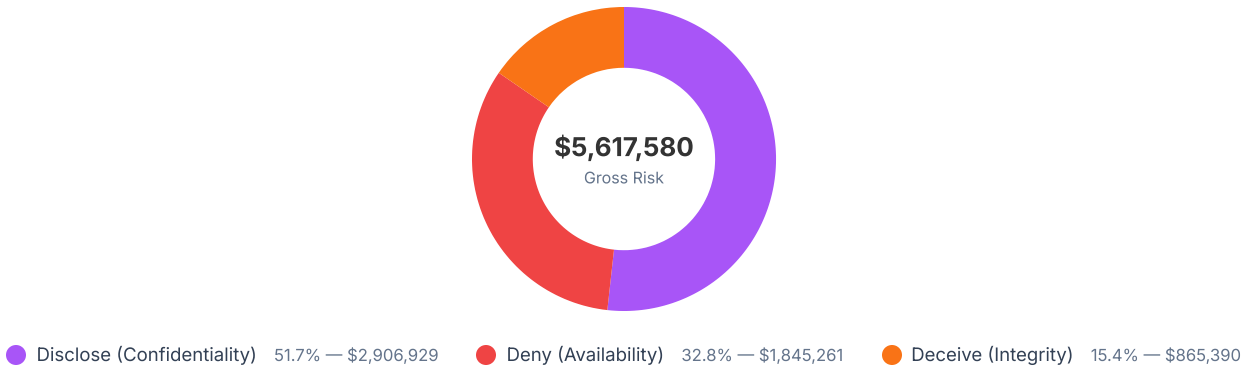
Risk Matrix



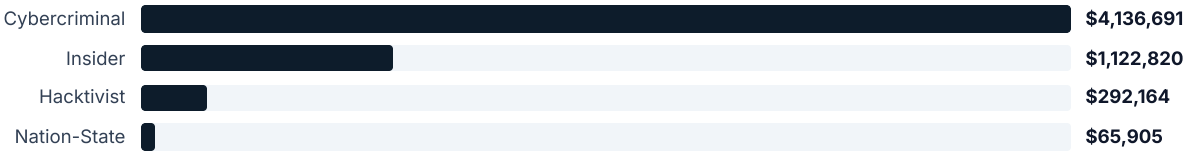
Risk by Mission Area



Risk by Effect Type



Risk by Threat Category



ℹ Cybercriminal threats account for 74% of total portfolio risk.

3

Assessment Overview

What is CORA?

CORA (Cyber Operational Risk Assessment) is a mission-centric cyber risk assessment methodology. It evaluates cyber risk in terms of how threats could impact an organization's critical missions, rather than focusing solely on technical vulnerabilities.

Mission

Deliver safe, reliable electricity and natural gas while meeting regulatory requirements and maintaining public trust.

FrontRange Energy & Gas (FREG) is a regulated investor-owned utility serving ~1.2M residents across a mixed service territory. The assessment focuses on safety, reliability, rapid restoration, accurate billing/cashflow, and regulatory compliance (NERC CIP, PHMSA, PUC).

This assessment covers 4 mission areas.

Scope

Notional demo assessment covering core IT and OT systems supporting electric and gas operations, customer communications, and billing. Excludes detailed plant ICS engineering and physical security controls.

Method

We defined mission outcomes, mapped critical functions and data, estimated effect impacts (Deny/Disclose/Deceive), scoped representative threats and their intent, estimated vulnerability probability (VEP), and summarized risk as frequency and magnitude. We then documented responses and mitigations as Risk Detail Records with expected risk reduction and year-1 costs.

Key Assumptions

Threat frequencies and VEP inputs are notional for demo purposes. Impact magnitudes represent typical mean event costs and do not include catastrophic tail outcomes.

Limitations

This demo does not include a detailed substation-by-substation inventory, detailed plant control system engineering review, or validated incident cost accounting. Values should be refined with stakeholder workshops and evidence collection.

4

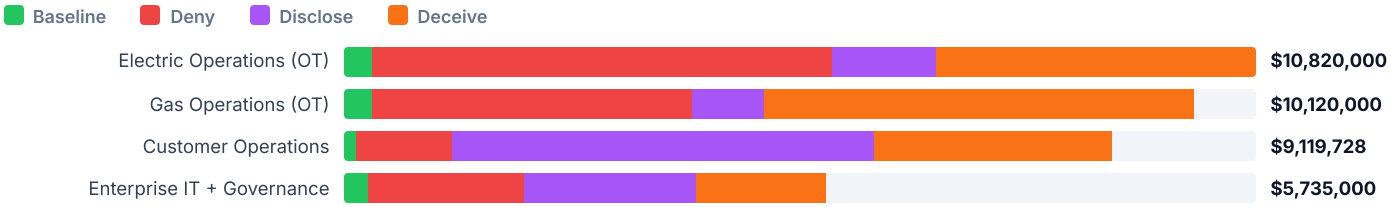
Mission Context

TOTAL MISSION IMPACT EXPOSURE

$35,794,728

Combined Deny + Disclose + Deceive + Baseline across all mission areas

Impact by Mission Area



ℹ Electric Operations (OT) carries the highest impact exposure at $10,820,000 (30% of total), making it the priority area for risk reduction.

Critical Items to Protect

The following critical data items are ranked by their mission impact and dependency footprint. Protecting these items should be the primary focus of risk treatment.

#	CRITICAL DATA	FUNCTION	MISSION AREA	CLASSIFICATIONS	LINKED ASSETS
1	SCADA EMS real-time telemetry	Grid monitoring and situational awareness	Electric Operations (OT)	OPS	2
2	Switching orders (approved)	Distribution switching and control execution	Electric Operations (OT)	OPS	2
3	Operating instructions (switching)	Distribution switching and control execution	Electric Operations (OT)	OPS,IP	2
4	Outage events	Outage detection and event triage	Electric Operations (OT)	OPS	2
5	Outage alarms	Outage detection and event triage	Electric Operations (OT)	OPS	2
6	Crew assignments	Crew dispatch and restoration coordination	Electric Operations (OT)	OPS	2
7	State estimator inputs	Grid monitoring and situational awareness	Electric Operations (OT)	OPS	1
8	SCADA point database	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1
9	Tag mappings	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1
10	Naming standards	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1
11	Operator displays	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1

#	CRITICAL DATA	FUNCTION	MISSION AREA	CLASSIFICATIONS	LINKED ASSETS
12	HMI configurations	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1
13	Grid one-lines	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1
14	Visualization layers	Grid monitoring and situational awareness	Electric Operations (OT)	OPS,IP	1
15	Dispatch tickets	Crew dispatch and restoration coordination	Electric Operations (OT)	OPS	1

Attack Points

Attack points map critical data items through their supporting assets to entry points where an adversary could gain access.

CRITICAL DATA	ASSET	ENTRY POINT	PROTOCOL	DIRECTION
SCADA EMS real-time telemetry	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**
SCADA EMS real-time telemetry	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**
SCADA EMS real-time telemetry	**Electric SCADA/EMS Server Cluster (VMs)**	**OT telemetry backhaul circuits**	**MPLS/IP**	**Bidirectional**
State estimator inputs	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**
State estimator inputs	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**
State estimator inputs	**Electric SCADA/EMS Server Cluster (VMs)**	**OT telemetry backhaul circuits**	**MPLS/IP**	**Bidirectional**
SCADA point database	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**
SCADA point database	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**
SCADA point database	**Electric SCADA/EMS Server Cluster (VMs)**	**OT telemetry backhaul circuits**	**MPLS/IP**	**Bidirectional**
Tag mappings	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**
Tag mappings	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**
Tag mappings	**Electric SCADA/EMS Server Cluster (VMs)**	**OT telemetry backhaul circuits**	**MPLS/IP**	**Bidirectional**
Naming standards	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**
Naming standards	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**
Naming standards	**Electric SCADA/EMS Server Cluster (VMs)**	**OT telemetry backhaul circuits**	**MPLS/IP**	**Bidirectional**
Operator displays	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**

CRITICAL DATA	ASSET	ENTRY POINT	PROTOCOL	DIRECTION
Operator displays	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**
Operator displays	**Electric SCADA/EMS Server Cluster (VMs)**	**OT telemetry backhaul circuits**	**MPLS/IP**	**Bidirectional**
HMI configurations	**Electric SCADA/EMS Server Cluster (VMs)**	**Vendor remote support to OT bastions**	**VPN/RDP**	**Inbound**
HMI configurations	**Electric SCADA/EMS Server Cluster (VMs)**	**ICCP telemetry exchange**	**ICCP**	**Bidirectional**

5

Threat Landscape

MEAN THREAT EVENT FREQUENCY

2.19/yr

Average adversary actions per year across 6 threat sources

6 threat sources are in scope for this assessment. The table below summarizes each threat's estimated frequency of action and targeting relevance to this organization.

