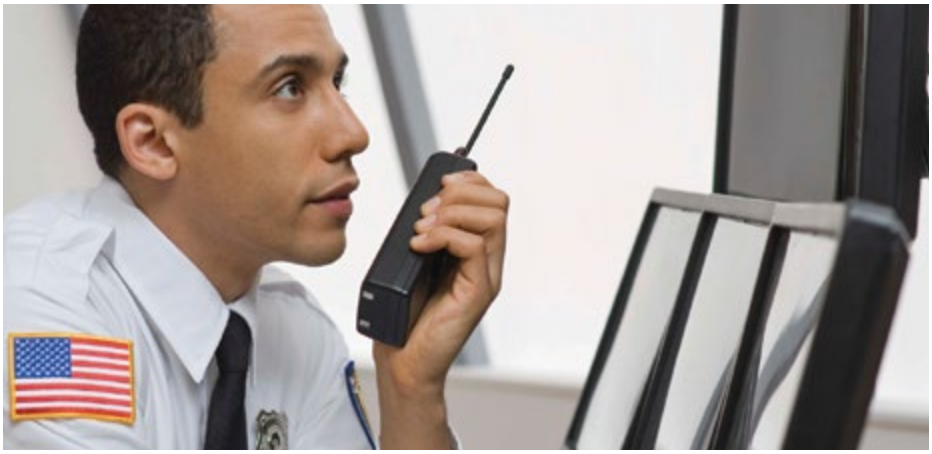
ZURICH

Site security assessment guide

The first step in creating a site security plan

Site security assessment guide



Facilities face endless security risks, including vandalism and theft, on-site security breaches, rogue or mentally unstable employees and even terrorism. Whether you own or manage hotels, office space, retail operations or residential buildings, securing your building is more important than ever.

An in-depth risk assessment and analysis are the first steps in effective site security planning. This guide will help you determine the likelihood and consequences of a security issue or gap, and help you prioritize the appropriate protective actions to take. Although security needs are unique for each organization, identifying the assets that need to be protected will determine the proper level of security.

Identifying your assets is also a critical part in this overall assessment. People assets include more than just the employees. They also include visitors, contractors, the surrounding community and others associated with the business operation. Property assets range from building, machinery and utilities to operations, equipment and systems. Informational assets are computer systems, processes and confidential business and employee information.

The various assessments presented in this guide are designed to help you identify the risks and target vulnerable assets in each category. Potential threats range from break-ins and thefts to previously overlooked risks of terrorism, espionage and sabotage.

The Zurich Site Security Assessment Guide will provide you with the framework to help you assess the level of security at your site. Property owners and managers needn't tackle building security alone. There are many resources to draw on. And, of course, Zurich Risk Services can provide expert guidance.

Site information

Reviewed by	
Company/customer	
Site address	
Site general manager	
Security manager	
Products/services	
Number of employees	
Operating hours	
Site area	
Neighborhood	
Description of "worst credible risk scenarios"	

Summary

1. Risk assessment

Observed strengths	Observed weaknesses	Action plan

2. Management policies

Observed strengths	Observed weaknesses	Action plan

3. Physical security

Observed strengths	Observed weaknesses	Action plan

Summary (Continued)

4. Access control

Observed strengths	Observed weaknesses	Action plan

5. Employee security

Observed strengths	Observed weaknesses	Action plan

6. Information security

Observed strengths	Observed weaknesses	Action plan

Summary (Continued)

7. Material security

Observed strengths	Observed weaknesses	Action plan

8. Emergency response

Observed strengths	Observed weaknesses	Action plan

9. Crisis communication

Observed strengths	Observed weaknesses	Action plan

Summary (Continued)

