ADVISORY | TECHNOLOGY RISK & GRC

Technology Risk & GRC Getting-Started Checklist

Fifteen questions to help leaders identify where technology governance, access, change, third-party, data, and resilience practices may need attention.

A starting conversation - not a full assessment

This checklist is intentionally high level. It helps leadership identify what is known, what is unclear, and which areas may warrant a deeper review.

What this resource helps you do

- Bring technology risk into leadership and governance discussions.
- Identify ownership gaps and areas where practices may be informal or inconsistent.
- Select a small number of priorities for follow-up rather than attempting to address everything at once.

How to use it

1	**Discuss** Review the questions with finance, operations, IT, compliance, and other relevant leaders.
2	**Mark** For each area, select Yes, Needs attention, or Not sure based on current evidence.
3	**Prioritize** Choose no more than three items for follow-up and assign an owner for the next conversation.

What this checklist does not cover

It is not a cybersecurity assessment, penetration test, regulatory compliance opinion, control design, vendor selection, implementation roadmap, or audit. Those activities require additional scope, evidence, and technical or regulatory context.

Technology Risk & GRC: 15 Starter Questions

Answer based on current evidence. A Not sure response can be as important as a Needs attention response.

1 | Governance & ownership

- Has leadership defined who owns technology risk and key decisions?
- Are significant technology risks discussed with the appropriate governing body?
- Are policies and responsibilities reviewed when the organization changes?

[ ] Yes [ ] Needs attention [ ] Not sure

2 | Access & user lifecycle

- Is access approved based on job responsibilities and business need?
- Are departures and role changes reflected in system access promptly?
- Are privileged or administrator accounts limited and periodically reviewed?

[ ] Yes [ ] Needs attention [ ] Not sure

3 | Change & third-party oversight

- Are significant system changes requested, tested, approved, and documented?
- Are critical technology vendors identified and assigned an internal owner?
- Does vendor oversight consider security, availability, data, and service continuity?

[ ] Yes [ ] Needs attention [ ] Not sure

4 | Data protection

- Does the organization know where sensitive or regulated data is stored?
- Are retention, sharing, and disposal expectations clearly communicated?
- Are backup responsibilities and recovery expectations defined and tested?

[ ] Yes [ ] Needs attention [ ] Not sure

5 | Resilience & incident response

- Is there a practical plan for responding to a technology or data incident?
- Are key contacts, escalation steps, and decision responsibilities current?
- Has leadership discussed how critical operations would continue during an outage?

[ ] Yes [ ] Needs attention [ ] Not sure

Priority notes

- Priority 1: _____
- Priority 2: _____
- Priority 3: _____
- Owner for next discussion: _____

A useful result is clarity

The objective is not to mark every answer Yes. It is to create a more accurate view of ownership, evidence, and the areas that matter most to the organization.

Turn the Checklist Into a Focused Next Step

What your answers may be telling you

- Many Not sure responses may indicate limited visibility, unclear ownership, or missing documentation.
- Different answers from different leaders may indicate inconsistent practices or expectations.
- Repeated Needs attention responses in one area may signal a focused assessment is more useful than isolated fixes.

A practical first 30 days

- Confirm the executive or governance owner for the priority area.
- Gather the policies, reports, contracts, access lists, or other evidence already available.
- Define one clear risk statement and the business impact leadership wants to address.
- Agree on the next decision, the people needed, and a realistic due date.

When deeper support may be appropriate

- The organization is subject to a new contract, regulation, audit, customer request, or board expectation.
- Technology responsibilities are split across internal teams and outside providers with no clear oversight model.
- Leadership needs evidence-based prioritization, control documentation, remediation support, or a readiness assessment.
- A major system change, acquisition, rapid growth, or incident has changed the risk profile.

How JConner can help

JConner can help leadership clarify governance, assess selected technology-risk and GRC areas, document controls, organize evidence, prioritize gaps, and support practical remediation planning. Learn more at jconnerpc.com.

Selected references

National Institute of Standards and Technology, Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework

Cybersecurity and Infrastructure Security Agency, Cyber Essentials
https://www.cisa.gov/resources-tools/resources/cyber-essentials

KPMG, Implement GRC technology the right way
https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/implement-grc-technology-right-way.pdf