



THE COMPLETE QUESTION SET

The Survivability Index™

Every question below is one an attorney, an insurer, or a grieving parent could ask you after an incident. The Survivability Index™ asks them first. This is the full 312-question framework — the same instrument ASPIRE uses to move organizations from reactive “run, hide, fight” response to proactive prevention across physical security, organizational culture, and mental health.

Read it as a diagnostic. The questions you cannot answer are the ones that matter most.

Why AI-enhanced matters. Static checklists age the moment they are printed. The Survivability Index™ is continuously monitored against updates from the U.S. Secret Service NTAC, FBI, CISA, DHS, CDC/NIOSH, OSHA, FEMA, the Department of Education, ASIS International, and state workplace violence prevention statutes — so your assessment reflects the current standard of care, not last year’s.

312	12	47	60+
QUESTIONS	CRITICAL DOMAINS	ASSESSMENT AREAS	AUTHORITATIVE SOURCES

THE 12 DOMAINS

1	ORGANIZATIONAL SECURITY PROGRAM STRUCTURE	31	7	EMERGENCY RESPONSE PROTOCOLS	34
2	PHYSICAL SECURITY INFRASTRUCTURE	38	8	TRAINING & PREPAREDNESS	33
3	SECURITY OPERATIONS	20	9	POST-INCIDENT RESPONSE & RECOVERY	22
4	HUMAN RESOURCES & ORGANIZATIONAL CULTURE	45	10	SPECIAL POPULATIONS & ACCESSIBILITY	16
5	MENTAL HEALTH INTEGRATION	23	11	INFORMATION SECURITY & CYBER INTEGRATION	18
6	COMMUNICATION SYSTEMS	17	12	LEGAL, INSURANCE & COMPLIANCE	15

01	02	03
READ STRAIGHT THROUGH	CIRCULATE IT	BRING US THE HARD ONES
Do not answer yet. Simply mark every question you cannot answer with confidence today. That set is your real exposure.	Send it to the people who would have to act: security, HR, counseling, facilities, legal. Where they disagree is where the gap is.	Come back to the booth with your three worst answers. That conversation is the beginning of an assessment.

START WITH THE FREE QUICK ASSESSMENT

Take the complimentary Quick Assessment at aspire-initiative.org to establish a baseline in minutes. Organizations serving vulnerable populations may qualify for a **Foundation Access Grant** — a fully sponsored Survivability Index™ assessment at no cost. Ask us at the booth.

PREPARATION. PREVENTION. SURVIVAL.

DOMAIN 1

ORGANIZATIONAL SECURITY PROGRAM STRUCTURE

31 QUESTIONS

1.1 SECURITY PROGRAM GOVERNANCE

- 1 Is the security risk owner clearly defined at your organization?
- 2 Is there a corporate senior security manager (VP Security, CSO, Regional/Area Security Manager, etc.)?
- 3 Does your organization have a full-time security manager at each facility?
- 4 Does the organization publish security guidelines/requirements/baseline expectations?
- 5 Is your organization regulated by industry or government security requirements?
- 6 Does the organization comply with OSHA's General Duty Clause regarding workplace safety?
- 7 Is security program performance reviewed regularly by senior leadership?
- 8 Is there a budget allocated for continuous security improvements?
- 9 Is the organization in compliance with state-specific workplace violence prevention laws (e.g., California SB 553, New York S. 8358B)?

1.2 RISK ASSESSMENT & SECURITY PLANNING

- 10 Have you conducted formal security risk assessments with security scenarios identified?
- 11 Do you have published site security plans?
- 12 If so - Do site security plans incorporate company and/or government requirements with security risk reduction measures?
- 13 Are clearly defined roles and responsibilities for security actions defined in the plan for security personnel?
- 14 Are clearly defined roles and responsibilities for security actions defined in the plan for non-security personnel?
- 15 Are security plans updated annually or after incidents/drills?
- 16 Are security vulnerabilities prioritized based on risk assessment?
- 17 Are benchmarking comparisons made with peer organizations?
- 18 Has the organization conducted a vulnerability assessment using CISA's Stakeholder-Specific Vulnerability and Resilience Assessment methodology?