10. Reviews/audits

Observed strengths	Observed weaknesses	Action plan

Risk assessment

Number	Questions	Response			Comments
		A	UA	NA	
1	Has your company completed a systematic risk assessment for security threats? Is it updated at least annually?				Date of last security assessment:
2	Does the risk assessment clearly identify key vulnerable assets and sensitive processes requiring protection? Are the threat levels clearly understood?				
3	Does the risk assessment identify the likelihood and severity of consequences with credible threat scenarios?				
4	Does a multi-disciplinary team conduct the risk assessment? Does the team have appropriate training to conduct the risk assessment?				
5	Is there a plan in place which utilizes an effective strategy for prevention and mitigation?				
6	Are any neighborhood operations, building tenants and location risk factors present that contribute to an increase in terrorism and other security threats?				
7	Are there designated people and procedures in place for monitoring the early warnings of increasing threat levels and an escalation of security efforts in response? Alpha = Normal conditions Bravo = Credible threats issued (alert) Charlie = Reported incidents elsewhere Delta = Actual incident				

A = Acceptable UA = Unacceptable NA = Not applicable

Management policies

Number	Questions	Response			Comments
		A	UA	NA	
1	Is top management support and involvement evident in the security planning? Consider policies, budgets, accountabilities and resources in the assessment.				
2	Is there a current security plan in place that addresses policies for access control and emergency response? Describe it.				
3	Is there a current emergency response and crisis management plan in place specific to the site?				
4	Does the emergency response plan address fire, explosion, bomb threat, civil disturbance and suspicious mail handling?				
5	Does the access control policy address visitor registration, ID badge usage, background checks, escorting and other requirements for all visitors and contractors?				
6	Is there a zero-tolerance workplace violence and weapons policy in place?				
7	Is there a system for centralized reporting and analysis of all security-related incidents and suspicious activities? Are response procedures for security breaches developed?				

A = Acceptable UA = Unacceptable NA = Not applicable

Management policies (Continued)

Number	Questions	Response			Comments
		A	UA	NA	
8	Has the local law enforcement agency reviewed the current security plan?				
9	Is the security plan reviewed at least annually? Has the latest revision taken into account: • New threats • Risk assessment • Change management				
10	Are there defined procedures and resources for heightening the site security efforts in response to escalating threat levels?				
11	Are there strict hiring and selection standards for security staff? Are there standards for security staff pertaining to the following: • Licensing • Background checks • Physical health • Psychological health • Training • Compensation • Weapons policy				
12	Is the security staff routinely involved in "non-security" tasks?				
13	Is a lockdown procedure in place in response to an immediate threat?				
14	Is there a business continuity plan in place based on business impact analysis?				

A = Acceptable UA = Unacceptable NA = Not applicable

Physical security

Number	Questions	Response			Comments
		A	UA	NA	
1	Is appropriate perimeter protection in place? Examples include: • Fences • Trenches • Terrain • Barricades • Landscaping • Turnstiles • Roof access • Waterside access				
2	Are redundant layers of protection considered for core assets?				
3	Are physical barriers in place that limit vehicle access to the building?				
4	Are the perimeter doors, gates, windows and docks secured and in good working condition? Items to be considered include: • Penetration resistance • Security hinges and hardware • Break and blast-resistant glass				
5	Are the perimeter doors, gates and docks adequately staffed during working hours and secured after hours?				
6	Are security surveillance cameras and perimeter (docks, doors, gates and windows) alarms in place? Suitable type and adequate number for appropriate coverage?				
7	Are cameras monitored in real-time to allow immediate response?				
8	Are surveillance video records properly archived?				
9	Are security cameras and alarms inspected and tested on a regular basis?				

A = Acceptable UA = Unacceptable NA = Not applicable

Physical security (Continued)

Number	Questions	Response			Comments
		A	UA	NA	
10	Is there regular patrolling of the perimeter to inspect the fence line damage, clear zone, obstructions, unoccupied/ unidentified vehicles and other breaches? • Are logs maintained? • Is there a prompt reporting and investigation of security breaches? • Guard dogs?				
11	Are the equipment and critical assets (utilities, HVAC/air intakes and control rooms and communication equipment) in the yard and on rooftops protected and monitored? Is access controlled?				
12	Is the perimeter lighting adequate? Is lighting adequate for use of a surveillance camera?				
13	Is there a parking lot security plan in place? The plan should include: • Illumination • Visitor parking restrictions • Executive parking location • Video surveillance and monitoring • Patrolling • Vehicle inspections				
14	Is there a maintenance program in place for all exterior grounds? Does the program cover inspection and emptying of trash receptacles?				
15	Does the reception/security desk have a clear, unobstructed view of all entrances? Best practices include: • Landscape trimming • No posters on glass • Watch tower or guard post				
16	Are proper warning signs posted (e.g. no trespassing, driver direction, restricted areas, etc.)?				

