2023 London Open House Festival Security Risk Management Project

Hsin Hua Sung

2023 London Open House Festival Security Risk Management Project

Introduction

The 2023 London Open House Festival will officially begin on September 10th. More than 800 buildings will be open to the public over the two weekends, expected to attract over 250,000 visitors. To ensure visitor safety, this project presents our approach and process for managing security risks in response to concerns raised by the Mayor's Office for Policing and Crime (MOPAC). To allocate the limited resources effectively and efficiently, we adopt the ISO 31000 standard (ISO, 2018) to conduct a systematic and structured risk management process. This approach will enable us to identify potential risks, prioritise vulnerable targets, and make objective decisions on risk treatment options.

General Approach

Our risk management (RM) process adheres to the core principles captured by six questions. During the risk assessment phase, we consider: (1) What are the potential risks? (2) What is the likelihood of the risks occurring? (3) What would be the consequences of those risks? (Kaplan & Garrick, 1981). As for RM, we address the following questions: (4) What actions can be taken, and what options are available to manage the risks? (5) What are the associated costs, benefits, and risks of each option? (6) What could be the future implications of our present RM decisions? (Haimes, 1991, 1998; Leung, Lambert & Mosenthal, 2004).

Meanwhile, our plan adopts the core principles of the ISO 31000 standard (ISO, 2018), which involve:

- Integrating RM as an integral part of all organisational processes and activities.
- Adopting a structured and comprehensive approach to ensure productivity and efficacy.
- Tailoring the RM process to the external and internal context to achieve objectives.
- Involving stakeholders to ensure their needs and expectations are considered.
- Maintaining a dynamic approach that can anticipate, detect, acknowledge, and respond to changes.
- Explicitly considering the best available information and acknowledging any limitations.
- Recognising the influence of human and cultural factors on all aspects of RM.
- Continually improving the RM process through learning and experience.

Scope, Context and Criteria

The first step of our RM process is to establish the context, which involves setting objectives and scope, defining external and internal parameters, identifying relevant stakeholders, and defining risk criteria (ISO, 2018).

To better tailor our security approach to meet the expectations and needs of stakeholders, we will adopt the following methods to identify potential stakeholders:

- Intuitive Method: Brainstorm to generate ideas for relevant stakeholders, such as visitors, volunteers, building managers, security personnel, local residents, etc.
- Document Analysis: Examine previous event reports, audit reports, inspections, site visit reports, and insurance claim reports; gather feedback from stakeholders on official event websites, news, social media or forums.

- Stakeholder Consultation: Conduct surveys, questionnaires, interviews or focus group discussions with stakeholders to explore their interests, tasks, roles, mandates, influence, resources, perceived problems, and required actions.

The collected data will be organised to list the stakeholders' expectations or criteria for judging event performance. As shown in Figure 1, the power versus interest grids will be used to group stakeholders based on their interests and power, allowing for classification and prioritisation (Eden & Ackermann, 1998; Bryson, 2004). To verify the results, we will monitor stakeholder feedback, conduct observations, and post-event evaluations.

Once the above factors are identified, a risk assessment plan will be developed, which outlines the objectives, scope, methodology, criteria, timeline, resources, roles and responsibilities to guide the assessment process.

Risk Assessment

1. Risk Identification

In the stage of risk identification, the primary objective is to recognise and describe risks that may have an impact on the stakeholders' objectives (ISO, 2018).

To comprehensively assess risk, we attempt to generate discrete, ideally non-overlapping, categories of scenarios. A risk event can be an event summarising a set of scenarios, or a state observed within a set of scenarios, such as an initiating event or an impact event. Risk events can be framed and defined in terms of stakeholder goals, unwanted changes in system state, or criminal actions; for instance, a decrease in visitor numbers, building damage, terrorists detonating an explosive device in a building, and so on.

To identify and create a preliminary list of risk events, we will use the following methods:

- Intuitive Method: Brainstorm to identify categories of scenarios worth examining in the risk analysis stage.
- Site Walkthrough: Conduct a walkthrough of the buildings and surroundings to identify potential hazards and security vulnerabilities.
- Document Analysis: Review existing building plans, emergency plans, and previous reports to identify potential risks.
- Risk Register: Build a list of risks based on past accidents or near-misses.
- Stakeholder Consultation: Engage with stakeholders to gather their input and perspectives on potential risks.
- Intelligence Gathering: Monitor news reports and intelligence sources to stay informed about emerging threats.
- Tabletop Exercises: Conduct exercises to simulate potential risk events and test response plans.