THREAT SOURCE	CATEGORY	THREAT FREQ. (EVENTS/YR)	TARGETING FACTOR
Ransomware Affiliate / Broker Organized groups monetizing encryption and extortion.	Cybercriminal	2.00	0.65
Intelligence Service Proxy Contractors or shell companies performing state tasks covertly.	Nation-State	0.35	0.25
Financial Fraud / Phishing Group Credential or card-harvesting operations.	Cybercriminal	5.00	0.75
Contractor / Temp Worker External personnel with short-term access.	Insider	0.80	0.45
Ideological Collective Decentralized activists (e.g., Anonymous-style).	Hacktivist	3.00	0.20
Negligent User Unintentional insider through error or carelessness.	Insider	2.00	0.85

Kill Chain Analysis — Reducing Adversary Reach

Each tactic below is a step in the adversary kill chain. Every step marked REQUIRED is a detection and disruption opportunity — hardening these increases the cost and complexity of an attack. Steps marked SKIPPABLE can be bypassed entirely, reducing the defender's response window. The strategic goal is to maximize required steps by isolating critical systems from the broader attack surface.

TACTIC	REQUIRED IN	SKIPPABLE IN	PRIORITY ACTION
Reconnaissance	4 areas	0 areas	MONITOR & DETECT
Resource Development	4 areas	0 areas	MONITOR & DETECT
Initial Access	4 areas	0 areas	MONITOR & DETECT
Execution	4 areas	0 areas	MONITOR & DETECT
Persistence	4 areas	0 areas	MONITOR & DETECT
Privilege Escalation	4 areas	0 areas	MONITOR & DETECT
Defense Evasion	4 areas	0 areas	MONITOR & DETECT
Credential Access	4 areas	0 areas	MONITOR & DETECT
Discovery	4 areas	0 areas	MONITOR & DETECT
Lateral Movement	4 areas	0 areas	MONITOR & DETECT

TACTIC	REQUIRED IN	SKIPPABLE IN	PRIORITY ACTION
Collection	4 areas	0 areas	MONITOR & DETECT
Command and Control	4 areas	0 areas	MONITOR & DETECT
Exfiltration	4 areas	0 areas	MONITOR & DETECT
Impact	4 areas	0 areas	MONITOR & DETECT

6

Vulnerability & Attack Surface

AVG. WORST-CASE VEP (PER AREA)

25.3%

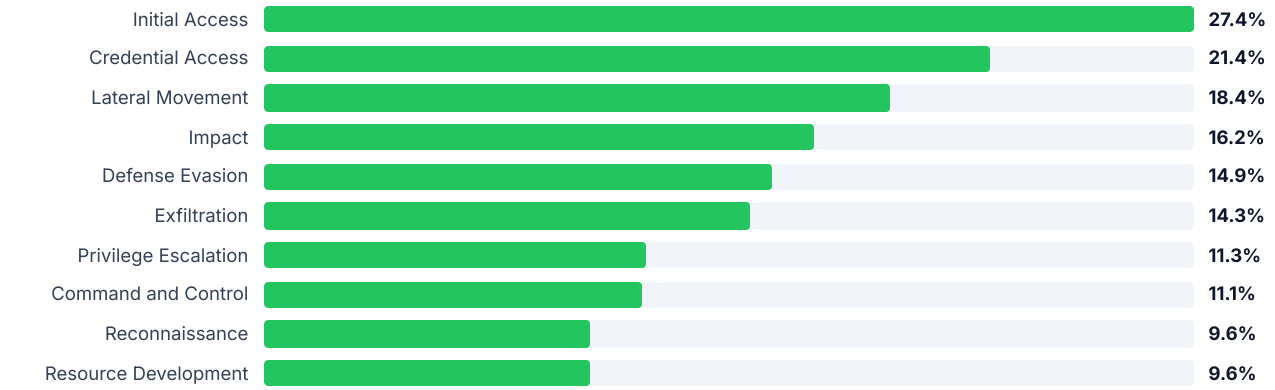
Average of worst-case vulnerability probability per mission area (max across in-scope threat sources)

Vulnerability Probability by Mission Area

Average vulnerability probability across assessed areas: 25.3%.

Highest-Risk Tactics

The following MITRE ATT&CK tactics have the highest average vulnerability probability across all mission areas. Risk management efforts should prioritize strengthening defenses against these tactics.



Attack Surface Coverage

⚠ 100% of the attack surface (12 of 12 entry points) directly reaches critical data. These represent the highest-priority hardening targets.

Attack Surface Hardening Priorities

Entry points are ranked by the number of critical assets they expose. Hardening these access points reduces the overall attack surface.

#	ENTRY POINT	EXTERNAL ENTITY	PROTOCOL	ASSETS EXPOSED
1	Vendor remote support to OT bastions	OT Vendor	VPN/RDP	OT Bastion / Jump Hosts (Hardened VMs), Gas SCADA Server Cluster (VMs), Electric SCADA/EMS Server Cluster (VMs)
2	Public outage website	Internet	HTTPS	Public Outage Website Web Server (DMZ), OMS Application Server (VMs)

#	ENTRY POINT	EXTERNAL ENTITY	PROTOCOL	ASSETS EXPOSED
3	Email phishing / credential theft	Internet	SMTP/HTTPS	Entra ID / Azure AD Tenant, Active Directory Domain Controllers (VMs)
4	Payment processing integration	Payment Processor	HTTPS	CIS Application Servers (VMs), CIS Database Server (VM)
5	OT telemetry backhaul circuits	Telecom Carrier	MPLS/IP	Electric SCADA/EMS Server Cluster (VMs), Gas SCADA Server Cluster (VMs)
6	Field laptops and tablets accessing work systems	Field Workforce	HTTPS/VPN	OMS Application Server (VMs), OMS Application Server (VMs)
7	VPN gateway remote access	Internet	VPN	Edge Firewall/VPN Gateway Appliance
8	ICCP telemetry exchange	RTO	ICCP	Electric SCADA/EMS Server Cluster (VMs)
9	Cloud identity and email services	Cloud Provider	HTTPS	Entra ID / Azure AD Tenant
10	External DNS resolution and zone transfers (if misconfigured)	Internet	DNS	DNS Servers (Primary/Secondary VMs)
11	Log forwarding to SIEM	Internal Systems	Syslog/Agent	SIEM Platform
12	GRC evidence repository access	Internal Users	HTTPS	GRC / Evidence Repository (VM)

7.1. Electric Operations (OT)

4 scenarios · $751,656 EAL

Operate and restore the electric grid safely using EMS/SCADA/DMS and field switching.

This mission area encompasses 6 critical functions, 24 critical data elements, 5 supporting assets.

BASELINE	DENY	DISCLOSE	DECEIVE	TOTAL
$330,000	$5,470,000	$1,220,000	$3,800,000	$10,820,000

Top Risk Scenarios

THREAT	EFFECT	LEF	LOSS MAGNITUDE	ANNUALIZED LOSS
Ransomware Affiliate / Broker	Deny	0.117	$5,827,778	$684,169
Intelligence Service Proxy	Deceive	0.007	$4,157,778	$30,219
Contractor / Temp Worker	Disclose	0.016	$1,577,778	$25,800
Intelligence Service Proxy	Disclose	0.007	$1,577,778	$11,467

4 total scenarios contributing $751,656 annualized loss (13.4% of portfolio).

