Physical security risk assessment template

For tech companies

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Introduction

Tech companies following the latest digital trends are not immune to physical threats. The workspace is evolving. The physical and digital worlds converge. The hybrid workspace is becoming a necessity, not a perk. The cloud allows modern companies to transform security risks into operating advantages.

The proactive approach to security allows your business to remain competitive by reducing risks. To keep your people and places safe, approach your physical security as you approach your digital strategies.

Use the physical security risk assessment template to protect your facility and staff by identifying gaps in your physical security.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

kisi

Define your objectives

Before starting the physical security risk assessment, take a minute to define your objectives. This way, you'll be able to see the bigger picture and ensure a more effective and valuable assessment.

Objectives examples

- Perform an analysis to determine the state of the security system and uncover the biggest risks to prioritize the next steps.
- Determine the effectiveness of your current security setup and identify opportunities for improvement.
- Validate the need to upgrade the current access control system to internal and external stakeholders.
- Evaluate the alignment of risk management with the overall company strategy.

I'm doing this physical security risk assessment to:

**Fill in using a PDF program or print it out*

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Physical space audit

Potential risk	Considerations	Current status	Recommended action
Natural barriers Do you use any natural barriers (e.g., doors, fences, signs) to discourage or prevent access where needed?	Do you use any natural barriers (e.g., doors, fences, signs) to discourage or prevent access where needed?		Add symbolic barriers to the outer parameter to direct people to a particular route and draw attention to whoever crosses the threshold.
Outside environment Bad actors have more opportunities to observe, plan, and commit criminal activity in secluded spaces with poor visibility and chances for natural surveillance.	What is the outside environment and visibility like? Is it a busy, easy-to-surveil, open space, or does it offer concealment areas for bad actors?		Increase the visibility and liveliness around your space to evoke natural surveillance and promote a sense of exposure to potential wrongdoers.
Facility maintenance Unmaintained facilities foster a sense of abandonment and neglect, which attracts criminals.	Are your spaces and their surroundings well maintained (e.g., well-lighted street, fresh paint, clear signage, maintained walkways)?		Regularly maintain your spaces and instantly refurbish any damage.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
Lighting Unlit outer access points provide better concealment to wrongdoers. Unmaintained inside lights are an additional threat in case of emergency, like nonfunctional exit lights.	Are all access points to your space well-lit?		Replace all the broken lights and do regular maintenance checks.
Space usage When spaces feel unwelcoming and don't engage the intended users, they often remain empty and look abandoned. In turn, the lack of legitimate activities can encourage criminal activities.	How do your spaces promote their intended use? Are they designed to engage legitimate visitors?		Add enticements to draw the desired users to your space.
Property boundaries Undefined and unmarked space can give the impression of no one's land and encourage trespassers.	Are your property's boundaries easily identified (e.g., through landscaping, barriers, or signs)?		Add real or symbolic markers to deter trespassers and promote a feeling of "psychological ownership" in employees.
Security layers Having just one security layer increases risks since it might not discourage or prevent attackers. The more layers, the more obstacles they'll have to tackle.	Is security implemented in multiple layers to delay penetration to the areas that need the most protection? Consider if your security elements start from the outer perimeter and move inward to the most sensitive company area.		If your outer perimeter doesn't allow for layered security, implement a modern high-tech access system at your entry and inner doors that secure more valuable assets. Integrate with cameras for enhanced security.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
Access points Undefined access points won't deter intruders, casual trespassers, or unauthorized personnel.	Can people access your spaces only through defined access points?		Add clear signage and deploy access control hardware to your access points.
Signage Inner areas with clear signs that define access requirements for the area, having access control readers with an intrusion detection system, and video surveillance to monitor access can significantly reduce risks. For instance, without clear signage unauthorized personnel can gain access to rooms where valuable assets are stored.	Are there signs defining the access requirements to interior areas with restricted access?		Deploy extended access control in inner rooms that house valuable assets. Add clear signs, access readers that support intrusion detection, and integrate with video surveillance.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Physical security system audit

