

WORKBOOK · CHECKLIST AND SCORECARD

How ready are you to recover from a cyber attack?

The ability to respond quickly and effectively to a cyber attack protects your operations, reputation and bottom line. Work through the checklist, then score your readiness, to set a baseline, find the gaps and decide what to fix first.

PART 1 · CHECKLIST

The foundations.

A foundational guide to a comprehensive recovery strategy: from roles and communication plans to your ransomware insurer's requirements and secure plan storage. It's an essential first step; true preparedness takes an approach tailored to your organization.

Any "no" is a gap worth closing first.

01	We have a clearly defined business continuity plan	☐ YES ☐ NO
02	We have an incident response plan	☐ YES ☐ NO
03	We have a recovery communication plan	☐ YES ☐ NO
04	Roles and responsibilities for recovery are defined	☐ YES ☐ NO
05	Critical contact information is written down	☐ YES ☐ NO
06	We revisit and update our plans at least quarterly	☐ YES ☐ NO
07	We self-audit accounts annually	☐ YES ☐ NO
08	Our plans are stored in a secure location	☐ YES ☐ NO
09	We have a list of all applications	☐ YES ☐ NO
10	We have defined SLAs for backup and recovery	☐ YES ☐ NO
11	We know, and meet, our ransomware insurer's requirements	☐ YES ☐ NO

NOTES · GAPS TO CLOSE, OWNERS, DATES

ABOUT RECOVERY CO-PILOT (RECO)

RECO by KELYN Technologies is a collaborative service that gives your team the expertise of proven KELYN engineers and industry best practices, so your organization is always prepared for a cyber attack.

PART 2 · SCORECARD

Score each area from 1 to 5.

Assign each item a score based on your current practices and processes. Use the results to see your strengths, highlight vulnerabilities and build a roadmap for improving your cyber readiness.

SCORING GUIDE

- 1 Minimal or no implementation, with significant risk exposure.
- 2 Basic implementation, but lacking comprehensive processes or coverage.
- 3 Moderate implementation, with some gaps in effectiveness or scope.
- 4 Strong implementation, with minor improvements needed.
- 5 Full implementation, with tested, optimized processes and maximum preparedness.

ENVIRONMENT HEALTH

01	Current service level agreement (SLA) How effective and clear are your SLAs at meeting recovery and uptime requirements?	
02	Offsite data copies Are offsite copies up to date, complete and secure?	
03	Library encryption Is encryption in place on your data libraries, for secure storage and transmission?	
04	Ransomware protection on the infrastructure How robust are your defenses against ransomware across the infrastructure?	
05	Data management platform version Is your platform up to date and aligned with industry best practices?	
SUBTOTAL		___ / 25

CYBER RECOVERY READINESS

09	Immutable copy Do you keep backups that can't be changed or tampered with?	
10	Air-gapped backup Do you keep physically or logically isolated backups?	
11	Restore testing after a cyber event How rigorous and frequent is testing of recovery after an attack?	
SUBTOTAL		___ / 15

DATA MANAGEMENT PLATFORM RECOVERY READINESS

06	Recovery plan for the data management infrastructure How good, clear and regularly updated is your recovery plan?	
07	DR primary copy and secondary location How redundant and ready are your disaster recovery systems?	
08	Restore testing strategy How often and how well do you test restores for disaster scenarios?	
SUBTOTAL		___ / 15

CYBER SECURITY

12	Security posture How strong is your overall security framework, policy and implementation?	
13	Active Directory integration How securely and efficiently is Active Directory integrated across your systems?	
14	Credential management How robust is your management of user credentials and permissions?	
15	Single sign-on (SSO) Is SSO in place for streamlined, secure access?	
SUBTOTAL		___ / 20

NEXT STEPS

Score it online at kelyntech.com/cyber-readiness-scorecard, or talk through your results with a KELYN cyber readiness specialist: sales@kelyntech.com.

Total ___ / 75