

PAPER TIGER TECHNOLOGIES

Risk Management Policy

1. Purpose

The purpose of this Risk Management Policy is to define how Paper Tiger identifies, evaluates, treats, and monitors risk in the illustrated environment. A current risk register is what keeps the program's priorities defensible and its resource decisions rational.

Risk management is the ordering function that tells the program where to spend effort first. Without a scored register, security work is driven by whichever threat is loudest this week; with one, it is driven by likelihood and impact weighted together and reviewed on a schedule.

This policy is fictional and illustrative. It describes no real risk, assessment, or organization.

The register is what keeps priorities defensible and resource decisions rational, because it replaces the question of what feels most urgent with a scored, reviewed ordering.

The policy turns risk from a vague concern into a scored, owned, and decided item, so the program's priorities trace to actual exposure rather than intuition.

The register is a decision tool, not a shelf, so the policy keeps it data-driven, top-reviewed, and fully documented on the decisions it records.

Risk management exists to make decisions about uncertainty explicit, and the policy turns an informal worry into a register with owners, ratings, and treatments.

2. Definitions

Term	Definition (illustrative)
Risk	The combination of the likelihood and impact of an undesirable event.
Risk register	The living inventory of risks with owners, scores, and treatments.
Likelihood	The illustrative probability a risk will materialize.
Impact	The illustrative consequence if a risk materializes.
Inherent risk	The risk before controls are applied.
Residual risk	The risk remaining after controls and treatment.
Treatment	The chosen response: mitigate, accept,

	transfer, or avoid.
Risk owner	The role accountable for a risk and its treatment.
Risk appetite	The level of risk the governance forum is willing to accept.
Assessment	The periodic evaluation that refreshes scores.
Scoring methodology	The documented likelihood and impact scales.
Portfolio view	The register reviewed for concentration.
Calibration	The alignment of assessors on scoring.
Risk tolerance	The acceptable variation around the stated appetite for a given category of risk.
Key risk indicator (KRI)	A metric that signals when a risk is trending toward the threshold.
Risk treatment	The chosen response to a risk: avoid, reduce, transfer, or accept.
Key risk indicator	A metric that gives early warning of rising risk.
Risk matrix	The grid that maps likelihood to impact.
Risk event	A realized risk that has actually occurred.
Threat	A potential cause of harm to an asset.
Risk mitigation	The action that reduces the likelihood or impact.
Risk acceptance	The documented decision to bear a risk.
Risk scoring	The rating of likelihood and impact on a documented scale.
Aggregate risk	The combined exposure of a cluster of risks.
Portfolio review	The top-down review of the register as a whole.
Risk register owner	The person accountable for keeping the register current.
Risk treatment plan	The documented actions chosen to address a risk.
Emerging risk	A risk that is new or materially changed and not yet fully understood or controlled.
Risk scenario	A described event with its causes, likelihood, and impact used to test the response to a risk.
Risk portfolio	The complete set of open risks and their treatments viewed together.

3. Scope and Boundaries

This policy applies to fictional security, privacy, availability, and third-party risks inside the service boundary. It covers the full risk lifecycle from identification through monitoring.

It applies to risks regardless of their origin, whether an assessment, an incident, a change, or a vendor review, so all risks land in the same register.

Out of scope are real risks and real organizations. This policy creates no real obligation.

Third-party risk is scored in the same register as internal risk, so a vendor failure is treated with the same rigor as an internal control weakness rather than as a separate concern.

Escalation follows the risk level: a risk within appetite stays with the risk owner, a risk above appetite goes to the governance forum, and a risk that threatens the demonstration's viability is escalated immediately to leadership.

The register captures the demonstration's own risks; a risk that could reach a customer is escalated so the customer is informed where appropriate.

The register is the demonstration's own risk picture; it is fictional and reflects illustrative risks rather than a real assessment.

The register is reviewed top-down as a portfolio, not just item by item, so a cluster of small risks is seen for the aggregate exposure it creates.

Risk management feeds the other policies by telling them which controls matter most, so the register is not an end in itself but the input that sets priorities.

This policy applies to security, privacy, operational, and supply-chain risks, including those introduced by new technology or a change in threat activity.

4. Roles and Responsibilities

Role	Illustrative responsibility
Risk Owner	Owns the policy and the risk register.
Risk Assessor	Performs assessments and updates likelihood and impact.
Control Owner	Operates the controls that treat an identified risk.
Governance Forum	Reviews the register and accepts residual risk.
Information Security Lead	Consumes the register to set program priorities.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for risk management:

Activity	Risk Assessor	Risk Owner	Control Owner	Governance Forum

Identify risks	R	C	I	I
Score risks	R	A	C	I
Treat risks	I	C	R	I
Accept residual risk	I	C	I	A
Refresh the register	R	A	I	I

5. Policy Requirements and Controls

PTT-POL-016-C01. Maintain a risk register

Identified risks are recorded with owner, likelihood, and impact, so the program has a single inventory of what it is worried about. Without the register, risks live in individual heads and disappear when people leave. The register is versioned and its owner is named.

