Modifying Risk: The Nexus between Likelihood, Consequence & Risk Control Measures

Peter Ashwin
Principal

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Revised: July 13, 2020

Today’s Global Risk Society

In today’s uncertain and complex world, event organizers, venue operators, cities, production companies & non-profit organizations find themselves operating in an uncertain environment with evolving risks ranging from homegrown violent extremism, cyber-criminals disrupting IT networks, event cancellations due to Covid-19 and a disrupted supply chain for people, products and services.

ERMS EVENT RISK MANAGEMENT SOLUTIONS

…we must identify and prioritize risks – understand the threat, the vulnerability and the consequence, and then apply resources in a cost-effective manner…

Michael Chertoff
Director, Dept. Homeland Security (2006)

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Proactive vs Reactive Risk Management

A proactive risk mitigation strategy identifies both the known and unknown risks, then evaluates and selects the most appropriate risk treatment (mitigation) option to reduce the designated risk to "a level as low as reasonably possible" (ALARP).

Risk mitigation focuses on implementing risk control measures that target reducing the likelihood of the risk event occurring and, in the case, the risk event occurs, minimizing the severity of potential consequences.

ERMS EVENT RISK MANAGEMENT SOLUTIONS

What is Risk?

the **loss or gain** arising from **people, systems or external events** which have the **potential** to **cause** the organization to deviate from its objectives

Risk Management Institute of Australasia

…the **effect** of **uncertainty** on **objectives** …

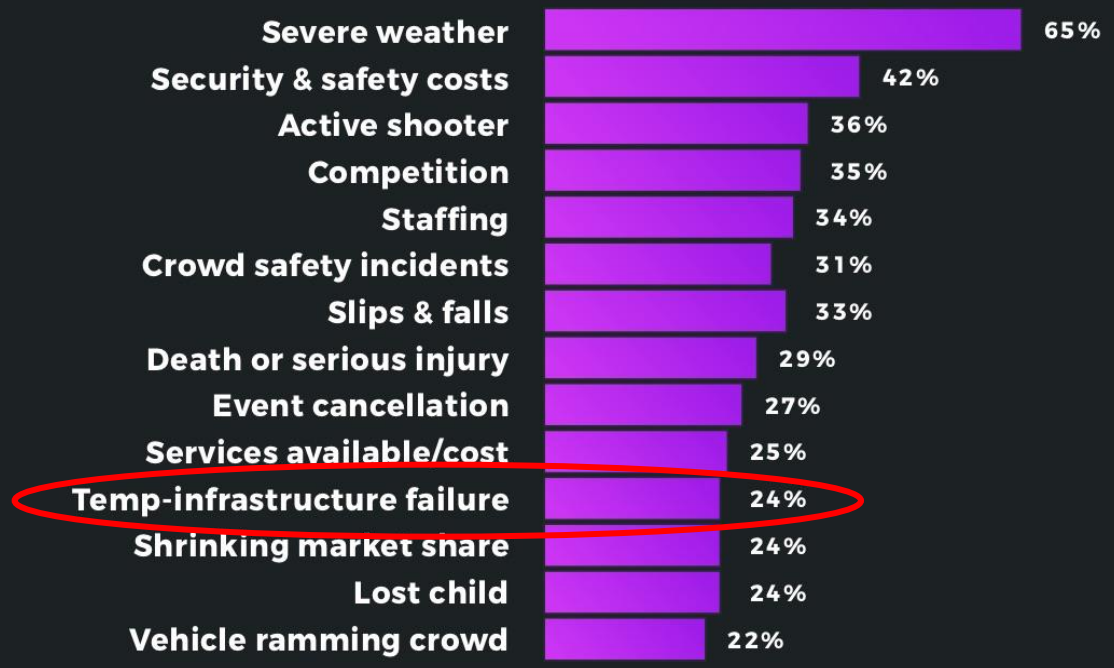
An effect is a deviation from the expected; it can be positive, negative or both.

ISO 31000 (2018) Risk Management

ERMS + Blerter

5

What you are most worried about...



