Hidden Risk Discover Worksheet

Structured Assessment of Controls, Mitigation Actions, and Process Changes

Step 1 – Define the Control, Change, or Mitigation:

Describe what is being evaluated:

(Write a clear description of the control, change, decision, process, or mitigation.)

What problem was this originally intended to solve?

(Write a clear description of the control, change, decision, process, or mitigation.)

What assumptions does this solution rely on?

Behavioral assumptions:

Capacity assumptions:

Data/information quality assumptions:

Technology/system assumptions:

Who owns this decision/control:

Department:	*Role:*	*Sponsor:*

Step 2 – Identify Potential Hidden Risks:

Use the table to document potential hidden risks.

Hidden Risk Description:	*Hidden Risk Types*[A]:	*Stakeholders Impacted*:	*Evidence/Notes*:

[A] *Hidden Risk Types*:

- Workaround/Bypass
- Shadow System
- Delay/Bottleneck
- Stakeholder Friction
- Misaligned Incentives
- Risk Displacement
- Compliance Burden
- Data Quality

Step 3 – Map First-, Second-, and Third-Order Effects:

Think beyond the immediate impact. Use the prompts.

First-Order Effects (Direct):

What happens immediately when this control/change is applied?

What becomes harder, slower, or more constrained?

Additional Notes:

Second-Order Effects (Ripple Effects):

How do other teams/functions experience this?

What new tasks, delays, or burdens emerge?

Additional Notes:

Third-Order Effects (Systemic & Longer-Term):

What patterns emerge over weeks/months?

What new risks or inefficiencies are introduced over time?

Could this create compliance, data quality, or reputational issues?

Additional Notes:

Step 4 – Map First-, Second-, and Third-Order Effects:

Evaluate options for address your most important hidden risks. A balanced solution should solve the real problem without creating new ones.

Too HEAVY (Overreaction): *Creates new burdens, slows the system, adds unnecessary controls*

Too Light (Underreaction): *Fails to address root cause, risk remains unmanaged*

Balanced Response: *Proportional, feasible, minimal side effects*

How would I explain this to leadership/ Audit Committee): *Clear rationale*

Step 5 – Early Warning Indicators & Monitoring Plan:

Identify signals that hidden risks are emerging.

Indicator	*Leading/ Lagging*	*Data Source*	*Threshold/ Trigger*	*Owner*

Monitoring Plan:

Frequency:

Responsibilities:

Follow-up path:

Lessons Learned/Future Design Notes:

Sample of completed worksheet

Sample -- Hidden Risk Discover Worksheet

Structured Assessment of Controls, Mitigation Actions, and Process Changes

Step 1 – Define the Control, Change, or Mitigation:

Describe what is being evaluated:

(Write a clear description of the control, change, decision, process, or mitigation.)

Implementation of a centralized Vendor Onboarding & Payment Approval Workflow in the financial system.

- All new vendors must be created through a standardized portal.
- Invoices over $25,000 require dual approval (requester + finance manager).
- System blocks payments to any vendor without a valid W-9 and banking verification.

What problem was this originally intended to solve?

(Write a clear description of the control, change, decision, process, or mitigation.)

This control establishes a standardized *Vendor Onboarding and Payment Approval Process* to ensure that vendors are properly verified before any payments are made. It introduces a centralized vendor-setup portal, requires complete tax and banking information, and adds dual approval for higher-value invoices. The process exists to prevent fraudulent or duplicate vendors from being created, reduce payment errors, ensure compliance with tax and financial regulations, and maintain a reliable audit trail. It was designed to address the risk that unauthorized vendors could be added to the system, payments could be made without proper oversight, or regulatory documentation could be incomplete or inaccurate.

What assumptions does this solution rely on?

Behavioral assumptions:

- Requesters will submit vendor requests early enough to allow for review time.
- Managers will thoroughly review and not just “rubber-stamp” approvals.
- Teams will stop using ad-hoc or legacy processes to add vendors.

Capacity assumptions:

- Accounts Payable (AP) team has enough capacity to review and validate all new vendors within 2 business days.
- IT can support any system issues within standard SLAs.
- Approvers (managers, finance) have time to review a higher volume of approval notifications.

Data/information quality assumptions:

- Requesters provide complete and accurate vendor details on first submission.
- Tax forms (W-9) are correctly filled out and validated.
- Vendor master data will be kept current (e.g., banking changes, address changes).

Technology/system assumptions:

- The vendor onboarding portal is available and stable during business hours.
- Integration with ERP is accurate (no mismatches between portal and ERP vendor records).
- Approval workflow logic correctly routes invoices to the right approvers every time.

