MARCH 21, 2023

RELIABILITY & SECURITY

Virtual Workshop

WECC

Oversight Planning & Risk Assessment

March 21, 2023

Scott Brooksby

Patrick VanGuilder

Agenda

- Oversight Process
- A Tale of Two Entities
- Compare performance considerations and profiles between the two entities
- Monitoring differences
- Oversight options

Oversight Process

A Tale of Two Entities

ORKO Electric Company

GO/GOP	GO/GOP
Medium sized	Medium sized
Cold climate/region	Warm climate/region
Detailed entity data available	Basic entity data available
Program validated with no issues at past two audits	Program issues found at past two audits
Few PNCs, mostly self-reported	PNCs generally found at audit and not self-detected

CIP Risk Assessment

CIP Key Performance Considerations	CIP Key Performance Considerations
Past audits: No findings, some positive observations	Past audits: Regular findings. Sunbear Power has few detective controls
PNCs: Low number, mature detective controls, strong future prevention	PNCs: Moderate number, minimal mitigation effort
No reported cybersecurity incidents	No reported cybersecurity incidents
Internal controls: Meets target maturity	Internal controls: Meets target maturity in less than half of controls
Culture of compliance: Aligned with NERC CIP standards, enforced throughout program	Culture of compliance: Not consistent. Different departments drive their compliance responsibility
	IT department: Inadequate funding and staffing compared to similar entities

CIP Operational Concerns

CIP Operational Concerns	CIP Operational Concerns
Failure to implement adequate security monitoring results in undetected cyber-events, the inability to manage remote connections, and increases the likelihood of losing data, control, or critical systems. Does Orko know when their vendors connect to their systems?	*Failure to coordinate product or service vendor representative access results in high-risk physical access to BCS.* Sunbear has failed to control logical and physical access from third parties in the past and appears to keep the minimum level to run the business.
Failure to coordinate incident notification with product or service vendors fails to implement risk mitigations. Is Orko notified when a third party is compromised? (e.g., SolarWinds)	*Failure to identify, document, and mitigate cyber-asset vulnerabilities results in an increased likelihood of successful, malicious activity and loss of data, control, or critical systems.* Sunbear's cyber-asset infrastructure is aging, and vulnerabilities are harder to compensate. Program is under resourced.

CIP Monitoring

CIP Monitoring Scope	CIP Monitoring Scope
CIP-005-7 R2.4, 2.5, R3	CIP-004-6 R4, R5
CIP-010-3 R1, R3	CIP-005-7 R2, R3
CIP-013-2 R1, R2	CIP-006-6 R1
	CIP-007-6 R2, R3
	CIP-010-3 R1, R3
	CIP-013-2 R1, R2

O&P Risk Assessment

O&P Key Performance Considerations	O&P Key Performance Considerations
No PNCs at last audit	Multiple PNCs at last audit
Low number of PNCs (all Self-Reports). Submitted within a reasonable time of discovery, including remediation steps and effective mitigation	Numerous PNCs, Self-Reports submitted routinely just before audit. Mitigation typically must be requested
Recent commissioning of a second combustion turbine site	No recent changes to BES equipment
RSAWs and response to data requests always prompt and complete	RSAWs indicate minimal effort. Response to data requests occasionally on time
Previous audit interviews indicate an open and transparent compliance program with WECC	Previous audit interviews do not indicate a strong culture of compliance

