A BOARD GUIDE

How to Run a Risk Assessment

Identifying, Scoring, and Acting on the Risks That Matter

The concepts, the four-phase process, and the heat map—how a board can tell whether its risk assessment is actually working

2026 | R. McConnell Group PLLC

WHY IT MATTERS

The Cornerstone of an Effective Program

Regulators, prosecutors, and good governance all start with: do you know your risks?

- **It sets priorities.** A risk assessment ranks where the real exposure is—so resources, controls, training, and monitoring follow the risk.
- **Regulators expect it.** A periodic, documented risk assessment is a hallmark of a well-designed program the DOJ and regulators look for.
- **It surfaces what's new.** Done regularly, it catches emerging risks and trends before they become incidents.
- **It informs the board.** It turns a sprawling risk universe into a clear, comparable picture leadership can act on.

THE ONE-LINE SUMMARY

A risk assessment is how a board turns ***"what could go wrong?"*** into a ranked, fundable plan.

THE VOCABULARY

Inherent Risk, Controls & Residual Risk

Four terms unlock the entire exercise

INHERENT RISK

The risk before any controls—what the activity would pose on its own.

—

CONTROLS

Policies, processes, and checks that reduce likelihood or impact.

=

RESIDUAL RISK

What remains after controls—the risk you actually carry.

LIKELIHOOD

The probability that an adverse event will occur, taking the controls in place into account.

IMPACT

The most probable financial, reputational, and operational harm—the likely case, not the worst case.

THE PROCESS

Four Phases, One Cycle

Most assessments run on a 12-to-16-week arc—then repeat

PHASE 01

Planning

Understand the business, scan the risk landscape, and define scope, stakeholders, and timeline.

PHASE 02

Execution

Interview owners, map controls, and score each risk for likelihood and impact.

PHASE 03

Reporting

Rank residual risk, build the heat map, and report findings to leadership and the audit committee.

PHASE 04

Follow-Up

Agree management action plans, assign owners, and track mitigation to closure.

Two flavors: a baseline assessment covers the whole program; a targeted assessment re-examines a narrower, higher-risk slice.

THE MATH

Scoring Each Risk

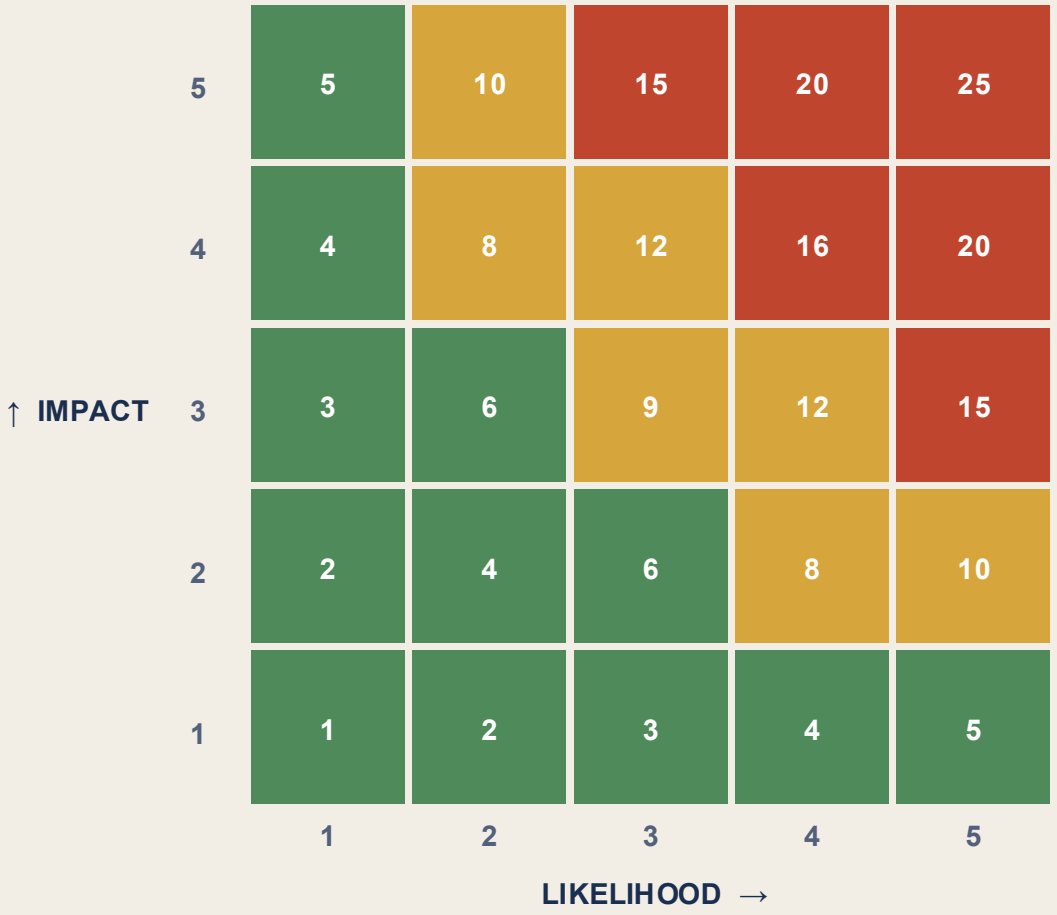
A simple, consistent formula makes risks comparable across the company

- **Score the likely case, not the worst case.** Rate the most probable event given today's controls—not the rare catastrophe.
- **Use a consistent 1–5 scale.** The same anchored definitions let business, legal, compliance, and audit score the same way.
- **Score residual, after controls.** The number reflects the risk that remains once existing controls are credited.

