

THE ALS GROUP

Managing Risk to Influence Successful Outcomes

What Are the 5 Principles of Risk Assessment?

Key Takeaways

- The five steps are identify, determine who is exposed, evaluate and prioritize, record and treat, then review. The same sequence applies to a job site hazard or an entire insurance program.
- The value is in measuring residual risk, what is left after controls and insurance, rather than assuming a policy is working because it exists.
- Assessments go stale. Review annually, and immediately after an acquisition, a major contract or entry into a new market.

A risk assessment is a structured process for identifying what could go wrong, judging how likely and how damaging it would be, and deciding what to do about it. The five principles behind that process are recognized across safety regulation, insurance underwriting and enterprise risk management alike. They originate in occupational risk frameworks but apply just as well to an insurance program, a portfolio of vendor contracts or a multi-site operation. Only the scale and the stakes change.

1. Identify the Risks

Identification is a systematic search for anything that could cause harm, financial loss or disruption: operational exposures, contractual liabilities, coverage gaps, financial concentration and emerging threats like cyber liability.

It is not the same as confirming that policies exist. It means actively looking for what is not yet covered, including exposures that have not produced a loss yet. That typically draws on input from managers and frontline staff, a line-by-line contract review of indemnification and insurance requirements, a review of the existing insurance program for gaps, sublimits and exclusions, and input from compliance and internal audit.

This is consistently where the most material findings surface. Across our Risk Management Assessment (RMA) engagements with construction and real estate development clients, identification has uncovered missing additional insured endorsements, incomplete Builder's Risk coverage and non-compliant cancellation provisions, deficiencies that often sit undetected for years, because no structured process was ever applied.

2. Decide Who or What Is Exposed

If the risk materializes, who or what gets harmed, and how? Which business units, projects, contracts, lenders or investors are exposed, and in what form?

This determines both who needs to be involved and how severe the consequences could be. A coverage gap on a small project carries different stakes than the same gap on a flagship development. A compliance failure by a routine subcontractor is different from one by a vendor tied to a lender covenant.

For portfolios rather than single assets, this step also means identifying concentration. The exposures that matter most are rarely the most frequent ones. They are the ones tied to the largest financial commitments, the most demanding



lender requirements or the weakest risk transfer language.

3. Evaluate the Risks and Decide on Precautions

For every identified risk, assess likelihood and severity. Multiplying the two produces a score that lets dissimilar risks, a cyber incident, a contractual liability, a property loss, to be compared on a common scale.

A common approach uses a five-point scale for each, producing scores from 1 to 25:

- **1–4:** monitor, typically without dedicated action
- **5–9:** defined controls or process changes
- **10–16:** significant intervention, such as contract renegotiation or expanded coverage
- **17–25:** immediate attention and senior leadership involvement

The critical distinction here is inherent versus residual risk. Inherent risk is the score before treatment; residual is what remains after controls, insurance and contractual protections. A high-impact risk may carry adequate insurance that reduces its residual score to negligible even though its likelihood is unchanged. Measuring both is what confirms whether current protections actually work.

This requires a defined risk appetite. Without that baseline, prioritization becomes opinion rather than a consistent standard.

4. Record Findings and Implement Controls

Findings are documented in a Risk Register, a central record capturing each risk's category, likelihood, severity, inherent and residual scores, and named owner. That documentation creates a defensible record for lenders, investors and boards.

Implementation means selecting a response, and most strategies combine more than one:

- **Avoidance:** eliminating the activity where the risk outweighs the benefit
- **Reduction:** controls or process changes that lower likelihood or severity
- **Transfer:** shifting financial consequence through insurance, indemnification or bonds
- **Retention:** knowingly accepting risk within tolerance, or where treatment costs more than the potential loss

The common mistake is defaulting to transfer, buying more insurance, without checking whether reduction or avoidance would solve the problem more efficiently. Contractual transfer deserves particular scrutiny: it is only as strong as the diligence applied to it. On a national affordable housing portfolio, insurance requirements were already written into thousands of vendor agreements, but without centralized oversight and renewal tracking, deficiencies went undetected until they surfaced as lender issues. A clause on paper is not a confirmed, active protection.