1.3 THREAT MONITORING & INTELLIGENCE

- 19 Do you routinely monitor threat situations within your operating area?
- 20 Do you routinely monitor local crime statistics in your area?
- 21 Is there a social media monitoring capability for threat detection?

- 22 Do you coordinate and collaborate with nearby local businesses on security matters?
- 23 Has your organization ever had a security failure that resulted in severe injury or very high loss?

1.4 THREAT ASSESSMENT TEAM

- 24 Do you have a Threat Assessment Team process to assess and action changes in threat situations?
- 25 Are mental health professionals integrated with security and HR for threat assessment?
- 26 Does the Threat Assessment Team include members from security, HR, legal, and mental health?
- 27 Are patterns of concerning behavior tracked across multiple reports?
- 28 Is there a process for intervention when concerning behaviors are identified?
- 29 Does your Threat Assessment Team use a structured behavioral threat assessment framework (such as the Secret Service NTAC model)?
- 30 Does the Threat Assessment Team assess whether individuals of concern are on a pathway to violence (ideation, planning, preparation, implementation)?
- 31 Are threat assessment protocols updated based on current research from the Secret Service NTAC, FBI, and other authoritative sources?

DOMAIN 2

PHYSICAL SECURITY INFRASTRUCTURE

38 QUESTIONS

2.1 PERIMETER SECURITY

- 32 Does your facility have perimeter fencing or barriers?
- 33 Is the perimeter fully lit?
- 34 Is the perimeter covered by CCTV?
- 35 Do you actively monitor all approaches to your building?
- 36 Are Crime Prevention Through Environmental Design (CPTED) principles applied to facility design and layout (natural surveillance, access control, territoriality)?
- 37 Are sight lines designed to maximize natural surveillance and minimize hiding spots or ambush locations?

2.2 ACCESS CONTROL

- 38 Do you perform Access Control functions including searches of personnel/bags/vehicles on entry?
- 39 Do you perform Access Control functions including searches of personnel/bags/vehicles on exit?
- 40 Are parking areas Access Controlled?
- 41 Is technology used for access control (card readers, x-ray, metal detectors, etc.)?
- 42 Do you conduct penetration testing to assess Access Control performance?
- 43 Are access control, CCTV, and alarm systems integrated into a single platform?

2.3 VIDEO SURVEILLANCE (CCTV)

- 44 Are entrances covered by CCTV?
- 45 Are parking areas covered by CCTV?
- 46 Are cameras monitored continuously?
- 47 Can you port out live video to law enforcement during an event?
- 48 Is there video analytics capability to detect concerning behavior?
- 49 Can systems provide real-time location of threats?

2.4 LOCKDOWN CAPABILITIES

- 50 Can doors be locked quickly from inside?
- 51 Are classroom/office doors equipped with internal locks?
- 52 Can a facility-wide lockdown be initiated remotely?
- 53 Are there backup manual lockdown procedures if systems fail?
- 54 Can high-risk areas be isolated quickly?

2.5 SAFE ROOMS & HARDENED AREAS

- 55 Have hardened areas been identified for use during active shooter incidents?
- 56 Are safe rooms equipped with communications equipment?
- 57 Do safe rooms have emergency supplies (first aid, water)?
- 58 Are safe room locations clearly marked and known to all?
- 59 Can safe room doors withstand forced entry?
- 60 Are safe rooms regularly inspected and maintained?
- 61 Do you have ballistic protected Executive Command Centers?
- 62 Is ballistic protection installed in high-risk areas?

2.6 ADVANCED SECURITY TECHNOLOGY

- 63 Are there gunshot detection systems installed?
- 64 Can systems automatically notify law enforcement?
- 65 Do you use Panic Alarms?
- 66 Are building layouts designed to minimize long corridors and maximize escape routes?
- 67 Are there barriers that could slow an attacker's movement?

2.7 HIGH-SENSITIVITY AREAS

- 68 Are areas of high sensitivity identified within sites that require additional security measures (Restricted areas, Labs, command centers, etc.)?
- 69 Are additional security measures in place for executives when on-site?

