UK NCSC CAF Gap Assessment

Dunmara OWF — WTG SCADA and comms network

ORGANISATION	Dunmara Offshore Wind Ltd (fictional sample operator)
SITE / SYSTEM	Dunmara OWF — WTG SCADA and comms network
ASSESSOR	A. Whitfield
ASSESSMENT DATE	2026-08-10
FRAMEWORK	UK NCSC CAF v4.0 (Aug 2025)
TARGET PROFILE	Enhanced, regulatory deadline 2027-12-31
SCOPE	Onshore control room, OSS LAN, WTG fibre ring. Excludes corporate IT (separately segmented). OEM remote support access in scope.
DOCUMENT STATUS	DRAFT (for review)

Executive summary

AI-drafted; reviewed and issued under the responsibility of the named assessor.

Dunmara Offshore Wind Ltd's WTG SCADA and communications environment achieves an overall CAF position of 40% across the 33 contributing outcomes assessed. Governance and risk management are comparatively mature at 61%, indicating that basic organisational foundations exist, and protective measures sit at 45% with a large body of partially implemented controls that could be closed with focused effort. The critical weakness is detection: Objective C scores 7%, with no implemented outcomes, no security monitoring at all on the WTG fibre ring, and OSS LAN logs collected but never reviewed. In practice this means an intrusion into the turbine control network would be unlikely to be identified by the operator.

Objective D compounds this exposure at 30%: response plans and recovery capability exist only in partial form, testing and exercising is absent, and there is no mechanism to feed incident learning back into control improvement. Third party risk is a further concern, as OEM remote support routes through a jump host without session recording, and secure software development and support, IdAM and cyber security training are recorded as full gaps. The combined picture is an operator that can articulate its risks but cannot yet see, contain or learn from an attack on operational technology. Priority should therefore be given to establishing baseline visibility and privileged access assurance, then consolidating the substantial partial outcomes into sustained practice.

1. Enable session recording and full logging on the OEM remote support jump host, and review all standing third party access rights (Immediate).
2. Deploy passive OT network monitoring on the WTG fibre ring and OSS LAN to establish baseline asset and traffic visibility (Immediate).
3. Stand up log aggregation with tamper resistant retention and a defined daily triage routine with named owners for OT alerts (Immediate).
4. Close the IdAM gap: complete account inventory, remove shared and orphaned accounts, and enforce multi factor authentication for all remote and privileged access (Immediate).
5. Complete and validate the OT incident response plan, including offshore specific scenarios, escalation routes and OEM contact paths (Near-term).
6. Run a tabletop exercise followed by a technical recovery test, proving backup restoration for SCADA servers and turbine controllers (Near-term).
7. Deliver role based cyber security training for control room, offshore technicians and engineering staff, with competence tracking (Near-term).
8. Formalise secure configuration baselines, supply chain security requirements in OEM contracts, secure development assurance and a post incident learning process (Planned).

1. Overall position

The assessment covered 41 contributing outcomes under UK NCSC CAF. Not yet meeting the Enhanced Profile: 31 outcomes below target. The CAF produces individual outcome judgements, not a score; assessment progress is **80%** of outcomes given a status. 9 contributing outcome(s) are recorded as not achieved and 15 as partially achieved; these are listed in the gap register (section 3) and should be addressed in order of severity. 8 of 41 contributing outcomes are evidenced (a justification or a linked evidence record).

UK NCSC CAF Gap Assessment

Dunmara OWF — WTG SCADA and comms network

Profile attainment

Not yet meeting the Enhanced Profile: 31 outcomes below target. Deadline 2027-12-31: 16 months remaining.