Critical Functions and Data

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Grid monitoring and situational awareness	SCADA EMS real-time telemetry	8000	OPS
Grid monitoring and situational awareness	State estimator inputs	8000	OPS
Grid monitoring and situational awareness	SCADA point database	8000	OPS,IP
Grid monitoring and situational awareness	Tag mappings	8000	OPS,IP
Grid monitoring and situational awareness	Naming standards	10	OPS,IP
Grid monitoring and situational awareness	Operator displays	800	OPS,IP
Grid monitoring and situational awareness	HMI configurations	700	OPS,IP
Grid monitoring and situational awareness	Grid one-lines	50	OPS,IP
Grid monitoring and situational awareness	Visualization layers	200	OPS,IP
Distribution switching and control execution	Switching orders (approved)	200000	OPS
Distribution switching and control execution	Operating instructions (switching)	5000	OPS,IP
Distribution switching and control execution	Control setpoints (current)	20000	OPS
Distribution switching and control execution	Protection settings (current)	20000	OPS
Outage detection and event triage	Outage events	500000	OPS
Outage detection and event triage	Outage alarms	500000	OPS
Outage detection and event triage	Customer outage reports (summary)	410000	OPS

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Crew dispatch and restoration coordination	Crew assignments	**300000**	OPS
Crew dispatch and restoration coordination	Dispatch tickets	**300000**	OPS
Crew dispatch and restoration coordination	Restoration plans	**120000**	OPS
Crew dispatch and restoration coordination	Switching backout plans	**120000**	OPS
RTO coordination and telemetry exchange (ICCP)	ICCP telemetry point list	**2000**	OPS,IP
RTO coordination and telemetry exchange (ICCP)	ICCP point mappings	**2000**	OPS,IP
RTO coordination and telemetry exchange (ICCP)	RTO dispatch instructions	**50000**	OPS
RTO coordination and telemetry exchange (ICCP)	RTO communications logs	**50000**	OPS

Overall Vulnerability Probability (VEP): 24.9% (see Appendix D for full tactic-level breakdown).

Technical footprint: 5 supporting assets (see Appendix F–G for complete inventories).

7.2. Gas Operations (OT)

3 scenarios · $348,190 EAL

Monitor and control gas pressure/flow, dispatch emergency response, and prevent public-safety incidents.

This mission area encompasses 5 critical functions, 19 critical data elements, 1 supporting asset.

BASELINE	DENY	DISCLOSE	DECEIVE	TOTAL
$330,000	$3,810,000	$860,000	$5,120,000	$10,120,000

Top Risk Scenarios

THREAT	EFFECT	LEF	LOSS MAGNITUDE	ANNUALIZED LOSS
Contractor / Temp Worker	Deceive	0.034	$5,477,778	$188,655
Contractor / Temp Worker	Deny	0.034	$4,167,778	$143,539
Intelligence Service Proxy	Deny	0.004	$4,167,778	$15,996

3 total scenarios contributing $348,190 annualized loss (6.2% of portfolio).

Critical Functions and Data

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Pressure and flow monitoring	Gas pressure telemetry	6000	OPS
Pressure and flow monitoring	Gas flow telemetry	6000	OPS
Pressure and flow monitoring	Valve state telemetry	6000	OPS
Pressure and flow monitoring	Compressor state telemetry	6000	OPS
Valve control and isolation operations	Valve control configurations	1200	OPS,IP
Valve control and isolation operations	Control logic parameters	1200	OPS,IP
Valve control and isolation operations	Isolation procedures	2000	OPS,IP
Valve control and isolation operations	Emergency shutdown steps	2000	OPS,IP
Alarm triage and operational decision support	Alarm thresholds (current)	4000	OPS
Alarm triage and operational decision support	Setpoint limits (current)	4000	OPS
Alarm triage and operational decision support	Shift notes	120000	OPS
Alarm triage and operational decision support	Operational decision logs	120000	OPS
Emergency dispatch and response coordination	Emergency calls	60000	OPS,PII
Emergency dispatch and response coordination	Dispatch tickets	90000	OPS,PII
Emergency dispatch and response coordination	Responder on-call rosters	5000	PII
Emergency dispatch and response coordination	Responder contact lists	5000	PII
Leak survey and safety inspection workflow	Leak survey records	250000	OPS

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Leak survey and safety inspection workflow	Inspection findings	**250000**	OPS
Leak survey and safety inspection workflow	Corrective action work orders	**150000**	OPS

Overall Vulnerability Probability (VEP): 26.3% (see Appendix D for full tactic-level breakdown).

Technical footprint: 1 supporting asset (see Appendix F–G for complete inventories).

7.3. Customer Operations

5 scenarios · $2,566,914 EAL

Maintain outage communications, call center operations, and meter-to-cash (billing/payments).

This mission area encompasses 6 critical functions, 18 critical data elements, 7 supporting assets.

BASELINE	DENY	DISCLOSE	DECEIVE	TOTAL
$130,000	$1,140,000	$5,029,728	$2,820,000	$9,119,728

Top Risk Scenarios

THREAT	EFFECT	LEF	LOSS MAGNITUDE	ANNUALIZED LOSS
Financial Fraud / Phishing Group	Disclose	0.377	$5,187,506	$1,957,906
Ransomware Affiliate / Broker	Disclose	0.041	$5,187,506	$211,181
Ideological Collective	Disclose	0.032	$5,187,506	$166,901
Ideological Collective	Deny	0.097	$1,297,778	$125,263
Ransomware Affiliate / Broker	Deny	0.081	$1,297,778	$105,664

5 total scenarios contributing $2,566,914 annualized loss (45.7% of portfolio).

Critical Functions and Data

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Inbound customer contact intake (IVR/call center)	IVR call routing configuration	1	OPS,IP
Inbound customer contact intake (IVR/call center)	Call logs	410000	PII
Inbound customer contact intake (IVR/call center)	Customer contact history	410000	PII
Outage notifications and public communications	Outage notification message templates	200	OPS
Outage notifications and public communications	Customer contact list for notifications	410000	PII
Customer account management	Customer account master records	705000	PII,FIN
Customer account management	Service address data	705000	PII
Customer account management	Premise data	705000	PII
Billing cycle execution	Billing rules configuration	2000	OPS,IP
Billing cycle execution	Tariff configuration	2000	OPS,IP
Billing cycle execution	Bills history	352500	PII,FIN
Billing cycle execution	Statements history	352500	PII,FIN
Payment processing and settlement	Payment transactions	705000	FIN,PII
Payment processing and settlement	Settlement records	705000	FIN,PII
Payment processing and settlement	Payment processor integration keys	50	CRED,OPS

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Payment processing and settlement	Payment processor integration configuration	**50**	OPS,IP
Meter data ingestion and validation	Electric smart meter interval data (15-min)	**410000**	OPS
Meter data ingestion and validation	Gas meter reads (monthly)	**295000**	OPS

Overall Vulnerability Probability (VEP): 26.0% (see Appendix D for full tactic-level breakdown).

Technical footprint: 7 supporting assets (see Appendix F–G for complete inventories).

7.4. Enterprise IT + Governance

6 scenarios · $1,950,820 EAL

Provide identity, network services, endpoint management, monitoring, and governance/compliance functions supporting all mission areas.

This mission area encompasses 10 critical functions, 31 critical data elements, 11 supporting assets.

BASELINE	DENY	DISCLOSE	DECEIVE	TOTAL
$285,000	$1,840,000	$2,050,000	$1,560,000	$5,735,000

Top Risk Scenarios

THREAT	EFFECT	LEF	LOSS MAGNITUDE	ANNUALIZED LOSS
Financial Fraud / Phishing Group	Deceive	0.345	$1,872,778	$646,516
Negligent User	Disclose	0.222	$2,362,778	$525,452
Financial Fraud / Phishing Group	Deny	0.173	$2,152,778	$371,589
Negligent User	Deny	0.111	$2,152,778	$239,375
Ransomware Affiliate / Broker	Deny	0.074	$2,152,778	$159,666
Intelligence Service Proxy	Disclose	0.003	$2,362,778	$8,222

6 total scenarios contributing $1,950,820 annualized loss (34.7% of portfolio).

