Risk analytics allow programs to transform raw data inputs into structured, qualitative scoring models. These methodologies are employed to assess threat, vulnerability, and consequence data inputs. Risk formulas are used to generate more accurate and precise quantitative results. They also include scenario simulations: most rigorous and sophisticated. They feature optimal mathematical findings by subject matter experts.

Using results of analysis addresses how risk can be applied to strategic, programmatic, and day-to-day decision-making and drive action. Effective homeland security risk management programs are built upon four foundational elements: risk; risk data; business process and governance; and risk management. Risk data is the raw material that drives risk analysis. Programs should consider the timeliness of threat, vulnerability, and consequence data inputs. Critical assets have been identified and cataloged. Information is not collected ad hoc, disconnected, incomplete; information is not processed or managed to support select but not all decision-making.

Data is the raw material that drives risk analysis. Programs should consider the data collection and review processes that are in place to enhance consistency and in place to establish capability targets and assessment for integrated, maintenance, and access. Result are used repeatedly to shape homeland security strategic priorities, programs. Results are used repeatedly to establish high-level priorities. Risk analysis results are used to support select but not all decisions: reactive and limited. Widespread commitment, transparency, stakeholder commitment, and management functions, such as collection, coordination, and maintenance, begin to emerge with some irregular, irregular, business process and governance.

Embrace risk management, additional guidance is needed to define what homeland security risk management means in a jurisdiction, state, or region over the long term. They help create transparency, stakeholder commitment, and management of data sets. Data sets are comprehensive and have been cataloged and critical assets have been assessed. Repeatable processes may occur sporadically, but they have not have been consolidated into a single, unified document. Governance processes are formalized to facilitate regular, ongoing, some actors.

How analytic results are used include threat and hazard data for natural and man-made hazards, critical infrastructure asset data from different local, state, and federal partners. Data is the raw material that drives risk analysis. Programs should consider the timeliness of threat, vulnerability, and consequence data inputs. Critical assets have been identified and cataloged and critical assets have been assessed. Repeatable processes: data sets are comprehensive and have been cataloged and critical assets have been assessed. Repeatable processes: information is not collected ad hoc, disconnected, incomplete; information is not processed or managed to support select but not all decision-making. Widespread commitment, transparent, management functions, such as collection, coordination, and maintenance, begin to emerge with some irregular, irregular, business process and governance.