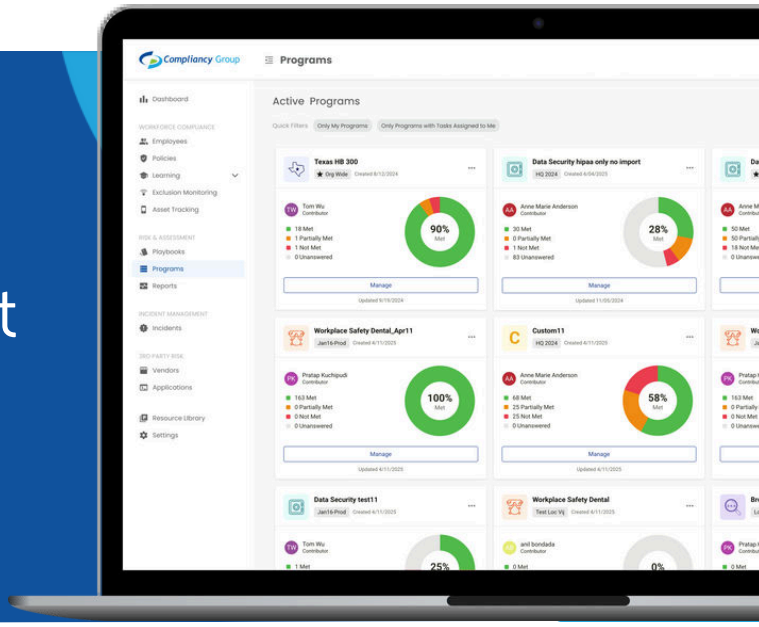
Compliancy Group

A Smarter Approach to Risk Management: Risk Assessment Checklist

Use this quick checklist to get started on assessing risk in your organization.



IDENTIFY RISKS

- [ ] Check for regulatory changes & new cyber threats
- [ ] Review your organization's past incident reports
- [ ] Ask for employee feedback

ADDRESS RISKS

- [ ] Implement controls to mitigate identified risks
- [ ] Update policies & procedures to account for identified risks
- [ ] Train employees on compliance & cybersecurity best practices

ASSESS RISKS

- [ ] Determine the likelihood & impact of each risk
- [ ] Rank risks based on their severity & likelihood
- [ ] Determine which risks to prioritize & which can wait until next quarter

MONITOR EFFECTIVENESS OF SAFEGUARDS

- [ ] Establish performance metrics that mark controls effective
- [ ] Test effectiveness of safeguards periodically
- [ ] Review new incident reports for gaps in controls
- [ ] Update and adapt controls to address new risks

💡 **PRO TIP:** Monitor changes in your organization, environment, regulatory requirements, and emerging threats. Conduct a new risk assessment when changes occur.

Contact Us

929-492-2234

sales@compliancygroup.com

Compliancy Group

5 Principles for Effective Risk Management in Healthcare

ONGOING | EVIDENCE-DRIVEN | SHARED | INTEGRATED | UPDATED

CONTINUOUS RISK MANAGEMENT

Principle: Risk management is not a once-a-year exercise; it must be a living, ongoing process.

Why it matters: Most HIPAA fines cite missing or insufficient documentation—not the absence of a risk assessment.

How Compliancy Group supports this: Built-in review cadences that schedule controls monthly, quarterly, or annually, with automated reminders.

RISK FINDINGS LINKED TO REMEDIATION

Principle: A risk assessment without follow-up action is just a report; true compliance comes from documented remediation.

Why it matters: Auditors don't just ask for a risk assessment—they ask, "Show us what you did to address the risks you found."

How Compliancy Group supports this: Every control can be linked to policies, vendor contracts, BAAs, incidents, or training evidence — all viewable from your dashboard.

OWNERSHIP ACROSS THE ORGANIZATION

Principle: Effective risk management requires shared accountability, not reliance on one individual.

Why it matters: Concentrating responsibility increases the chance of oversights and burnout. Distributing ownership builds resilience.

How Compliancy Group supports this: Role-based permissions let IT, Compliance, and Security manage their domains. Tasks and reminders are assigned by control.

INTEGRATE RISK WITH COMPLIANCE THE BROADER COMPLIANCE ECOSYSTEM

Principle: Risk analysis shouldn't live in isolation; it should connect to policies, vendors, workforce compliance, and incidents.

Why it matters: Fragmented tools and spreadsheets create gaps. Regulators evaluate the whole compliance program, not just one document.

How Compliancy Group supports this:

- **Vendor risk:** monthly OIG/state exclusion checks, contract/BAA tracking, due-diligence questionnaires.
- **Incident management:** anonymous reporting, digital case files, linkage back to risk register.
- **Policy & application inventories:** one system for audit-ready traceability.

STAY CURRENT WITH REGULATORY CHANGE

Principle: Compliance requirements evolve; risk programs must evolve with them.

Why it matters: Static assessments quickly become outdated, leaving organizations exposed.

How Compliancy Group supports this:

- **Built-in guidance:** for every control, updated as regulations change.
- **Regulatory notifications:** keep teams ahead of new requirements without extra consulting fees.
- **Monthly educational webinars and content:** extend the organization's regulatory intelligence.

Contact Us

929-492-2234

sales@compliancygroup.com