DOMAIN 3

SECURITY OPERATIONS

20 QUESTIONS

3.1 SECURITY PERSONNEL

- 70 Do you have full-time security officers (personnel)?
- 71 If so - Are they armed?
- 72 If so - Do you have a security training program for security personnel?
- 73 Do security personnel receive specialized active shooter response training?
- 74 Is there a security control center or operations center at the site?
- 75 Do you perform routine security program reviews of security functions to identify gaps and close them?
- 76 Does the Security Operations Center have documented standard operating procedures for active shooter response?
- 77 Do security personnel have detailed post orders that include specific active shooter response duties?
- 78 Are security personnel's active shooter response skills validated through practical exercises (not just classroom training)?
- 79 Is there a designated security liaison who maintains regular contact with local law enforcement and first responders?

3.2 VISITOR & CONTRACTOR MANAGEMENT

- 80 Is there a visitor management system in place?
- 81 Are all visitors required to sign in and show identification?
- 82 Are visitor badges issued and clearly distinguishable from employee badges?
- 83 Are visitors escorted while in sensitive areas?
- 84 Is there a process for verifying visitor legitimacy before entry?
- 85 Are delivery personnel required to check in?
- 86 Are background checks required for contractors with regular access?
- 87 Are contractors badged separately from employees?
- 88 Are contractors included in emergency drills and plans?
- 89 Is there a contractor orientation that includes security requirements?

DOMAIN 4

HUMAN RESOURCES & ORGANIZATIONAL CULTURE

45 QUESTIONS

4.1 WORKPLACE VIOLENCE PREVENTION POLICY

- 90 Does the organization have a published workplace violence prevention policy?

- 91 Is there a zero-tolerance statement from leadership regarding workplace violence?
- 92 Does the policy include definitions of unacceptable behaviors?
- 93 Are consequences for policy violations clearly stated?
- 94 Is leadership visibly committed to violence prevention (not just compliance)?
- 95 Does the organization regularly assess workplace climate and employee satisfaction as violence prevention indicators?

4.2 REPORTING CULTURE & NON-RETALIATION

- 96 Are employees explicitly protected from retaliation when reporting concerns?
- 97 Is there an anonymous reporting option available?
- 98 Are reporting mechanisms well-publicized and accessible 24/7?
- 99 Is there a documented process for how reports are investigated and resolved?
- 100 Do employees receive feedback when they report concerns?
- 101 Do you have formal security reporting processes for everyone (see something, say something, hotline, email, portal)?
- 102 Do you have a culture that allows reporting suspicious activities without reprisal?

4.3 CONFLICT RESOLUTION & GRIEVANCE PROCEDURES

- 103 Does the organization have formal conflict resolution procedures?
- 104 Are there grievance mechanisms for employees to address workplace issues?
- 105 Is there mediation available for workplace disputes?
- 106 Are supervisors trained in de-escalation and conflict management?

4.4 PRE-EMPLOYMENT SCREENING

- 107 Are background checks performed on all employees?
- 108 Are background checks performed on all nested contractors/vendors?
- 109 Are psychological evaluations conducted for high-risk positions?
- 110 Are references checked thoroughly?
- 111 Are gaps in employment history investigated?
- 112 Are social media checks conducted where legally permissible?

4.5 BEHAVIORAL WARNING SIGNS & INSIDER THREAT

- 113 Are employees trained to recognize behavioral indicators of potential violence?
- 114

Are supervisors and managers trained to recognize warning signs of potential violence?

- 115 Is there a documented list of concerning behaviors that should be reported?
- 116 Is there a process for documenting and escalating concerning behaviors?
- 117 Does HR track patterns of concerning behavior across the organization?
- 118 Are there wellness checks for employees showing signs of distress?
- 119 Do you monitor employee criminal records?

4.6 HIGH-RISK SITUATIONS & TERMINATIONS

- 120 Is there a high-risk termination protocol for potentially volatile employees?
- 121 Are disciplinary actions assessed for violence risk?
- 122 Is security notified BEFORE high-risk terminations occur?
- 123 Are terminations conducted with security present when necessary?
- 124 Is IT access immediately terminated during high-risk terminations?
- 125 Are exit interviews conducted to assess risk?
- 126 Does management or HR inform security of terminated personnel as soon as terminated?
- 127 Does the organization use a "Banned List" to identify people not allowed on site?
- 128 Are there protocols for assessing employees returning from extended medical or mental health leave?

