



STONEBRIDGE
STRATEGIC

Strategy. Security. Resilience.

Occupational Security™

*A Practical Framework for Enterprise Life-Safety,
Continuity, and Training Readiness*

Authored by:

Stonebridge Strategic, Inc.

Daniel Puckett

Thomas Seithel

Contact:

Stonebridge Strategic, Inc.

www.StonebridgeStrategic.com

info@StonebridgeStrategic.com

(910) 421-0243

Document ID: SS-WP-OCCSEC-2025

Version 1.2 | Published October 2025

© 2025 Stonebridge Strategic, Inc. All rights reserved.

Table of Contents

1. Executive Summary	4
2. The Risk & Compliance Backdrop	5
3. Defining Occupational Security	6
4. Emergency Preparedness & Continuity Planning	8
5. Security Consulting & Violence Prevention	10
6. Training & Readiness	12
7. BridgeShield™: Emergency Action & First Minutes Response	14
8. BridgeSentinel™: Behavioral Threat Assessment & Management	16
9. BridgeContinuity™: Continuity of Operations & Recovery	18
10. Tiered Maturity Model	20
11. Mapping to Standards & Regulations	23
12. Case Study: BridgeShield in Action	26
13. Next Steps & Call to Action	29
14. Glossary & Appendices	32
15. References & Acknowledgments	34

Authorship and Acknowledgments

About Stonebridge Strategic

Stonebridge Strategic, Inc. is a veteran-owned security and resilience consultancy specializing in life-safety, emergency preparedness, and continuity solutions for enterprise, public, and critical-infrastructure clients. Its leadership brings decades of combined experience across U.S. military, law enforcement, fire/rescue, and private-sector security operations.

About the Authors

Daniel Puckett, Chief Operating Officer, draws on his military, government security, and public safety background to integrate operational realism into Stonebridge's consulting and training programs.

Thomas Seithel, Chief Executive Officer, is a career security professional and ASIS CPP with extensive experience in federal investigations, enterprise risk management, and organizational leadership.

This paper represents the combined expertise of the Stonebridge Strategic team and its ongoing research into the emerging discipline of **Occupational Security™**, a unified approach to safety, continuity, and workforce readiness.

Executive Summary

Occupational Security is an emerging holistic approach to safeguarding the workplace, uniting emergency preparedness, violence prevention, business continuity, and training readiness under one strategic framework. In an era of escalating risks, from active shooter incidents to natural disasters, organizations can no longer treat safety, security, and continuity as siloed functions. This white paper introduces Occupational Security as a practical framework that integrates life-safety planning, crisis response, continuity of operations, and workforce training into a single cohesive program. Corporate leaders in safety, HR, operations, and compliance will discover how aligning these elements not only protects employees and assets but also ensures organizational resilience and regulatory compliance in the face of crises.

Stonebridge Strategic, a veteran-owned security and resilience consultancy, has developed a tiered program to help enterprises strengthen their Occupational Security posture. Key services, from emergency action and continuity planning to security consulting, leadership training, and real-world exercise delivery, are mapped to industry standards and regulations (OSHA, NFPA, ASIS, CISA, FEMA, ISO) to ensure best-practice alignment. These services are delivered through an integrated suite of solutions: **BridgeSentinel™**, **BridgeShield™**, and **BridgeContinuity™**, which correspond respectively to prevention, protection, and recovery. A unifying theme is practicality: plans must be more than documents on a shelf, and training must be more than a checkbox. Through its flagship BridgeShield training product, a real-time modular tabletop exercise platform with companion communications scripts and decision matrices, Stonebridge empowers teams to act decisively under pressure.

The paper outlines a tiered maturity model (Foundation, Audit & Enhance, Full Program Build) that meets organizations where they are, whether establishing core plans, auditing and improving existing programs, or building a full Occupational Security program from the ground up. A fictional case study illustrates how a BridgeShield tabletop exercise uncovered gaps and drove improvements that later paid dividends in a crisis. Finally, we provide a crosswalk of Stonebridge services to key standards and a glossary of regulatory frameworks (OSHA 1910.38, NFPA 3000, ASIS WVPI-AA, CISA's EAP guides, FEMA HSEEP, ISO 22301).

In summary, Occupational Security offers a pathway to not only comply with mandates, but to create a culture of safety and readiness. Organizations that adopt this framework can expect enhanced life-safety for personnel, minimized downtime during disasters, and sustained operations through adverse events, all supported by trained, confident leaders and employees. Stonebridge Strategic stands ready with proven solutions like BridgeSentinel, BridgeShield, and BridgeContinuity, as well as expert consulting, to guide enterprises on this journey from planning to execution. The call to action is clear: invest in Occupational Security now to protect your people and mission, whatever the future brings.

Introduction: Evolving Threats Demand an Integrated Approach

Modern enterprises face a spectrum of threats that can strike without warning, from natural disasters and pandemics to workplace violence and cyber-physical attacks. In this environment, life-safety, security, and business continuity have converged into a single priority: keeping people safe while sustaining operations during crises. However, many organizations still address these areas in silos (safety drills separate from continuity plans, security policies separate from training), leading to gaps and inefficiencies. The concept of “**Occupational Security**” has emerged to close these gaps by taking an integrated approach to organizational resilience.

Occupational Security refers to a holistic framework that unifies emergency preparedness, violence prevention, business continuity, and training readiness into one strategy. It recognizes that a workplace emergency, whether a fire, an active shooter, or a network outage, has implications not just for immediate life-safety but also for long-term operations and employee well-being. By managing these domains together, companies can ensure a faster, more coordinated response when incidents occur, reducing confusion and downtime. Moreover, this integrated approach aligns with regulatory expectations; for example, OSHA requires employers to have Emergency Action Plans (EAPs) with clear evacuation procedures, alarm systems, and employee training for emergencies. Simply put, Occupational Security is about proactively safeguarding “the whole enterprise”, its people, processes, and ability to function, under a comprehensive life-safety and resilience program.

Leading standards bodies and government agencies reinforce this integrated perspective. The National Fire Protection Association’s **NFPA 3000 Active Shooter/Hostile Event** standard, for instance, urges a unified plan for response and recovery across stakeholders. ASIS International’s **Workplace Violence Prevention and Active Assailant (WVPI-AA)** standard similarly calls for comprehensive violence prevention programs with threat assessment, incident management, and active shooter preparedness all under one umbrella. These frameworks make clear that organizational safety is not just about locks on doors or data backups, it’s about a culture of preparedness and the agility to respond to any disruption.

In the sections that follow, we break down the components of the Occupational Security framework and demonstrate how Stonebridge Strategic applies this model in practice. We will discuss how emergency and continuity planning, security consulting and violence prevention, and training/exercises each contribute to resilience, and how they interlock. Stonebridge’s BridgeShield platform will be presented as a case study in delivering realistic, real-time crisis scenarios that test and improve an organization’s readiness. By mapping these activities to compliance frameworks (OSHA, NFPA, ISO 22301, etc.), decision-makers will see not only the “why” of Occupational Security, but the “how”, concrete steps to implement it in their enterprise.