Critical Functions and Data

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Identity and authentication services (AD/LDAP/SSO)	Directory objects (users)	100000	CRED,OPS
Identity and authentication services (AD/LDAP/SSO)	Directory group objects	5000	CRED,OPS
Identity and authentication services (AD/LDAP/SSO)	Directory role assignments	500	CRED,OPS
Identity and authentication services (AD/LDAP/SSO)	Authentication logs	4500000	OPS
Identity and authentication services (AD/LDAP/SSO)	Sign-in logs	4500000	OPS
Privileged access management (PAM + admin workflows)	Privileged account inventory	5000	CRED,OPS
Privileged access management (PAM + admin workflows)	PAM vault policies	500	CRED,OPS
Privileged access management (PAM + admin workflows)	Privileged access workflows	500	CRED,OPS
Core network services (DNS/DHCP/NTP)	DNS zone data	2000	OPS
Core network services (DNS/DHCP/NTP)	DNS resolver configuration	2000	OPS
Core network services (DNS/DHCP/NTP)	DHCP scopes	5000	OPS
Core network services (DNS/DHCP/NTP)	DHCP reservations	5000	OPS
Core network services (DNS/DHCP/NTP)	NTP configuration	50	OPS
Core network services (DNS/DHCP/NTP)	Time source list	10	OPS

FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Core network services (DNS/DHCP/NTP)	Upstream time references	**40**	OPS
Remote access services (VPN, bastions, vendor access)	VPN configuration	**200**	OPS,CRED
Remote access services (VPN, bastions, vendor access)	VPN access policies	**200**	OPS,CRED
Remote access services (VPN, bastions, vendor access)	Bastion session logs	**250000**	OPS
Remote access services (VPN, bastions, vendor access)	Bastion session recordings	**250000**	OPS
Backup/restore and disaster recovery operations	Backup catalogs	**500**	OPS,IP
Backup/restore and disaster recovery operations	Restore runbooks	**500**	OPS,IP
Backup/restore and disaster recovery operations	Golden images	**200**	OPS,IP
Backup/restore and disaster recovery operations	Baseline configurations for recovery	**200**	OPS,IP
Compliance evidence management and audit readiness	NERC CIP evidence artifacts	**45000**	OPS
Compliance evidence management and audit readiness	Audit trail for evidence repository	**45000**	OPS
Compliance evidence management and audit readiness	Control test results	**20000**	OPS
Compliance evidence management and audit readiness	Remediation tracking records	**20000**	OPS
Incident reporting and regulatory notifications	Incident timelines	**1500**	OPS
Incident reporting and regulatory notifications	Notification records	**1500**	OPS
Incident reporting and regulatory notifications	Regulatory submissions	**2500**	OPS
Incident reporting and regulatory notifications	Regulatory correspondence	**2500**	OPS

Overall Vulnerability Probability (VEP): 23.9% (see Appendix D for full tactic-level breakdown).

Technical footprint: 11 supporting assets and 12 service dependencies (see Appendix F–G for complete inventories).

8

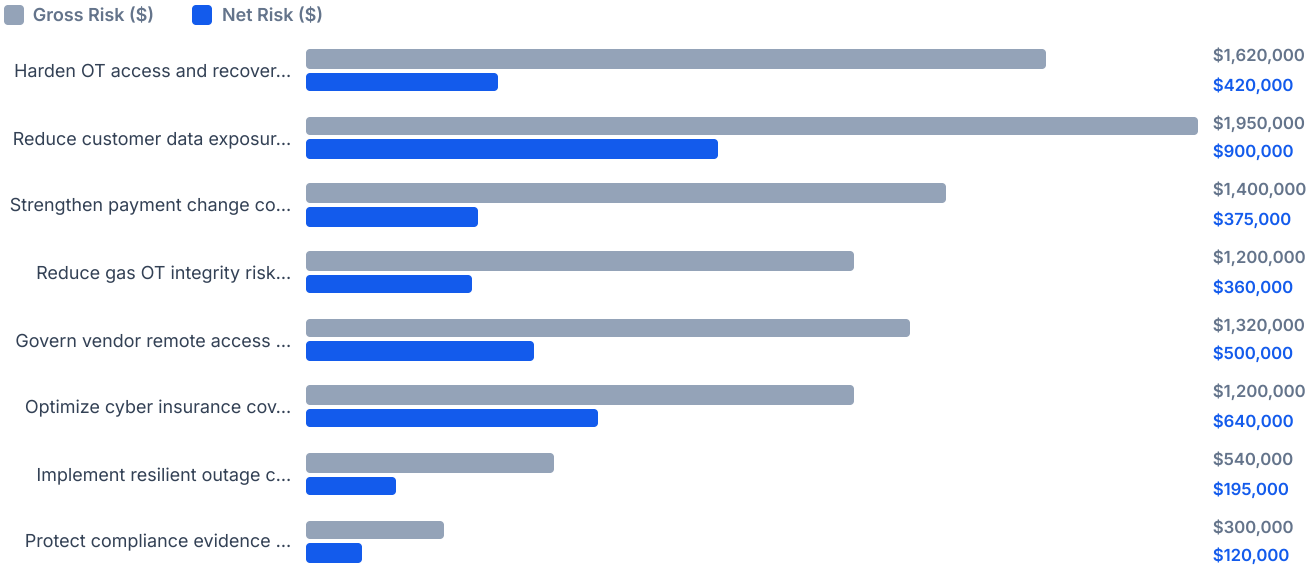
Recommendations and Residual Risk

GROSS ANNUAL RISK	NET ANNUAL RISK	RISK REDUCED	YEAR 1 COST	ROI
$4,310,000	$1,715,000	$2,595,000	$2,080,000	25%

Priority Decisions

#	RECOMMENDATION	RESPONSE	OWNER	RISK REDUCTION ($)	YEAR 1 COST ($)	ROI
1	Harden OT access and recovery to reduce ransomware disruption risk	MITIGATE	OT Security Program Manager	$1,200,000	$1,250,000	-4%
2	Reduce customer data exposure via access controls and detection on CIS/MDM	MITIGATE	Customer Systems Manager	$1,050,000	$560,000	88%
3	Strengthen payment change controls to reduce BEC fraud risk	MITIGATE	Controller (Finance)	$1,025,000	$150,000	583%
4	Reduce gas OT integrity risk with segmentation and change monitoring	MITIGATE	Gas Operations Director	$840,000	$970,000	-13%
5	Govern vendor remote access to OT using PAM, approvals, and monitoring	MITIGATE	Cybersecurity Director	$820,000	$390,000	110%
6	Optimize cyber insurance coverage to cap tail financial exposure	TRANSFER	Risk Manager	$560,000	$325,000	72%
7	Implement resilient outage communications (DDoS protection + failover channels)	MITIGATE	Customer Communications Lead	$345,000	$270,000	28%
8	Protect compliance evidence integrity with immutability and access controls	MITIGATE	Compliance Program Owner	$180,000	$125,000	44%
9	Accept minor email/collaboration outages	ACCEPT	IT Operations Manager	$0	$0	0%

Risk Reduction Impact



Risk Detail Records

Each entry below is a risk decision record capturing the full context of the risk, response decision, and treatment plan.

1. Reduce customer data exposure via access controls and detection on CIS/MDM

Customer Operations

Response	Mitigate
Owner	Customer Systems Manager
Gross Risk ($)	$1,950,000
Net Risk ($)	$900,000
Risk Reduction ($)	$1,050,000
Year 1 Cost ($)	$560,000
ROI	88%
Review Date	August 15, 2026

Risk Statement

If attackers access CIS/MDM data stores and exfiltrate customer PII, then FREG will incur notification and remediation costs and face regulatory and trust impacts.

Mitigations

- Implement least-privilege role design for CIS/MDM with quarterly access reviews and separation of duties for exports/admin actions
- Enable alerting for bulk exports, unusual query patterns, and anomalous admin actions against customer data stores
- Enforce strong admin authentication: MFA, device compliance, and conditional access for privileged and high-risk sign-ins
- Implement encryption key management hardening and reduce stored sensitive fields where feasible (data minimization)
- Define breach response playbook for customer data including notification workflow, regulator contacts, and customer support surge plan

2. Harden OT access and recovery to reduce ransomware disruption risk

Electric Operations (OT)

Response	Mitigate
Owner	OT Security Program Manager
Gross Risk ($)	$1,620,000
Net Risk ($)	$420,000
Risk Reduction ($)	$1,200,000
Year 1 Cost ($)	$1,250,000
ROI	-4%
Review Date	August 15, 2026

Risk Statement

If ransomware compromises IT/DMZ systems that support OT access and operations, then operators may lose visibility/control and restoration speed will degrade, increasing outage duration and safety risk.

Mitigations

- Implement phishing-resistant MFA for privileged and OT-access roles (FIDO2 where feasible) and enforce conditional access
- Deploy privileged session management for OT bastions: session recording, command auditing, and just-in-time elevation
- Remove/disable clipboard and file transfer on OT jump hosts; implement controlled transfer workflow with malware scanning
- Implement immutable and offline backups for OT-supporting systems (bastions, identity dependencies, key configs) with quarterly restore tests
- Segment OT DMZ to restrict lateral movement: allow-list protocols, restrict admin pathways, and separate vendor access from internal admin access
- Establish ransomware response runbook for OT-supporting systems (restore order, decision points, communications) and run tabletop + technical drill

Note: Notional: assumes vendor remote access and OT/IT dependencies exist as described in the dossier.