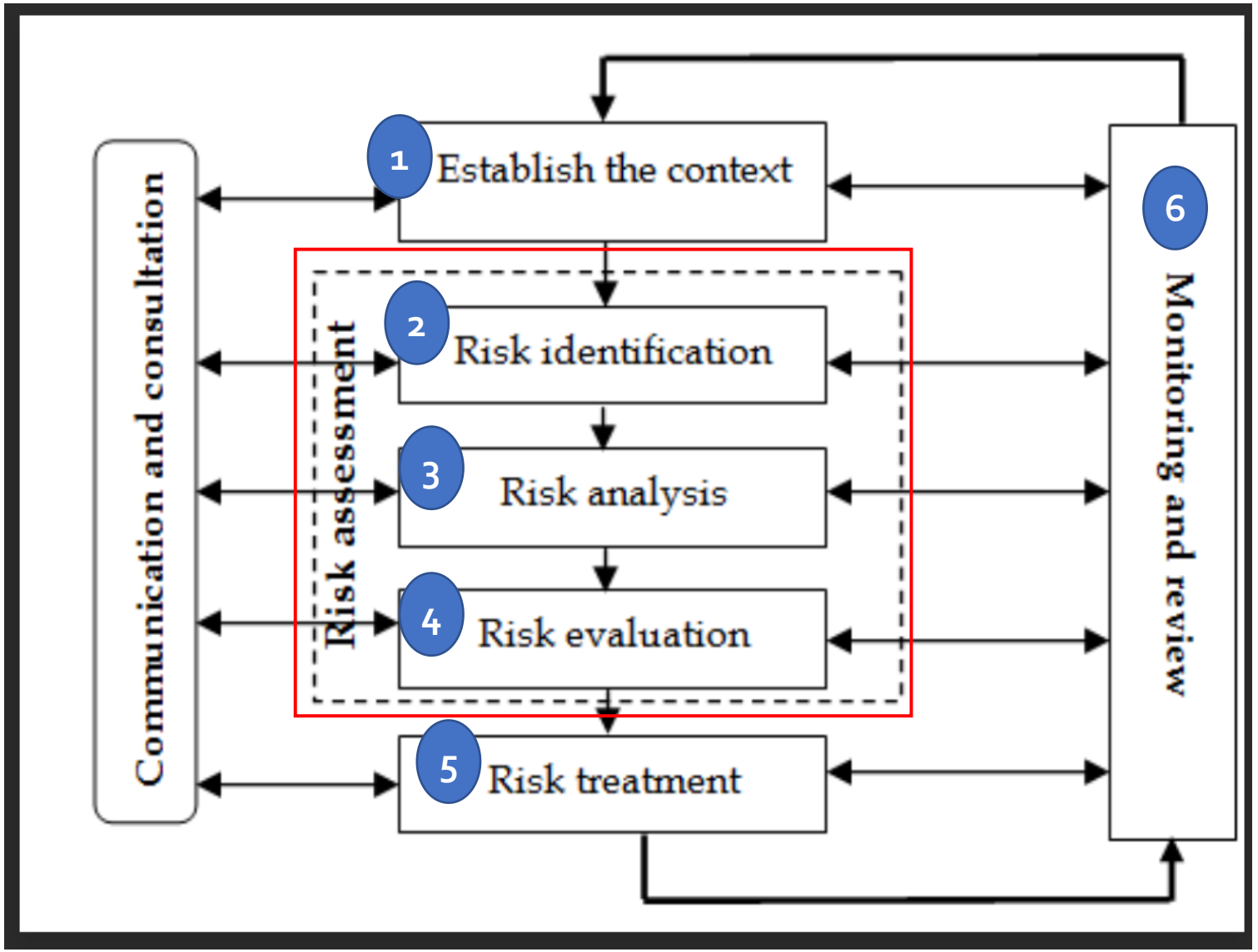
What is actually happening at your events...

