

BACKUP SECURITY & RECOVERY ASSESSMENT FORM

Professional Backup Risk Assessment for SMB

 +60 12 349 9477  progifitsolutions.com



Company Information	
Company Name	
Industry	
Contact Person	
Phone	
Email	
Assessment Date	
Assessor	
Prepared by	ProGif IT Solutions

Assessment Scoring

For each question, assign a score from **0 to 5**.

Score	Description
0	Not Implemented / Critical Risk
1	Very Poor
2	Basic Implementation
3	Adequate
4	Good Practice
5	Best Practice / Fully Implemented

SECTION A – Backup Strategy

Maximum Score: 20

No	Assessment Item	Score (0–5)
A1	A documented backup policy exists.	
A2	Critical business data has been identified.	
A3	Backup scope includes all critical systems.	
A4	Backup responsibilities are clearly assigned.	

Section Score: ____ /20

SECTION B – Backup Schedule

Maximum Score: 20

No	Assessment Item	Score (0–5)
B1	Backup frequency meets business requirements.	
B2	Backup jobs run automatically.	
B3	Backup completion is monitored daily.	
B4	Failed backups are investigated promptly.	

Section Score: ____ /20

SECTION C – 3-2-1 Backup Rule

Maximum Score: 30

C1 – Three Copies of Data	
Assessment	Score
No backup copy	0
One backup copy	2
Two backup copies	4
Three copies with verification	5

Score: ____

C2 – Two Different Storage Media	
Assessment	Score
Single storage device	0
Different disks only	2
NAS + External Disk	4
Different technologies (NAS + Cloud/Tape)	5

Score: _____

C3 – One Offsite Copy	
Assessment	Score
None	0
Manual offsite copy	2
Cloud backup	4
Automated offsite backup	5

Score: _____

C4 – Backup Retention	
Assessment	Score
No retention policy	0
Less than 7 days	2
30 days	4
90+ days with versioning	5

Score: _____

C5 – Backup Verification

Assessment	Score
Never verified	0
Occasionally	2
Monthly verification	4
Automatic verification	5

Score: _____

Section Score: ____ /30

SECTION D – Backup Security

Maximum Score: 30

No	Assessment Item	Score (0–5)
D1	Backup files are encrypted.	
D2	MFA protects backup administration.	
D3	Backup administrator uses separate account.	
D4	Backup repository is isolated from production.	
D5	Immutable backup or ransomware protection is enabled.	
D6	Backup access follows least-privilege principles.	

Section Score: ____ /30

SECTION E – Recovery Readiness

Maximum Score: 25

No	Assessment Item	Score (0–5)
E1	Restore testing is performed regularly.	
E2	Disaster recovery procedures are documented.	
E3	Recovery Time Objective (RTO) is defined.	
E4	Recovery Point Objective (RPO) is defined.	
E5	Staff know the recovery procedures.	

Section Score: ____ /25

SECTION F – Cloud & Microsoft 365 Protection

Maximum Score: 20

No	Assessment Item	Score (0–5)
F1	Microsoft 365 is backed up independently.	
F2	OneDrive data is protected.	
F3	SharePoint data is protected.	
F4	Cloud backup is tested regularly.	

Section Score: ____ /20

SECTION G – Backup Monitoring

Maximum Score: 20

No	Assessment Item	Score (0–5)
G1	Backup success reports are reviewed.	
G2	Email alerts are configured.	
G3	Backup storage capacity is monitored.	

Section Score: ____ /15

SECTION H – Business Continuity

Maximum Score: 20

No	Assessment Item	Score (0–5)
H1	Critical systems can be restored within required time.	
H2	Alternate recovery procedures exist.	
H3	Business continuity plan includes backup recovery.	
H4	Disaster recovery drills are performed.	

Section Score: ____ /20

Assessment Summary

Section	Maximum	Score
A	20	
B	20	
C	30	
D	30	
E	25	
F	20	
G	15	
H	20	

Total Maximum Score: 180

Actual Score: _____

Final Percentage

Backup Security Score (%)

(Actual Score ÷ 180) × 100 = _____ %

Risk Rating		
Percentage	Rating	Status
90–100%	Excellent	 Excellent Protection
75–89%	Good	 Good Protection
60–74%	Fair	 Improvement Recommended
40–59%	Poor	 High Risk
Below 40%	Critical	 Immediate Action Required

Recommended Actions	
Rating	Recommendation
Excellent	Continue regular backup verification and testing.
Good	Improve automation, monitoring, and offsite protection.
Fair	Strengthen 3-2-1 compliance and increase recovery testing.
Poor	Implement a centralized backup solution with encryption, monitoring, and offsite storage.
Critical	Establish a complete backup strategy immediately to reduce the risk of permanent data loss.

NIST Cybersecurity Framework (CSF 2.0)

Mapping

Assessment Area	NIST CSF Category
Critical Data Identification	ID.AM
Backup Policy & Governance	GV.PO
Backup Strategy	PR.DS
Encryption	PR.DS
Identity & Access Control	PR.AA
Backup Monitoring	DE.CM
Recovery Planning	RC.RP
Recovery Testing	RC.IM
Business Continuity	RC.CO

ProGif IT Solutions

Protect Your Business. Secure Your Future.

Our Services:

- ✓ Cybersecurity Assessment
- ✓ Fortigate Firewall Solution
- ✓ Network Infrastructure
- ✓ Managed IT Services
- ✓ Microsoft 365 Security
- ✓ Server & Virtualization
- ✓ Backup & Disaster Recovery
- ✓ CCTV & Surveillance
- ✓ Cloud Solutions

Contact

ProGif IT Solutions

Website:

progifitsolutions.com

Email:

seanpong@progifitsolutions.com