3. Strengthen payment change controls to reduce BEC fraud risk

Enterprise IT + Governance

Response	Mitigate
Owner	Controller (Finance)
Gross Risk ($)	$1,400,000
Net Risk ($)	$375,000
Risk Reduction ($)	$1,025,000
Year 1 Cost ($)	$150,000
ROI	583%
Review Date	August 15, 2026

Risk Statement

If attackers compromise email accounts and manipulate AP workflows, then unauthorized wire transfers or vendor payment diversion may occur.

Mitigations

- Implement dual authorization for vendor banking changes and wire transfers with out-of-band verification
- Enforce phishing-resistant MFA for finance roles and admins; restrict legacy authentication
- Enable mailbox rule and forwarding detection with automated alerts and periodic audits for finance users
- Add payment workflow monitoring: flag changes to vendor banking, invoice routing, and approval anomalies
- Run quarterly BEC simulations tailored to AP/AR and procurement workflows; track and remediate repeat failure patterns

4. Govern vendor remote access to OT using PAM, approvals, and monitoring

Enterprise IT + Governance

Response	Mitigate
Owner	Cybersecurity Director
Gross Risk ($)	$1,320,000
Net Risk ($)	$500,000
Risk Reduction ($)	$820,000
Year 1 Cost ($)	$390,000
ROI	110%
Review Date	August 15, 2026

Risk Statement

If vendor remote access is overly permissive or vendor credentials are compromised, then attackers may reach OT jump hosts and critical OT systems.

Mitigations

- Create vendor access policy: time-bound approvals, just-in-time access, and mandatory MFA
- Route all vendor access through bastions with session recording; prohibit direct-to-OT access
- Require unique vendor accounts; disable shared credentials; enforce rotation and immediate deprovisioning at contract end
- Implement monthly access reviews and remove stale entitlements; monitor for anomalous vendor access times and actions
- Integrate vendor access logs into SIEM with alerts for high-privilege sessions and unusual activity

5. Reduce gas OT integrity risk with segmentation and change monitoring

Gas Operations (OT)

Response	Mitigate
Owner	Gas Operations Director
Gross Risk ($)	$1,200,000
Net Risk ($)	$360,000
Risk Reduction ($)	$840,000
Year 1 Cost ($)	$970,000
ROI	-13%
Review Date	August 15, 2026

Risk Statement

If an attacker gains OT access and manipulates gas alarms/setpoints, then unsafe pressure conditions may occur, increasing likelihood of leaks, emergency response, and regulatory escalation.

Mitigations

- Implement zone-based segmentation in gas OT (especially legacy Segment B): firewall allow-lists and restricted management networks
- Require MFA and PAM-backed workflows for all vendor OT access; eliminate shared vendor credentials and enforce time-bound access
- Deploy OT change detection for setpoints/alarms/configs with independent alerting to operators and security
- Define and test an operational integrity verification procedure (manual validation steps for critical setpoints after incidents)
- Harden engineering workstations and restrict programming interfaces; implement removable media controls
- Run a joint cyber-safety tabletop exercise focused on integrity manipulation and emergency response escalation

6. Optimize cyber insurance coverage to cap tail financial exposure

Enterprise IT + Governance

Response	Transfer
Owner	Risk Manager
Gross Risk ($)	$1,200,000
Net Risk ($)	$640,000
Risk Reduction ($)	$560,000
Year 1 Cost ($)	$325,000
ROI	72%
Review Date	August 15, 2026

Risk Statement

If a major cyber incident drives large restoration and response costs, then FREG may exceed planned financial tolerance; transfer mechanisms can cap exposure.

7. Implement resilient outage communications (DDoS protection + failover channels)

Customer Operations

Response	Mitigate
Owner	Customer Communications Lead
Gross Risk ($)	$540,000
Net Risk ($)	$195,000
Risk Reduction ($)	$345,000
Year 1 Cost ($)	$270,000
ROI	28%
Review Date	August 15, 2026

Risk Statement

If hacktivists or botnets disrupt the outage website or IVR, then customers lose visibility and call volumes surge, increasing operational burden during events.

Mitigations

- Place outage website behind DDoS protection and CDN caching; enable automatic origin failover
- Add WAF rules and rate limiting for common abuse patterns and bots
- Establish a secondary status channel (separate domain/provider) and pre-approved messaging templates for rapid switch-over
- Implement SMS provider failover and a recorded hotline script that can operate independently of OMS integration
- Run outage communications drills with IT and customer ops; validate RTO for OMS-to-web feed

8. Protect compliance evidence integrity with immutability and access controls

Enterprise IT + Governance

Response	Mitigate
Owner	Compliance Program Owner
Gross Risk ($)	$300,000
Net Risk ($)	$120,000
Risk Reduction ($)	$180,000
Year 1 Cost ($)	$125,000
ROI	44%
Review Date	August 15, 2026

Risk Statement

If compliance evidence repositories are altered or unavailable, then audit outcomes degrade and regulatory penalties become more likely.

Mitigations

- Implement immutable retention (WORM or object-lock) for key compliance evidence artifacts
- Add least-privilege access controls and quarterly access reviews for evidence repositories
- Enable change logging and checksum-based integrity verification for critical evidence sets
- Perform an annual audit readiness exercise and validate evidence collection procedures

9. Accept minor email/collaboration outages

Enterprise IT + Governance

Response	Accept
Owner	IT Operations Manager
Gross Risk ($)	$200,000
Net Risk ($)	$200,000
Risk Reduction ($)	$0
Year 1 Cost ($)	$0
ROI	0%
Review Date	August 15, 2026

Risk Statement

If M365 experiences a short service disruption, then some productivity loss will occur but mission impact remains manageable with established workarounds.

Residual Risk Summary

The proposed risk treatments reduce gross annual risk exposure from $4,310,000 to $1,715,000, a 60.2% reduction in expected annualized loss.

Top Residual Risks

RISK	MISSION AREA	NET RISK ($)	OWNER
Reduce customer data exposure via access controls and detection on CIS/MDM	**Customer Operations**	**$900,000**	**Customer Systems Manager**
Optimize cyber insurance coverage to cap tail financial exposure	**Enterprise IT + Governance**	**$640,000**	**Risk Manager**
Govern vendor remote access to OT using PAM, approvals, and monitoring	**Enterprise IT + Governance**	**$500,000**	**Cybersecurity Director**
Harden OT access and recovery to reduce ransomware disruption risk	**Electric Operations (OT)**	**$420,000**	**OT Security Program Manager**
Strengthen payment change controls to reduce BEC fraud risk	**Enterprise IT + Governance**	**$375,000**	**Controller (Finance)**
Reduce gas OT integrity risk with segmentation and change monitoring	**Gas Operations (OT)**	**$360,000**	**Gas Operations Director**
Accept minor email/collaboration outages	**Enterprise IT + Governance**	**$200,000**	**IT Operations Manager**
Implement resilient outage communications (DDoS protection + failover channels)	**Customer Operations**	**$195,000**	**Customer Communications Lead**
Protect compliance evidence integrity with immutability and access controls	**Enterprise IT + Governance**	**$120,000**	**Compliance Program Owner**

Complete Risk Register

RISK	MISSION AREA	RESPONSE	OWNER	GROSS RISK ($)	NET RISK ($)
Reduce customer data exposure via access controls and detection on CIS/MDM	Customer Operations	MITIGATE	Customer Systems Manager	**$1,950,000**	**$900,000**
Harden OT access and recovery to reduce ransomware disruption risk	Electric Operations (OT)	MITIGATE	OT Security Program Manager	**$1,620,000**	**$420,000**
Strengthen payment change controls to reduce BEC fraud risk	Enterprise IT + Governance	MITIGATE	Controller (Finance)	**$1,400,000**	**$375,000**
Govern vendor remote access to OT using PAM, approvals, and monitoring	Enterprise IT + Governance	MITIGATE	Cybersecurity Director	**$1,320,000**	**$500,000**
Reduce gas OT integrity risk with segmentation and change monitoring	Gas Operations (OT)	MITIGATE	Gas Operations Director	**$1,200,000**	**$360,000**
Optimize cyber insurance coverage to cap tail financial exposure	Enterprise IT + Governance	TRANSFER	Risk Manager	**$1,200,000**	**$640,000**
Implement resilient outage communications (DDoS protection + failover channels)	Customer Operations	MITIGATE	Customer Communications Lead	**$540,000**	**$195,000**