What is Risk Management ?

the **identification, assessment, and prioritization of risks**, followed by the coordinated and economical application of resources, to minimize, monitor, and **control the probability** and/or **impact** of unfortunate events

DHS Risk Lexicon

Event Risk Management Framework



Source: ISO 31000 (2018) Risk Management - Guidelines

ERMS EVENT RISK MANAGEMENT SOLUTIONS

"Yesterdays Incident is Tomorrows Risk"™

A Simplified Approach to Event Risk Assessments

1. What **could** happen (risk)?
2. What would **cause** it to happen (source)?
3. What are the potential **consequences** (impact)?
4. What can we do **to prevent** it (controls to reduce likelihood)?
5. What can we do to **minimize the consequences** (controls to reduce severity)?

ERMS EVENT RISK MANAGEMENT SOLUTIONS

"Yesterdays Incident is Tomorrows Risk"™

Event Risk Assessment & Management Framework

1. Understand your Risk Ecosystem

1.1 **Review business strategy –** what is your mission, values & objectives

1.2 Identify & document **mission critical activities**, functions & assets (people, process, information etc)

1.3 **Identify risk stakeholders** both external and internal

1.4 Establish organizational / event **criteria for risk appetite/tolerance**

1.5 Establish **criteria & rating metrics** for **likelihood & consequence**

RISK ASSESSMENT

2. Identify the Risks

2.1 **Review the risk environment / identify risks:** (1) what has happened before (incidents & claims) (2) What has happened at other events (3) what keeps you up at night (the unknowns)

2.2 **Categorize (group) risks** & document them in your **Event Risk Register**

2.3 Identify **risk sources** - the hazards & threats that may cause or trigger the risk event

3. Analyze the Risks

3.1 **Identify** existing **risk control measures**

3.2 **Benchmark existing risk controls** against industry best practices & assess "what's missing"

3.3 Evaluate & assess **effectiveness of risk controls** (gap analysis)

3.4 Conduct preliminary **business (event) impact analysis** – what are the potential impacts on our mission & objectives?

4. Evaluate the Risks

4.1 Assign **likelihood**

4.2 Assign **consequence**

4.3 Calculate **RISK LEVEL: LIKELIHOOD x CONSEQUENCE**

4.4 Assess whether the **risk level** is within risk appetite?

4.5 If no, **identify risk treatment** options

*Note: while **R=L x C** is based on semi-quantitative metrics, due to inherent subjectivity, the risk level should be regarded as a 'risk estimate' & not as a definitive risk statement*

5. Treat the Risks

5.1 **Select risk treatments: (1) accept** *risk as being "as low as reasonably possible"* **(2) Reduce** *likelihood & or consequence;* **(3) Avoid** *risk source (hazard or threat)/ cease activity;* **(4) Share /** *thin the risk through indemnification, insurance, contracts etc*

5.2 Conduct **cost benefit analysis** – does the cost justify the outcome?

5.3 Identify & assign **Risk Owners & Control Owners**

5.4 **Prioritize & rank** your risks

5.5 Draft / prepare **Event Risk Assessment & Management Plan**

6. Risk Reviews & Reporting

6.1 Establish risk governance guidelines /policy: organizational policy statement, risk working group (roles & responsibilities) & reporting format for senior management / board