PTT-POL-016-C02. Assess on a cadence

The register is refreshed at least annually and after material change, so scores reflect current conditions rather than a one-time snapshot. Material changes such as a new service trigger an immediate reassessment. The assessment is dated and a miss is escalated.

PTT-POL-016-C03. Rate likelihood and impact

Risks are scored on a defined scale for consistent ranking, so two assessors looking at the same risk arrive at comparable scores. The scale is documented so scoring is repeatable. The rating uses the documented scale.

PTT-POL-016-C04. Choose a treatment

Each risk is treated by mitigation, acceptance, transfer, or avoidance, and the choice is recorded. An untreated risk is not a valid end state; every risk must have a decision. The chosen treatment is recorded with its rationale.

PTT-POL-016-C05. Track treatment actions

Treatments become dated, owned action items, so a decision to mitigate actually produces work rather than a note. Actions are followed to closure like any other program action. The action is tracked to closure.

PTT-POL-016-C06. Review residual risk

The governance forum confirms acceptance of remaining risk, so residual risk is an explicit decision made by the right level rather than an implicit leftover. The residual is recorded after treatment.

PTT-POL-016-C07. Report to the program

Risk trends feed the information security program review, so the program's priorities track the register rather than diverging from it. The register feeds the program, so priorities are set from risk.

PTT-POL-016-C08. Include third-party risk

Vendor and subprocessor risk is scored in the same register, so the supply path is not treated as a separate, unmanaged category. Third-party risk is included, so a vendor's risk is not invisible.

PTT-POL-016-C09. Document risk appetite

The governance forum records its appetite, so assessors know what level of risk is acceptable without escalating every finding. The appetite is written, so acceptance has a threshold.

PTT-POL-016-C10. Escalate above appetite

Risks above the accepted appetite are escalated for a decision, so no risk silently exceeds the threshold the forum set. A risk above appetite is escalated to governance.

PTT-POL-016-C11. Document the scoring methodology

The likelihood and impact scales are documented so two assessors arrive at comparable scores, and the methodology is reviewed when scoring shows inconsistency. The scoring method is documented, so ratings are consistent.

PTT-POL-016-C12. Review the register as a portfolio

The register is reviewed as a portfolio rather than risk by risk, so concentration across risks is visible and addressed. The portfolio view catches aggregate exposure, not just single risks.

PTT-POL-016-C13. Feed risk into planning

The register feeds planning so that the highest residual risks receive the next cycle's resources, closing the loop between assessment and action. Risk feeds planning, so resources go to the highest exposure.

PTT-POL-016-C14. Document risk decisions

Each risk decision is recorded with its rationale and approver, so the register shows not just what was decided but why. A decision is recorded with its rationale, so it is not silent.

PTT-POL-016-C15. Review the risk appetite

The risk appetite is reviewed annually and after a material event, so the threshold tracks the environment's reality. The appetite is reviewed, so it stays current with the business.

PTT-POL-016-C16. Escalate aggregate risk

Aggregate risk across the portfolio is escalated when concentration rises, so the forum sees the whole rather than only individual risks. Aggregate risk is escalated, so a cluster of small risks is seen.

PTT-POL-016-C17. Track treatment to closure

Each mitigation has an owner and a date and is followed to completion, so the register reflects action, not intention. Treatment is tracked to closure, so it does not stall.

PTT-POL-016-C18. Track key risk indicators

A small set of indicators is watched to signal when a risk is moving, so the register is refreshed by data rather than by periodic recollection. Indicators give early warning of rising risk.

PTT-POL-016-C19. Assign an owner to every risk

Each risk has a named owner, so there is a single person accountable for watching it and driving its treatment.

PTT-POL-016-C20. Document accepted risk

A risk that is accepted is recorded with its rationale and an expiry, so acceptance is a decision with a review date rather than a silent default. The acceptance records its rationale and expiry.

PTT-POL-016-C21. Link risks to controls

Each risk is tied to the control that treats it, so a gap is visible when a risk has no control assigned.

6. Operating Procedures

Identify risks.

Risks are gathered from assessments, incidents, changes, and vendor reviews, and each is entered into the register.

Rate each risk.

The assessor scores likelihood and impact using the documented scale, and records the inherent score.

Select treatment.

The owner chooses mitigation, acceptance, transfer, or avoidance, and records the decision.

Assign action items.

Treatments become dated, owned actions that are tracked to closure.

Escalate residual risk.

Remaining risk above appetite is presented to the governance forum for acceptance.

Refresh the register.

The register is updated on its cadence and after material change.

Report trends.

Risk trends are summarized for the program review.

Calibrate scoring.

Assessors calibrate on a sample of risks so scoring is consistent before a full assessment.

Review the portfolio.

The governance forum reviews the register as a whole and addresses concentration.

Record a decision.