A = Acceptable UA = Unacceptable NA = Not applicable

Access control

Number	Questions	Response			Comments
		A	UA	NA	
1	Is the access approaching, and entry into, the facility controlled? Are there restricted access points?				
2	Is there a documented access control procedure in place? Access control could include: • Photo identification check • Proximity access cards • Strict key control program • Biometrics				
3	Are all visitors and contractors screened and required to sign-in/sign-out and produce valid photo identification? Are the logs reviewed regularly?				
4	Are all visitors and contractors clearly identified and escorted while on the property?				
5	Are the visitors and contractors briefed on the site's safety and security procedures including evacuation, restricted areas, search policies, etc.?				
6	Are search procedures for packages and delivery/contractor/visitor vehicles activated in case of heightened security? Search procedures could include: • X-ray scanning • Metal detectors • Physical searches • Surprise security sweeps				

A = Acceptable UA = Unacceptable NA = Not applicable

Access control (continued)

Number	Questions	Response			Comments
		A	UA	NA	
7	Is there a list of approved contractors/ vendors, delivery and messenger services available to security staff? Is the approved list reviewed regularly?				
8	Are deliveries restricted to regular working hours only?				
9	Are sensitive areas identified and properly secured for authorized access?				
10	Is the access control program organized to react promptly to lost/stolen identification and access cards and employee terminations?				
11	Are locks changed immediately when the key controls are compromised?				

A = Acceptable UA = Unacceptable NA = Not applicable

Employee security

Number	Questions	Response			Comments
		A	UA	NA	
1	Is there a program for verification of past employment, academic credentials and references prior to start of employment?				
2	Are background checks conducted on all employees in sensitive jobs and following transfer requests to more sensitive jobs?				
3	Are personnel and employee medical records properly secured?				
4	Does the new employee orientation program cover: • Security • Emergency evacuation • Bomb threat procedures • Drug policy • Zero-tolerance workplace violence policy • Confidentiality				
5	Are photo identifications issued to all employees for access security and verification?				
6	Are there controls in place for the issuance of replacement photo identification, missing ID and access cards?				

A = Acceptable UA = Unacceptable NA = Not applicable

Employee security (continued)

Number	Questions	Response			Comments
		A	UA	NA	
7	Are employees required to carry photo identification while on the property?				
8	Are employees encouraged to report all suspicious activities and security lapses? Best practices include: • Challenging individuals without identification • Confidential phone number for reporting				
9	Is there a telephone number list for employee notification in case of an emergency? Is it kept current?				
10	Are confidentiality agreements/ background checks required for employees with proprietary and confidential information?				
11	Is company property (credit cards, identification, keys, PCs, etc.) retrieved during exit interviews?				
12	Is there a corporate policy on travel restrictions to dangerous locations?				
13	Is there a plan to address the security of employees working alone and/or late hours?				

A = Acceptable UA = Unacceptable NA = Not applicable

Information security

Number	Questions	Response			Comments
		A	UA	NA	
1	Is there a document control program in place? Best practices include: • Electronic/paper records • Confidential/proprietary data • Protection of records • Back-up copies • Retention and archiving • Destruction/shredding of sensitive information				
2	Is access to the network computer room and equipment restricted to authorized personnel only? Issues include: • Physical access • Working/non-working hours • Monitored • Remote/network access				
3	Are authorization levels for sensitive information reviewed periodically?				
4	Is there an effective audit ability to trace access/hacking into secured and sensitive work areas and computer networks?				
5	Are all computers and networks equipped with appropriate fire walls and anti-virus protection? Are virus-protection patches updated regularly?				
6	Is there a data center security plan in place? Considerations include: • Fire and physical protection • Intrusion protection/safes • Virus protection and regular updates • UPS (uninterruptible power supply) protection • Electronic media and tapes • Daily back-ups • Off-site storage (distance?) • Disaster recovery plans				

A = Acceptable UA = Unacceptable NA = Not applicable

Information security (continued)