Who owns this decision/control:

Department:	*Role*:	*Sponsor*:
Finance/Accounts Payable	AP Manager (process owner); Director of Finance (control owner)	Chief Financial Officer (CFO)

Step 2 – Identify Potential Hidden Risks:

Use the table to document potential hidden risks.

Hidden Risk Description:	*Hidden Risk Types*[A]:	*Stakeholders Impacted*:	*Evidence/Notes*:
To meet project deadlines, business units may bypass the portal by using existing vendors as "generic" pass-throughs (e.g., coding new suppliers' invoices to a generic "Other Services Vendor").	• Workaround/Bypass • Shadow System • Data Quality	• Project managers and business units • Accounts Payable • Internal Audit • Actual vendors who are not properly recorded in the system	• Informal feedback from project managers that vendor setup "takes too long." • Increase in invoices coded to a small set of generic vendors after go-live. • Audit testing found invoices where the payee's name on the invoice does not match the ERP vendor name.
Dual approval for all invoices over $25,000 may create bottlenecks when managers are traveling or busy, delaying critical payments and damaging supplier relationships.	• Delay/Bottleneck • Stakeholder Friction • Compliance Burden	• Vendors (cash flow, willingness to do business) • Procurement and AP teams • Business units relying on time-sensitive services	• AP helpdesk tickets citing "urgent payment" escalations. • Late payment interest charges observed in the last quarter. • Vendor satisfaction survey: several comments about "slow payment/unpredictable timing."

Hidden Risk Description:	*Hidden Risk Types*[A]:	*Stakeholders Impacted*:	*Evidence/Notes*:
Because AP is now the gatekeeper for vendor setup, some business units create and maintain their own "shadow vendor lists" in spreadsheets to track suppliers they *intend* to onboard later.	• Shadow System • Data Quality • Risk Displacement	• Business unit admins • AP team (reconciliation burden) • IT and Security (data stored outside controlled systems)	• Discovery of multiple Excel vendor lists on shared drives with banking details. • Inconsistent vendor names and tax IDs across these shadow lists. • Security concern: sensitive vendor data stored without proper access controls.
Strict documentation requirements (e.g., mandatory W-9 and banking verification) may lead some vendors to refuse or delay onboarding, especially international or small vendors unfamiliar with requirements.	• Stakeholder Friction • Compliance Burden • Risk Displacement	• Small/international vendors • Procurement (difficulty sourcing niche services) • Legal and Compliance teams	• Several vendors declining to provide bank details electronically. • Increased use of "personal reimbursements" to employees as a workaround. • Legal concerns about inconsistent treatment of vendor documentation.

[A] *Hidden Risk Types*:

- Workaround/Bypass
- Delay/Bottleneck
- Misaligned Incentives
- Compliance Burden
- Shadow System
- Stakeholder Friction
- Risk Displacement
- Data Quality

Step 3 – Map First-, Second-, and Third-Order Effects:

Think beyond the immediate impact. Use the prompts.

First-Order Effects (Direct):

What happens immediately when this control/change is applied?

- All new vendors must go through a standardized portal.
- AP validates tax forms and banking before activation.
- Invoices over $25,000 now wait for dual approval.
- Audit trail for vendor setup and approvals improves significantly.

What becomes harder, slower, or more constrained?

- Setting up new vendors for urgent/one-off needs.
- Processing high-value invoices when approvers are unavailable.
- Working with small or international vendors unfamiliar with documentation requirements.

Additional Notes:

- Direct improvement in control effectiveness: fewer unauthorized vendors, better documentation.
- Direct cost: longer cycle time from initial vendor request to first payment.

Second-Order Effects (Ripple Effects):

How do other teams/functions experience this?

- **Procurement:** More time spent explaining requirements to vendors; may push back on AP over perceived "red tape."
- **Project teams:** Build extra lead time into their project schedules, or ignore the process and push AP at the last minute.
- **IT/Security:** Concern about spreadsheets and shadow lists containing vendor bank data.

What new tasks, delays, or burdens emerge?

- AP fielding more "status check" emails and escalations from business units.
- Managers spending more time reviewing and approving high-value invoices.
- Additional reconciliations between shadow vendor lists and ERP to ensure no duplicate or missing vendors.

Additional Notes:

- Some operational risk is displaced from "fraudulent vendor setup" to "late payment/strained vendor relationships."
- Informal workarounds develop where risk is less visible (e.g., personal reimbursements).

Third-Order Effects (Systemic & Longer-Term):

What patterns emerge over weeks/months?

- Vendors begin to perceive the company as "slow payer," potentially impacting pricing and willingness to contract.
- Business units maintain their own databases of preferred vendors, which diverge from ERP master data.
- AP becomes a perceived bottleneck, harming cross-functional trust.

What new risks or inefficiencies are introduced over time?