RISK	MISSION AREA	RESPONSE	OWNER	GROSS RISK ($)	NET RISK ($)
Protect compliance evidence integrity with immutability and access controls	Enterprise IT + Governance	MITIGATE	Compliance Program Owner	**$300,000**	**$120,000**
Accept minor email/collaboration outages	Enterprise IT + Governance	ACCEPT	IT Operations Manager	**$200,000**	**$200,000**

9

Appendix

A. Glossary | B. Methodology | C. Risk Scenario Master List | D. Threat Catalog | E. VEP Details by Mission Area | F. Critical Data Inventory | G. Asset Inventory | H. Service Inventory | I. Attack Surface Characterization | J. Mission Impact Detail | K. Data Notes & Disclaimers

A Glossary

TEF	Threat Event Frequency — how often a threat actor is expected to act against the target.
VEP	Vulnerability Event Probability — the probability a threat event results in a loss event.
LEF	Loss Event Frequency — the expected number of loss events per year (TEF × VEP).
LM	Loss Magnitude — the dollar impact of a single loss event.
EAL	Expected Annualized Loss — LEF × LM, the average yearly cost of a risk.
CORA	Cyber Operational Risk Assessment — a mission-centric risk assessment methodology.
RDR	Risk Detail Record — a documented risk with response strategy and mitigation plan.
Deny	Impact to availability — mission operations are interrupted or degraded.
Disclose	Impact to confidentiality — sensitive data is exposed to unauthorized parties.
Deceive	Impact to integrity — data is modified, corrupted, or made untrustworthy.

B Methodology

The CORA assessment follows an eight-step analytical flow:

1. Define the organization's mission and critical operational outcomes.
2. Model mission impact by quantifying financial consequences of Deny, Disclose, and Deceive effects.
3. Identify critical data and map it to mission areas through critical functions.
4. Analyze failure modes — how critical data can be corrupted, lost, or exposed.
5. Trace critical assets that store, process, or transmit critical data.
6. Trace service dependencies that support critical assets.
7. Assess the threat landscape — frequency, intent, capability, and targeting.
8. Evaluate vulnerability and attack surface exposure to determine loss event probability.

Risk is quantified as: Annualized Loss = Impact × Threat Event Frequency × Vulnerability Probability. This formula produces a dollar-denominated expected annual loss for each risk scenario.

C Risk Scenario Master List

THREAT	MISSION AREA	EFFECT	TEF	VEP	LEF	LOSS MAGNITUDE	ANNUALIZED LOSS
Financial Fraud / Phishing Group	**Customer Operations**	**Disclose**	**1.500**	**25.2%**	**0.377**	**$5,187,506**	**$1,957,906**
Ransomware Affiliate / Broker	**Electric Operations (OT)**	**Deny**	**0.488**	**24.1%**	**0.117**	**$5,827,778**	**$684,169**
Financial Fraud / Phishing Group	**Enterprise IT + Governance**	**Deceive**	**1.500**	**23.0%**	**0.345**	**$1,872,778**	**$646,516**

THREAT	MISSION AREA	EFFECT	TEF	VEP	LEF	LOSS MAGNITUDE	ANNUALIZED LOSS
Negligent User	Enterprise IT + Governance	Disclose	1.133	19.6%	0.222	$2,362,778	$525,452
Financial Fraud / Phishing Group	Enterprise IT + Governance	Deny	0.750	23.0%	0.173	$2,152,778	$371,589
Negligent User	Enterprise IT + Governance	Deny	0.567	19.6%	0.111	$2,152,778	$239,375
Ransomware Affiliate / Broker	Customer Operations	Disclose	0.163	25.1%	0.041	$5,187,506	$211,181
Contractor / Temp Worker	Gas Operations (OT)	Deceive	0.144	23.9%	0.034	$5,477,778	$188,655
Ideological Collective	Customer Operations	Disclose	0.150	21.4%	0.032	$5,187,506	$166,901
Ransomware Affiliate / Broker	Enterprise IT + Governance	Deny	0.325	22.8%	0.074	$2,152,778	$159,666
Contractor / Temp Worker	Gas Operations (OT)	Deny	0.144	23.9%	0.034	$4,167,778	$143,539
Ideological Collective	Customer Operations	Deny	0.450	21.4%	0.097	$1,297,778	$125,263
Ransomware Affiliate / Broker	Customer Operations	Deny	0.325	25.1%	0.081	$1,297,778	$105,664
Intelligence Service Proxy	Electric Operations (OT)	Deceive	0.029	24.9%	0.007	$4,157,778	$30,219
Contractor / Temp Worker	Electric Operations (OT)	Disclose	0.072	22.7%	0.016	$1,577,778	$25,800
Intelligence Service Proxy	Gas Operations (OT)	Deny	0.015	26.3%	0.004	$4,167,778	$15,996
Intelligence Service Proxy	Electric Operations (OT)	Disclose	0.029	24.9%	0.007	$1,577,778	$11,467
Intelligence Service Proxy	Enterprise IT + Governance	Disclose	0.015	23.9%	0.003	$2,362,778	$8,222

D Threat Catalog

Ransomware Affiliate / Broker (Cybercriminal)

Organized groups monetizing encryption and extortion.

TEF: 2.00/yr | Targeting: 0.65

Intelligence Service Proxy (Nation-State)

Contractors or shell companies performing state tasks covertly.

TEF: 0.35/yr | Targeting: 0.25

Financial Fraud / Phishing Group (Cybercriminal)

Credential or card-harvesting operations.

TEF: 5.00/yr | Targeting: 0.75

Contractor / Temp Worker (Insider)

External personnel with short-term access.

TEF: 0.80/yr | Targeting: 0.45

Ideological Collective (Hacktivist)

Decentralized activists (e.g., Anonymous-style).

TEF: 3.00/yr | Targeting: 0.20

Negligent User (Insider)

Unintentional insider through error or carelessness.

TEF: 2.00/yr | Targeting: 0.85

E VEP Details by Mission Area

Electric Operations (OT) — VEP: 24.9%

TACTIC	NECESSITY	PREVENTION	MITIGATION	WEIGHT	TACTIC VEP
Reconnaissance	60.0%	60.0%	60.0%	1.0	9.6%
Resource Development	60.0%	60.0%	60.0%	1.0	9.6%
Initial Access	100.0%	45.0%	55.0%	1.5	24.8%
Execution	60.0%	60.0%	60.0%	1.0	9.6%
Persistence	60.0%	60.0%	60.0%	1.0	9.6%
Privilege Escalation	60.0%	60.0%	60.0%	1.0	9.6%
Defense Evasion	70.0%	55.0%	50.0%	1.0	15.7%
Credential Access	80.0%	50.0%	55.0%	1.5	18.0%
Discovery	60.0%	60.0%	60.0%	1.0	9.6%
Lateral Movement	90.0%	45.0%	50.0%	1.5	24.8%
Collection	60.0%	60.0%	60.0%	1.0	9.6%
Command and Control	60.0%	60.0%	60.0%	1.0	9.6%
Exfiltration	60.0%	55.0%	55.0%	1.0	12.1%
Impact	90.0%	55.0%	55.0%	1.5	18.2%

Gas Operations (OT) — VEP: 26.3%

TACTIC	NECESSITY	PREVENTION	MITIGATION	WEIGHT	TACTIC VEP
Reconnaissance	60.0%	60.0%	60.0%	1.0	9.6%
Resource Development	60.0%	60.0%	60.0%	1.0	9.6%
Initial Access	100.0%	40.0%	50.0%	1.5	30.0%

TACTIC	NECESSITY	PREVENTION	MITIGATION	WEIGHT	TACTIC VEP
Execution	60.0%	60.0%	60.0%	1.0	9.6%
Persistence	60.0%	60.0%	60.0%	1.0	9.6%
Privilege Escalation	60.0%	60.0%	60.0%	1.0	9.6%
Defense Evasion	70.0%	50.0%	45.0%	1.0	19.3%
Credential Access	80.0%	45.0%	50.0%	1.5	22.0%
Discovery	60.0%	60.0%	60.0%	1.0	9.6%
Lateral Movement	90.0%	40.0%	45.0%	1.5	29.7%
Collection	60.0%	60.0%	60.0%	1.0	9.6%
Command and Control	60.0%	60.0%	60.0%	1.0	9.6%
Exfiltration	55.0%	55.0%	55.0%	1.0	11.1%
Impact	95.0%	55.0%	55.0%	1.5	19.2%