Defining “Occupational Security” and Its Pillars

Occupational Security can be defined as *“the coordinated management of all policies, plans, and trainings that protect an organization’s people and operations from disruptive threats.”* It encompasses four core pillars: **Emergency Preparedness**, **Violence Prevention**, **Business Continuity**, and **Training & Readiness**. Each pillar addresses a critical question: (1) How do we prepare for and respond to immediate crises that threaten life-safety? (2) How do we prevent and mitigate acts of violence in the workplace? (3) How do we ensure the business can continue or recover quickly from disruptions? (4) How do we equip our people with the skills and confidence to handle emergencies?

Prevent–Protect–Recover Model: In practice, Stonebridge organizes these pillars into a streamlined three-phase continuum: **Prevent**, **Protect**, and **Recover**. **Prevent** encompasses all measures taken before an incident occurs, principally the violence prevention and security consulting pillar aimed at stopping threats early. **Protect** covers the actions during an incident, the emergency preparedness and immediate crisis response, reinforced by training and exercises to protect life and assets in real time. **Recover** focuses on the aftermath, the business continuity planning and recovery efforts that restore operations post-incident. Each phase is supported by Stonebridge’s purpose-built programs: **BridgeSentinel™** underpins the *Prevent* phase with a formal behavioral threat assessment and management process; **BridgeShield™** anchors the *Protect* phase via live emergency exercises and interactive training; and **BridgeContinuity™** drives the *Recover* phase by structuring continuity plans, defining recovery objectives, and conducting recovery-focused drills. This three-part model ensures that organizations address threats holistically, **preventing** violence before it starts, **protecting** people when crisis strikes, and **recovering** operations to sustain the business afterward.

These pillars are deeply interrelated. For example, a robust Emergency Action Plan (EAP) for a building evacuation (pillar 1) must be complemented by workplace violence protocols (pillar 2) if the emergency is an active assailant scenario; both of those feed into broader continuity plans (pillar 3) for maintaining or restoring operations after the incident; and none of the plans will succeed without training and readiness (pillar 4) to rehearse the response. Occupational Security sits at the intersection of safety, security, and continuity, ensuring that all these considerations inform one another rather than exist in isolation.

Tying these elements together provides multiple benefits. First, it eliminates blind spots; for instance, a business continuity plan that focuses only on IT disasters might overlook active shooter scenarios, whereas an Occupational Security approach forces a 360-degree risk assessment. Second, it creates consistency in response: staff and leadership train under one overarching program, so whether faced with a fire or a hostile intruder, they follow familiar incident management structures and communications protocols. Third, it strengthens corporate culture, employees see that leadership prioritizes their safety and is investing in preparedness, which improves morale and trust. Finally, Occupational Security yields practical compliance: by addressing major regulations and standards collectively, organizations avoid duplication and ensure nothing falls through the cracks. For instance, an Occupational Security program can simultaneously satisfy OSHA's requirements for evacuation training, CISA's guidelines for active shooter preparedness (which emphasize tailored EAPs and drills), and ISO 22301's mandate for continual improvement of continuity capabilities.

In summary, Occupational Security is both a philosophy and a playbook. It is the **philosophy** that safety, security, and continuity are fundamentally linked, and the **playbook** that provides an organized, standards-aligned method to achieve resilience. The next sections delve into each pillar in detail, illustrating how a unified approach transforms these practices from check-the-box compliance activities into a dynamic, effective defense system for the enterprise.

Emergency Preparedness and Business Continuity Planning

Emergency Preparedness and Business Continuity Planning form the foundational layer of Occupational Security. This is where organizations identify potential crises and devise plans to protect people and sustain critical operations. An Emergency Action Plan (EAP) typically addresses immediate life-safety measures, evacuation routes, alarm systems, accountability for employees, and rescue/medical duties in scenarios like fires, chemical spills, or active threats. Business Continuity Plans (BCPs) extend the focus to maintaining or rapidly restoring mission-critical functions (e.g. communications, IT systems, supply chain) during and after a disruption. Together, the EAP and BCP answer two questions: “How do we keep everyone safe right now?” and “How do we keep the business running (or get it running again)?”

Stonebridge Strategic emphasizes that emergency and continuity plans must be practical, scalable, and tailored, not generic templates. In its consulting practice (via its BridgeContinuity™ service), Stonebridge helps organizations build and implement plans that are realistic for their environment and workforce. For example, a coastal manufacturing facility’s plan for severe weather evacuation and hurricane recovery will differ from a tech company’s plan for a data center outage. Yet both will share the goal of minimizing confusion and downtime. A clear plan is only effective if it’s understood by those who must execute it; thus, Stonebridge ensures that leadership and staff are empowered to act decisively, minimize disruption, and maintain critical operations when it matters most. In practice, this means defining decision-makers and alternates, communication protocols (who communicates what to employees, stakeholders, first responders), and step-by-step response checklists that have been vetted through drills.

Critically, Stonebridge treats these plans as “living frameworks, not documents on a shelf.” As noted in their philosophy, **“We ensure your plans aren’t just documents on a shelf, but living frameworks that enhance resilience. Our goal is to give your people confidence, your leadership clarity, and your organization the ability to continue operations under stress.”** To live up to this, plans are regularly reviewed, tested, and updated (for example, after an exercise or real incident). This aligns with industry best practices like **ISO 22301**, the international standard for Business Continuity Management Systems, which calls for organizations to “plan, establish, implement, operate, monitor, review, maintain, and continually improve” their continuity programs to protect against and recover from disruptive incidents. Stonebridge’s approach inherently incorporates this continuous improvement cycle. (Stonebridge’s BridgeContinuity program, in particular, is built around this same cycle, aligning to ISO 22301’s plan-do-check-act methodology and FEMA’s HSEEP guidelines, to ensure continuity plans are regularly exercised and refined.)

From a compliance standpoint, robust EAP/BCP development also positions organizations to meet regulatory requirements. OSHA's regulation 29 CFR 1910.38 specifically mandates written Emergency Action Plans for applicable workplaces, including minimum elements such as procedures for reporting emergencies, evacuation, accounting for employees, and critical operations shutdown procedures. Stonebridge's Emergency Action & Business Continuity Planning service (delivered through its BridgeContinuity™ suite) directly addresses these elements, delivering custom EAP documents and continuity frameworks aligned to OSHA and local regulations. Likewise, Stonebridge aligns plans with guidance from agencies like CISA (which publishes Active Shooter Emergency Action Plan templates and recommendations emphasizing the need for site-specific planning and employee training). By integrating these guidelines, the resulting plans not only check the compliance boxes but also follow what works in real-world emergencies as distilled by experts.

In summary, the Emergency Preparedness and Continuity pillar of Occupational Security ensures that when the unthinkable happens, be it a fire, flood, or violent incident, the organization has a roadmap to follow. Employees know how to evacuate or shelter; managers know how to make decisions and coordinate with first responders; and backup systems or processes kick in to keep essential functions running. Stonebridge's BridgeContinuity™ offering reinforces this pillar by helping organizations document these continuity playbooks and run recovery-focused drills, so that as we'll see later in the case study, having plans in place *and practiced* can make the difference between a controlled, effective response and a chaotic, costly one.

Security Consulting and Violence Prevention Programs

Even the best emergency plan is of little comfort if an organization fails to prevent foreseeable threats from materializing. That's why Occupational Security dedicates a pillar to **Security Consulting and Workplace Violence Prevention**. This domain covers everything from physical security measures (access controls, cameras, facility hardening) to behavioral threat assessment and violence prevention policies. The goal is twofold: deter or stop incidents before they occur, and integrate security protocols with emergency response.