4.7 DOMESTIC VIOLENCE WORKPLACE IMPACT

- 129 Does the organization have a domestic violence workplace policy?
- 130 Are employees encouraged to report if they have protective orders?
- 131 Do you track restraining orders affecting employees?
- 132 Are security measures taken for employees at risk from domestic partners?
- 133 Is there coordination with local domestic violence resources?
- 134 Does management or HR inform security of "at risk" personnel on-site (domestic issues)?

DOMAIN 5 MENTAL HEALTH INTEGRATION 23 QUESTIONS

5.1 MENTAL HEALTH RESOURCES & SUPPORT

- 135 Does the organization have an Employee Assistance Program (EAP)?
- 136 Are mental health resources readily available and communicated to all employees?

- 137** Is there a crisis intervention capability or team?
- 138** Does the organization provide stress management and resilience training?
- 139** Are there confidential channels for employees to seek mental health support?
- 140** Does the company screen for and address workplace stress factors?
- 141** Do you track mental health-related terminations?
- 142** Does the organization have proactive mental health wellness programs (not just reactive crisis intervention)?
- 143** Are supervisors trained to recognize signs of mental health distress and connect employees with resources?
- 144** Are employees trained in Mental Health First Aid or similar evidence-based mental health support programs?
- 145** Does the organization actively work to reduce mental health stigma and encourage help-seeking behavior?
- 146** Are substance abuse support programs integrated with mental health and violence prevention efforts?
- 147** Can employees access mental health professionals within 24-48 hours when needed?
- 148** Does the organization have trained peer support specialists or employee resource networks for mental health?
- 149** Are there structured return-to-work protocols for employees who have experienced mental health crises?
- 150** Does the organization systematically monitor and address workplace stress factors that could contribute to violence risk (excessive workload, toxic management, etc.)?
- 151** Is there a designated mental health crisis response team that can respond to behavioral emergencies?
- 152** Are confidentiality protections clearly communicated for employees seeking mental health support?
- 153** Is there a protocol for mental health professionals to consult with security when employees are in crisis (with appropriate privacy protections)?

5.2 POST-INCIDENT MENTAL HEALTH SUPPORT

- 154** Are trauma counseling services available for employees after critical incidents?
- 155** Is there a post-incident psychological support plan?
- 156** Are employees trained in psychological first aid?
- 157** Is there a Critical Incident Stress Management (CISM) team?

DOMAIN 6

COMMUNICATION SYSTEMS

17 QUESTIONS

6.1 EMERGENCY COMMUNICATION SYSTEM CAPABILITIES

- 158** Do you use a PA/GA or mass communication system (Voice, digital, visual, telephonic, etc.)?
- 159** Does the emergency communication system have redundant methods (voice, text, email, app)?

- 160** Can the system reach ALL areas of the facility including parking lots, remote buildings, and outdoor spaces?
- 161** Can targeted messages be sent to specific zones or buildings?
- 162** What is the speed of alert deployment - can alerts be sent in seconds?
- 163** Is there a backup power supply for all communication systems?
- 164** Can the system integrate with personal devices (smartphones)?
- 165** Is there a sitewide radio system which includes security?

6.2 TWO-WAY COMMUNICATION & EMPLOYEE SAFETY STATUS

- 166** Can employees report incidents through the communication system?
- 167** Is there a way for employees to confirm their safety status to the organization?
- 168** Can security communicate with employees during an active incident?
- 169** Can the organization communicate with employees who are off-site during an incident?

6.3 INTEROPERABILITY & SYSTEM TESTING

- 170** Are communication systems interoperable with first responder radio systems?
- 171** How frequently are emergency communication systems tested - at least quarterly?
- 172** Are employees required to participate in communication system tests?
- 173** Do you have an emergency communication system to immediately alert law enforcement?
- 174** Is there a system for providing ongoing updates to families during extended incidents (hostage situations, lockdowns lasting hours)?

DOMAIN 7

EMERGENCY RESPONSE PROTOCOLS

34 QUESTIONS

7.1 EMERGENCY RESPONSE PLAN QUALITY & ACCESSIBILITY

- 175** Do you have a published Emergency Response Plan?
- 176** Does the Emergency Response Plan include (Lockdown, Active Shooter, and Evacuation)?
- 177** Is an active shooter or shooting incident part of your overall Emergency Response Plan?
- 178** Are emergency response plans easily accessible to all employees?
- 179** Are plans available in multiple languages if needed?
- 180** Are plans updated annually or after incidents/drills?
- 181** Do plans include site-specific maps with evacuation routes and safe areas?

