AIPHONE

Assessing Risk

Building an effective comprehensive security plan can be a major undertaking without expert guidance.

Think of a risk assessment as a road map for your current and future security planning. Risk assessments are key foundational elements of comprehensive security plans. With guidance from security experts, discovering where improvements are needed is more streamlined, and resources can be channeled into key areas with confidence.

WHITE PAPER
SITE ASSESSMENT

ASSESSING YOUR SECURITY RISKS

A proper risk assessment is very comprehensive and involves a lot more than just checking the lights and rattling the doors.

Determining Security Needs and Expectations

Any project is better executed when there is a strategic plan of action and buy-in.

Discuss with key administrators, department heads, and staff members

Building an effective comprehensive plan requires inclusion of representatives from security or police, staff, and executives. Local first responders, along with nearby community residents and businesses may also be useful contributors. Typically, an outside security integrator who can bring a fresh view to the project leads the effort. A good risk assessment is very comprehensive and involves a lot more than just checking the lights and rattling the doors.

Any project will go more smoothly when there is an early agreement from decision makers. Talk with top administrators and the IT group to determine needs, existing capabilities, and expectations.

Remember employees and security personnel, too. They'll live with the plan every day and likely offer valuable insight. Consider reaching out to your local first responders. They are another great source of security information.

The support from these groups is critical, so keep them regularly updated as the plan is implemented. You want to get things done right the first time. Effort in the early stages could help save time and money during the run of the project.

Tailor a Plan

With input from your top stakeholders, you're ready to start thinking about equipment, budgets, and new policies. But security isn't sold as an off-the-shelf, one-size-fits-all plan. This means you'll likely be working with a security integrator to tailor a plan specifically for your building.

A security integrator guides you through combining all of the security, property access, and utility systems on your property. While security integrators might choose to install new hardware on your property, their main focus is creating one cohesive system to manage existing security devices.

Best Practices

Policies, Procedures, and Equipment

Best practices are policies, procedures, and equipment that have been proven to work on buildings of any size.

Expect the Unexpected

By creating written policies and procedures for handling emergencies you'll be better prepared to handle any security event.

Businesses vary in many ways and so will their policies and procedures. But here are some basics that should be part of all security plans

Basics for Your Policies and Procedures

☑ Create emergency roles for all staff members. This might include communications, traffic control, or overseeing evacuation muster stations to account for staff. Designate contacts and alternates for reaching out to first responders, the community, and the media in case of a major event.

☑ You never know who may be needed during an emergency. Be prepared with a list of all contact names with phone numbers and email addresses along with the jobs they will fill.

☑ Create a site map and locate building blueprints to share with first responders.

☑ Conduct emergency drills considering different scenarios. Include first responders when possible. Practice makes perfect – and there are always new employees, so repeat drills often.

Expectations for Staff

Staff expectations should be outlined in written policies and procedures — a document the inspection team will want to review. Written policies help staff understand how visitors are approved for entry; why doors can't be left propped open; and when to shelter-in-place or evacuate during an emergency.

Management should also consider training staff to look for signs of distressed, and potentially-violent employees or visitors while providing ways to get help for them.

Other best practices include mental health screenings, stricter HR policies, and established relationships with local law enforcement and first responders.

Indoors

How to Protect Your Building

With flexible and expandable intercom systems, a single person can regulate access and monitor grounds across an entire networked building or commercial campus.

There are multiple products and components that make up a comprehensive security system. Businesses rely on master stations, door stations, wall boxes, emergency towers, and more to work in tandem to create a reliable system.

SAFETY TIP

Lock all doors. Use signage, walkways, and fencing to funnel visitors to one approved public entry. From there, they can be buzzed in only after staff identifies and speaks with them using a video intercom.

Building Interiors

Security experts put an emphasis on entries and how staff controls who gets into buildings. Doors, windows, and locks are checked to see if they can resist a criminal attack. Even ventilation ducts are looked at to make sure they can't be used to get inside.

Stairwells, Hallways, and Restrooms

All common areas get inspected to make sure they aren't creating opportunities to hide weapons or contraband.

Security Sytems

Security systems such as access control, video surveillance, burglar alarms, and communications are checked to confirm they're working as expected.

Signage and Visuals

An inspector also looks for signage and other visual indicators to aid the hearing impaired during an emergency.

Outdoors

Many tools used to protect building interiors are different than those used to secure outdoor spaces. Emergency stations, low-light cameras, and other equipment—even landscaping—can be utilized as effective security enhancements.