6.2 Implement risk assurance program – audit & evaluation program to assess effectiveness of controls

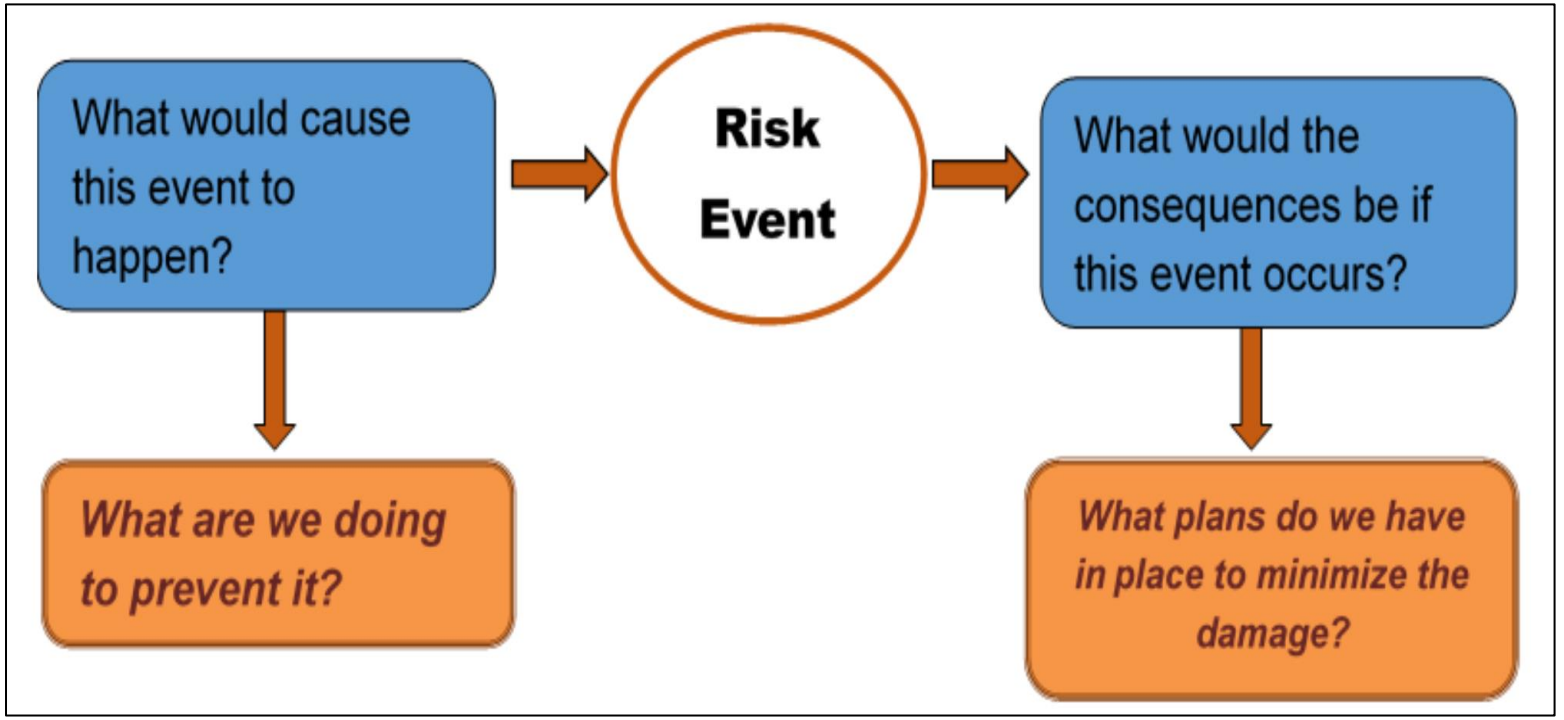
Source: Adapted from ISO 31000 (2018): Risk Management - Guidelines

Revised: 2020-07-05

Risk = Likelihood x Consequence

LIKELIHOOD
is **the chance** of something happening

CONSEQUENCE
is the **impact outcome** of a risk event



Likelihood Metrics

Rating & Descriptor		Probability	Qualitative Statement
1	Rare	<5%	**May have occurred once** in last 20 years
2	Unlikely	5-20%	**Unlikely to occur**, may occur once every 5-20 years
3	Possible	20-50%	**May occur** once every 2-5 years
4	Likely	50-80%	**Occurs frequently,** typically once every 1-2 years
5	Almost Certain	>80%	**Expected to occur** in most circumstances , typically one or more times in a 12 months

(1) Process is based subjective assessment of likelihood; data analysis from incident reporting provides a more robust assessment

(2) There is a direct correlation between the effectiveness of risk controls & likelihood (not indicated here)

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Consequence (Impact) Metrics