Potential risk	Considerations	Current status	Recommended action
Doors			
Exterior wood and most glass doors can easily break under impact and pose a security risk. Glass doors often limit the type of access control hardware that can be installed, including locks, sensors, and readers. Hinges can also be defeated.	What materials are exterior and interior doors that protect valuable assets made of? Are their hinges spot welded, or do they use set screws?		Cover solid wood or sturdy hollow metal doors with metal to strengthen them against a tool attack. Retrofit exterior glass doors with polycarbonate security glazing. Anchor the door frames, add kick plates and use set screws in hinges or spot weld hinges.
Structure			
Some access points are easy to overlook, like windows, building facades, skylights, and ventilation ducts. Neglecting these entry points may encourage penetration.	Are all the external and important internal access points structurally reinforced to prevent penetration?		Take care of inconspicuous access points by incorporating protective lighting, intrusion detection systems, doors and window bars, and reinforce your skylights and ventilation ducts.
Locks			
Malfunctioning locks pose a huge risk. The type of lock can pose a security risk as well. Electronic locks often offer higher security and lower the risk of credential duplication. Reprogramming electronic locks takes less effort than rekeying mechanical ones.	Do you have functional locks in place at all office access points? Are they mechanical or electronic?		Do regular checks and maintenance of your locks. Enhance your security by connecting your electronic locks to a cloud-based access control system.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

kisi

Potential risk	Considerations	Current status	Recommended action
Electromagnetic locks Your space's occupants are at risk in case of an emergency if your electromagnetic locks don't comply with code requirements.	Do your electromagnetic locks meet all safety codes?		Follow the code requirements. Add external release devices such as motion sensors or request-to-exit switches to allow building occupants to exit.
Key management Keeping track of keys is among the most prominent risks of using mechanical key locks. You need to account for all keys at the beginning and end of the workday and ensure that any risk damage hasn't occurred.	Do you use a key management system to inventory keys? Do you have documented processes for key management?		Implement a key management system to control and account for all your keys. Conduct initial and periodic inventories of keys, maintain records of who has which keys, and secure the key storage facility. Consider implementing a keyless access control system for extended security and peace of mind.
Access control system Relying on mechanical keys to secure your space presents a huge security risk. Keys are simple to duplicate or lose. Unmaintained legacy access control systems present a threat as well.	Do you have an access control system in place? When was it last updated?		Deploy a cloud-based access control system or migrate your legacy system to the cloud. Benefit from over-the-air (OTA) updates and remotely manage your spaces and users.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
People flow Avoid congestion due to slow and unreliable access systems or using one authentication method to validate access. These can cause congestion during the busiest times, like the beginning of the work day or lunch.	Does your access control system support the varying people flow?		Modern access control systems are faster, more reliable, and offer multiple authentication methods. Mobile access control encourages more efficient flow since people don't spend time searching for their cards or fobs but use their mobile phones to enter.
Access cards Using key cards as the sole access control method causes operational burdens and poses security risks. Key cards are easy to steal, and card cloners are available online. There is also the risk of numerous key cards belonging to visitors, past occupants, and lost cards in circulation.	Do you issue access cards? How do you handle visitor cards and lost cards?		Upgrade your access system to the cloud to better manage your card systems and add additional credential methods. Integrate with SCIM to keep user information up to date. Share visitor links with limited access hours and privileges.
Credential sharing Shared credentials like access cards pose an unauthorized access risk. It can result in loss of access or allow access privileges to specific areas to unauthorized personnel.	Do you allow access card sharing?		Have a clear policy on the use of access cards to guide your employees as to what they can and cannot do with their access cards to help deter unauthorized card sharing. Introducing mobile phones as credentials is an effective way to prevent credential sharing.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
PIN Using a single, common PIN for all users when using a keypad reader makes your spaces and people extremely vulnerable. So does using multiple ones since it increases the chances of intruders guessing the correct PIN.	If you use keypad readers, how do you manage pin sharing?		Change PINs regularly and enforce two-factor authentication for an extra layer of security. For instance, users will need to scan their credentials and enter an individual PIN to gain access.
Surveillance Relying solely on people to monitor your spaces poses many threat mitigation and response risks. Knowing who is on your premises, or within close range, at all times is vital to protecting your business. Video surveillance helps you monitor your spaces while providing accurate, unbiased data that lets you explore incidents after they happen.	Do you use a video surveillance system? Which other systems assist you in video monitoring (e.g., access control integration, motion detection, analytics)?		Install a video system to keep track of any suspicious activity, deter criminals, monitor entry points, and identify safe practices and best risk management approaches.Think about how it will integrate with your other security elements like access control, sensors, and data analytics. All components should work seamlessly together for enhanced security.
Intrusion detection Intruders are a potential risk during out-of-office and office hours. Deploying sensors to detect intruders at the main entry is a common practice. Pay attention to the potential inside security threats like unauthorized personnel accessing unsecured offices.	Do you have sensors at all office access points to detect possible intrusion? Does your intrusion detection system meet your company's security needs? How does it integrate with your access control system?		Implement an intrusion detection system to detect the presence of an intruder attempting to breach the outer perimeter or secured inner areas. An access control system that supports cloud-based intrusion detection will prevent unauthorized entries by monitoring, registering, and alerting you about policy violations, like when a door is forced or propped open.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