5. Review and Update the Assessment

Operations change, contracts renew, vendors turn over and regulations shift. An assessment that was accurate a year ago can be materially out of date today.

A review cycle should include scheduled reassessment of the Risk Register (not just a reaction to a claim or lender request), ongoing tracking of certificates of insurance and endorsement status, input from frontline managers, and



updated reporting to leadership.

This is the principle most likely to lapse. Confirming a certificate is on file at the start of a vendor relationship is straightforward. Confirming eighteen months later that the policy has not lapsed and still meets contractual requirements takes a sustained monitoring function. Review fully at least annually, with any material change triggering an update outside that cycle.

A Worked Example

A mid-sized developer begins a multifamily construction project financed by an institutional lender.

- **Identify.** Review finds the general contractor's indemnification language is weaker than the developer's standard template, and the Builder's Risk policy excludes flood despite a moderate flood zone site.
- **Who is exposed.** The developer carries the financial exposure, the lender's collateral is at risk, and subcontractors could face liability disputes if the indemnification fails.
- **Evaluate.** The flood exclusion scores high on both likelihood and severity, putting it in the upper range that demands immediate attention. The indemnification gap scores moderate likelihood, high severity.
- **Record and treat.** Supplemental flood coverage is secured before construction begins; the indemnification language is renegotiated before the contract is executed.
- **Review.** Both are logged in the Risk Register with named owners and renewal dates, checked at each project milestone and reassessed if scope or timeline changes materially.

How a Formal Risk Assessment Is Structured

Organizations that formalize this process typically produce a defined set of deliverables: an enterprise risk scorecard, a broker performance review, an insurance program evaluation, a contractual risk transfer review, a coverage gap analysis and a prioritized mitigation roadmap.

Because the process directly evaluates insurance placement decisions, who conducts it matters. A broker reviewing its own program carries an inherent conflict of interest. An independent, fee-based advisor whose compensation is not tied to placement has no incentive other than an accurate result.

Frequently Asked Questions

What are the 5 principles of risk assessment? Identify the risks, decide who or what is exposed, evaluate and prioritize, record findings and implement controls, and review regularly. The framework originates in occupational safety models and applies equally to enterprise and insurance risk.

Are the 5 principles the same as the 5 steps? Yes. Terminology varies, but the sequence is consistent.

What is the difference between inherent and residual risk? Inherent risk is the exposure before treatment; residual is what remains after controls, insurance or other treatments. Comparing the two shows whether a treatment is actually reducing exposure.

How often should a risk assessment be updated? At minimum annually. An acquisition, major contract, new market or significant operational shift should trigger an update outside the normal schedule.



Should a broker or an independent advisor conduct it? An independent, fee-based advisor can evaluate coverage, broker performance and contractual risk transfer without the conflict inherent in a broker reviewing its own program.

The ALS Take

Most organizations believe their insurance program protects them until a claim, an audit or a lender request proves otherwise. The deficiency is rarely a missing policy. It is the distance between what a company assumes it has transferred and what its contracts, endorsements and certificates actually deliver, and that distance stays invisible until someone applies a structured process to it.

Across our RMA engagements, the costliest findings cluster in the same places: indemnification language that does not transfer risk as intended, coverage gaps and limits that no longer match how the business operates, exposures managed in separate departments so no one holds a complete view, and vendor certificates collected once and never tracked through renewal. These are ordinary exposures that went unexamined, and they persist because an annual renewal conversation is a placement exercise, not an assessment.

The discipline that prevents this is unglamorous: maintain a Risk Register with named owners, measure residual risk rather than assuming a treatment works, and evaluate cost as Total Cost of Risk, combining premiums, retained losses and deductibles and the expense of managing risk, since a program can look inexpensive on premium alone. This matters most for organizations carrying significant exposure without a dedicated internal risk function: real estate owners and developers, construction firms, property managers, healthcare organizations, manufacturers, private equity portfolio companies and middle market businesses.

That is why we conduct this work on a fee basis. The ALS Group does not sell insurance and earns no commission on placement, so our findings are not shaped by which policies are bought or which broker keeps the account.

If you need help with any risk or insurance related questions, please contact our Managing Principal, Albert Sica, at asica@thealsgroup.com or at 732.395.4251.