Stonebridge Strategic brings deep expertise in this arena, crafting programs that address both preventive and reactive aspects of workplace threats. On the preventive side, Workplace Violence Prevention & Mitigation services focus on policies and training to identify warning signs and intervene early. Stonebridge helps clients develop comprehensive workplace violence prevention programs, including establishing threat assessment teams, reporting mechanisms for concerning behavior, and procedures for escalation when a threat is identified. This comprehensive preventive approach is delivered through **BridgeSentinel™**, Stonebridge's Behavioral Threat Assessment and Management (BTAM) program. BridgeSentinel formalizes the Threat Assessment and Management Team (TAMT) workflows, provides confidential reporting pathways for employees to flag concerning behaviors, offers micro-training modules to build awareness of warning signs, and maintains clear documentation protocols for each case. It aligns with the ASIS WVPI-AA-2020 standard (Workplace Violence and Active Assailant – Prevention, Intervention, and Response), which provides a blueprint for organizations to *“detect threats of violence, intervene through incident management, and mitigate consequences should violence erupt”*. BridgeSentinel also draws on principles highlighted by U.S. Secret Service research into targeted violence, for example, watching for early “leakage” indicators (when a potential perpetrator signals intent to do harm). By incorporating these best practices, BridgeSentinel enables organizations to recognize and address threats well before they escalate to violence, creating a culture where employees report concerns early and every credible threat is managed through a structured, vetted process.

Stonebridge's approach mirrors the ASIS guidance: a spectrum of strategies from prevention (training employees to recognize and report early indicators) to intervention (having a plan if an employee exhibits violent behavior or an intruder enters) to response (integrating with emergency action plans for scenarios like an active shooter). On the consulting side, Security & Risk Consulting by Stonebridge often begins with risk assessments of facilities, campuses, or operations. These assessments identify vulnerabilities, for example, an office lacking controlled entry, or a production site with hazardous materials stored insecurely, and provide recommendations to strengthen defenses. Stonebridge's experts, which include former military, law enforcement, and emergency responders, ensure that solutions are practical and aligned with the client's mission (they are vendor-neutral, focusing on the right measures rather than selling products). Typical outputs might include improved physical security design (access control systems, visitor management processes), updated emergency notification systems, or revised HR policies on workplace violence and harassment.

A critical aspect is aligning these security measures with regulatory and industry standards. For instance, **NFPA 3000** (Standard for Active Shooter/Hostile Event Response) emphasizes a “whole community” approach and coordination with law enforcement. Stonebridge helps organizations incorporate law enforcement liaison and local emergency services coordination into their plans (e.g., inviting police to walk through facilities, establishing pre-incident communication channels). Additionally, many U.S. states and federal guidelines (such as OSHA’s general duty clause or state active shooter preparedness requirements) expect employers to address workplace violence. Stonebridge’s Compliance Advisory services ensure that policies and training meet these expectations, and even go beyond minimums to follow best practices like Run-Hide-Fight training for active shooter situations, a methodology reinforced by NFPA 3000 as crucial for staff to know.

In summary, the Security Consulting and Violence Prevention pillar seeks to harden the target and prepare the people. It’s about reducing the likelihood of incidents (through environmental design, procedures, and awareness) and, should one occur, breaking the pathway to violence as early as possible through rapid identification and intervention (the core mission of BridgeSentinel™). Stonebridge Strategic’s services in this area range from high-level program development (e.g., creating a workplace violence prevention program per ASIS guidelines and standing up a BridgeSentinel threat management process) to hands-on improvements (e.g., conducting an active shooter drill in coordination with local police, or delivering employee training on de-escalation techniques). These efforts create a safer everyday work environment and directly support the emergency response and continuity plans discussed earlier, because if a threat does emerge, the security measures and violence prevention protocols will activate in tandem with emergency actions. The next section will delve into how training ties all these pieces together, ensuring that plans and policies translate into effective action.

Training and Readiness: Building a Culture of Preparedness

No Occupational Security program is complete without robust training and exercise. Training is the glue between planning and reality; it turns written protocols into muscle memory and confident action. As Stonebridge Strategic often notes, preparedness is only as strong as the people behind it. Even the most thorough plans will falter if employees and leaders are not trained to execute them under pressure. This pillar focuses on building a culture of preparedness through regular training sessions, drills, and realistic exercises that engage staff at all levels.

Stonebridge's approach emphasizes interactivity and realism. Tabletop exercises, live drills, and hands-on workshops ensure knowledge isn't merely theoretical. Employees practice evacuation routes, internal alerts, the 911 call, accountability procedures, decision-making, and first aid in scenarios that mirror real crises. Training ties directly to the other pillars: emergency plans are taught and rehearsed, security protocols (e.g., lockdown and room-hardening) are drilled, and continuity plans are validated through simulation. In doing so, organizations can assess both plan effectiveness and team readiness in a low-risk environment, and fix gaps before an actual emergency.

Leadership engagement is integral. Executives and managers participate in exercises and rehearse crisis leadership roles, signaling that preparedness is a priority. Content is tailored by audience: executives receive crisis leadership and communications practice; supervisors and wardens rehearse first-minutes actions; frontline staff receive brief, recurring micro-trainings. Over time, these efforts build a workforce that knows what to do when alarms sound or notifications appear.

Finally, every training event feeds a cycle of continuous improvement. Facilitators lead after-action debriefs; lessons learned are documented and used to update plans and design the next iteration, echoing FEMA's HSEEP plan–train–exercise–evaluate–improve rhythm. As new risks emerge, content is updated so the Occupational Security program remains relevant and effective.

The Bridge Series (three courses, one system). Stonebridge delivers this pillar through an integrated sequence that maps to Prevent–Protect–Recover:

- **BridgeSentinel™ (Prevent)** — Behavioral Threat Detection & Security Interviewing training that teaches teams to spot, triage, and manage concerning behaviors before violence.
- **BridgeShield™ (Protect)** — Emergency action and first-minutes training, culminating in a live, timed tabletop to execute alerts, the 911 call, evacuate vs. secure-in-place, movement, and accountability.
- **BridgeContinuity™ (Recover)** — Continuity and recovery training that defines essential functions, protects people, stabilizes the scene, and restores priority functions under control.

Together, these courses build individual skill, team coordination, and organizational confidence, linking day-one awareness to practiced response and documented recovery so the whole Occupational Security framework performs under real conditions.

BridgeShield™: Emergency Action & First-Minutes Response

Most failures in crisis response happen in the **first minutes**, unclear alerts, slow 911 calls, indecision between evacuate vs. secure-in-place, and incomplete headcounts. **BridgeShield™** is an emergency action and first-minutes **training course** that equips leaders and wardens to execute site-specific procedures with speed, clarity, and accountability under real-time pressure.

Course format and objectives.

Blended instruction with a live, timed tabletop. Participants learn to (1) compose plain-language internal alerts; (2) deliver an effective, dispatch-ready 911 call; (3) choose evacuate vs. secure-in-place based on threat proximity and cues; (4) move people and account for them rapidly; and (5) operate basic incident roles (IC/PIO/wardens) until responders arrive.

Core modules.

Alerts and the 911 call. Plain-language internal messaging (no codes), notification pathways, 911 content checklist, sequencing alerts with building systems.