Impact Categories	Impact Factors	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
	Financial	Financial impact of event is less than $50,000.	Financial impact of event exceeds $50,000 but is less than $200,000.	Financial impact of event exceeds $200,000 but is less than $1 million.	Financial impact of event exceeds $1 million but is less than $10 million.	Financial impact of event exceeds $10 million.
	Human Resources	Temporary impact on ability to meet minor service commitments	HR issues temporarily impact delivery of services or compliance with partnership agreements in some areas but could be dealt with under normal circumstances.	High personnel turnover or significant understaffing is distracting management from achieving strategic objectives; and/or Widespread staff morale problems and high turnover.	Inability to retain staff to manage operations or administration sufficient to meet agreements for some key segments of the organization/partners; and/or HR issues threaten continued, effective provision of services and require senior management intervention.	Inability to retain staff to manage operations or administration results in inability to continue operations in key segment(s) of the organization; and/or Loss of multiple senior leaders.
	Health & Safety	On-site first aid to employee, volunteer, member of public and/or participant.	Off-site medical attention required to employee, volunteer, member of public and/or participant; and/or Regulatory complaint; and/or Location/activity correction mandate.	Lost time injury to employee, volunteer, member of public and/or participant; and/or Regulatory penalties of $100,000 or less; and/or Location/activity closure or investigation for up to 5 days.	Single fatality/injury resulting in long-term care and/or incapacitation injury to employee, volunteer, member of public and/or participant; and/or Regulatory penalties of more than $100,000; and/or Location/activity closure or investigation for more than 5 days.	Multiple loss of life or multiple long-term care and/or incapacitation injuries to employees/volunteers, members of public and/or participants.
	Operational	Disruption of less than 1 day would be managed by routine changes in operations. Minor impact on continuing operations and meeting customer demands.	Disruption of more than 1 day but less than 6 days managed by routine changes to operations; and/or Minor quality deficiencies are noted; and/or Minor loss of corporate memory/capacity.	Measurable impact on operations or meeting customer demand. May lose customers or smaller program/division and/or shut-down for more than 5 days during operating season.	Shut down for more than 30 days during operating season and/or loss of major customer/program and/or shut down of division. Serious quality deficiencies are noted. Serious loss of corporate memory/capacity.	Shut down of major profit centre(s) or entire business; and/or Major loss of corporate memory/capacity.
	Strategic/ Reputational	Has little impact on organization's strategic plan or objectives; and/or One negative article in one publication.	Has minor impact on organization's strategic plan and requires minor changes to 1 or more strategic objectives; and/or Negative articles in more than one publication.	At least one strategic objective of the organization will not be achieved; and/or Short term negative media focus and concerns raised by stakeholders.	Multiple strategic objectives will not be achieved; and/or Long term negative media focus and/or sustained concerns raised by stakeholders.	Strategic plan is impacted in its entirety; and/or Sport Stakeholders (NSO's, PSO's, Gov't) lose faith in, and actively disassociate themselves, from the organization.

Evaluating & Ranking Risks : 5 x 5 Matrix [Heat Map]

PROBABLILITY	RISK LEVEL				
ALMOST CERTAIN (5)	LOW (5)	MEDIUM (10)	HIGH (15)	VERY HIGH (20)	VERY HIGH (25)
LIKELY (4)	LOW (4)	MEDIUM (8)	HIGH (12)	HIGH (16)	VERY HIGH (20)
POSSIBLE (3)	LOW (3)	MEDIUM (6)	MEDIUM (9)	HIGH (12)	HIGH (15)
UNLIKELY (2)	LOW (2)	LOW (4)	MEDIUM (6)	MEDIUM (8)	HIGH (10)
RARE (1)	LOW (1)	LOW (2)	LOW (3)	MEDIUM (4)	MEDIUM (5)
CONSEQUENCE	INSIGNIFICANT (1)	MINOR (2)	MODERATE (3)	SIGNIFICANT (4)	SEVERE (5)

What are Risk Control Measures?