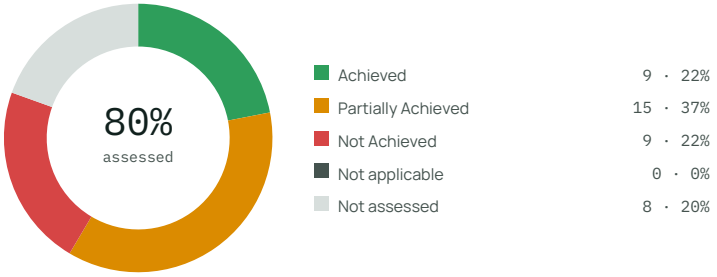
REF	CONTRIBUTING OUTCOME	PRINCIPLE	TARGET	CURRENT
A1.c	Decision-making	A1	Achieved	Partially Achieved
A2.c	Assurance	A2	Achieved	Not assessed
A4.a	Supply Chain	A4	Achieved	Partially Achieved
A4.b	Secure Software Development and Support	A4	Achieved	Not Achieved
B1.b	Policy, Process and Procedure Implementation	B1	Achieved	Partially Achieved
B2.a	Identity Verification, Authentication and Authorisation	B2	Achieved	Partially Achieved
B2.c	Privileged User Management	B2	Achieved	Partially Achieved
B2.d	Identity and Access Management (IdAM)	B2	Achieved	Not Achieved
B3.b	Data in Transit	B3	Achieved	Not assessed
B3.c	Stored Data	B3	Achieved	Not assessed
B3.d	Mobile Data	B3	Achieved	Not assessed
B3.e	Media / Equipment Sanitisation	B3	Achieved	Not assessed
B4.a	Secure by Design	B4	Achieved	Partially Achieved
B4.b	Secure Configuration	B4	Achieved	Partially Achieved
B4.d	Vulnerability Management	B4	Achieved	Not assessed
B5.a	Resilience Preparation	B5	Achieved	Partially Achieved
B5.c	Backups	B5	Achieved	Partially Achieved
B6.a	Cyber Security Culture	B6	Achieved	Partially Achieved
B6.b	Cyber Security Training	B6	Achieved	Not Achieved
C1.a	Sources and Tools for Logging and Monitoring	C1	Achieved	Not Achieved
C1.b	Securing Logs	C1	Achieved	Not Achieved
C1.c	Generating Alerts	C1	Achieved	Partially Achieved
C1.d	Triage of Security Alerts	C1	Achieved	Not Achieved
C1.e	Personnel Skills for Monitoring and Detection	C1	Achieved	Not assessed
C1.f	Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	C1	Partially Achieved	Not assessed
C2.a	Threat Hunting	C2	Partially Achieved	Not Achieved

UK NCSC CAF Gap Assessment

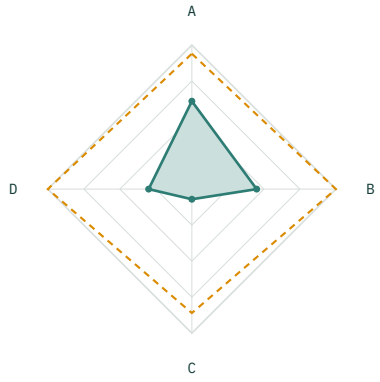
Dunmara OWF — WTG SCADA and comms network

REF	CONTRIBUTING OUTCOME	PRINCIPLE	TARGET	CURRENT
D1.a	Response Plan	D1	Achieved	Partially Achieved
D1.b	Response and Recovery Capability	D1	Achieved	Partially Achieved
D1.c	Testing and Exercising	D1	Achieved	Not Achieved
D2.a	Post Incident Analysis	D2	Achieved	Partially Achieved
D2.b	Using Incidents to Drive Improvements	D2	Achieved	Not Achieved

STATUS DISTRIBUTION



POSITION BY OBJECTIVE



Solid: current position. Dashed: Enhanced Profile target.

Principles: status counts

REF	PRINCIPLE	MET?	ACHIEVED	PARTIALLY ACHIEVED	NOT ACHIEVED	NOT APPLICABLE	NOT ASSESSED
OBJ A · MANAGING SECURITY RISK							
A1	Governance	Not met (1)	2	1	0	0	0
A2	Risk Management	Not met (1)	1	1	0	0	1
A3	Asset Management	Met	1	0	0	0	0
A4	Supply Chain	Not met (2)	0	1	1	0	0
OBJ B · PROTECTING AGAINST CYBER ATTACK							
B1	Service Protection Policies, Processes and Procedures	Not met (1)	1	1	0	0	0
B2	Identity and Access Control	Not met (3)	1	2	1	0	0
B3	Data Security	Not met (4)	1	0	0	0	4
B4	System Security	Not met (3)	1	2	0	0	1
B5	Resilient Networks and Systems	Not met (2)	1	2	0	0	0

UK NCSC CAF Gap Assessment

Dunmara OWF — WTG SCADA and comms network

REF	PRINCIPLE	MET?	ACHIEVED	PARTIALLY ACHIEVED	NOT ACHIEVED	NOT APPLICABLE	NOT ASSESSED
B6	Staff Awareness and Training	Not met (2)	0	1	1	0	0
OBJ C · DETECTING CYBER SECURITY EVENTS							
C1	Security Monitoring	Not met (6)	0	1	3	0	2
C2	Threat Hunting	Not met (1)	0	0	1	0	0
OBJ D · MINIMISING THE IMPACT OF CYBER SECURITY INCIDENTS							
D1	Response and Recovery Planning	Not met (3)	0	2	1	0	0
D2	Lessons Learned	Not met (2)	0	1	1	0	0