Parking Lots and Garages

Parking lots, garages, and other exterior areas require adequate lighting, fencing, emergency stations, and security cameras. The inspector wants to see that facilities are regularly patrolled or monitored by either campus security or other first responders.

Outdoor Facilities

It's easy to overlook walking trails and other outbuildings. These are not only frequent targets for illegal activity, but tend to be areas where health-related assistance may be necessary.

Surrounding Neighborhoods

Other environments, open space, and traffic patterns can impact your security and should be included in an overall strategy.

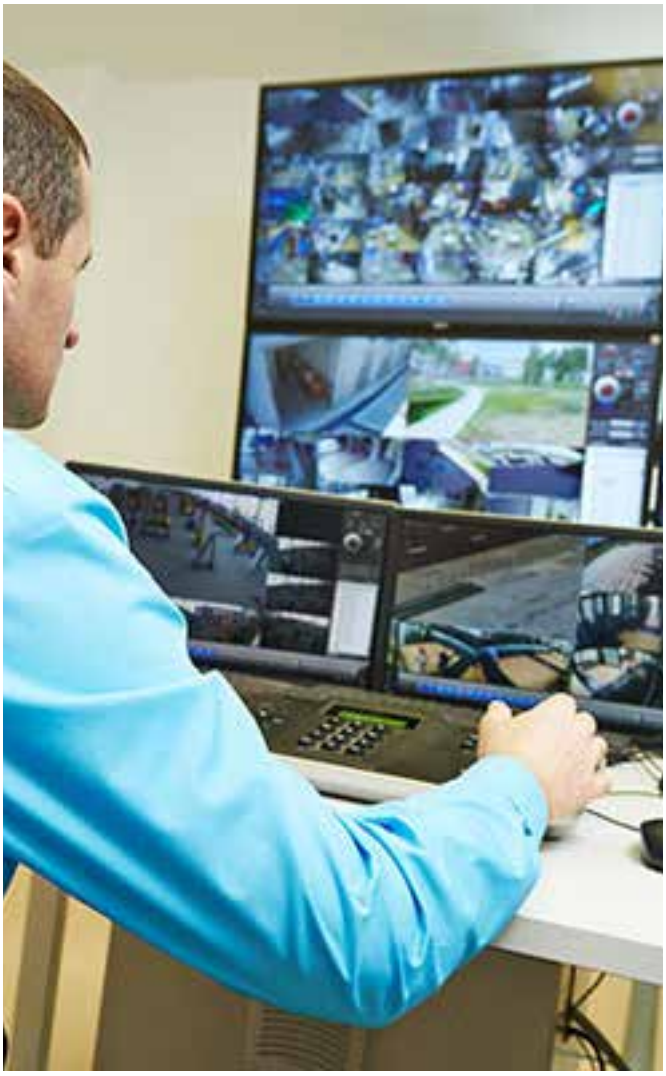
Annexes and Urban Campuses

Remote annexes and larger urban campuses present more of a security and communication challenge. Look for network-based security systems to bring information into a centralized security operations center.

Today's Technology

As security has become more computer- and network-based, technological changes have come along at an almost dizzying pace. More companies have entered the market bringing with them an overwhelming number of choices.

However, there's a silver lining! Your property is unlike any other, so you need solutions that fit your specific security needs. Look to your integrator to help sort through the many products to find the right combination that works best for your property.



Considering different technologies? Things to discuss with your integrator

Analog or Digital Is this an analog- or digital-based product? In some cases, analog may be less expensive and meet your needs today. But digital technology is the future of security. Choosing digital technology today is one way of future-proofing your investment.

Digital Benefits Digital technology also provides better performance. It allows for easier integration of various systems. And it may bypass analog technology's distance limitations, making it easier for linking other buildings to the main office.

System Size What is the required capacity? Will expansion be necessary in the future? Knowing the size of your application, with the potential to grow, helps to ensure you select a system that can scale at your pace.

Backward and Forward Compatibility Ask if the technology is backward and forward compatible. Many security projects are completed in phases. You'll likely want any new technology to work with your existing systems—either analog or digital. Look for a manufacturer that takes that into consideration when designing new products and updates.

Future-proof your investment.

Choosing digital technologies that are backward and forward compatible will contribute to the longevity of your security system

Maintenance

Regular maintenance conducted by experienced techinicians helps optimize system performance and ensures system functionality.

In some cases, regular system checkups are necessary to maintain warranties. They also ensure your systems will be working when you need them most. One bad component can affect your entire system.