A risk decision is recorded with rationale and approver.

Review the appetite.

The risk appetite is reviewed at the annual cycle.

Score a new risk.

The owner assigns likelihood and impact, computes the resulting level, and records the rationale.

Present a risk decision.

Risk above appetite is presented to the governance forum with options and a recommendation, and the decision is recorded.

Review a key risk indicator.

The indicator is checked against its threshold, and a breach triggers a risk review.

Review the register.

The risk owner walks the register, updates the likelihood and impact, and flags any risk that has changed enough to need a new decision.

Document a risk decision.

The owner records the chosen treatment, the rationale, and the review date, so the decision is not silent.

Score a risk.

The owner rates likelihood and impact on the documented scale and records the result.

Escalate above appetite.

A risk above appetite is raised to governance with its treatment options.

Close a treatment action.

The owner confirms the action is done and records the closure.

Update the register.

The owner changes a risk's rating or treatment and records the date and rationale.

Review key risk indicators.

The owner checks the indicators for early warning and flags any movement.

Escalate aggregate risk.

A cluster of small risks is raised to governance as one aggregate exposure.

Feed risk into planning.

The owner passes the register to planning so resources go to the highest exposure.

Document the scoring methodology.

The owner records how likelihood and impact are rated, so ratings stay consistent.

Track emerging risks.

The risk owner reviews new technologies, threat reports, and regulatory changes on a set cadence and records any risk that is new or materially different.

Document tolerance per category.

The risk function records the acceptable level of risk for each category, so decisions about a specific risk are measured against a stated tolerance.

Review the risk portfolio.

The risk function reviews all open risks together on a set cadence to spot concentration, competing treatments, or risks that have outgrown their owner's authority.

7. Frequency and SLAs

Illustrative risk cadence:

Activity	Frequency (illustrative)
Risk register refresh	Quarterly and after material change
Full assessment	Annually
Governance acceptance	Quarterly
Policy review	Annually

8. Exceptions and Lifecycle

An exception permits accepting a risk above the normal threshold when the governance forum documents the business rationale and a review date. The acceptance names the risk and the compensating context.

Accepted risks are revisited at least quarterly, and a risk that keeps exceeding appetite is treated as a signal to re-treat it rather than accept it indefinitely.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Risk register	The current inventory with scores and treatments.
Assessment records	The scored likelihood and impact.
Treatment action items	The dated, owned mitigations.
Governance acceptance notes	The residual risk decisions.
Trend summary	The program-facing risk trends.
Risk appetite statement	The documented threshold.
Scoring methodology	The documented scales.
Portfolio review	The concentration analysis.
Treatment log	The mitigations and their closure status.
Treatment action log	The recorded actions and their closure.
Risk matrix	The documented likelihood-to-impact scale.
Risk event log	The recorded realized risks.
Threat register	The tracked threats relevant to the demonstration.
Acceptance records	The documented accepted risks.
Emerging risk register	Lists new risks with their source, owner, and initial assessment.
Tolerance statement	Records the acceptable risk level for each category.
Portfolio review record	Summarizes the aggregate view of open risks and any concentration found.

10. Oversight and Metrics

- Register currency: 100 percent of risks assessed within the cadence (illustrative).
- Treatment action closure: at least 90 percent closed on time.
- Risks above appetite: each escalated and decided.
- Open risk count: trending down or stable.
- Scoring consistency: assessor variance within the documented tolerance.
- Risk above appetite: the count of unaccepted risks above threshold trending toward zero.
- Treatment timeliness: mitigations closed within their committed date.
- Percentage of risks with an owner and a treatment.
- Treatment action closure on time.
- Percentage of risks with an owner and treatment.
- Inherent versus residual risk movement per period.
- Risk events correlated to register entries.
- Accepted risks past their expiry.
- Mitigations completed on time.

11. Appendix

Illustrative risk scoring:

Likelihood	Impact	Rating (illustrative)
Unlikely	Minor	Low
Possible	Moderate	Medium
Likely	Major	High
Almost certain	Severe	Critical

12. Related Policy Dependencies

- Information Security Program Policy (consumes the register to set priorities)
- Vulnerability Management Policy (feeds technical risk into the register)
- Subprocessor List (feeds third-party risk)
- Business Continuity and Disaster Recovery Policy (treats availability risk)

13. Review Cadence

The Risk Owner reviews this policy at least annually, after a material change to the illustrated environment, and after a significant simulated risk event.

Revision History

Version	Date	Change summary	Author
1.0	September 28, 2026	Original enterprise-	Paper Tiger

		depth fictional demo policy for controlled trust-center testing.	Technologies
--	--	--	--------------

Document Control

Field	Value
Document ID	PTT-POL-016
Document Owner	Risk Owner
Status	Fictional demo artifact
Effective Date (illustrative)	September 28, 2026
Review Cadence	At least annually and after material fictional changes
Classification	Internal Demo
Approval	Illustrative governance approval only; no real adoption represented