OFFICIAL CYBER PROTECTION PARTNER

Blue Light Operational Recovery Readiness Assessment

A practical assessment for emergency-service continuity, control-room resilience and critical operational systems

CORE QUESTION
If a critical control-room, mobilisation or operational system failed today, how confidently could emergency response operations be restored?

PURPOSE
Use this assessment to identify where operational recovery confidence is supported by evidence, where assumptions remain, and where further validation is required.

ASSESSMENT DETAILS

Organisation: _____	Service / operation: _____
Completed by: _____	Date: _____ Review date: _____

EVIDENCE EXAMPLES
Recovery-test records, critical-system inventories, dependency maps, RTO/RPO agreements, recovery runbooks, configuration backups, clean recovery-point evidence, escalation procedures and documented post-test actions.

HOW TO USE THIS ASSESSMENT

Score each statement from 0 to 3. Use evidence rather than assumptions. If the answer is unknown, score 0 and record the discovery action required.

Score	Meaning
0	Unknown or not in place
1	Partially defined
2	Implemented but not recently validated
3	Implemented, tested and evidenced

1. Critical Operations and Dependencies

Establish which operational services must return first and what emergency response depends on.

Assessment statement	Score 0-3	Evidence	Action required
Critical control-room, mobilisation and operational systems are identified and prioritised.			
Dependencies between operational systems, IT, communications and supporting infrastructure are documented.			
Recovery-time objectives and acceptable data-loss tolerances are agreed for critical services.			
Operational owners understand which systems and services must be restored first.			

2. Operational Recovery Validation

Test whether complete critical services can be restored, not simply whether backups complete.

Assessment statement	Score 0-3	Evidence	Action required
Full restores of critical control-room and operational workloads have been completed.			
System, application, network and identity dependencies are included in recovery tests.			
Tests demonstrate that critical services can be restored within agreed operational timeframes.			
Test results, recovery evidence and lessons learned are documented.			

3. Legacy and Specialist System Coverage

Confirm that older, specialist and difficult-to-replace systems are included in the recovery strategy.

Assessment statement	Score 0-3	Evidence	Action required
Legacy operating systems and specialist operational workloads are identified and documented.			
Critical physical and virtual workloads are included within recovery plans.			
Specialist control-room, mobilisation and communications systems have documented recovery methods.			
Replacement hardware and infrastructure requirements are understood.			

4. Isolated and Restricted-Connectivity Recovery

Check whether critical systems can still be recovered when external connectivity or remote access is unavailable.

Assessment statement	Score 0-3	Evidence	Action required
Critical isolated, segmented and restricted-connectivity environments are identified.			
Recovery can be managed locally where external connectivity or remote access is unavailable.			
Recovery procedures account for dependencies between isolated systems and supporting infrastructure.			
Local recovery resources, documentation and responsible personnel are available.			

5. Cyber Incident and Emergency-Service Recovery

Define how clean recovery is initiated, prioritised and verified following a cyber incident or major system failure.

Assessment statement	Score 0-3	Evidence	Action required
Authority to initiate recovery of critical operational services is clearly defined.			
Known-good recovery points can be identified for critical systems.			
The restoration sequence for control-room, mobilisation and supporting systems is agreed.			
Recovered systems are validated before being returned to operational service.			

6. Recovery Governance and Operational Ownership

Make recovery responsibilities, escalation routes and operational decisions accountable.

Assessment statement	Score 0-3	Evidence	Action required
IT, operational and service-recovery responsibilities are clearly assigned.			
Escalation and communications procedures are documented for major disruption.			
Recovery plans are reviewed following significant system, infrastructure or operational change.			
Identified recovery gaps have accountable owners and target actions.			

Recovery Maturity Interpretation

Add the 24 scores to calculate a total out of 72. Use the maturity band as a starting point for prioritisation, not as a substitute for technical validation.

Total score	Recovery maturity	Recommended response
0-18	Operational exposure not yet understood	Prioritise critical-service discovery and dependency mapping.
19-36	Protection in place, recovery evidence limited	Validate full restores, dependencies and emergency-response recovery requirements.
37-54	Recovery defined, further assurance needed	Exercise priority operational systems and close remaining evidence gaps.
55-72	Operational recovery evidence established	Maintain recovery testing, governance and continuous improvement.

YOUR RESULT
Total score: _____ / 72 Maturity band: _____ Immediate priority: _____

Priority Recovery-Gap Summary

Most critical control-room or operational system requiring validation

_____

Oldest or hardest-to-recover operational workload

_____

Largest operational dependency or documentation gap

_____

Isolated or restricted-connectivity environment requiring local recovery

_____

Next recovery exercise or technical review

_____

Action Plan

Record the priority actions required to strengthen recovery evidence and operational readiness.

#	Priority action	Owner	Target date	Evidence of completion
1				
2				
3				
4				
5				

RECOMMENDED FOLLOW-UP
Use these findings to scope a Blue Light Operational Recovery Readiness Review with Switchshop and Acronis. The review should validate critical control-room and operational workloads, mobilisation and infrastructure dependencies, legacy system coverage, isolated environments, recovery ownership and evidence that critical services can be restored within required operational timeframes.

Secure recovery for emergency services, control room environments and critical OT systems.