After identification, the risk events will be filtered based on their relevance and impact. Filtering criteria will include decision-making level, scope, and temporal domain (Haimes, Kaplan, & Lambert, 2002). The results will then be validated to improve quality by conducting further analysis, simulations, or obtaining stakeholder feedback.

2. Risk Analysis

In this stage, we aim to develop a detailed understanding of the risk events, including their underlying causes, contributing factors, and potential consequences. This involves generating specific classes of scenarios to estimate their severity. To better analyse the consequence and likelihood, we will review existing measures and conduct a vulnerability assessment.

(1) Scenario Structuring

To identify potential sequences of events preceding or following the risk events, it is crucial to consider the mechanisms and factors involved in the chain of events. The bowtie approach will be employed to identify and visualise additional scenarios related to the risk events.

As eliminating potential risk scenarios may introduce bias and uncertainty into the outcome of the risk analysis, it is crucial to exercise caution when outlining the main scenarios (Kaewunruen, Alawad, & Cotruta, 2018). To address this issue, the Hierarchical Holographic Modeling (HHM) will be applied to generate a wider range of scenarios (Figure 2). We will then use fault tree and event tree diagrams to conduct cause and consequence analysis (Figure 3). These diagrams are preliminary and will be refined during the formal RM process.

(2) Vulnerability Assessment

To assess potential vulnerabilities, existing security measures will be reviewed. We will identify the existing measures or controls that are already in place. This involves existing policies, procedures, or guidelines related to event management and security, as well as physical equipment currently in use.

Next, a vulnerability assessment will be carried out to identify the critical assets and potential vulnerabilities that could result in safety hazards or operational failures. This includes assessing the physical festival grounds, infrastructure, information systems, and other resources necessary for the event's success. (Kaewunruen, Alawad & Cotruta, 2018) The assessment will be evaluated in terms of its defensive properties, which could be broadly categorised as redundancy, robustness, resilience, and security (Haimes, Kaplan & Lambert, 2002).

(3) Risk Estimation

Further, the severity of risk scenarios will be estimated by the joint effect of consequence and likelihood. Consequence assessments will consider safety, reputation, performance, services, financial loss, and other relevant aspects. The likelihood of risk scenarios will be estimated based on available historical data. However, when data are scarce, expert opinion will be necessary (Othmane et al., 2015).

To estimate the severity of each risk scenario, we will use a severity-scale matrix based on qualitative scales for consequence and likelihood (Figure 4). This matrix will help us categorise each scenario as low, medium, high, or extremely high severity (Leung, Lambert, & Mosenthal, 2004).

For risk scenarios with high and extremely high severity, we will use event trees to quantify the likelihood of a specific outcome by tracing all possible branches from the initiating event to the leaves of the tree (Figure 5). The probability of each branch is assigned to represent the relative likelihood of the outcome of that branch. The probabilities at each node are assessed

conditionally under the assumption that all the preceding events leading up to that node are true (Ezell et al., 2010).

In the case of terrorist attacks, due to the scarcity of data, the Bayesian approach will be utilised to quantify the likelihood of each scenario based on subjective probabilities and all relevant available evidence (Haimes, Kaplan, & Lambert, 2002; Aven & Zio, 2011). Terrorist attacks can result in various consequences such as environmental damage, social impact, economic loss, and casualties, and even unsuccessful attacks can cause mass panic, indirectly affecting the stakeholders' goals. To estimate these losses, game-theory methods and modelling approaches such as event trees, fault trees, and decision trees will be employed (Kaewunruen, Alawad & Cotruta, 2018). The losses will be converted into a single value, and casualties will be priced through insurance data to reflect expected economic losses. The risk of a terrorist attack can be quantified as the product of the threat, vulnerability, and expected consequences, i.e., Risk = p(attack occurs) * p(attack causes damage|attack occurs) * E[damage|attack occurs and causes damage] = threat * vulnerability * expected consequences (Willis, 2007).

