RISK MANAGEMENT FRAMEWORK

Evaluate your current environment, identify gaps across your security systems, and build a consistent, repeatable approach to managing risk.

Physical security risk assessment worksheet.

Evaluate your current environment, identify gaps across your security systems, and build a consistent, repeatable approach to managing risk.

siteowl®

60%

Of security professionals report that threats change significantly within a single year.

30%

of physical assets in large enterprises go unaccounted for.

40%

Inventory inaccuracy is common across multi-site programs.

THE PROBLEM.

WHY MOST RISK ASSESSMENTS FALL SHORT.

Physical security risk assessment shouldn't be a once-a-year checklist. Yet for most organizations, that's exactly what it is. Over 60% of security professionals report that the threats facing their organizations change significantly within a single year. An annual assessment leaves most of that risk unaccounted for.

Risk doesn't wait for your review cycle. New vulnerabilities emerge. Security systems age. Vendors change. And the gap between what you think is protected and what's actually secured widens, quietly, continuously, and often invisibly. But most organizations are still managing risk assessments with incomplete data, disconnected systems, and documentation that's outdated before the ink dries. The result is predictable: gaps go unnoticed, issues take longer to resolve, and decisions get made without the full picture. This worksheet gives security decision-makers, from coordinators to seasoned directors, a structured tool to identify, evaluate, and act on risk across their security systems.

A physical security risk assessment should be a living part of your security program, one that helps security leaders stay ahead of potential threats, close vulnerabilities before they become incidents, and protect critical assets without disrupting business operations.

THE FRAMEWORK.

5 STEPS TO A SMARTER RISK ASSESSMENT.

1	**Establish full asset visibility.**	Account for every device, map accurate locations to floor plans, and build a single system of record across all sites.
2	**Identify vulnerabilities and threats.**	Go beyond obvious gaps, surface risks in the overlap between systems, processes, and human behavior.
3	**Standardize your evaluation criteria.**	Create a common language for risk across all locations, teams, and providers so assessments are consistent, not subjective.
4	**Prioritize risk based on business impact.**	Not all risks are equal. Focus resources where they matter most, critical assets, high-traffic areas, compliance exposure.
5	**Maintain, monitor, and improve continuously.**	Tie remediation to specific assets, track progress in real time, and hold vendors accountable from start to finish.

THE PHYSICAL SECURITY VISIBILITY GAP.

What you think is protecting your environment often doesn't match what's actually deployed on-site. Industry benchmarks suggest that large enterprises are unaware of up to 30% of their physical assets, including edge devices like sensors, auxiliary locks, and older cameras.

Assumption.	Reality.	Impact.
Complete camera coverage.	Hidden blind spots and misaligned views.	Up to 30% of cameras miss intended coverage.
Secured entry points.	Unmonitored or misconfigured access points.	Common source of unauthorized access.
Fully functional access control systems.	Doors propped open or readers offline.	Gaps in critical security controls.
Accurate asset inventory.	Missing or outdated devices.	20–40% inventory inaccuracy is common.
Standardized security measures.	Inconsistent setups across sites.	Weakens overall security posture.

ASSESSMENT WORKSHEET.

EVALUATE YOUR CURRENT SECURITY ENVIRONMENT.

Rate each item 1–3 (1 = not in place 2 = partially in place 3 = fully in place).
Note gaps and priority actions.

Step 1: Asset visibility.

Assessment item.	Rating	High / Med / Low	Notes:
Complete, current inventory of all cameras, sensors, and edge devices.	● ● ●		_____ _____
All devices mapped to accurate, current floor plans.	● ● ●		_____ _____
Real-time operational status and service history accessible.	● ● ●		_____ _____

Warranty and lifecycle data centralized in one system of record.	● ● ●		_____ _____

Step 2: Vulnerability & threat identification.

Assessment item.	Rating	High / Med / Low	Notes:
Camera blind spots and coverage gaps identified across all sites.	● ● ●		_____ _____
Access control systems verified for correct configuration and use.	● ● ●		_____ _____
Threat model accounts for industry-specific risks and environment.	● ● ●		_____ _____
Vendor and provider performance tracked and reviewed regularly.	● ● ●		_____ _____

Step 3: Standardization & evaluation criteria.

Assessment item.	Rating	High / Med / Low	Notes:
Consistent risk scoring criteria applied across all sites and teams.	● ● ●		_____ _____
Security policies and standards documented, shared, and enforced.	● ● ●		_____ _____
Compliance and regulatory requirements mapped to specific controls.	● ● ●		_____ _____
All vendors working from the same design and documentation standards.	● ● ●		_____ _____

Step 4: Risk prioritization.

Assessment item.	Rating	High / Med / Low	Notes:
Critical assets and high-risk areas identified and ranked.	● ● ●		_____
Business impact used to drive prioritization not just likelihood.	● ● ●		_____
Stakeholders aligned on risk thresholds and escalation criteria.	● ● ●		_____
Budget and capital planning informed by lifecycle and failure data.	● ● ●		_____

Step 5: Monitoring & continuous improvement.

Assessment item.	Rating	High / Med / Low	Notes:
Ongoing device health and system performance monitoring in place.	● ● ●		_____
Lifecycle tracking flags aging equipment before it becomes a failure.	● ● ●		_____
Vendor accountability tracked beyond installation service and response.	● ● ●		_____
Assessment process reviewed and updated on a defined, regular cycle.	● ● ●		_____

RISK PRIORITY MATRIX.

A high-priority risk isn't necessarily the one most likely to happen, it's the one that costs the most when it does. Use this matrix to categorize and rank risks by impact.

Risk level.	Likelihood	Business impact.	Required action.
CRITICAL	**High or low**	Operations halt, safety risk, or regulatory breach.	Immediate remediation required.
HIGH	**Moderate–high**	Significant disruption to business operations or compliance exposure.	Prioritize in current planning cycle.
MEDIUM	**Moderate**	Operational inconvenience or limited exposure.	Schedule with defined timeline.
LOW	**Low**	Minimal impact if exploited.	Monitor and address in routine maintenance.

COMMON QUESTIONS.

PHYSICAL SECURITY RISK ASSESSMENT FAQS.

What is a physical security risk assessment in simple terms?

It's the process of identifying vulnerabilities in your security systems, understanding the threats that could exploit them, and evaluating the potential impact on your people, assets, and operations.

What are the most common gaps found during a risk assessment?

Typical gaps include incomplete asset visibility, blind spots in camera coverage, misconfigured access control systems, and inconsistent security measures across locations.

How do you prioritize risks once they're identified?

Risks should be prioritized based on their potential impact on critical assets and business operations, not just how easy they are to fix.

Why do physical security risk assessments often fail?

They break down when data is incomplete, processes aren't standardized, and teams rely on disconnected tools. Without consistency and visibility, assessments become subjective and hard to act on.

How can organizations improve their overall security posture?

By making risk assessment a continuous, structured process, supported by accurate data, consistent evaluation criteria, and clear alignment across teams and systems.

About SiteOwl

SiteOwl is the only physical security system lifecycle management platform that brings enterprise security teams, their security vendors, and assets together on one unified platform.

The solution's suite of applications connect real-time data and workflows, specific to the physical security industry, to drive collaboration, visibility and efficiency.

To learn more, please visit getsiteowl.com.