kisi

Potential risk	Considerations	Current status	Recommended action
System maintenance Various physical security components tend to deteriorate with time. Worn-out access control equipment like doors, latches, access control readers, and cards is easy to identify but can create a loophole in the security system. An improperly working smoke detector, ventilation, or alarm system may go unnoticed until a security incident occurs. Security software poses a risk as well. Outdated software is prone to cyberattacks, while unmaintained access databases may pose threats such as unauthorized access, espionage, and vandalism.	How often do you maintain (hardware) and update (software) your security system?		Perform regular hardware preventive maintenance inspections to identify performance deficiencies and signs of deterioration in your physical security equipment. Deploy cloud-based security solutions to upgrade your software easily. Modern access control systems offer OTA updates and can integrate door access with your SSO provider to streamline operations and gain valuable insights.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

kisi

Operating procedures audit

Potential risk	Considerations	Current status	Recommended action
Physical security manager Physical security plays an important role in protecting people and spaces, but also critical information and data. As work and collaboration paradigms shift, new cases of security threats arise.	Who is responsible for your physical security? Are they part of senior management, and do they understand all technological and legal aspects?		If you keep physical security in-house, make sure the person responsible is part of senior management. Demonstrate that your company considers security vital by involving the physical security manager in the planning and decision-making process. They should understand both the technology and the legal aspects and have a modern perspective on security to grasp all the risks and potentials.
Access privileges management Things can quickly get out of hand if all personnel have the same access privileges. Without properly managed access control, people can access places outside working hours or simply access spaces they shouldn't. Access groups are essential to security but they can pose operational challenges to admins.	How do you ensure people only have access to the place they need? How do you manage various access groups?		Implement a user-friendly access control system that follows the principle of least privilege. Consider solutions that offer various admin roles for ease of operations and allow you to manage access based on users, groups, places, locations, devices, and time.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
Security policies and procedures Without proper security policies and procedures documentation, you risk compliance with numerous, ever-changing security regulations and legal requirements. Security processes are prone to be inconsistent and potentially flawed, with no clear standards, policies, and procedures that you can point to. And when it comes to security, inconsistency means increased risk.	How are your security policies and procedures documented? Are they effectively communicated to all employees? How often are they applied?		To establish strategic security objectives and priorities, identify the people accountable for physical security, and set forth responsibilities and expectations, present your security policies and procedures as forms or as lists of steps to be taken. Communicate them effectively to all personnel so they can adhere accordingly. Apply security policies consistently to minimize liability.
Security awareness Each employee not considered part of the security program poses a security risk. Expecting your employees to understand and participate in your security program and practices without training increases the risk of human-born error. Educate and empower employees to change their behaviors and protect the company from potential risk.	How do you ensure security awareness? Do you security train all your employees?		Create and conduct a security awareness program to help employees understand the relationship between the company's security and success. Encourage them to learn their security obligations, explain why they need the various security measures, and familiarize them with the resources available to help with security concerns. Onboard users and train admins on using the access control system. A modern, user-friendly access solution minimizes these efforts.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
