GRC PRE-AUDIT READINESS: 8 QUESTIONS EVERY SMB MUST ANSWER

Preparing for a governance, risk, and compliance (GRC) audit can feel daunting—especially for small and midsized businesses (SMBs) balancing growth, limited resources, and evolving regulatory demands. Audit readiness isn't just about passing an assessment; it's about building a culture of accountability, transparency, and control.

This checklist will help you evaluate whether your organization is truly ready for its next compliance audit by guiding you through eight essential questions. Each question highlights a key area of your GRC framework that should be reviewed and documented before the audit process begins.

1 Do we have clearly defined GRC policies and procedures?

Well-documented policies and procedures provide the foundation for compliance. Without them, employees may interpret standards inconsistently, leaving gaps in accountability.

2 Are roles and responsibilities for compliance clearly assigned?

A successful GRC framework depends on ownership. Ensure every control, task, and policy has a responsible person or team to maintain visibility and enforcement.

3 Do we have a centralized repository for compliance documentation?

Auditors will expect to see organized, accessible records. Storing compliance data in a single, secure system helps streamline audits and reduce time spent on manual retrieval..

4 Are we tracking and managing risks proactively?

An effective GRC program doesn't just react to risk—it anticipates it. Conduct regular risk assessments to identify, rank, and mitigate emerging threats before they escalate.

GRC PRE-AUDIT READINESS: 8 QUESTIONS EVERY SMB MUST ANSWER

5

Do we have monitoring and reporting mechanisms in place?

Continuous monitoring tools and periodic compliance reports demonstrate that your organization takes an active approach to governance and accountability.

6

Have we recently tested our controls for effectiveness?

Auditors will review your internal controls to ensure they work as intended. Regular internal testing validates compliance readiness and reveals areas needing remediation.

7

Are we maintaining vendor and third-party compliance documentation?

Third-party risk is often overlooked. Make sure your vendors and partners follow the same compliance standards—especially when handling sensitive data or customer information.

8

Do we have an incident response and remediation plan?

When noncompliance or a breach occurs, having a documented response plan ensures quick action, minimizes damage, and demonstrates control maturity to auditors.

Answering these eight questions honestly gives your organization a clear picture of where it stands on the compliance maturity curve. Gaps don't mean failure—they highlight opportunities to strengthen your governance, risk management, and control environment before an external audit does.

By addressing weak spots early, documenting your processes, and building accountability across teams, your SMB can move from reactive compliance to proactive confidence.

GRC PRE-AUDIT READINESS PRINTABLE CHECKLIST

Use this page to document your organization's audit readiness and identify next steps.

Question	Yes/No	Notes/Action Items
Do we have clearly defined GRC policies and procedures?		
Are roles and responsibilities for compliance clearly assigned?		
Do we have a centralized repository for compliance documentation?		
Are we tracking and managing risks proactively?		
Do we have monitoring and reporting mechanisms in place?		
Have we recently tested our controls for effectiveness?		
Are we maintaining vendor and third-party compliance documentation?		
Do we have an incident response and remediation plan?		

Readiness Score

Count the number of "Yes" answers:

- 7–8: Strong audit readiness
- 4–6: Moderate readiness; some improvements needed
- 0–3: High risk of noncompliance; urgent action required

10 SIGNS YOUR GOVERNMENT IS READY FOR AN ECM UPGRADE

At 3SG Plus, we specialize in helping organizations simplify compliance, manage risk, and build strong governance frameworks. Our GRC services are designed to support businesses of all sizes through every phase of their compliance journey—from risk assessments and policy development to certification support and continuous monitoring.

With deep expertise in frameworks like SOC and NIST, we provide the guidance, tools, and automation needed to maintain audit readiness and mitigate evolving threats.

We deliver a full range of digital transformation solutions that streamline operations, strengthen cybersecurity, and modernize IT infrastructure. As a trusted technology reseller and IT managed services provider, we serve both public and private sector clients with offerings that include enterprise content management (ECM), network architecture, cybersecurity, AI-powered automation, and IT project delivery.

Our digital transformation solutions include:

- Governance, Risk, and Compliance (GRC)
- Cybersecurity and Threat Mitigation
- IT Infrastructure and Network Services
- Business Process Assessments
- IT Projects on Demand (PODs) Staffing and Support
- Enterprise Content Management
- AI and Intelligent Document Processing

Don’t wait for the next audit to find out you’re not ready.

Contact 3SG Plus today to schedule a GRC Readiness Review and strengthen your compliance framework before your next audit.

CONTACT US

614.407.7990 sales@3sgplus.com www.3sgplus.com