2. Principle summary

REF	PRINCIPLE	MET?	ACHIEVED	PARTIAL	NOT ACHIEVED	NOT ASSESSED
OBJ A · MANAGING SECURITY RISK						
A1	Governance	Not met (1)	2	1	0	0
A2	Risk Management	Not met (1)	1	1	0	1
A3	Asset Management	Met	1	0	0	0
A4	Supply Chain	Not met (2)	0	1	1	0
OBJ B · PROTECTING AGAINST CYBER ATTACK						
B1	Service Protection Policies, Processes and Procedures	Not met (1)	1	1	0	0
B2	Identity and Access Control	Not met (3)	1	2	1	0
B3	Data Security	Not met (4)	1	0	0	4
B4	System Security	Not met (3)	1	2	0	1
B5	Resilient Networks and Systems	Not met (2)	1	2	0	0
B6	Staff Awareness and Training	Not met (2)	0	1	1	0
OBJ C · DETECTING CYBER SECURITY EVENTS						
C1	Security Monitoring	Not met (6)	0	1	3	2
C2	Threat Hunting	Not met (1)	0	0	1	0
OBJ D · MINIMISING THE IMPACT OF CYBER SECURITY INCIDENTS						
D1	Response and Recovery Planning	Not met (3)	0	2	1	0
D2	Lessons Learned	Not met (2)	0	1	1	0

3. Gap register

SEVERITY	REF	CONTRIBUTING OUTCOME	NOTES / EVIDENCE
GAP BELOW TARGET	A4.b	Secure Software Development and Support	-

UK NCSC CAF Gap Assessment

Dunmara OWF — WTG SCADA and comms network

SEVERITY	REF	CONTRIBUTING OUTCOME	NOTES / EVIDENCE
GAP BELOW TARGET	B2.d	Identity and Access Management (IdAM)	-
GAP BELOW TARGET	B6.b	Cyber Security Training	-
GAP BELOW TARGET	C1.a	Sources and Tools for Logging and Monitoring	No security monitoring on the WTG ring; OSS LAN logs are collected but not reviewed.
GAP BELOW TARGET	C1.b	Securing Logs	-
GAP BELOW TARGET	C1.d	Triage of Security Alerts	-
GAP BELOW TARGET	C2.a	Threat Hunting	-
GAP BELOW TARGET	D1.c	Testing and Exercising	-
GAP BELOW TARGET	D2.b	Using Incidents to Drive Improvements	-
PARTIAL BELOW TARGET	A1.c	Decision-making	-
PARTIAL	A2.b	Understanding Threat	-
PARTIAL BELOW TARGET	A4.a	Supply Chain	-
PARTIAL BELOW TARGET	B1.b	Policy, Process and Procedure Implementation	-
PARTIAL BELOW TARGET EXCEPTION	B2.a	Identity Verification, Authentication and Authorisation	-
PARTIAL BELOW TARGET	B2.c	Privileged User Management	OEM remote support uses the jump host, but session recording is not yet enabled. [DUN-OPS-0201]
PARTIAL BELOW TARGET	B4.a	Secure by Design	[DUN-OPS-0142] [DUN-NET-0031]
PARTIAL BELOW TARGET	B4.b	Secure Configuration	[DUN-NET-0031]
PARTIAL BELOW TARGET	B5.a	Resilience Preparation	-
PARTIAL BELOW TARGET	B5.c	Backups	-
PARTIAL BELOW TARGET	B6.a	Cyber Security Culture	-
PARTIAL BELOW TARGET	C1.c	Generating Alerts	-
PARTIAL BELOW TARGET	D1.a	Response Plan	-
PARTIAL BELOW TARGET	D1.b	Response and Recovery Capability	-

UK NCSC CAF Gap Assessment

Dunmara OWF — WTG SCADA and comms network

SEVERITY	REF	CONTRIBUTING OUTCOME	NOTES / EVIDENCE
PARTIAL BELOW TARGET	D2.a	Post Incident Analysis	-

Appendix A. Evidence register

TITLE	REFERENCE	TYPE	STATUS	LOCATION	OWNER	VERSION	DATE	REVIEW DUE	OUTCOMES
OT Asset Register OT assets are recorded with owners and criticality	DUN-OPS-0142	Register	Approved	-	OT Operations	2.4	-	2027-03-10	A3.a, B4.a
OT Security Policy Board-approved policy covering the OT estate	DUN-POL-001	Policy	Published	-	CISO	3.1	-	2027-06-10	A1.a, A1.b, B1.a
Network segmentation diagram Zoning between OSS LAN, WTG ring and corporate boundary	DUN-NET-0031	Diagram	Draft	-	OT Engineering	0.9	-	2026-07-29	B4.a, B4.b
OEM remote access procedure Remote support access by the turbine OEM is controlled and logged	DUN-OPS-0201	Procedure	In review	-	OT Operations	1.2	-	2026-12-10	B2.c

4. Exception systems register

SYSTEM / ASSET CLASS	SITES	AFFECTED OUTCOMES	JUSTIFICATION	COMPENSATING CONTROLS	IN RISK REGISTER
Legacy turbine controller network	WTG strings 1-4	B2.a	Controllers cannot authenticate individual users; firmware is vendor-locked and cannot be modified without voiding OEM support.	Physical access control at the towers, access only via the recorded jump host, segmentation from the OSS LAN.	Yes