Decision: evacuate vs. secure-in-place. Threat-proximity and intel cues, room-hardening basics, movement discipline, special populations/visitors/contractors.

Movement and accountability. Warden roles, route control, assembly and shelter procedures, headcount methods and reconciliation, contractor/visitor tracking.

Role execution in the first minutes. Incident Commander and PIO basics, law-enforcement liaison, situational updates, initial logs.

Communications under stress. Radio/phone discipline, rumor control, initial family and stakeholder messages.

Hot-wash to improvement. Facilitated debrief, timing benchmarks, prioritized fixes, and drafting the AAR/IP.

Participant outcomes.

Attendees leave with a practical kit: internal alert library, a scripted 911 guide, an evacuate/secure-in-place decision matrix, warden checklists, headcount templates, and timing baselines for notifications, movement, and accountability. Teams rehearse decisions and communications in a **real-time** scenario and produce an improvement plan with owners and deadlines.

Standards alignment.

Aligned to **OSHA 29 CFR 1910.38** (Emergency Action Plans), incorporates **CISA** Active Assailant EAP guidance and messaging principles, reinforces **NFPA 3000** first-minutes coordination concepts, and follows **FEMA HSEEP** exercise/improvement methodology.

Who should attend.

Site leaders and supervisors, floor/area wardens, Security/Facilities, Safety/HR/Comms, reception/front-of-house staff, and anyone designated in the EAP for initial actions.

Delivery options.

- **One-Day: BridgeShield™ Essential** — Awareness + live, timed tabletop focused on first-minutes decisions and accountability.
- **Two-Day: BridgeShield™ Pro Day (Add-On)** — Day 1 Essential + Day 2 on-site validation with expanded scenarios, comms stress-tests, and a coached AAR/IP; optional light-movement drills where appropriate.
- **Enterprise Series (By arrangement)** — Multi-site rotations, role-specific micro-labs, and integrated recovery injects that hand off to BridgeContinuity.

BridgeSentinel™: Behavioral Threat Detection & Interviewing

Organizations often observe warning signs before an incident, leakage, fixation, intimidation, boundary-testing, policy violations, stalking. Without a defensible, repeatable process, these signals are missed or inconsistently handled. **BridgeSentinel™** is a behavioral threat detection and interviewing **training course** that equips leaders and designated team members to identify, document, and manage persons of concern early, reducing escalation risk while protecting due process and employee trust.

Course format and objectives.

Blended instruction (classroom + scenario workshop) that builds practical behavioral threat assessment & management (BTAM) capability. Participants learn to (1) stand up or refine a Threat Assessment & Management Team (TAMT); (2) triage reports using a structured matrix; (3) conduct structured, ethical interviews and follow-up; and (4) interface with emergency procedures when risk becomes imminent.

Core modules.

Governance and team operations. TAMT charter, roles/RACI, decision thresholds, confidentiality, recordkeeping, and law-enforcement liaison.

Reporting and triage. Multi-channel intake, initial screening (imminence, intent, capability, context, protective factors), and documentation standards.

Security interviewing lab Leaders conduct structured, ethical interviews using **PEACE** (Preparation/Planning; Engage/Explain; Account/Clarify/Challenge; Closure; Evaluation).

Manager enablement. Micro-trainings for supervisors; conversation guides; documentation that supports fair and defensible actions.

Program integration. Hand-offs to incident command/EAP, alignment with internal alerts, and readiness to transition to BridgeShield if risk spikes.

Participant outcomes.

Attendees leave with a practical toolkit: BTAM policy template, intake form, triage matrix, case tracker, defensibility checklist, and a quarterly metrics starter (volume, time-to-triage, dispositions). Teams practice decision-making on realistic scenarios and rehearse documentation that stands up to scrutiny.

Standards alignment.

Aligned to **ASIS WVPI/AA-2020** program elements; incorporates widely recognized behavioral “leakage” indicators reflected in U.S. Secret Service research; complements OSHA general duty expectations and integrates with site EAPs and BridgeShield communications.

Who should attend.

HR, Security, Operations, Legal, and designated leaders who will serve on or support the TAMT; site managers and supervisors responsible for early intervention.

Delivery options.

One-day workshop with scenario labs and coached case practicums.

BridgeContinuity™: Security-Led Continuity & Recovery

Most organizations can clear a building; fewer can re-establish safe, secure, revenue-critical operations quickly. BridgeContinuity™ is a continuity and recovery course that teaches teams to protect people, stabilize the scene, and restore priority functions under control, linking Emergency Action Plans (EAP) to business continuity run-books and recovery exercises anchored to recognized standards.

Course format and objectives

Interactive instruction plus facilitation labs. Participants learn to (1) identify essential functions and security-critical dependencies (access control, guard force, CCTV, credentialing); (2) author concise run-books for security-relevant disruptions; (3) conduct recovery-focused exercises; and (4) apply a Crisis Management module that bridges incident response to operational recovery (decision rights, liaison with first responders, controlled re-entry, evidence preservation, and reunification).

Core modules

Threat-informed continuity. Map likely threats (workplace violence/active assailant, fire, cyber/IT outage, utility loss, supply chain failure) to business functions and security postures; define activation triggers tied to the EAP.

Crisis Management (the incident bridge). Establish a small, empowered team to manage the transition from life-safety to recovery: confirm accountability, coordinate with law enforcement/fire, control access and perimeter, protect evidence, authorize phased re-entry, and plan reunification and staff care.

Secure re-entry & facility recovery. Define entry control points, badging/credential checks, vendor escorts, temporary barriers, critical systems checks, and safety inspections before resuming operations

Strategies & run-books. Build short, role-clear playbooks for: loss of facility; IT/ERP outage; staff shortage; vendor or logistics failure; and post-assailant recovery (scene transition, communications, continuity of operations).

Recovery tabletop & AAR/IP. Design objectives, score decision-making and movement toward RTOs, and produce an Improvement Plan with owners, timelines, and budget implications, using FEMA HSEEP methodology.

Participant outcomes

Teams produce a starter continuity package with a **Security Annex**: first-hour checklists, controlled-reentry procedures, accountability and credentialing lists, vendor and MOU/ SLA contacts, role-based run-books, pre-approved messages, and an improvement tracker connected to budgets and deadlines. A coached HSEEP-style tabletop validates assumptions and prioritizes fixes.

Standards alignment

Aligned to **ISO 22301** business continuity concepts; intersects with **OSHA 1910.38** EAP elements (reporting, evacuation/secure-in-place, accountability); incorporates **NFPA 3000** ASHER recovery considerations (unified planning, access control, reunification); references **ASIS WVPI/AA-2020** for workplace-violence prevention/response; and uses **FEMA HSEEP (2020)** for exercise and improvement planning.

Who should attend

Security, Safety/EHS, Facilities, Operations, IT/Systems, HR/Comms, and leaders responsible for sustaining customer commitments and mission-critical services during and after disruptions.

Delivery options

One-day fundamentals or a two-day build-and-exercise format, including a full recovery tabletop and coached AAR/IP development.