182 Are roles and responsibilities clearly defined for ALL employee types (not just security)?

7.2 DECISION-MAKING & COMMAND STRUCTURE

183 Is there a clear decision tree for when to evacuate vs. shelter-in-place vs. lockdown?

184 Who has authority to initiate lockdown or evacuation - is this clearly defined?

185 Is there a designated incident commander?

186 Is the Incident Command System (ICS) structure implemented?

187 Are there succession plans if key personnel are unavailable?

188 Do you have assigned roles for active shooter incidents?

7.3 EVACUATION & ACCOUNTABILITY PROCEDURES

189 Are primary and secondary evacuation routes clearly marked and unobstructed?

190 Are assembly points designated and known to all employees?

191 Is there an accountability system to confirm all employees are safe?

192 Are there procedures for evacuating individuals with disabilities or special needs?

193 Are visitors and contractors accounted for in evacuation procedures?

7.4 FIRST RESPONDER COORDINATION

194 Do you have a formal/deliberate working relationship with local law enforcement?

195 Does the site have updated floor plans and facility information readily available for first responders?

196 Is there a designated liaison to coordinate with arriving law enforcement?

197 Are there procedures for providing facility access to first responders?

198 Does the organization conduct joint planning sessions with local first responders?

199 Are first responder contact information and protocols current?

200 Do sites conduct on-site response actions/rehearsals with First Responders (Fire, Law Enforcement, Medical)?

7.5 FAMILY REUNIFICATION

201 Is there a family reunification plan and designated location?

202 How are families notified during an incident?

203 Is there a process for releasing employees to family members?

204 Are there protocols for managing family members arriving at the scene?

205

Is the family reunification location secured and separated from the incident scene to prevent secondary attacks?