3. Risk Evaluation

In this phase, we will compare the estimated risks with criteria to determine their significance and decide whether they are acceptable or require mitigation or management. The risk criteria are directly linked to the stakeholders' goals and risk scenarios are evaluated against them. The risk evaluation process considers factors including the organisation's risk appetite, risk tolerance, potential thresholds, and strategic objectives.

In rational decision-making, a feasible alternative must meet or exceed a threshold value for each criterion to be considered for selection. Multi-criteria decision-making involves evaluating feasible alternatives based on several criteria simultaneously. Each criterion is assigned a weight (ωi) reflecting its relative importance compared to other criteria.

Risk Treatment

Risk treatment aims to ensure that effective strategies are in place to minimise the frequency and severity of identified risks. We will develop and implement appropriate risk treatment strategies, including risk avoidance, risk reduction, risk sharing or risk acceptance.

To determine the most effective risk treatment options while considering budgetary constraints, a complete quantitative decision analysis will be conducted, including estimates of costs, performance benefits, risk reduction, and management options. Expert judgment will be employed to generate quantitative estimates of damage and costs, and damage probability distributions can be generated using the triangular method (Haimes, 1998). A multi-objective trade-off analysis will be employed to evaluate RM options, enabling decision-makers to choose from a set of Pareto-optimal options (Leung, Lambert & Mosenthal, 2004).

Monitoring and Review

Continual monitoring and review of the RM process are essential to ensure that important scenarios are not overlooked, and emerging threats are addressed. This includes monitoring changes in the tolerance for certain risks and assessing the adequacy of controls (The University of Adelaide, 2019). The involvement of stakeholders can help identify scenarios that may have been filtered out in the initial stage.

Recording and Reporting

A structured recording and reporting process is crucial to confirm the effectiveness of the RM process and ensure accountability. A risk register will be used to record the identified risks, their significance, rating, and how they are managed or treated (The University of Adelaide, 2019). The process, outcomes, and decisions will be reported to stakeholders.

Communication and Consultation

Effective communication and consultation are significant to the success of the RM process. This ensures that relevant stakeholders and those responsible for implementing RM are properly informed.

Conclusion

The ISO 31000 standard provides a systematic and structured framework for managing the security risks associated with the Open House Festival. Our risk management approach incorporates both qualitative and quantitative methods to enable objective decision-making and to ensure that limited resources are directed to the most critical risk scenarios. The entire process revolves around meeting stakeholders' goals, and their timely involvement is critical at every step. Feedback from stakeholders will be incorporated to continuously improve the process. As circumstances change and new information becomes available, ongoing monitoring and modification of treatment strategies are necessary to ensure their effectiveness.

References

International Organization for Standardization. (2018). *ISO 31000: Risk Management: Guidelines*. ISO.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, 1(1), 11-27.

Haimes, Y. Y. (1991). Total risk management. *Risk Analysis*, 11(2), 169-171.

Haimes, Y. Y. (1998). Risk Modeling, Assessment, and Management. New York: John Wiley and Sons.

Leung, M., Lambert, J.H. and Mosenthal, A. (2004) 'A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks', *Risk Analysis*, 24(4), 963–984. Available at: https://doi.org/10.1111/j.0272-4332.2004.00500.x.

Eden, C. and Ackermann, F. (1998) Making Strategy: The Journey of Strategic Management, London: Sage Publications.

Bryson, J. M. (2004). What to do when stakeholders matter: stakeholder identification and analysis techniques. *Public management review*, 6(1), 21-53.

Haimes, Y.Y., Kaplan, S. and Lambert, J.H. (2002) Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling, *Risk Analysis*, 22(2), 383-397. Available at: https://doi.org/10.1111/0272-4332.00020.

Kaewunruen, S., Alawad, H. and Cotruta, S. (2018) A Decision Framework for Managing the Risk of Terrorist Threats at Rail Stations Interconnected with Airports, *Safety*, 4(3), 36. Available at: https://doi.org/10.3390/safety4030036.

ben Othmane, L., Ranchal, R., Fernando, R., Bhargava, B. and Bodden, E. (2015) Incorporating attacker capabilities in risk estimation and mitigation. *Computers & Security*, 51, 41-61.

Ezell, B.C. et al. (2010) Probabilistic Risk Analysis and Terrorism Risk, *Risk Analysis*, 30(4), 575-589. Available at: https://doi.org/10.1111/j.1539-6924.2010.01401.x.

