SIXWAY

SIXWAY CYBERSECURITY CHECKLIST

# Cyber Risk Executive Checklist

A decision-focused checklist for understanding material cyber risk, clarifying ownership, and setting defensible priorities.

| SECURE | MODERNIZE | OPERATE |
|---|---|---|

**HOW TO USE**

Use this checklist with business, technology, security, risk, and operational leaders. Mark items that are established, uncertain, or require follow-up. It is a planning aid, not a certification or comprehensive assessment.

## Executive context

### 01 Critical services and information

Start with what the organization must protect and sustain.

[ ] Critical business services and essential operating processes are identified.

[ ] Technology, data, facilities, people, and third parties supporting those services are mapped at a useful level.

[ ] Business impact and tolerance for disruption are understood by accountable leaders.

### 02 Risk ownership and governance

Cyber risk decisions require visible accountability.

[ ] Material cyber risks have named business owners, not only technical owners.

[ ] Risk acceptance, escalation, and exception decisions follow a documented process.

[ ] Executives receive reporting that connects exposure to business services, decisions, owners, and due dates.

SIXWAY

### 03 Identity and access

Identity controls should reflect the sensitivity and privilege of each role.

- [ ] Multi-factor authentication is required for remote, administrative, and material business access.
- [ ] Privileged accounts are limited, monitored, and reviewed on a defined schedule.
- [ ] Joiner, mover, and leaver processes remove or adjust access promptly.

# Exposure and resilience

### 04 Vulnerability and configuration risk

Prioritization should combine technical severity with business context.

- [ ] Asset ownership and internet exposure are sufficiently visible to support prioritization.
- [ ] Remediation considers known exploitation, criticality, compensating controls, and accountable deadlines.
- [ ] Security configuration baselines and exceptions are documented and reviewed.

### 05 Detection and response

Operational readiness depends on decisions, evidence, and coordination.

- [ ] Monitoring covers priority identities, systems, cloud services, endpoints, and network activity.
- [ ] Incident roles, escalation paths, communications, and external contacts are documented.
- [ ] Response plans are exercised and lessons are assigned to owners through completion.

### 06 Continuity and recovery

Recovery capability must be demonstrated, not assumed.

- [ ] Backup scope, protection, retention, and administrative access are appropriate for critical services.
- [ ] Restore procedures and dependencies are tested at a frequency aligned with business needs.
- [ ] Recovery objectives are understood, achievable, and connected to continuity plans.

### 07 Third-party dependencies

Supplier access and service dependencies should remain visible throughout the relationship.

- [ ] Critical suppliers and the services, information, and access they depend on are identified.
- [ ] Security responsibilities, incident notification, continuity expectations, and evidence needs are defined.
- [ ] Access revocation, data handling, and transition requirements are included in exit planning.

SIXWAY

# Turn observations into decisions

Record the highest-priority observations below. A useful action has a business context, accountable owner, practical next step, and target date.

| PRIORITY | OBSERVATION / BUSINESS IMPACT | OWNER | NEXT ACTION / DATE |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |

**NEXT STEP**

Where material uncertainty remains, a structured cyber risk assessment can establish the current posture, validate assumptions, and create a prioritized roadmap tied to organizational objectives.

## About Sixway

Sixway is a Canadian-owned cybersecurity and technology company connecting cyber strategy, technology transformation, infrastructure, implementation, and managed operations.