ASSESSMENTS: FAST FACTS

Risk vs. Vulnerability vs. Security Assessments, and the TVRA

The terms **risk assessment**, **vulnerability assessment**, **security assessment**, and **TVRA** are often used interchangeably, but they actually are not the same thing.

They answer different questions; are performed with different inputs; and produce distinct outputs—yet they also overlap in methods, data sources, and follow-on actions.

Risk Assessment

- **Core Question:** *What could go wrong, how likely it is, and how bad would it be?*
- **Focus:** Consequences to people, operations, finances, reputation, and compliance. It considers **threats** × **vulnerabilities** × **impact** to produce a prioritized risk picture.
- **Output:** Ranked risks and mitigation plan (avoid, reduce, transfer, accept).

Vulnerability Assessment

- **Core Question:** *Where are we weak, and how could known threats exploit those points?*
- **Focus:** Conditions that make an incident more likely or more severe. Validation could include walkthroughs, scans, testing, or red-teaming.
- **Output:** A list of specific weaknesses with severity ratings and remediation steps.

Security Assessment

- **Core question:** *Given our risk and vulnerability, how effective is our security posture?*
- **Focus:** Technical, physical, and administrative controls (policies, staffing, technology, incident response) measured against standards, laws, or best practices.
- **Output:** System maturity findings, effectiveness ratings, and a roadmap to improve.

Threat, Vulnerability, and Risk Assessment (TVRA)

In critical infrastructure, individual assessments are often bundled together into a Threat, Vulnerability, and Risk Assessment (TVRA), combining all the assessments into a single, integrated process.

- **Core question:** *What threats do we face, where are we vulnerable to them, and what is the resulting risk to our people, assets, and operations?*
- **Focus:** Integrates **threat identification**, **vulnerability analysis**, and **risk evaluation** into a single, continuous process, showing how specific threats can exploit particular vulnerabilities to produce measurable risks.
- **Output:** A unified, prioritized list of risks **directly linked to the threats and vulnerabilities that create them**, with recommended mitigations, responsible parties, and timelines.

The TVRA is the predominantly used for security master planning; facility design reviews; critical infrastructure protection; and compliance frameworks that demand a complete "*threat–vulnerability–risk*" chain. It creates a single, coherent logic trail from threat to risk, but is the most resource-intensive, and requires coordination across multiple specialties.

State-Specific Notes (CA, TX, GA, FL)

California

- **Workplace Violence Prevention (SB 553; Labor Code §6401.9):** Most California employers must maintain a written Workplace Violence Prevention Plan (WVPP), keep a violent-incident log, train employees, and **assess/mitigate workplace violence hazards**. A risk or vulnerability assessment for people-safety should align with the WVPP and document hazards, corrective actions, and training.
- **Healthcare settings:** California requires workplace-violence plans in healthcare (Title 8 §3342). Assessments of hospitals/clinics must ensure that findings map to plan, training, and incident-log obligations.

Texas

- **K–12 security audits and vulnerability assessments:** Texas districts must conduct safety and security audits at least every three years and may receive **district vulnerability assessments** and **intruder detection audits** coordinated with the Texas Education Agency (TEA) and the Texas School Safety Center. Findings trigger corrective actions and board reporting.
- **Healthcare workplace violence (SB 240):** Texas healthcare facilities must adopt a workplace-violence prevention policy/plan, train annually, and implement response/post-incident practices—assessments should document hazards and mitigation consistent with the plan.

Florida

- **Florida Safe Schools Assessment Tool (FSSAT):** Public schools must complete an annual **school security risk assessment** in the FSSAT system, with state-set windows (templates released by May 1; submissions typically due by October 1). The FSSAT specifically calls out threats, vulnerabilities, and appropriate safety controls.

Georgia

- **School safety plans and threat assessment:** Georgia law requires each public school to maintain and regularly update a school safety plan that addresses security measures, emergency preparedness, and **school threat assessment** best practices. The state provides checklists and templates through GEMA/HS that include assessment elements.