Aven, T., & Zio, E. (2011). Some considerations on the treatment of uncertainties in risk assessment for practical decision making. *Reliability Engineering & System Safety*, 96(1), 64-74.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis: An International Journal*, 27(3), 597-606.

The University of Adelaide (2019) *RISK MANAGEMENT Legal and Risk Handbook*. 12-22. Available at: https://www.adelaide.edu.au/legalandrisk/system/files/media/documents/2019-04/Risk%20Management%20Handbook%20-%20April%202019.pdf

Břeň, J., & Zeman, T. (2017). Fault tree analysis of terrorist attacks against places of worship. In 2017 2nd *International Conference on System Reliability and Safety (ICSRS)* (531-535). IEEE.

Appendix

Figure 1. Power versus interest grids. Stakeholders will be grouped into 4 categories: players with high interest and significant power; subjects with interest but little power; context-setters with power but little direct interest; and the crowd with little interest and power (Eden and Ackermann, 1998; Bryson, 2004).

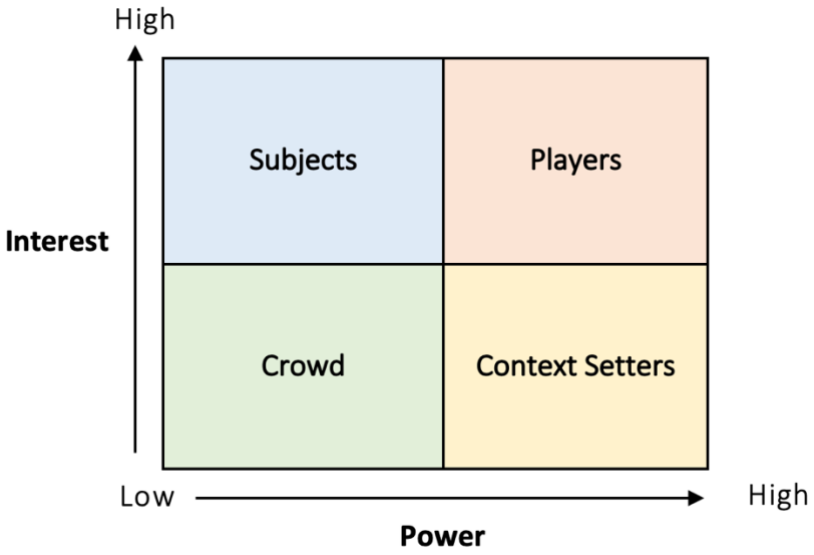

Figure 2. Hierarchical Holographic Modeling (HHM) can be applied to generate a wider range of scenarios.