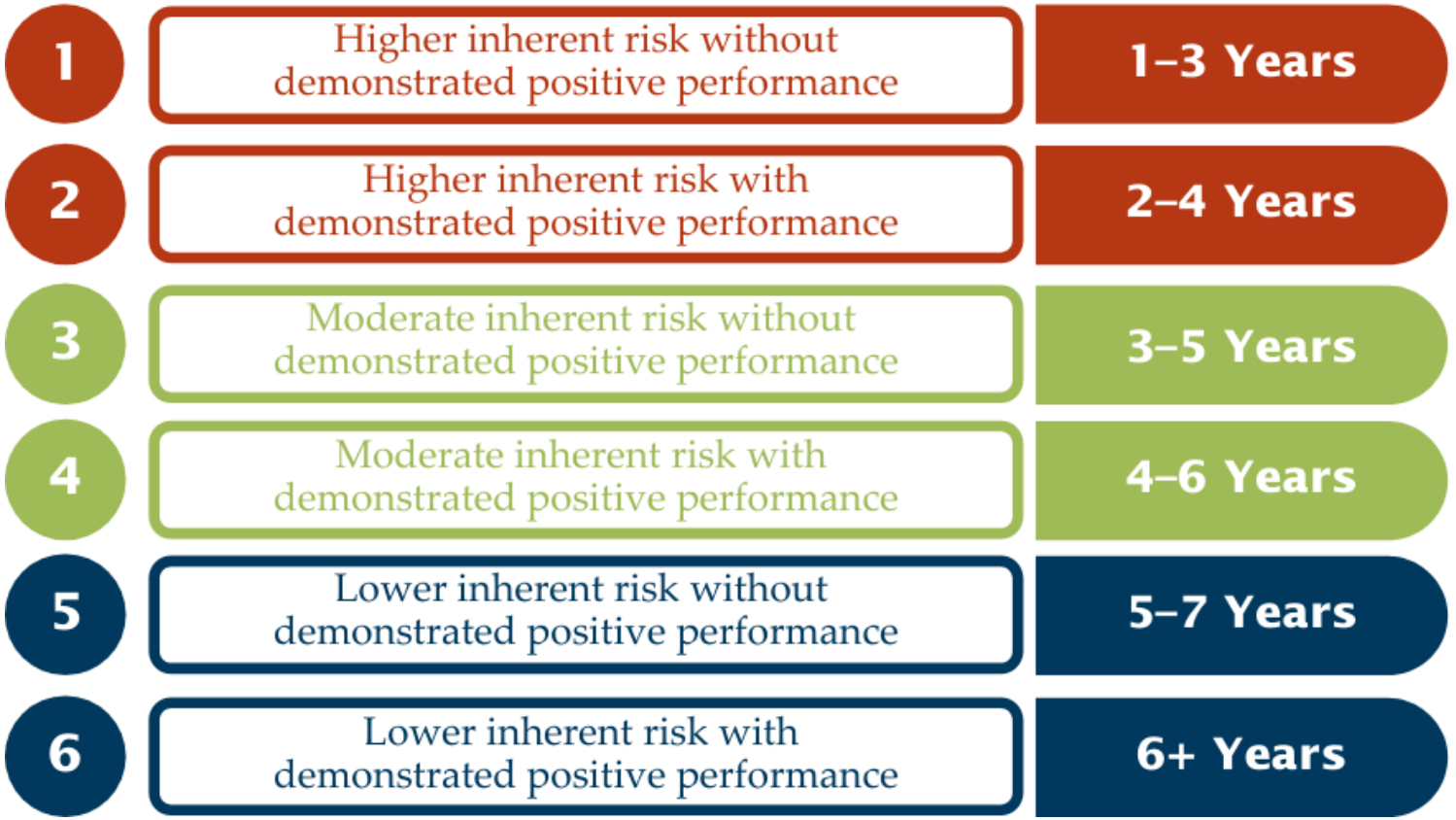
O&P Operational Concerns

O&P Operational Concerns	O&P Operational Concerns
Failure to maintain an updated cold weather preparedness plan could result in an omission of new equipment from the plan. What process has Orko developed to ensure its cold weather preparedness plan is periodically reviewed and updated?	*Failure to develop an adequate cold weather preparedness plan could result in equipment not being maintained as needed.* Sunbear Power has had asset identification failures in the past and has not demonstrated positive performance when implementing new Requirements.
Failure to identify all applicable personnel that need training on the cold weather preparedness plan could result in untrained personnel and increase the likelihood of failing to implement necessary measures. Has Orko identified the appropriate personnel at its new generating station?	*Failure to train personnel on the implementation of a cold weather preparedness plan could result in equipment not operating as expected and increase the likelihood of affecting the output of the generating station.* Sunbear Power has had issues in the past with adequately training its personnel.

O&P Monitoring

O&P Monitoring Scope	O&P Monitoring Scope
COM-002-4 R3	COM-002-4 R3
FAC-008-5 R6	FAC-003-4 R6
EOP-011-2 R7, R8	FAC-008-5 R6
MOD-025-2 R1, R2	EOP-011-2 R7, R8
PRC-024-3 R1, R2	MOD-025-2 R1, R2
	PRC-005-6 R3
	PRC-019-2 R1
	PRC-024-3 R1, R2
	VAR-002-4.1 R1, R2

Oversight Options



- Self-Certification
- Spot Check
- Investigation
- Audit

WECC

Electric Reliability and Security for the West

www.wecc.org