A Tiered Maturity Model for Occupational Security Programs

Organizations vary widely in their preparedness; some may be starting from scratch with no formal emergency plans, while others have mature programs that need fine-tuning. Stonebridge Strategic recognizes this and offers a **tiered maturity model**, essentially three levels of engagement that map to an organization's current state and goals. These tiers are **Foundation**, **Audit & Enhance**, and **Full Program Build**. An organization can enter at any tier based on need, and progress through them over time to continually elevate their Occupational Security posture.

(Figure: Stonebridge's tiered maturity model allows organizations to start at the level that fits their current preparedness and scale up their Occupational Security program. Each tier builds on the previous, from establishing the fundamentals to auditing and improving, and finally to developing a comprehensive program.)

1. Foundation: The Foundation tier is about establishing the core foundations of Occupational Security. It's ideal for organizations that need to get basic plans and training in place quickly. In this tier, Stonebridge typically focuses on delivering a Bridge Series exercise and the development of key emergency documents. For example, Stonebridge will work with the client to create an OSHA-compliant Emergency Action Plan (if one doesn't exist) or update an outdated one. They ensure that at least minimal continuity strategies are identified for critical operations (guided by BridgeContinuity™ templates for recovery procedures). Concurrently, basic workplace violence prevention measures are introduced, such as a simple BridgeSentinel-informed reporting policy for employees to flag threats, to begin addressing the "Prevent" aspect even at this early stage. Then, a BridgeShield tabletop exercise (real-time, scenario-based) is conducted to introduce the organization to its new plans **in action**. This exercise, at the Foundation level, might be relatively straightforward (e.g., a single scenario like a building fire evacuation) but is enough to surface gaps and build initial muscle memory. The outcome of the Foundation tier is that the organization has a practical emergency plan, a trained initial response team, and first-hand experience in crisis response. It's a quick win that significantly reduces liability and anxiety; leadership knows they have taken the first step to protect their people. Many clients opt for BridgeShield as a starting engagement or even as a pilot program, after which they often recognize the value and commit to deeper development. *Even at this foundational tier, Stonebridge incorporates elements of prevention and recovery: for instance, introducing a basic BridgeSentinel threat-reporting protocol and outlining essential function backup plans via BridgeContinuity. This ensures that from the very beginning, the program addresses all three phases – Prevent, Protect, and Recover.*

2. Audit & Enhance: The second tier is for organizations that have some measures in place but want to benchmark them against best practices and systematically improve. Stonebridge's team conducts a thorough audit of existing emergency plans, security policies, continuity plans, and training records. They might use standards checklists, for instance, evaluating an Emergency Action Plan against OSHA 1910.38 requirements and CISA guidelines, or reviewing a workplace violence policy in light of ASIS WVPI standards. Gaps and areas of non-compliance are identified. Then comes the "Enhance" phase: Stonebridge provides targeted consulting to address these gaps. This could involve updating plans (adding missing elements like family reunification procedures in a continuity plan), enhancing physical security (perhaps the audit revealed a need for better door locking mechanisms or visitor protocols), or delivering focused training to address weaknesses (if the audit shows employees aren't drilled on lockdown procedures, Stonebridge might run an active shooter workshop). An important component at this tier is also **testing the enhancements**, often through another round of exercises. For example, after improvements, an advanced BridgeShield scenario might be run to ensure the changes are effective. In many cases this includes exercising the continuity plan as well, incorporating a BridgeContinuity-style recovery scenario to validate that new backup systems or procedures work as intended. The Audit & Enhance tier is essentially a continuous improvement cycle: assess -> improve -> validate. Organizations at this stage often see significant gains in confidence and capability, as they transform patchwork plans into a more unified, reliable program. If the audit reveals the absence of a formal threat assessment process, Stonebridge will help establish one as part of the enhancements (introducing a BridgeSentinel program, such as chartering a Threat Assessment Team and training its members). Similarly, identified weaknesses in continuity planning are addressed by developing more robust recovery strategies through BridgeContinuity, for example, defining clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical functions and documenting playbooks for various outage scenarios.

3. Full Program Build: The Full Program Build is a comprehensive engagement aimed at organizations that seek a top-to-bottom Occupational Security program or a major overhaul of their current one. Here, Stonebridge operates as a partner in building a fully integrated security, emergency, and continuity program. This can span months or even year-long collaborations. Activities include: developing all necessary policies and plans (Emergency Action Plan, Crisis Management Plan, Business Continuity Plan, IT Disaster Recovery Plan, Workplace Violence Prevention Program, etc.), establishing governance (e.g., forming a Crisis Management Team with charters and roles, and a dedicated Threat Assessment Team under BridgeSentinel), implementing training curricula for different employee levels, scheduling regular drills/exercises (a multi-year exercise plan in line with HSEEP principles, often integrating **BridgeContinuity** tabletop drills for recovery scenarios), and setting up program metrics and audit processes. Essentially, Stonebridge helps institutionalize Occupational Security into the organization's DNA, it becomes part of regular operations and leadership oversight. At this full-build tier, the Prevent, Protect, and Recover elements (via BridgeSentinel, BridgeShield, and BridgeContinuity) are fully integrated into the client's culture and daily operations. A Full Program Build engagement might culminate in a large-scale exercise that ties everything together, possibly a full-scale exercise involving local emergency services, multiple departments, and even external stakeholders to truly stress-test the organization's preparedness. By the end of this tier, the organization not only aligns with all relevant standards (OSHA, NFPA, ISO, etc.) but often exceeds them, becoming a potential model of best practice in their sector. Stonebridge provides documentation and training for continuity (with BridgeContinuity ensuring the continuity program is sustainable internally) so that the program can be maintained by the organization moving forward.

A key aspect of this maturity model is flexibility: an organization can jump in at the level they need. For instance, a company that already has ISO 22301 certification (indicative of a strong continuity program) might not need "Foundation" and could go straight to Audit & Enhance to refine specific areas like violence prevention or training frequency. Conversely, a fast-growing company that suddenly has to meet client-mandated safety requirements might start with Foundation to get basics in place, then rapidly progress to the next tiers as they mature. Stonebridge's tiered approach ensures a right-sized solution, you get neither an overwhelming Cadillac program when you just needed the basics, nor a skimpy solution when you actually face complex risks.

The maturity model also fosters long-term partnership. Many clients begin with a single BridgeShield exercise (Foundation tier as a toe in the water), then engage Stonebridge for an annual audit and exercise program (Audit & Enhance as an ongoing service). If a major incident or close call happens, those clients often decide to invest in the Full Program Build to really fortify their organization. Stonebridge is equipped to support at each step, scaling its involvement up or down as needed. The outcome is a roadmap for continuous improvement in Occupational Security, much like a quality program, there is always another level of maturity to achieve, and the tiered model provides that path.

Mapping Services to Standards and Regulatory Frameworks

Corporate decision-makers often must justify safety and continuity investments in terms of compliance and industry standards. A strong Occupational Security program not only improves safety and resilience; it also ensures alignment with legal requirements and best-practice frameworks. Stonebridge Strategic takes pride in mapping all its services and deliverables to the relevant standards, effectively providing a “compliance crosswalk” for clients. The diagram below highlights how Stonebridge’s offerings correspond to key regulatory and guidance frameworks:

(Figure: Crosswalk of major standards/regulations to Stonebridge Strategic’s service areas. This mapping illustrates that an Occupational Security program addresses compliance obligations across OSHA (safety regulations), NFPA (life-safety standards), ASIS (security management standards), CISA (federal guidance on emergency planning), FEMA (exercise and preparedness programs), and ISO (continuity management systems).)