7.6 SPECIAL EMERGENCY SITUATIONS

206 Do you have a non-emergency lockdown plan in case of a nearby active shooter?

207 Have hardened areas been identified for use during natural disasters (tornado, hurricane) for shelter-in-place?

208 Do you have procedures to check mail and email for suspicious actions?

DOMAIN 8

TRAINING & PREPAREDNESS

33 QUESTIONS

8.1 TRAINING FREQUENCY & PARTICIPATION

209 Are security scenarios rehearsed or trained on a routine basis?

210 Have site personnel been trained in Run, Hide, Fight (Active shooter response)?

211 How frequently is active shooter training conducted - at least annually?

212 What percentage of employees have completed training in the past 12 months - greater than 90%?

213 Is attendance at drills mandatory?

214 Are contractors and temporary workers included in training?

215 Is there refresher training for long-term employees?

8.2 TRAINING TYPES & METHODS

216 Are tabletop exercises conducted with leadership?

217 Are full-scale drills conducted (not just discussions)?

218 Is training scenario-based and realistic?

219 Are drills conducted at various times (day/night, shift changes)?

220 Does training include force-on-force or simulation components?

221 Is your active shooter training realistic based on your assessment?

222 Do training scenarios include diverse attack methods (multiple shooters, vehicle attacks, IED, mixed tactics)?

8.3 ROLE-SPECIFIC & SPECIALIZED TRAINING

223 Are executives trained in executive protection during active shooter situations?

224 Are facility managers trained in lockdown procedures and building systems?

225 Are HR personnel trained in threat assessment and concerning behavior recognition?

226 Are medical staff trained in tactical casualty care or "Stop the Bleed"?

227 Are receptionists/front desk staff trained (as they're often first to encounter threats)?

228 Are employees trained in recognizing pre-attack warning signs?

229 Is bystander intervention training provided?

230 Are employees trained in basic first aid and bleeding control?

231 Is there training on supporting individuals in crisis?

232 Are employees trained to recognize and report pre-attack indicators based on Secret Service NTAC research?

8.4 MULTI-AGENCY EXERCISES & ICS TRAINING

233 Are drills conducted jointly with law enforcement, fire, and EMS?

234 Have multi-agency tabletop exercises been conducted?

235 Is Incident Command System (ICS) training provided to key personnel?

8.5 ONBOARDING & ONGOING TRAINING

236 Does the site have induction training which outlines security requirements for new employees and contractors?

237 Does the site have formalized refresher training on security requirements for employees and contractors?

238 Are personnel routinely trained in Information Protection requirements?

8.6 AFTER-ACTION REVIEWS & CONTINUOUS IMPROVEMENT

239 Are after-action reviews conducted after every drill?

240 Are lessons learned from drills incorporated into plan updates?

241 Are deficiencies identified in drills tracked until resolved?

DOMAIN 9

POST-INCIDENT RESPONSE & RECOVERY

22 QUESTIONS

9.1 IMMEDIATE POST-INCIDENT RESPONSE

242 Is there a documented post-incident response plan?

243 Are procedures in place for securing the scene and preserving evidence?

244 Is there a protocol for accounting for all personnel after an incident?

245 Are procedures in place for notifying families of victims?

246 Is there a designated media/PR spokesperson?

247 Are crisis communication protocols established?

9.2 VICTIM SERVICES & SUPPORT

248 Are victim assistance services identified and available?

249 Is there a process for providing immediate support to victims and families?

250

Are there protocols for managing victim information and privacy?

251 Is there access to legal support for victims?

252 Is there a plan for providing psychological support beyond immediate crisis counseling (weeks and months after the incident)?

9.3 BUSINESS CONTINUITY & RECOVERY

253 Do you have an emergency recovery plan for post-crisis?

254 Is there a business continuity plan to resume operations?

255 Are critical functions identified for priority recovery?

256 Is there an alternate site identified if the primary location is unavailable?

257 Are data backup and recovery systems in place?

258 Is there a documented plan for phased return to normal operations that considers employee readiness?

9.4 AFTER-ACTION & ORGANIZATIONAL LEARNING

259 Is there a formal after-action review process for actual incidents?

260 Are lessons learned documented and shared?

261 Is there a process for updating plans based on lessons learned?

262 Are after-action reports shared with all stakeholders?

263 Is there a protocol for memorial services and ongoing commemoration in a way that supports healing?

DOMAIN 10

SPECIAL POPULATIONS & ACCESSIBILITY

16 QUESTIONS

10.1 VULNERABLE POPULATIONS & SPECIAL NEEDS

264 Are procedures in place for protecting individuals with disabilities during an incident?

265 Are evacuation procedures adapted for those with mobility challenges?

266 Is there specialized communication for those with hearing or visual impairments?

267 Are there provisions for protecting children if the facility includes daycare or educational programs?

268 Are emergency plans, training materials, and alerts available in languages spoken by employees, students, or visitors?

269 Is there a system for communicating with limited English proficiency individuals during emergencies?

270 If children are present, are emergency protocols adapted to be age-appropriate (different for elementary, middle, high school)?

271 If the facility serves elderly populations, are evacuation and shelter-in-place procedures adapted for mobility and cognitive limitations?

- 272** Are evacuation procedures adapted for pregnant employees or students who may have limited mobility or endurance?
- 273** Are procedures in place for individuals with cognitive or intellectual disabilities who may not understand standard emergency instructions?
- 274** Are there protocols for protecting individuals who may be in psychiatric crisis during an emergency evacuation?
- 275** Are evacuation and shelter-in-place procedures adapted to accommodate individuals with service animals?
- 276** Are there protocols for individuals dependent on medical equipment (oxygen, dialysis, etc.) during evacuations or lockdowns?
- 277** Do emergency protocols respect religious or cultural considerations (e.g., women who cannot be touched by male rescuers)?
- 278** Is there a process for identifying visitors with special needs upon entry so they can be assisted during emergencies?
- 279** Does the organization maintain a confidential registry of employees/students with special needs to facilitate emergency assistance?

DOMAIN 11

INFORMATION SECURITY & CYBER INTEGRATION

18 QUESTIONS

11.1 INFORMATION & PHYSICAL SECURITY INTEGRATION

- 280** Does the company have a robust Information Protection program for IT systems?
- 281** Are physical security systems protected against cyber threats?
- 282** Is there coordination between physical security and cybersecurity teams?
- 283** Does the organization monitor social media for threats against the organization, its employees, or facilities?
- 284** Is there capability to monitor dark web forums for threats or planning discussions related to the organization?
- 285** Are IT systems monitored for behavioral indicators of insider threats (unusual access patterns, downloading sensitive data, researching violence)?
- 286** Do cybersecurity and physical security teams conduct joint threat assessments and planning sessions?