Access control lists Onboarding, offboarding, and promoting employees require access level changes which can be tasking for managers as your tech company grows. Neglecting to update the access levels and hours will leave your spaces open to breaches. For instance, former employees can freely walk in at any time.	How do you maintain access control lists that define levels of access and access hours?		Deploy a cloud-based access control system that enables you to easily manage access control lists remotely at all times. Integrate it with your SSO provider to manage users securely and seamlessly through real-time provisioning. Set different groups by organizing users with the same access points and restrictions. To increase after-hours security, set time restrictions, like OOO hours and holiday schedules.
Visitor management Keeping track of the people entering your facilities every day minimizes security risks. A manual sign-in process is risk prone and inefficient. Access cards can make the process smoother, but visitors can forget to return them. The lack of time restrictions increases the risks as well. For instance, your cleaning staff can access your spaces at any time.	How do you regulate visitors' access?		Only allow temporary access for low-security doors. Deploy a modern access control solution to manage visitors securely. Some solutions allow sending access links to allow one-time users, visitors, and temporary staff to unlock specific doors at specific times without downloading an app or using credentials that can be misplaced, lost, or forgotten.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
Onboarding and offboarding Employees constantly come and go in growing tech companies. Providing access to new hires from the very beginning is essential for them to feel welcomed and to minimize the risks of access sharing. When employees leave, you need to quickly ensure they don't walk out with credentials that allow them to continue accessing your spaces and all the valuables and data stored there.	How fast do you on- and off-board employees and visitors? Do some of your former employees still have access?		Assure to terminate your former employee's access rights the moment they exit your space for the last time. Welcome new employees by granting them access on their first day. To manage users securely, streamlined access through real-time provisioning by integrating your access control solution with your SSO provider.
Fragmented access management The global, flexible, remote workforce poses cyber and physical security challenges. Restricting access management to business hours only or using legacy systems that only manage one location can be the downfall of any tech company.	Do you have control of all your locations anywhere, anytime?		Upgrade your physical security environment to the cloud to enable remote and global access control and monitoring. Stay on top by empowering admins to manage access to all your locations on the fly.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

kisi

Potential risk	Considerations	Current status	Recommended action
Unlimited access If the credentials grant access to your employees regardless of working hours, they pose a security threat. Robberies and property crimes tend to increase during the holidays. Those times when your spaces are most likely empty are the perfect opportunity for intruders and other criminal activities.	Can your employees enter your spaces during non-working hours (e.g., how do you manage access to your spaces during holidays)?		Deploy an access control system that will enable you to set time restrictions. For more effective management, set access schedules for specific groups to only allow access during needed time periods. For example, allow access to your full-time employees during their working hours on the weekdays or to specific weekdays for the hybrid workers. Modern access control systems have holiday lists for specific countries, so you can easily choose yours to feel safer during the holidays.
Reports and audit Even people with valid access during working hours can intentionally or unintentionally pose a security risk. Having precise information on who is present at your facility, who has left, and when is important for compliance, security audits, and in case of emergencies. An audit trail with a highly granular level of detail mitigates risk by enabling you to trace security-related events back to their source.	Do you keep track of everyone who has entered and exited your spaces? How far do the records go?		Install access readers at the spaces you need to track entries and exits. Modern access control systems support event logs, storing the user responsible for the event, the event type (e.g., lock, unlock), and the date and time of it. You can then view these events in real time or export them as reports for an effective audit trail.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