- Fragmented and inconsistent vendor datasets across the organization.
- Heightened cyber and privacy risk due to uncontrolled storage of vendor data.
- Increased use of non-standard payment methods (e.g., reimbursements) that bypass the intended control.

Could this create compliance, data quality, or reputational issues?

- Yes. Poor data quality and shadow systems complicate tax reporting and sanctions screening.
- Vendors' negative experiences can harm reputation and bargaining power.
- If a fraud event occurs via a workaround, the organization could be criticized for designing an "unusable" control that people felt forced to bypass.

Additional Notes:

- Over time, an initially strong control may erode in practice if not adjusted to real-world behaviors and constraints.

Step 4 – Map First-, Second-, and Third-Order Effects:

Evaluate options for address your most important hidden risks. A balanced solution should solve the real problem without creating new ones.

Too HEAVY (Overreaction): *Creates new burdens, slows the system, adds unnecessary controls*

- Further tighten controls by requiring triple approval for all invoices over $10,000.
- Block any payment to vendors not created through the portal. No exceptions.
- Prohibit spreadsheet containing vendor information, and immediate deletion of all legacy lists.

Too Light (Underreaction): *Fails to address root cause, risk remains unmanaged*

- Send a reminder email saying, "please don't use generic vendors" and "avoid shadow lists."
- Ask AP to "do their best" to process vendor requests faster, without additional resources or design changes.
- Assume vendors will adjust over time without additional support.

Balanced Response: *Proportional, feasible, minimal side effects*

Risk-based thresholds:

- Keep dual approval at $25,000 but introduce:
  - Fast-track path for *pre-approved* low-risk vendors.
  - Temporary emergency override with after-the-fact reviews for time-critical payments.

Process & capacity adjustments:

- Allocate additional AP resources during month-end and project peaks.
- Introduce SLA commitments: e.g., 1 business day for standard vendor setups when documentation is complete.

Design out the workarounds:

- Regularly monitor use of generic vendors and require justification.
- Provide a simple "one-time vendor" process with controls for low-risk, low-value payments.

Support & education:
- Short video + one-pager for vendors explaining documentation requirements.
- Training for business units on lead times, using real examples from this analysis.

How would I explain this to leadership/ Audit Committee): *Clear rationale*

We identified that our strengthened vendor onboarding control significantly reduced the risk of fraudulent vendors but created new hidden risks, including workarounds, payment delays, and shadow systems. Instead of simply tightening or loosening the control, we redesigned it on a risk-based basis: faster processing for low-risk cases, clearer guidance for vendors and requesters, and specific monitoring of high-risk behaviors like use of generic vendors and shadow lists. This preserves the core control objective while reducing unintended consequences and improving overall system reliability.

Step 5 – Early Warning Indicators & Monitoring Plan:

Identify signals that hidden risks are emerging.

Indicator	*Leading/ Lagging*	*Data Source*	*Threshold/ Trigger*	*Owner*
% of invoices coded to generic vendors ("Misc Services," "Other Vendor")	Leading	ERP invoice report	>10% of invoices in any business unit for two consecutive months	AP Manager
Average vendor setup cycle time (request to activation)	Leading	Vendor portal & ERP logs	>3 business days average for two months OR spikes around key project periods	Process Excellence Team
Number of vendor payment escalations marked "urgent"	Lagging	AP helpdesk ticket system	>20 escalations per month OR 50% increase vs prior quarter	AP Supervisor
Count of late payment fees/interest charges	Lagging	ERP and bank statements	Any sustained increase (>25% quarter-over-quarter)	Director of Finance
Discovery of shadow vendor lists with sensitive data	Leading	Internal Audit / IT security reviews	Any instance triggers root cause analysis and corrective action	Internal Audit Lead

Monitoring Plan:

Frequency:
- Monthly review of key indicators in AP/Finance dashboard.
- Quarterly deep-dive with Internal Audit and Procurement to review patterns and adjust thresholds.

Responsibilities:
- AP Manager: maintain dashboard, analyze trends, propose adjustments.
- Procurement: monitor vendor feedback, support communication and training.
- Internal Audit: independently test for workarounds and shadow systems each quarter.

Follow-up path:

- If thresholds are breached:
  - AP Manager documents incident, root cause, and proposed corrective actions.
  - Escalate significant issues (e.g., fraud or repeated workarounds) to Director of Finance and, if needed, Audit Committee.
  - Update process documentation, training materials, or system configuration as appropriate.

Lessons Learned/Future Design Notes:

- Build user feedback loops into any new control design within 60 days of implementation.
- Always define at least 3–5 early warning indicators when launching new controls or major process changes.
- Consider usability and capacity constraints as "first-class" design requirements, not afterthoughts.