As shown above, here are some of the primary alignments:

- **OSHA 29 CFR 1910.38 (Emergency Action Plans):** Stonebridge’s Emergency Action Planning service ensures organizations meet OSHA’s requirements for a written Emergency Action Plan including evacuation procedures, reporting methods, and employee training. During consulting engagements, Stonebridge uses OSHA’s checklist to verify that all required EAP elements are in place. By conducting drills and evacuation training (as in BridgeShield exercises), Stonebridge also helps fulfill OSHA’s mandate that employers designate and train individuals to assist in a safe and orderly evacuation.
- **NFPA 3000 (ASHER Program Standard):** Stonebridge’s planning and training approach aligns with NFPA 3000, which emphasizes integrated incident command, joint training between private and public sectors, and recovery protocols. For example, BridgeShield exercises often involve local law enforcement or at least include their role in scenarios, addressing NFPA’s call for unified response. By following NFPA 3000’s guidance (such as family reunification plans and mental health support in recovery), Stonebridge helps clients ensure that even worst-case hostile events are met with a swift, coordinated, and effective response.

- **ASIS WVPI-AA (Workplace Violence Prevention and Intervention – Active Assailant Standard, 2020):** Stonebridge’s Workplace Violence Prevention programs and BridgeSentinel BTAM service map directly to ASIS WVPI-AA guidelines. The creation of threat assessment teams, establishment of reporting and intervention processes, and training on active assailant response all mirror the standard’s recommendations. By adhering to WVPI-AA, organizations working with Stonebridge are proactively addressing behavioral threats and ensuring readiness to handle violent incidents. This not only improves safety but also demonstrates due diligence should regulators or stakeholders inquire about violence prevention efforts.
- **CISA Active Shooter Emergency Action Plan Guide:** Stonebridge incorporates best practices from the U.S. Cybersecurity and Infrastructure Security Agency’s Active Shooter guides and toolkits. In developing Emergency Action Plans and training, Stonebridge references CISA’s templates and guidance (for example, integrating the “Run, Hide, Fight” protocol and site-specific procedures). The result is that clients’ emergency plans and exercises (like those run through BridgeShield) reflect the fundamental concepts CISA promotes for active shooter preparedness.
- **FEMA HSEEP (Homeland Security Exercise and Evaluation Program):** Stonebridge’s exercise methodology, including BridgeShield and continuity tabletop drills via BridgeContinuity, follows FEMA’s HSEEP principles of design, conduct, evaluation, and improvement planning. Each exercise has clearly defined objectives, is evaluated against those objectives, and is followed by an after-action report and improvement plan. This means that Stonebridge-run exercises don’t just “check a box”; they lead to concrete improvements in programs, aligning with FEMA’s national best practices for emergency preparedness exercises.
- **ISO 22301 (Business Continuity Management Systems – Requirements):** Stonebridge’s continuity planning (BridgeContinuity) is aligned with ISO 22301:2019, which outlines how to establish, maintain, and improve a Business Continuity Management System. Clients who engage in Stonebridge’s continuity services will find that their programs naturally fulfill ISO 22301 requirements, from conducting business impact analyses and setting recovery objectives, to implementing and testing continuity plans, and ensuring leadership review and continual improvement. For organizations aiming for ISO 22301 certification, Stonebridge can help get them audit-ready through this alignment.

By mapping services to these standards and frameworks, Stonebridge provides assurance that an Occupational Security program is not just effective in practice but also defensible and compliant on paper. This dual benefit, improved resilience and demonstrated conformity to guidelines, helps safety and security leaders build a strong business case for investment in Occupational Security. In essence, by partnering with Stonebridge, organizations are investing in a program that hits all the marks: protecting people, preserving operations, and proving to stakeholders (be they regulators, insurers, or clients) that internationally recognized best practices are being followed.

Case Study: Occupational Security in Practice - Prevent, Protect, Recover

Background: HarborWest Logistics (a fictional name for a real mid-sized regional logistics provider) operated a headquarters and two cross-dock warehouses with roughly 650 employees. They had basic safety measures (evacuation maps, fire drills) and a vendor-managed access system, but no formal behavioral threat process, no documented continuity plans, and uneven training across shifts. After a series of concerning behaviors, an agitated former contractor loitering at a gate and a supervisor receiving hostile messages from a disgruntled employee, leadership recognized gaps in both prevention and response. They engaged Stonebridge Strategic to implement an integrated Occupational Security program encompassing BridgeSentinel™, BridgeShield™, and BridgeContinuity™.

Engagement: Stonebridge began by establishing a formal Behavioral Threat Assessment & Management (BTAM) process through BridgeSentinel: a Threat Assessment & Management Team (TAMT) with a written charter, a confidential intake workflow (QR/email/phone), and a triage matrix to sort reports by imminence and risk factors. In parallel, the team updated HarborWest's Emergency Action Plan (EAP) for site-specific threats, active assailants, severe weather, and vehicle-borne hazards common to truck yards, and introduced plain-language internal alert templates. Using BridgeContinuity, Stonebridge facilitated a business impact review to identify essential functions (yard operations, Transportation Management System [TMS], shipping/receiving, payroll, customer communications) and set recovery targets (e.g., TMS RTO 4 hours, RPO 15 minutes). With these "living" documents in place, Stonebridge delivered a BridgeShield tabletop exercise to validate first-minutes decisions, communications, and accountability under pressure.

Scenario Summary: The BridgeShield exercise unfolded on a Thursday afternoon at shift change. It began with a security call reporting a banned former contractor on the public sidewalk filming the west gate and yelling at inbound drivers. Minutes later, injects indicated the individual had crossed onto company property and an argument with a guard was escalating. Participants had to choose between lockdown of the admin building versus partial evacuation of the west loading bays, referencing the updated EAP. As the scenario advanced, facilitators introduced simultaneous stressors: social media posts from bystanders, a rumor of a weapon, and a distracted forklift operator nearly striking a pedestrian during the commotion. The team coordinated the 911 call using the prepared script, issued a site-wide text alert, designated an Incident Commander (IC), and activated floor wardens to move non-essential staff out of the bay area. After law enforcement "arrived" and the immediate threat was neutralized, the exercise transitioned into early recovery: leadership had to decide whether to resume operations, how to brief drivers and customers, and how to account for contractors and visitors in the yard. A final inject simulated a TMS service degradation, forcing the team to reference the BridgeContinuity run-book for manual bill of lading workflows and carrier notifications.

Challenges & Learnings:

- **Communication Coverage:** The initial PA announcement did not cut through ambient noise in the cross-dock. Wardens in the far bay relied on runners. (Debrief action: expand SMS alerting to all badges, add bay-level strobes, and deploy a warden radio channel.)
- **Incident Command Clarity:** A senior ops manager and the security supervisor both attempted to lead. (Debrief action: codify IC/Deputy IC by incident type; publish an org card on lanyards.)
- **Accountability & Visitors:** HR could not quickly distinguish on-site contractors from drivers waiting at the gate. (Debrief action: tighten visitor/contractor logging and add a driver accountability count at assembly areas.)
- **Hand-off from Prevention to Response:** The team hesitated to use details from prior complaints in real-time decisions. (Debrief action: BridgeSentinel case summaries and LE liaison contacts made available to IC in a quick-read format.)
- **Recovery Workarounds:** The TMS fallback procedure was not widely known, and printers for offline bills were in a locked office. (Debrief action: stage offline packets at both docks; pre-authorize emergency procurement for spare printers and mobile hotspots.)