THE PICTURE

The Risk Heat Map

Plotting likelihood against impact turns scores into priorities at a glance



HOW TO READ IT

High. Act now—mitigate or escalate

Medium. Plan mitigation; monitor closely

Low. Accept and monitor

The map focuses attention: the top-right corner—high likelihood, high impact—is where the board's time and the company's money should go first.

THE RECORD

The Risk Register

Every risk, its controls, and its rating live in one matrix—the engine of the assessment

Risk statement	Type	Key controls	Inherent	Residual	Owner
Unauthorized data access	Privacy	Access controls; logging; training	HIGH	MED	CISO
Third-party bribery	Anti-corruption	Due diligence; approvals; audits	HIGH	MED	Compliance
Wage-and-hour breach	Employment	Timekeeping; reviews; training	MED	LOW	HR
Sanctions violation	Trade	Screening; geofencing; escalation	HIGH	HIGH	Legal

Illustrative only. *A real register also captures risk owners' action plans, target dates, and the trend since the last assessment.*

WHAT YOU DO WITH IT

From Scores to Action

A risk assessment is a means to an end—the end is better-allocated effort

1. Prioritize

Rank residual risks so the highest exposures get attention first.

2. Allocate resources

Direct budget, headcount, and controls toward the top of the heat map.

3. Build action plans

Assign each priority risk an owner, a mitigation plan, and a target date.

4. Feed the program

Channel results into standards, training, communications, and monitoring.

WHO AND HOW OFTEN

Governance & Cadence

Independence and rhythm are what make the assessment credible

WHO IS INVOLVED

- **First line—the business.** Owns the risks and the controls, and provides the front-line view.
- **Second line—compliance/risk.** Runs the assessment, sets the methodology, and challenges the scoring.
- **Third line—internal audit.** Independently tests and assures the board the program works.
- **The board / audit committee.** Receives the results and holds management to the action plans.

HOW OFTEN

- **Periodically, on a schedule.** Refresh the full picture at least annually, not only after something breaks.
- **Baseline, then targeted.** A full baseline up front; focused re-assessments as risk profiles change.
- **Triggered by change.** New products, acquisitions, or regulations should prompt a fresh look.
- **Documented throughout.** Scope, scoring, and decisions are recorded—so the work is defensible.

FOR THE BOARD

Five Questions to Ask About the Assessment

You don’t run it—but you should interrogate it

Does it cover the whole risk universe?

Scope should be deliberate, documented, and refreshed—not last year’s list.

Are the scores honest?

Residual ratings should reflect real control effectiveness, not optimism.

Do resources follow the heat map?

Spending and attention should track the top-right corner.

Is there an action plan with owners?

Every high risk needs a named owner and a date.

5. **And the real test:** *would this assessment have caught last year’s surprise?*

Firm Lawyers

Matthew Boyden

is a trial lawyer and former federal prosecutor with more than thirty-five years of experience. He represents companies and executives in high-stakes criminal, civil, regulatory, and governance matters. He is regularly engaged where litigation risk, regulatory scrutiny, and institutional exposure intersect. Matthew's practice includes federal criminal defense, complex civil litigation, internal investigations, and board-level advisory work. He has represented clients in matters involving securities fraud, sanctions and trade controls, anti-corruption, anti-money laundering, and financial misconduct, as well as parallel civil and regulatory proceedings.

Larry Finder

is a trial lawyer and former United States Attorney with more than four decades of experience handling complex criminal, civil, and regulatory matters of national significance. He represents individuals, corporations, and boards confronting serious legal, institutional, and reputational risk. He joined the U.S. Department of Justice, serving in increasingly senior leadership roles, including Chief of the Criminal Division and First Assistant U.S. Attorney, before being appointed United States Attorney for the Southern District of Texas in 1993.

Ryan McConnell

is a former federal prosecutor and trial lawyer who represents companies, boards, and executives in high-stakes criminal, civil, and governance matters. He is called when litigation risk, regulatory exposure, and institutional credibility intersect. Ryan has tried nearly twenty federal jury trials and conducted hundreds of investigations involving complex fraud, cross-border enforcement, and sensitive regulatory issues. His practice focuses on federal criminal defense, complex civil litigation, internal investigations, and advising boards and senior executives on governance issues and matters requiring judgment under pressure.