Customer Operations — VEP: 26.0%

TACTIC	NECESSITY	PREVENTION	MITIGATION	WEIGHT	TACTIC VEP
Reconnaissance	60.0%	60.0%	60.0%	1.0	9.6%
Resource Development	60.0%	60.0%	60.0%	1.0	9.6%
Initial Access	100.0%	40.0%	50.0%	1.5	30.0%
Execution	60.0%	60.0%	60.0%	1.0	9.6%
Persistence	60.0%	60.0%	60.0%	1.0	9.6%
Privilege Escalation	60.0%	60.0%	60.0%	1.0	9.6%
Defense Evasion	60.0%	60.0%	60.0%	1.0	9.6%
Credential Access	85.0%	45.0%	50.0%	1.5	23.4%
Discovery	60.0%	60.0%	60.0%	1.0	9.6%
Lateral Movement	60.0%	60.0%	60.0%	1.5	9.6%
Collection	60.0%	60.0%	60.0%	1.0	9.6%
Command and Control	70.0%	50.0%	55.0%	1.0	15.7%
Exfiltration	80.0%	45.0%	55.0%	1.0	19.8%
Impact	80.0%	55.0%	55.0%	1.5	16.2%

Enterprise IT + Governance — VEP: 23.9%

TACTIC	NECESSITY	PREVENTION	MITIGATION	WEIGHT	TACTIC VEP
Reconnaissance	60.0%	60.0%	60.0%	1.0	9.6%

TACTIC	NECESSITY	PREVENTION	MITIGATION	WEIGHT	TACTIC VEP
Resource Development	60.0%	60.0%	60.0%	1.0	9.6%
Initial Access	100.0%	45.0%	55.0%	1.5	24.8%
Execution	60.0%	60.0%	60.0%	1.0	9.6%
Persistence	60.0%	60.0%	60.0%	1.0	9.6%
Privilege Escalation	80.0%	55.0%	55.0%	1.0	16.2%
Defense Evasion	75.0%	55.0%	55.0%	1.0	15.2%
Credential Access	90.0%	45.0%	55.0%	1.5	22.3%
Discovery	60.0%	60.0%	60.0%	1.0	9.6%
Lateral Movement	60.0%	60.0%	60.0%	1.5	9.6%
Collection	60.0%	60.0%	60.0%	1.0	9.6%
Command and Control	60.0%	60.0%	60.0%	1.0	9.6%
Exfiltration	70.0%	55.0%	55.0%	1.0	14.2%
Impact	70.0%	60.0%	60.0%	1.5	11.2%

F Critical Data Inventory

MISSION AREA	FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Electric Operations (OT)	Grid monitoring and situational awareness	SCADA EMS real-time telemetry	8000	OPS
Electric Operations (OT)	Grid monitoring and situational awareness	State estimator inputs	8000	OPS
Electric Operations (OT)	Grid monitoring and situational awareness	SCADA point database	8000	OPS,IP
Electric Operations (OT)	Grid monitoring and situational awareness	Tag mappings	8000	OPS,IP
Electric Operations (OT)	Grid monitoring and situational awareness	Naming standards	10	OPS,IP
Electric Operations (OT)	Grid monitoring and situational awareness	Operator displays	800	OPS,IP
Electric Operations (OT)	Grid monitoring and situational awareness	HMI configurations	700	OPS,IP
Electric Operations (OT)	Grid monitoring and situational awareness	Grid one-lines	50	OPS,IP
Electric Operations (OT)	Grid monitoring and situational awareness	Visualization layers	200	OPS,IP
Electric Operations (OT)	Distribution switching and control execution	Switching orders (approved)	200000	OPS

MISSION AREA	FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Electric Operations (OT)	Distribution switching and control execution	Operating instructions (switching)	5000	OPS,IP
Electric Operations (OT)	Distribution switching and control execution	Control setpoints (current)	20000	OPS
Electric Operations (OT)	Distribution switching and control execution	Protection settings (current)	20000	OPS
Electric Operations (OT)	Outage detection and event triage	Outage events	500000	OPS
Electric Operations (OT)	Outage detection and event triage	Outage alarms	500000	OPS
Electric Operations (OT)	Outage detection and event triage	Customer outage reports (summary)	410000	OPS
Electric Operations (OT)	Crew dispatch and restoration coordination	Crew assignments	300000	OPS
Electric Operations (OT)	Crew dispatch and restoration coordination	Dispatch tickets	300000	OPS
Electric Operations (OT)	Crew dispatch and restoration coordination	Restoration plans	120000	OPS
Electric Operations (OT)	Crew dispatch and restoration coordination	Switching backout plans	120000	OPS
Electric Operations (OT)	RTO coordination and telemetry exchange (ICCP)	ICCP telemetry point list	2000	OPS,IP
Electric Operations (OT)	RTO coordination and telemetry exchange (ICCP)	ICCP point mappings	2000	OPS,IP
Electric Operations (OT)	RTO coordination and telemetry exchange (ICCP)	RTO dispatch instructions	50000	OPS
Electric Operations (OT)	RTO coordination and telemetry exchange (ICCP)	RTO communications logs	50000	OPS
Gas Operations (OT)	Pressure and flow monitoring	Gas pressure telemetry	6000	OPS
Gas Operations (OT)	Pressure and flow monitoring	Gas flow telemetry	6000	OPS
Gas Operations (OT)	Pressure and flow monitoring	Valve state telemetry	6000	OPS
Gas Operations (OT)	Pressure and flow monitoring	Compressor state telemetry	6000	OPS
Gas Operations (OT)	Valve control and isolation operations	Valve control configurations	1200	OPS,IP
Gas Operations (OT)	Valve control and isolation operations	Control logic parameters	1200	OPS,IP
Gas Operations (OT)	Valve control and isolation operations	Isolation procedures	2000	OPS,IP
Gas Operations (OT)	Valve control and isolation operations	Emergency shutdown steps	2000	OPS,IP
Gas Operations (OT)	Alarm triage and operational decision support	Alarm thresholds (current)	4000	OPS

MISSION AREA	FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Gas Operations (OT)	Alarm triage and operational decision support	Setpoint limits (current)	4000	OPS
Gas Operations (OT)	Alarm triage and operational decision support	Shift notes	120000	OPS
Gas Operations (OT)	Alarm triage and operational decision support	Operational decision logs	120000	OPS
Gas Operations (OT)	Emergency dispatch and response coordination	Emergency calls	60000	OPS,PII
Gas Operations (OT)	Emergency dispatch and response coordination	Dispatch tickets	90000	OPS,PII
Gas Operations (OT)	Emergency dispatch and response coordination	Responder on-call rosters	5000	PII
Gas Operations (OT)	Emergency dispatch and response coordination	Responder contact lists	5000	PII
Gas Operations (OT)	Leak survey and safety inspection workflow	Leak survey records	250000	OPS
Gas Operations (OT)	Leak survey and safety inspection workflow	Inspection findings	250000	OPS
Gas Operations (OT)	Leak survey and safety inspection workflow	Corrective action work orders	150000	OPS
Customer Operations	Inbound customer contact intake (IVR/call center)	IVR call routing configuration	1	OPS,IP
Customer Operations	Inbound customer contact intake (IVR/call center)	Call logs	410000	PII
Customer Operations	Inbound customer contact intake (IVR/call center)	Customer contact history	410000	PII
Customer Operations	Outage notifications and public communications	Outage notification message templates	200	OPS
Customer Operations	Outage notifications and public communications	Customer contact list for notifications	410000	PII
Customer Operations	Customer account management	Customer account master records	705000	PII,FIN
Customer Operations	Customer account management	Service address data	705000	PII
Customer Operations	Customer account management	Premise data	705000	PII
Customer Operations	Billing cycle execution	Billing rules configuration	2000	OPS,IP
Customer Operations	Billing cycle execution	Tariff configuration	2000	OPS,IP
Customer Operations	Billing cycle execution	Bills history	352500	PII,FIN