Service and Maintenance Agreements

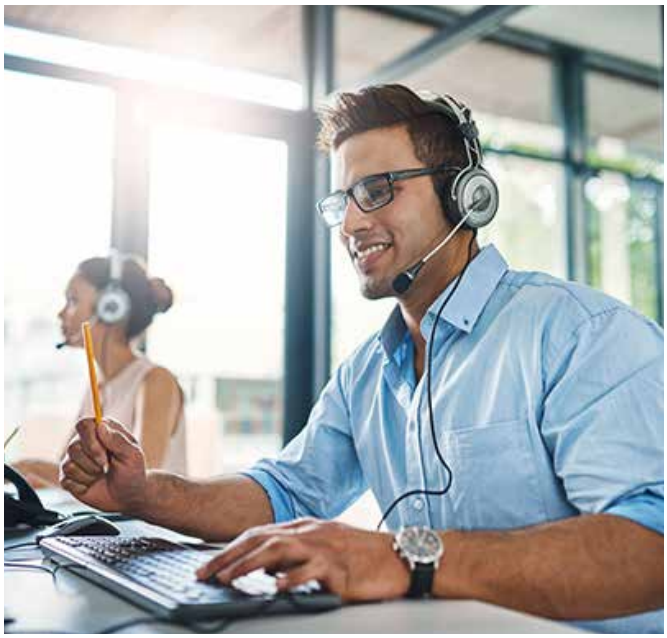
One of the easiest ways to ensure your system is always tuned and ready to go is to purchase a service and maintenance agreement from a security integrator. These plans guarantee you'll get regular system inspections. If you do need a repair, you'll likely get faster service if you have a plan. And a service contract provides a predictable annual expense for system maintenance.

Automated Maintenance

Look for products that include line supervision and device check features. Line supervision enables the system to send you a notification when a device is offline or restarts. Device check manually tests components on a scheduled basis.

Get the Best Support Available

Consider manufacturers who provide great telephone, online, and on-site support. This saves time and trouble if there are questions about operating the system—and can be a real lifesaver for those campuses that maintain their own security equipment.



Your Staff

Your people are an incredibly valuable security resource. Not much happens that someone among your staff doesn't know about.

They see suspicious activities. They notice unlocked doors. They hear conversations about dangerous or illegal activities.

Your staff are valuable resources. Include them when creating a security task force and involve every major department.

For Example, They Might...

- ☑ Direct fellow employees to muster sites, which are designated areas to assemble in an emergency, during an evacuation
- ☑ Be a contact for local police and fire departments, keeping them informed of events on campus
- ☑ Provide checklists for department heads to follow during an emergency
- ☑ Help people learn their roles by conducting regular drills of various scenarios

BEST PRACTICE

Many people are hesitant to report problems in person, so create phone and/or website hotlines where they can leave anonymous information.

Tips for a Successful Project

Move forward confidently with your next major new security installation or retrofit job. This list of best practices will help ensure no detail is missed. Refer to this list to help your team prepare before, during, and after completion of your project.

Before the Project Begins

- Select a knowledgable security integrator
- Obtain a thorough risk assessment for your entire property. Look at all campus areas—indoors and out
- Involve key decision makers including security, network administrators, and other affected departments
- Obtain leadership buy in, so there are no surprises
- Input from the people that will be using the system every day may be useful
- Establish a detailed budget—including:
  - A firm completion date
  - Ask about any licensing and software update fees
  - Costs for an ongoing service and maintenance agreement
- Ask about open standard technology
- Make sure different systems will work together
- Future proof your investment—make sure products are scalable to meet your needs as your campus grows

During Project Installation

- Set up regular meetings with your project manager
- Involve IT and other departments critical to the project's success
- Prepare your security operations center (SOC)
- Consider any needed additions to utilities and telephone service
- Ensure network drops are operational
- Make sure you're properly staffed
- Update your written security policies and procedures taking into account the new equipment

After Project Installation

- Walk through the property, confirm all components are working properly
- Begin training of appropriate SOC employees
- Discuss maintenance plans with integrator for regular system checks
- Run emergency drills regularly

AIPHONE

SECURITY
COMMUNICATION
SOLUTIONS

aiphone.com

Customer Service and Technical Support

(800) 692-0200

Headquarters – Redmond, WA

East Office – Cherry Hill, NJ

Canada Office – Laval, QC

WATCH | CONNECT | LIKE | FOLLOW

Assessing Risk
White Paper