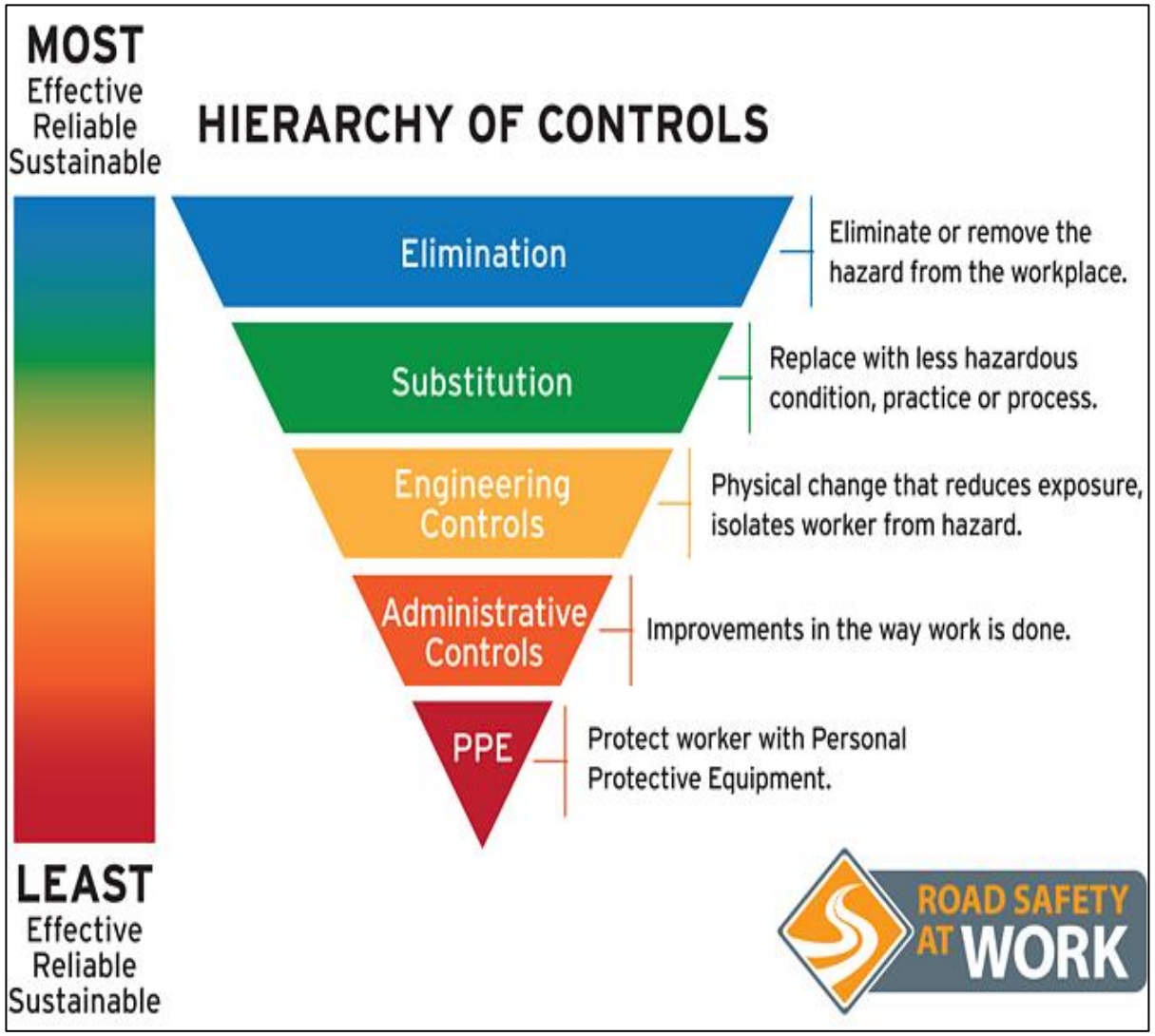
A **risk control measure** is any process, policy, device, practice, or other action that modifies risk through reducing the likelihood and, or the severity of consequences associated with the risk

ISO 31000 (2018) Risk Management – Guidelines

Critical Controls – not all controls are equal, focus should be on those controls critical to mitigating the risk or that mitigate multiple risks across the organization

Risk Control Measures

- **Preventative Controls** reduces the likelihood of the onset /trigger for the risk event
- **Detective Controls –** detects early onset of the risk or identifies failures / gaps in the existing risk control environment e.g. near misses = early warning signs
- **Responsive Controls** reduces the severity of potential consequences/impact to people, financial return & reputation (critical success factors) after the onset of the risk (business continuity)