MISSION AREA	FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Customer Operations	Billing cycle execution	Statements history	352500	PII,FIN
Customer Operations	Payment processing and settlement	Payment transactions	705000	FIN,PII
Customer Operations	Payment processing and settlement	Settlement records	705000	FIN,PII
Customer Operations	Payment processing and settlement	Payment processor integration keys	50	CRED,OPS
Customer Operations	Payment processing and settlement	Payment processor integration configuration	50	OPS,IP
Customer Operations	Meter data ingestion and validation	Electric smart meter interval data (15-min)	410000	OPS
Customer Operations	Meter data ingestion and validation	Gas meter reads (monthly)	295000	OPS
Enterprise IT + Governance	Identity and authentication services (AD/LDAP/SSO)	Directory objects (users)	100000	CRED,OPS
Enterprise IT + Governance	Identity and authentication services (AD/LDAP/SSO)	Directory group objects	5000	CRED,OPS
Enterprise IT + Governance	Identity and authentication services (AD/LDAP/SSO)	Directory role assignments	500	CRED,OPS
Enterprise IT + Governance	Identity and authentication services (AD/LDAP/SSO)	Authentication logs	4500000	OPS
Enterprise IT + Governance	Identity and authentication services (AD/LDAP/SSO)	Sign-in logs	4500000	OPS
Enterprise IT + Governance	Privileged access management (PAM + admin workflows)	Privileged account inventory	5000	CRED,OPS
Enterprise IT + Governance	Privileged access management (PAM + admin workflows)	PAM vault policies	500	CRED,OPS
Enterprise IT + Governance	Privileged access management (PAM + admin workflows)	Privileged access workflows	500	CRED,OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	DNS zone data	2000	OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	DNS resolver configuration	2000	OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	DHCP scopes	5000	OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	DHCP reservations	5000	OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	NTP configuration	50	OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	Time source list	10	OPS
Enterprise IT + Governance	Core network services (DNS/DHCP/NTP)	Upstream time references	40	OPS

MISSION AREA	FUNCTION	DATA	RECORDS	CLASSIFICATIONS
Enterprise IT + Governance	Remote access services (VPN, bastions, vendor access)	VPN configuration	200	OPS,CRED
Enterprise IT + Governance	Remote access services (VPN, bastions, vendor access)	VPN access policies	200	OPS,CRED
Enterprise IT + Governance	Remote access services (VPN, bastions, vendor access)	Bastion session logs	250000	OPS
Enterprise IT + Governance	Remote access services (VPN, bastions, vendor access)	Bastion session recordings	250000	OPS
Enterprise IT + Governance	Backup/restore and disaster recovery operations	Backup catalogs	500	OPS,IP
Enterprise IT + Governance	Backup/restore and disaster recovery operations	Restore runbooks	500	OPS,IP
Enterprise IT + Governance	Backup/restore and disaster recovery operations	Golden images	200	OPS,IP
Enterprise IT + Governance	Backup/restore and disaster recovery operations	Baseline configurations for recovery	200	OPS,IP
Enterprise IT + Governance	Compliance evidence management and audit readiness	NERC CIP evidence artifacts	45000	OPS
Enterprise IT + Governance	Compliance evidence management and audit readiness	Audit trail for evidence repository	45000	OPS
Enterprise IT + Governance	Compliance evidence management and audit readiness	Control test results	20000	OPS
Enterprise IT + Governance	Compliance evidence management and audit readiness	Remediation tracking records	20000	OPS
Enterprise IT + Governance	Incident reporting and regulatory notifications	Incident timelines	1500	OPS
Enterprise IT + Governance	Incident reporting and regulatory notifications	Notification records	1500	OPS
Enterprise IT + Governance	Incident reporting and regulatory notifications	Regulatory submissions	2500	OPS
Enterprise IT + Governance	Incident reporting and regulatory notifications	Regulatory correspondence	2500	OPS

G Asset Inventory

ASSET	TYPE	ZONE	OWNER
Electric SCADA/EMS Server Cluster (VMs)	Application	OT-E	Grid Operations
Electric DMS Application Server (VMs)	Application	OT-E	Grid Operations
Electric Historian Server (VM)	Application	OT-E	Grid Operations
Gas SCADA Server Cluster (VMs)	Application	OT-G	Gas Operations
OMS Application Server (VMs)	Application	IT/DMZ	Grid Operations

ASSET	TYPE	ZONE	OWNER
OMS Database Server (VM)	Platform	IT	Grid Operations
Public Outage Website Web Server (DMZ)	Application	DMZ	Customer Ops
Call Center / IVR Platform	Platform	IT	Customer Ops
CIS Application Servers (VMs)	Application	IT	Customer Ops
CIS Database Server (VM)	Platform	IT	Customer Ops
MDM Ingestion/Processing Server (VMs)	Application	IT	Customer Ops
MDM Database Server (VM)	Platform	IT	Customer Ops
Active Directory Domain Controllers (VMs)	Infrastructure	IT	IT Operations
Entra ID / Azure AD Tenant	Platform	Cloud	IT Operations
DNS Servers (Primary/Secondary VMs)	Infrastructure	IT	IT Operations
DHCP Servers (VMs)	Infrastructure	IT	IT Operations
NTP Time Source Appliance	Infrastructure	IT	IT Operations
Edge Firewall/VPN Gateway Appliance	Infrastructure	IT/DMZ	IT Operations
OT Bastion / Jump Hosts (Hardened VMs)	Infrastructure	DMZ	Cybersecurity
PAM Vault Server (VM)	Application	IT	Cybersecurity
Backup Platform Server/Appliance	Infrastructure	IT	IT Operations
SIEM Platform	Platform	IT	Security Operations
GRC / Evidence Repository (VM)	Application	IT	Compliance

H Service Inventory

SERVICE	TYPE	VENDOR	EXTERNAL
Active Directory Service (LDAP/Kerberos)	Internal	Microsoft	No
Entra ID Service	Cloud	Microsoft	Yes
DNS Service	Internal	Microsoft/BIND	No
DHCP Service	Internal	Microsoft	No
NTP Time Sync Service	Internal	Meinberg/Appliance	No
Remote Access VPN Service	Internal	Palo Alto/Fortinet/Cisco	No
OT Bastion Jump Host Service	Internal	Windows/Linux	No
Privileged Access Management Service	Internal	CyberArk/BeyondTrust	No
Backup Service	Internal	Veeam/Commvault	No
Restore and Recovery Service	Internal	Veeam/Commvault	No

SERVICE	TYPE	VENDOR	EXTERNAL
Central Logging Service	Internal	Syslog/Agent	No
SIEM Service	Internal	Splunk/QRadar/Sentinel	No

I Attack Surface Characterization

ENTITY	ENTRY POINT	PROTOCOL	DIRECTION	PRIVILEGES
Internet	Public outage website	HTTPS	Inbound	user
Internet	Email phishing / credential theft	SMTP/HTTPS	Inbound	user
Internet	VPN gateway remote access	VPN	Inbound	user
OT Vendor	Vendor remote support to OT bastions	VPN/RDP	Inbound	admin
RTO	ICCP telemetry exchange	ICCP	Bidirectional	service
Payment Processor	Payment processing integration	HTTPS	Bidirectional	service
Telecom Carrier	OT telemetry backhaul circuits	MPLS/IP	Bidirectional	service
Cloud Provider	Cloud identity and email services	HTTPS	Bidirectional	service
Internet	External DNS resolution and zone transfers (if misconfigured)	DNS	Bidirectional	service
Internal Systems	Log forwarding to SIEM	Syslog/Agent	Outbound	service
Internal Users	GRC evidence repository access	HTTPS	Bidirectional	user
Field Workforce	Field laptops and tablets accessing work systems	HTTPS/VPN	Bidirectional	user

J Mission Impact Detail

MISSION AREA	BASELINE	DENY	DISCLOSE	DECEIVE	TOTAL
Electric Operations (OT)	$330,000	$5,470,000	$1,220,000	$3,800,000	$10,820,000
Gas Operations (OT)	$330,000	$3,810,000	$860,000	$5,120,000	$10,120,000
Customer Operations	$130,000	$1,140,000	$5,029,728	$2,820,000	$9,119,728
Enterprise IT + Governance	$285,000	$1,840,000	$2,050,000	$1,560,000	$5,735,000
Total	$1,075,000	$12,260,000	$9,159,728	$13,300,000	$35,794,728

K Data Notes & Disclaimers

- Schema: CORA-v1
- Assessment created: 2026-02-15
- Last updated: 2026-02-15
- Mission areas defined: 4
- Threats in scope: 6
- Risk detail records: 9

What to Do Next

Validate OT remote access paths and segmentation (especially gas OT Segment B), confirm backup/restore RTO/RPO for OT-supporting systems, and run a combined tabletop exercise for ransomware and OT safety scenarios. Then convert the top mitigations into an owned roadmap with dates.

Disclaimers

Notional demo output only. Not based on an actual assessment of FREG systems.