Results: In the weeks following the exercise, HarborWest implemented a series of targeted improvements. They rolled out SMS/text alerting to all employees and long-term contractors, extended PA coverage in noisy bays, and issued warden radios. The EAP was updated to designate IC/Deputy IC roles by scenario, with HR owning headcount and family communications, and Operations coordinating with first responders. The TAMT began meeting biweekly, using BridgeSentinel's tracker and metrics to review open cases and dispositions. BridgeContinuity run-books for TMS outage, partial facility closure, and staff shortages were finalized, and a recovery-focused tabletop validated the manual shipping/receiving workflow. HarborWest scheduled quarterly drills, two announced and one no-notice per year, alternating evacuation and secure-in-place, and committed to a six-month follow-up exercise that blends a hostile-visitor scenario with a TMS outage.

Outcome: Six weeks later, a real incident tested the system. A transformer failure caused a partial power loss at the west warehouse during inbound peak. Floor wardens executed the EAP calmly; accountability reached 98% in under 10 minutes, and operations were paused in the affected bays while the rest of the facility continued under modified procedures. Simultaneously, the TAMT received a report that the previously banned contractor had posted threatening comments online. BridgeSentinel intake triggered an immediate review; law enforcement was notified through the established liaison, and site access controls were adjusted for the remainder of the shift. Meanwhile, a TMS vendor issue slowed transaction processing; the team activated the BridgeContinuity run-book, switched to offline bills of lading, and used pre-written customer messages to prevent cascading schedule impacts. By the next morning, power and TMS performance were restored, and the backlog was cleared without missed delivery windows. No injuries occurred, and customer KPIs for the week held within normal variance.

In the after-action review, HarborWest leadership credited the integrated Occupational Security program for the orderly response: “Before, we would have been scrambling across three separate playbooks. Now the pieces connect, Sentinel gives us early warning and structure, Shield proves the plan under pressure, and Continuity keeps freight moving when systems wobble.” Employees reported greater confidence in alerts and roles, and supervisors noted fewer gray-area escalations because the TAMT provided a predictable path for handling concerning behavior. The case underscores the core value of Occupational Security: by aligning **Prevent (BridgeSentinel)**, **Protect (BridgeShield)**, and **Recover (BridgeContinuity)**, organizations build adaptive capacity for all-hazards events, not just the scenario they trained on.

Next Steps: Advancing Your Occupational Security Program

This white paper has presented the concept of Occupational Security and outlined how Stonebridge Strategic's framework can elevate an organization's safety, continuity, and readiness. For decision-makers reading this, the logical question is: **"What do we do next?"** Whether your company is just beginning to formalize emergency plans or looking to refine and integrate existing programs, below are practical next steps and a call to action to consider:

1. **Assess Your Current State:** Take stock of what you already have in place. Do you have an up-to-date Emergency Action Plan, and has it been reviewed recently? Are there violence prevention or security protocols? Have you conducted drills or exercises in the past year? Identifying gaps is the first step. Stonebridge offers a complimentary initial consultation or an "Emergency Action Plan (EAP) Scan", a quick review of your current EAP against OSHA and CISA guidelines. This can highlight immediate areas of concern (for instance, missing elements or outdated procedures).
2. **Engage with Bridge Series Course:** For many organizations, the fastest way to kickstart improvement is to schedule the BridgeShield course. This two-day engagement not only provides eye-opening insights into your team's readiness but also delivers tangible value. You get validation of your existing Emergency Action Plan, and employees receive hands-on training. Consider it a "stress test" for your current preparedness. Even if you anticipate shortcomings, it is far better to discover them in an exercise than during a real crisis. BridgeShield is an excellent onboarding pathway into the Occupational Security program; it builds buy-in among leadership and staff when they see the realistic scenario unfold.
3. **Prioritize Quick Wins and Critical Fixes:** Based on the outcomes of an assessment or initial exercise, identify which gaps carry the highest risk and address those immediately. This could be as simple as fixing an alarm system, or as involved as developing a workplace violence policy. Stonebridge can assist in triaging these actions, often, there are "essential fixes" that can dramatically improve safety (for example, training front-desk staff on threat response, or establishing a clear lockdown procedure) with minimal cost. Quick wins build momentum and prove the value of the program to stakeholders.

4. **Plan for an Ongoing Program (Audit & Enhance or Full Build):** Occupational Security is not a one-off project but an ongoing commitment. Organizations should plan for regular reviews, updates, and training cycles. Depending on your needs:
 - If you have a moderate foundation, consider an Audit & Enhance engagement in the next budget cycle. This will systematically evaluate your program, document improvements, and ensure you're keeping pace with evolving threats and standards (remember, standards like NFPA and ISO are periodically updated, as are best practices).
 - If your risk profile is high (e.g., large workforce, public-facing facilities, critical infrastructure) or you have regulatory pressures, you may opt for a Full Program Build sooner rather than later. Stonebridge can develop a multi-year roadmap for you, outlining the projects and milestones to achieve a gold-standard program that covers **Prevent–Protect–Recover** end-to-end (for instance, establishing a BridgeSentinel threat management process, attaining ISO 22301 certification for continuity via BridgeContinuity, or becoming a “StormReady” site in partnership with emergency agencies).
5. **Foster Leadership and Employee Engagement:** True culture change comes when safety and preparedness are championed from the top and embraced at the grassroots. We recommend establishing a cross-functional Resilience Committee or incorporating Occupational Security into an existing safety or risk committee. Stonebridge often meets with such committees during engagements to ensure alignment and transfer knowledge. Encourage your leaders to speak about safety readiness in town halls or internal communications; this reinforces its importance. Likewise, empower employees to take part (for example, train volunteer floor wardens or first aiders, run contests or quizzes on emergency procedures, etc.). Stonebridge provides toolkits and creative ideas for maintaining engagement, drawn from years of experience in different organizational cultures.
6. **Leverage External Resources and Partnerships:** Part of Occupational Security maturity is knowing you're not alone. Build relationships with local first responders, invite the fire department to do a walkthrough of your facility, or local law enforcement to observe or participate in your drills. Many agencies appreciate proactive businesses and will collaborate (some even offer free assessments or training). Stonebridge can facilitate these introductions as needed. Also, stay connected with industry groups or information-sharing organizations relevant to your sector for updates on threats and best practices. (This white paper's Appendix provides references to resources from OSHA, FEMA, etc., which are great starting points to further explore.)

7. **Contact Stonebridge Strategic for Support:** Lastly, we invite you to reach out to Stonebridge Strategic to discuss your unique needs. Whether it's scheduling a BridgeShield exercise, implementing the BridgeSentinel threat assessment program, developing a continuity playbook with BridgeContinuity, or simply seeking advice on a compliance question, our team is ready to assist. We pride ourselves on being professional, confidential, and mission-focused. Our only goal is to help you safeguard what matters most and operate with confidence in an uncertain world. As a veteran-led firm with multidisciplinary expertise, we bring both the tactical know-how and the strategic insight to elevate your Occupational Security posture.