Number	Questions	Response			Comments
		A	UA	NA	
7	Is there information security awareness/training for all employees? Issues requiring consideration include: • New hires • Password protection • Unauthorized/unlicensed software • Sensitive information on laptops • Traveling with laptops • Policy on using laptops and cell phones in public • Unattended sensitive				
8	Is there password protection in place for employee access to all computers and electronic records? Is there a periodic password change policy in place?				
9	Is there a priority for prompt revocation of computer access to all terminated and disgruntled employees?				
10	Is access to fax machines restricted to reduce unauthorized reading of sensitive messages?				
11	Is there a policy in place for controlling and shredding of sensitive materials at the end of business meetings? Sensitive materials may include: • Flip charts and scrap papers • Extra handouts • Dry erase boards • Residual memory from electronic whiteboards				

A = Acceptable UA = Unacceptable NA = Not applicable

Material security

Number	Questions	Response			Comments
		A	UA	NA	
1	Is there any theft-prone material on property? Are there theft control procedures in place: • Precious metals • Laptops • Highly toxic chemicals • Biohazard material • Radioactive material				
2	Are screening procedures in place for recognizing suspicious mail and packages? Methods to mitigate risk include: • Employee training • X-ray • Explosive sniffing dogs				
3	Is there a "package pass" program in place for removal of any company-owned property from the facility?				
4	Are controls in place for scrap disposal and pick-up?				
5	Are accurate inventory records maintained for sensitive materials? Is inventory reduction implemented in response to heightened security?				

A = Acceptable UA = Unacceptable NA = Not applicable

Emergency response

Number	Questions	Response			Comments
		A	UA	NA	
1	Is there a current site-specific emergency response plan in place?				
2	Does the emergency response plan address specific threats such as fire, explosion, utility failures, civil disturbance, bomb threat, product contamination and natural hazards?				
3	Is there an incident command (IC) to coordinate and deploy internal assets/ resources and external resources? Considerations include: • Designated people • Alternates • First responders • Damage assessment • Communication				
4	Does the security staff play a role in emergency response?				
5	Are the emergency numbers posted prominently?				
6	Are the pagers and cell phone numbers for the emergency response team verified and tested periodically?				
7	Is there an effective program for training/refresher training for emergency responders? • Protective equipment • Resources				
8	Is there a bomb threat response procedure? Considerations include: • Telephone instructions • Law enforcement notification • Systematic searches (who) • Employee training				

A = Acceptable UA = Unacceptable NA = Not applicable

Crisis communication

Number	Questions	Response			Comments
		A	UA	NA	
1	Is there a media and public relations plan in place?				
2	Is there a qualified designated spokesperson to manage all media inquiries? Is there an alternate?				
3	Does management receive appropriate media training?				

A = Acceptable UA = Unacceptable NA = Not applicable

Review/Audits

Number	Questions	Response			Comments
		A	UA	NA	
1	Are comprehensive security audits conducted randomly? Review the following: • Last audit • Results • Corrective actions				
2	Is employee and management training support provided to address changing security needs and emerging threats and enhance skill levels?				

A = Acceptable UA = Unacceptable NA = Not applicable

Resources

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) – *Explosives Safety and Security Guides*	www.atf.gov
Centers for Disease Control and Prevention (CDC) – *Emergency Preparedness and Response*	www.bt.cdc.gov
Department of Homeland Security (DHS) – *How to Prepare your Business for an Emergency*	www.dhs.gov
Federal Emergency Management Agency (FEMA) – *Terrorist Hazards*	www.fema.gov
Stimson: *Pragmatic Solutions for Global Security – Biological and Chemical Weapons Information*	www.stimson.org
USPS Mail Security Center – *Information on identifying and responding to security threats in mail centers*	www.usps.com
US-CERT Computer Emergency Readiness Team – *Posts current breach and vulnerability information*	www.us-cert.gov
U.S. Food and Drug Administration (FDA) – *Recalls, outbreaks and emergencies with food*	www.fda.gov

Zurich
1400 American Lane, Schaumburg, IL 60196-1056
800 382 2150 www.zurichna.com

A1-16560-D (03/15) 112004839

ZURICH®