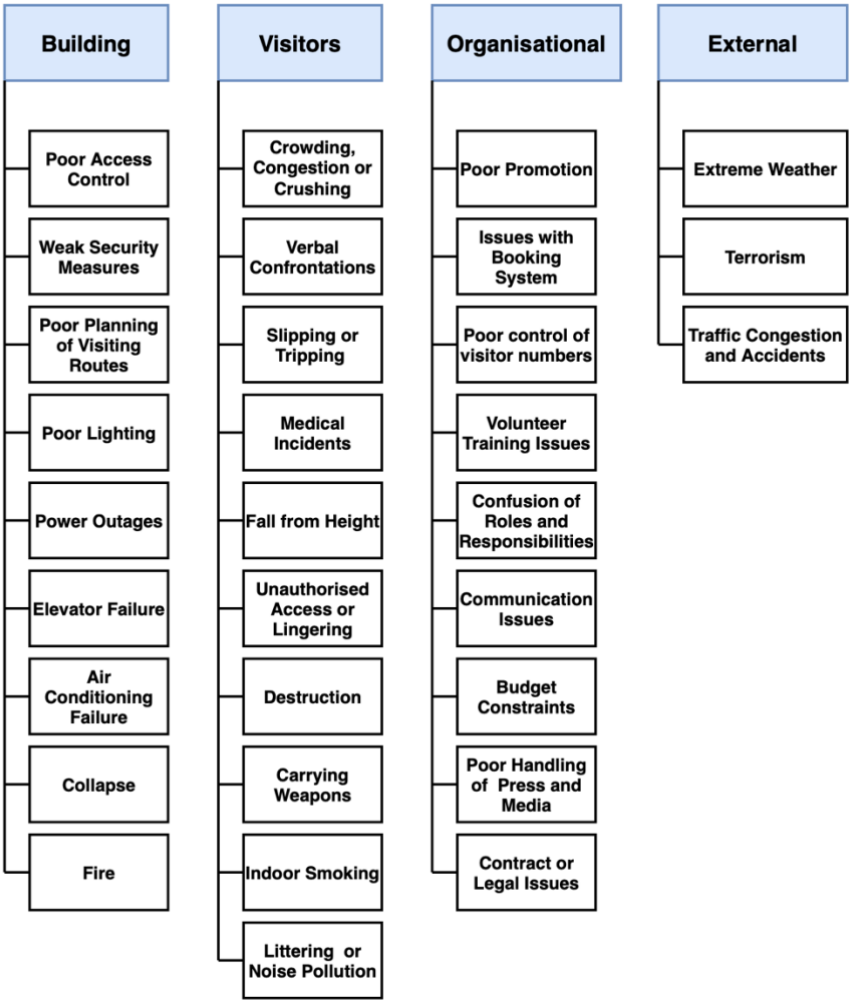

Figure 3. Fault tree. This diagram uses the scenario of terrorists entering a building with weapons as an example to analyse the factors involved (Břeň, J., & Zeman, T., 2017).