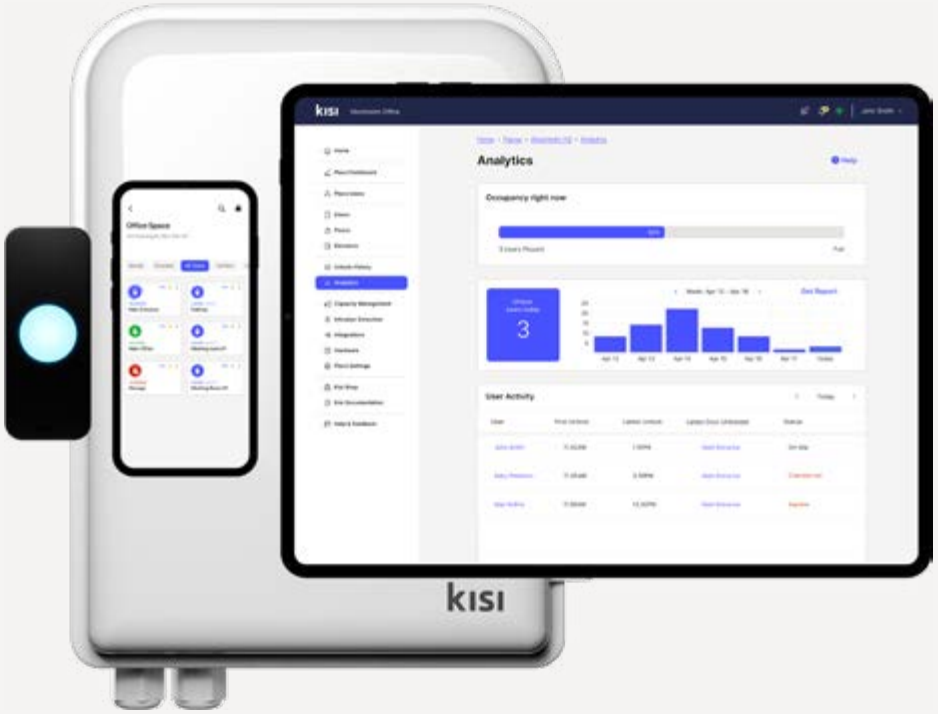
Potential risk	Considerations	Current status	Recommended action
Intrusion alerts Lower and mitigate potential security policy violations by detecting the presence of an intruder attempting to breach the physical perimeter of your property or secured areas. Your intrusion detection system should monitor, register, and promptly inform you if there is a security policy violation.	Who and how is notified if there is a possible intrusion taking place?		Deploy a physical intrusion detection system based on sensors to detect the presence of an intruder and important security policy violations. An integrated, cloud-based intrusion detection system unifies access control, alarms, video surveillance, and automation workflows. Enable admins to get instant alerts on their mobile phones when violations are taking place (e.g., when a door is forced or propped open) so they can take immediate action.
Emergencies Even modern tech companies should prepare for unexpected emergencies, like fire, active shooter, earthquake, hazardous material spills, and floods. Access control should not only restrict unauthorized people from entering the building but also facilitate quick egress of people during emergencies or contain the incident to a specific space.	How prepared are you for unexpected emergencies? Can you put your whole space or parts of your facility on emergency lockdown?		Emergency entry and exit points and access control systems go hand-in-hand. Upgrade to cloud-based access control to automate your emergency exit doors, meet exit door compliances, and be able to put your whole space or specific areas in lockdown. Using the access control dashboard, you'll be able to effectively respond to an emergency by remotely locking or unlocking your doors at any time.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Potential risk	Considerations	Current status	Recommended action
Capacity management Operating a space, like a hybrid workplace, with a lot of different people moving in and out can quickly put you up against the fire safety codes or health regulations of your facility. Gather and analyze access data to ensure compliance, manage your hybrid workforce effectively, and maximize space utilization without sacrificing security and safety.	Do you have real-time insights on current capacity and data on how to optimize space utilization?		To have data on exactly who is in your space at any given moment, you need a cloud-based access control solution. Monitor and manage facility capacity by combining real-time and estimated space utilization data. The modern access systems go one step further and warn you about reaching or exceeding capacity limits. Integrate it with other software to prevent people from accessing your spaces when you are at full capacity.
Prohibited materials Depending on your company's core, various things, such as weapons, explosives, drugs, audio recording devices, cameras, or even tools, can be considered dangerous or contraband. To minimize risk, you need to make people aware that these specific things are prohibited.	Do you have a documented list of prohibited materials? How do you communicate it with employees and visitors?		Define and list all the potential sources of hazards in your company. Consider adding the documented list of prohibited items in your safety handbooks so your employees can use it as a reference whenever in doubt. Communicate the list's existence and constantly remind employees of the importance of following safety guidelines.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

Is it worth the risk?