11.2 PHYSICAL SECURITY SYSTEMS CYBERSECURITY

- 287** Are electronic access control systems hardened against cyber attacks (network segmentation, encryption, intrusion detection)?
- 288** Are video surveillance systems protected against hacking, tampering, or unauthorized access?
- 289** Are emergency notification and communication systems hardened against cyber attacks that could prevent alerts during an incident?

- 290** Do critical security systems have offline backups or redundant systems in case of cyber compromise?
- 291** Are building management systems (HVAC, elevators, lighting) protected against cyber attacks that could be weaponized?
- 292** Are third-party vendors who have network access to security systems vetted for cybersecurity practices?

11.3 CYBER-PHYSICAL CONVERGENCE

- 293** Do threat assessments and emergency plans include scenarios where cyber attacks are combined with physical attacks?
- 294** Is there IT forensics capability to investigate cyber aspects of threats or incidents?
- 295** Are employees trained to recognize and report suspicious emails or communications that could indicate threat planning?
- 296** Are there protocols for protecting sensitive data during emergency evacuations or facility compromise?
- 297** Does the incident response plan address scenarios where both cyber and physical security teams must respond simultaneously?

DOMAIN 12

LEGAL, INSURANCE & COMPLIANCE

15 QUESTIONS

12.1 LEGAL COMPLIANCE & REGULATORY REQUIREMENTS

- 298** Are workplace violence prevention requirements documented?
- 299** Is the organization in compliance with state-specific workplace violence laws?
- 300** Are security plans compliant with industry-specific regulations (schools, healthcare, etc.)?
- 301** Have you worked with governance to ensure your program meets regulatory requirements?
- 302** If operating in California, is the organization in full compliance with SB 553 workplace violence prevention requirements (written plan, training, incident log)?
- 303** Is there documented evidence of compliance with OSHA's General Duty Clause regarding workplace violence hazards?
- 304** If a healthcare facility, is the organization in compliance with CMS Emergency Preparedness Rule requirements?
- 305** If an educational institution, is the organization in compliance with state education department safety and security requirements?
- 306** Are workplace violence incidents, threat assessments, and prevention activities documented and retained per legal requirements?
- 307** Are workplace violence reporting mechanisms integrated with whistleblower protection policies?
- 308** Have emergency plans been reviewed for compliance with Americans with Disabilities Act requirements?

12.2 INSURANCE & LIABILITY MANAGEMENT

- 309 Has the organization's insurance coverage been reviewed for active shooter incidents?
 - 310 Are liability concerns addressed in preparedness planning?
 - 311 Is legal counsel involved in reviewing response plans?
 - 312 Are workplace violence incidents properly documented and coordinated with workers' compensation processes?
-

THREE WAYS TO BEGIN

QUICK ASSESSMENT

NO COST • ONLINE

A short, self-guided baseline available directly on the ASPIRE website. Identifies your most urgent gaps and shows where a deeper look is warranted. Start today, no commitment.

SURVIVABILITY INDEX™

BY CONSULTATION

The complete 312-question assessment across all 12 domains, AI-enhanced and continuously updated against evolving standards and regulations. Delivers a scored index and a prioritized, organization-specific roadmap.

SPONSORED

FOUNDATION ACCESS GRANT

NO COST TO RECIPIENTS

Underwritten Survivability Index™ assessments for qualifying organizations serving vulnerable populations — schools, faith communities, and nonprofits. Safety should not depend on budget. Ask us whether you qualify.

Note: scoring weights and response fields are omitted from this handout. The complete instrument, including domain weighting and the scored index, is delivered as part of a full Survivability Index™ engagement.



BE PART OF THE SOLUTION.



**SCAN FOR THE FREE
QUICK ASSESSMENT**

aspire-initiative.org

A 501(c)(3) nonprofit organization
©2026 ASPIRE — An Active Shooter Prevention Initiative