IT COMPLIANCE READINESS CHECKLIST

Use this checklist to identify gaps and prioritize next steps.

1. Conduct a Self-Assessment

- Evaluate current security and compliance posture
- Identify systems, data, and environments in scope
- Use tools or internal reviews to detect deficiencies

2. Identify and Prioritize Gaps

- Document control gaps and vulnerabilities
- Assess risk impact and likelihood
- Prioritize remediation based on risk and effort

3. Build a Compliance Roadmap

- Define timelines for remediation
- Assign ownership for each task
- Align roadmap with business and audit deadlines

4. Prepare for Audit Readiness

- Ensure documentation is complete and organized
- Validate controls are operating effectively
- Begin preparation at least 6 months in advance if needed

5. Evaluate Automation Opportunities

- Identify tools to streamline compliance processes
- Ensure alignment with governance and risk strategies
- Implement monitoring for ongoing compliance

6. Assess Cloud Security Risks

- Review cloud configurations (AWS, Azure, etc.)
- Evaluate identity and access controls
- Assess vendor and third-party risks

7. Strengthen Overall Security Posture

- Address vulnerabilities identified in assessments
- Improve governance and policies
- Continuously monitor and update controls

8. Plan for Ongoing Compliance

- Schedule regular assessments and audits
- Track compliance metrics and reporting
- Maintain a continuous improvement approach

Not Sure Where to Start?

Talk with an LBMC cybersecurity advisor to walk through your results and identify your next steps.

Request Assessment

Contact our team by emailing *info@lbmc.com* or filling out the form at www.lbmc.com/contact/.