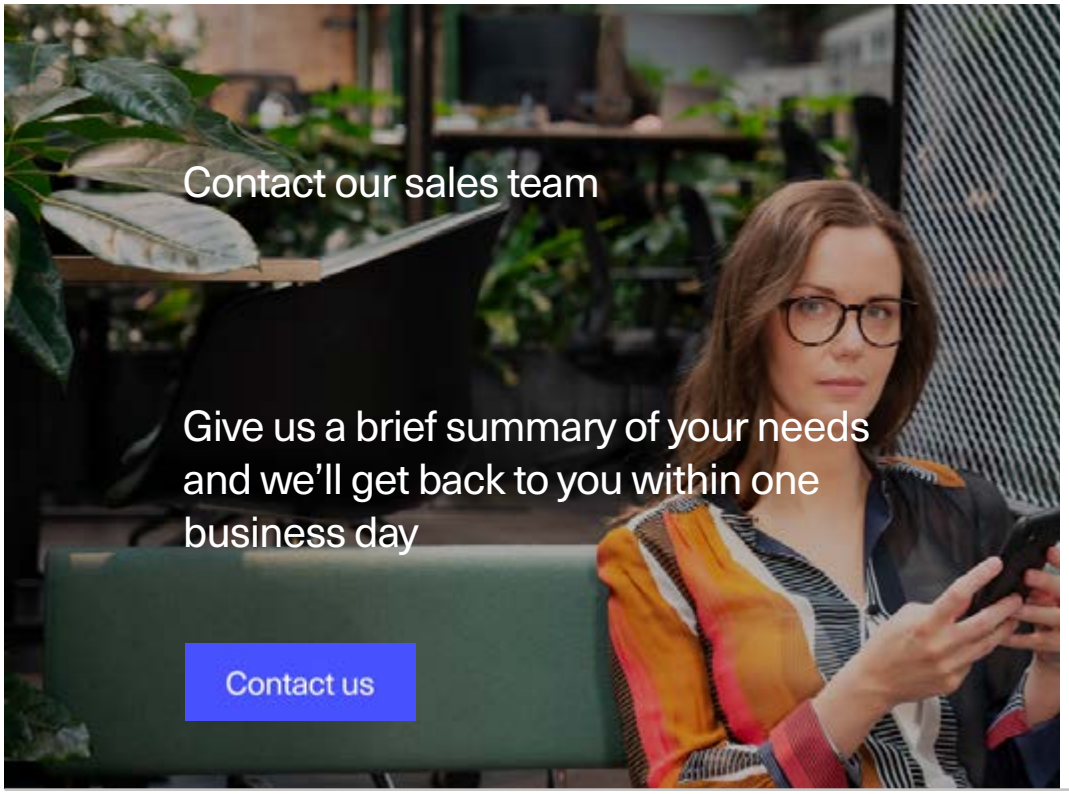
Filling out this template will help you identify the risks and the specific physical security threats you are likely to face based on your current setup. A cloud-based access control system is essential to preventing security-related issues. It will save time, enhance security, and empower you to protect your people, spaces, and assets.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com

kisi

Kisi

A modern *all-in-one solution* for tech companies



Deploy the complete Kisi solution that scales with you or upgrade your existing access control system.

- Enhance the security of your spaces and minimize security risks by introducing Kisi's sleek hardware and user-friendly software. Empower people to unlock doors with their phones with a tap on the Kisi app, by holding their device to the reader, or by waving their hand.
- Onboard employees in a few clicks and save time by sending temporary access links that act as visitor passes. Stay on top of hybrid work by seamless capacity management and automating unlock and access schedules.
- Remotely manage your spaces from a single pane of glass at any time. Easily set specific access levels across your entire facility.
- Minimize security threats and keep user information up to date across all platforms by connecting Kisi with SCIM. Streamline operations by integrating door access with your SSO provider.

Kisi inc.
45 Main street,
11201 Brooklyn
USA
sales@getkisi.com
getkisi.com