Call to Action: To get started, consider scheduling a BridgeShield workshop as a practical first step. You can also request Stonebridge's Occupational Security Program Starter Kit, which includes a self-assessment checklist (covering OSHA EAP items, basic continuity elements, and foundational threat reporting practices), an emergency contacts template, and a sample drill schedule. These tools can jumpstart your internal discussions. Visit our website or contact us at info@stonebridgestrategic.com to schedule a consultation. Remember, emergencies give no notice; the best time to strengthen your preparedness is now. By adopting the Occupational Security framework, addressing **prevention** (BridgeSentinel), **protection** (BridgeShield), and **recovery** (BridgeContinuity), you are investing in the safety of your employees, the continuity of your operations, and the long-term resilience of your enterprise.

Stonebridge Strategic is here to partner with you on this journey from uncertainty to resilience. Together, let's build a safer, more secure future for your organization.

Glossary & Appendices

Appendix: Glossary of Key Standards and Frameworks

- **OSHA 29 CFR 1910.38 (Emergency Action Plans):** An OSHA regulation that requires employers to develop an Emergency Action Plan covering procedures for reporting emergencies, evacuation routes, accounting for employees, and other essential steps to ensure safe and orderly evacuation. It also mandates employee alarm systems and training for designated evacuation assistants. Compliance with 1910.38 helps organizations reduce chaos and injuries during emergencies by having clear, practiced plans.
- **NFPA 3000 (ASHER Program Standard):** A standard published by the National Fire Protection Association titled “Standard for an Active Shooter/Hostile Event Response (ASHER) Program.” It provides guidance for communities and organizations to plan for, respond to, and recover from active shooter or hostile events in a unified, multi-agency way. NFPA 3000 emphasizes integrated incident command, joint training between private and public sectors, and recovery protocols (e.g., family reunification, mental health support). Following NFPA 3000 helps ensure that in worst-case violent incidents, the response is swift and coordinated, minimizing casualties and aiding recovery.
- **ASIS WVPI-AA (Workplace Violence Prevention and Intervention – Active Assailant Standard, 2020):** A security management standard from ASIS International (in coordination with SHRM) that outlines best practices for preventing workplace violence and responding to active assailant situations. It covers establishing a workplace violence prevention program, threat assessment teams, reporting and intervention processes, and active shooter response planning. The standard also includes an annex on active assailant preparedness. Adhering to WVPI-AA helps organizations create safer workplaces by proactively addressing behavioral threats and ensuring readiness to handle violent incidents should they occur.
- **CISA Active Shooter Emergency Action Plan Guide:** Guidance and tools from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) focused on active shooter preparedness. CISA’s “Active Shooter Emergency Action Plan Product Suite” includes a guide, video, and template that *describe the fundamental concepts of developing an Active Shooter Emergency Action Plan (EAP), stress the importance of early planning, and review the basic emergency response practices that can improve survivability in an incident*. Stonebridge uses these resources to inform its emergency planning and training services.

- **FEMA HSEEP (Homeland Security Exercise and Evaluation Program):** FEMA's doctrine for exercise planning and evaluation, which provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Stonebridge's exercise methodology (for both BridgeShield and BridgeContinuity drills) follows HSEEP guidelines, ensuring that exercises result in actionable improvement plans and that programs are continuously improved.
- **ISO 22301:2019 (Security and Resilience – Business Continuity Management Systems – Requirements):** An international standard that specifies the requirements for setting up and managing an effective Business Continuity Management System (BCMS). It covers identifying business impact, setting recovery objectives, developing plans and procedures, and continual improvement of preparedness. Organizations that implement ISO 22301-aligned continuity programs (like those guided by BridgeContinuity) demonstrate a commitment to sustaining operations through disruptions and often gain confidence from customers and stakeholders for their resilience.

(Additional references and frameworks are detailed in the full References section, covering sources from OSHA, NFPA, ASIS, CISA, FEMA, ISO, and more.)

References

ASIS International. 2020. *Workplace Violence and Active Assailant—Prevention, Intervention, and Response (WVPI-AA-2020)*. Alexandria, VA: ASIS International.

CISA (Cybersecurity and Infrastructure Security Agency). *Active Shooter/Active Assailant Emergency Action Plan Product Suite*. Washington, DC: U.S. Department of Homeland Security.

CISA (Cybersecurity and Infrastructure Security Agency). *Active Shooter Preparedness: Products and Resources*. Washington, DC: U.S. Department of Homeland Security.

FBI (Federal Bureau of Investigation). 2024. *Active Shooter Incidents in the United States in 2023*. Washington, DC: U.S. Department of Justice.

FEMA (Federal Emergency Management Agency). 2020. *Homeland Security Exercise and Evaluation Program (HSEEP): 2020 Doctrine*. Washington, DC: U.S. Department of Homeland Security.

FEMA (Federal Emergency Management Agency). 2025. *HSEEP Program Overview*. Washington, DC: U.S. Department of Homeland Security.

ISO (International Organization for Standardization). 2019. *ISO 22301:2019 — Security and Resilience — Business Continuity Management Systems — Requirements*. Geneva: ISO.

ISO (International Organization for Standardization). 2021. *ISO 31030:2021 — Travel Risk Management — Guidance for Organizations*. Geneva: ISO.

NFPA (National Fire Protection Association). *NFPA 3000® (ASHER) Program – Fact Sheet*. Quincy, MA: NFPA.

NFPA (National Fire Protection Association). *NFPA 3000 – Standard for an Active Shooter/Hostile Event Response (ASHER) Program (Overview)*. Quincy, MA: NFPA.

NIST (National Institute of Standards and Technology). 2018. *SP 800-37, Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Gaithersburg, MD: U.S. Department of Commerce.

OSHA (Occupational Safety and Health Administration). *29 CFR 1910.38 — Emergency Action Plans*. Washington, DC: U.S. Department of Labor.

OSHA (Occupational Safety and Health Administration). *Evacuation Plans and Procedures – Emergency Action Plan (EAP)*. Washington, DC: U.S. Department of Labor.

U.S. Bureau of Labor Statistics. 2024. *National Census of Fatal Occupational Injuries in 2023 (USDOL-24-2564)*. Washington, DC: U.S. Department of Labor.

(Additional internal research, client experiences, and Stonebridge Strategic proprietary methodologies contributed to this paper. We acknowledge the contributions of the Stonebridge Strategic team and the invaluable feedback from clients and industry peers in shaping the Occupational Security framework.)

About Stonebridge Strategic:

Stonebridge Strategic, Inc. is a Wyoming-registered S Corporation specializing in security & risk consulting, emergency and continuity planning, training and exercise delivery, and leadership development. Through products like **BridgeShield™**, **BridgeSentinel™**, and **BridgeContinuity™**, Stonebridge converts recognized standards into practical, actionable programs that help organizations strengthen life-safety and continuity readiness.

Headquarters: Cheyenne, WY

Email: info@StonebridgeStrategic.com

Web: www.StonebridgeStrategic.com | *Phone:* (910) 421-0243

Copyright and Trademark Notice:

© 2025 Stonebridge Strategic, Inc. All rights reserved. **BridgeShield™**, **BridgeSentinel™**, **BridgeContinuity™**, and **Occupational Security™** are trademarks of Stonebridge Strategic, Inc. No portion of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of Stonebridge Strategic, Inc.