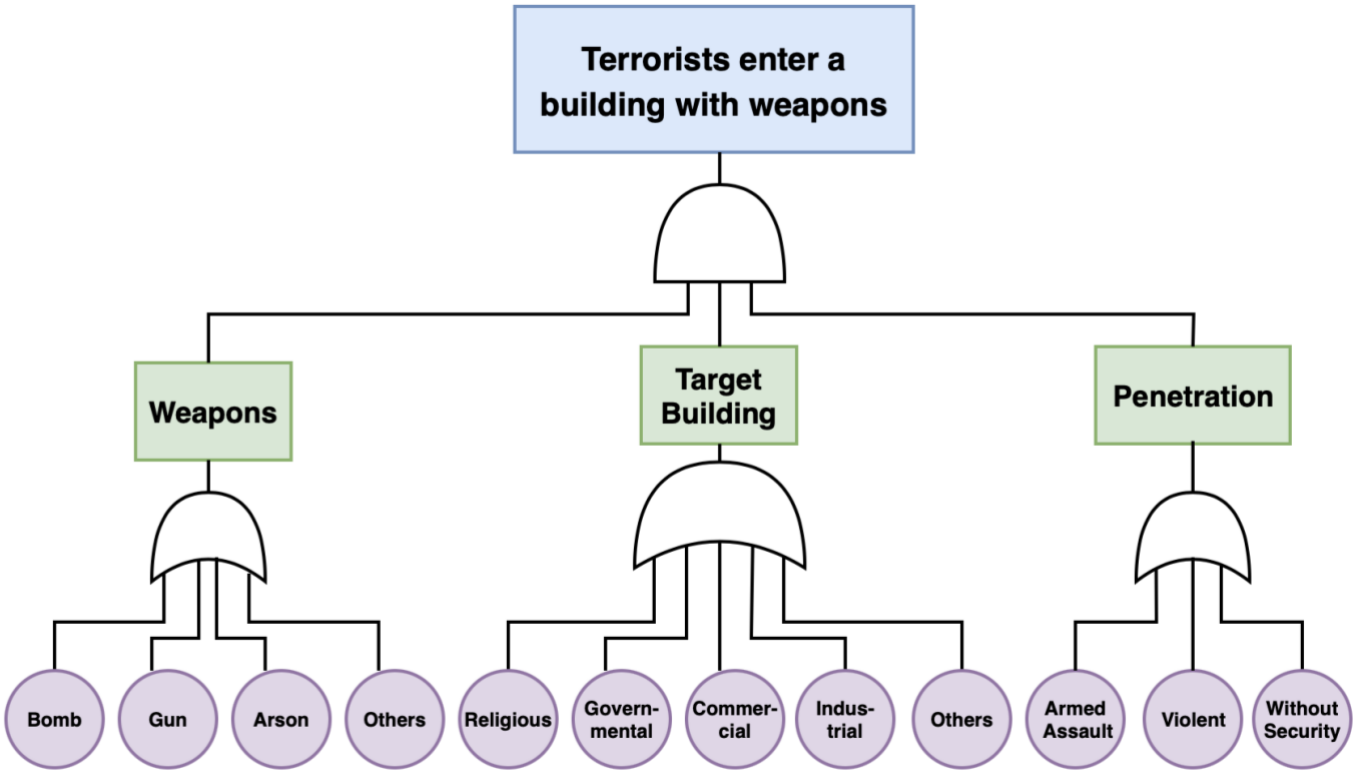

Figure 4. Severity-scale matrix. The matrix shows the combination of likelihood and consequence to assess severity, and risk scenarios can be mapped into the matrix for initial filtering before quantitative estimation.

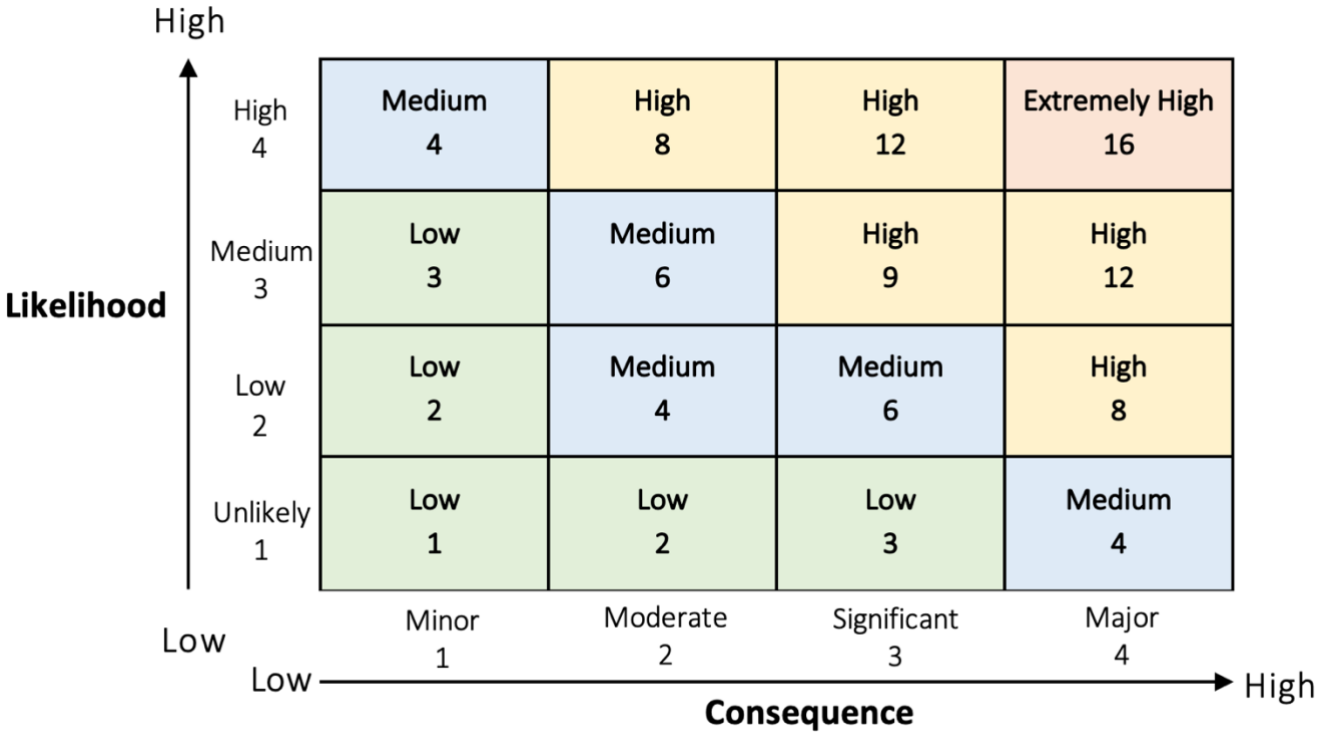

Figure 5. Event tree. This diagram uses terrorist attacks as an example to explain the way we calculate the likelihood through event trees. Each branch has a corresponding probability value (represented by P), which helps calculate the likelihood of each scenario.