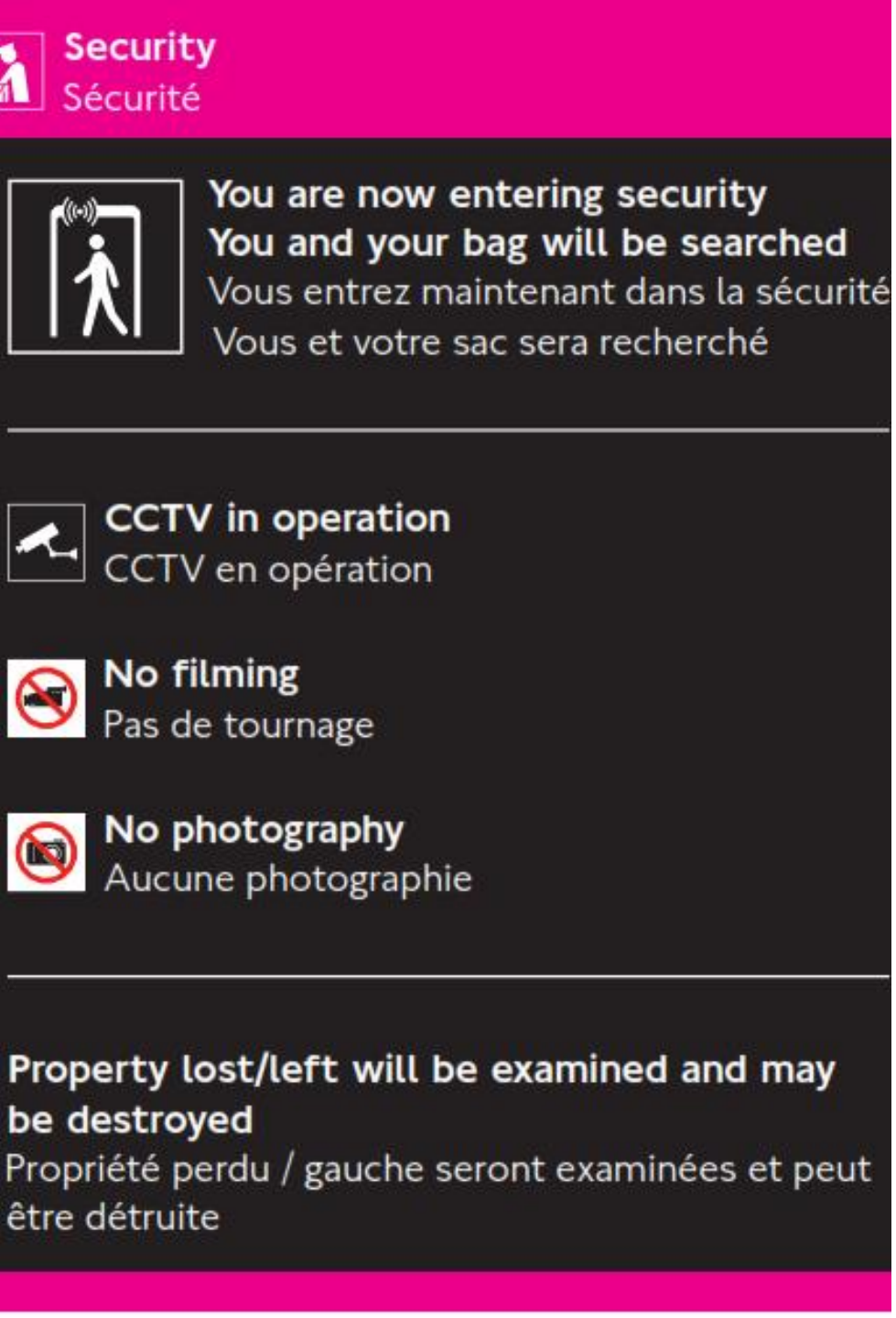
Source: Department of Transport, Queensland

Hierarchy of Controls: Safety Management Systems

Engineering Controls: Hostile Vehicle Mitigation

Bourbon Street, New Orleans

Matador Surface Mount Bollard System

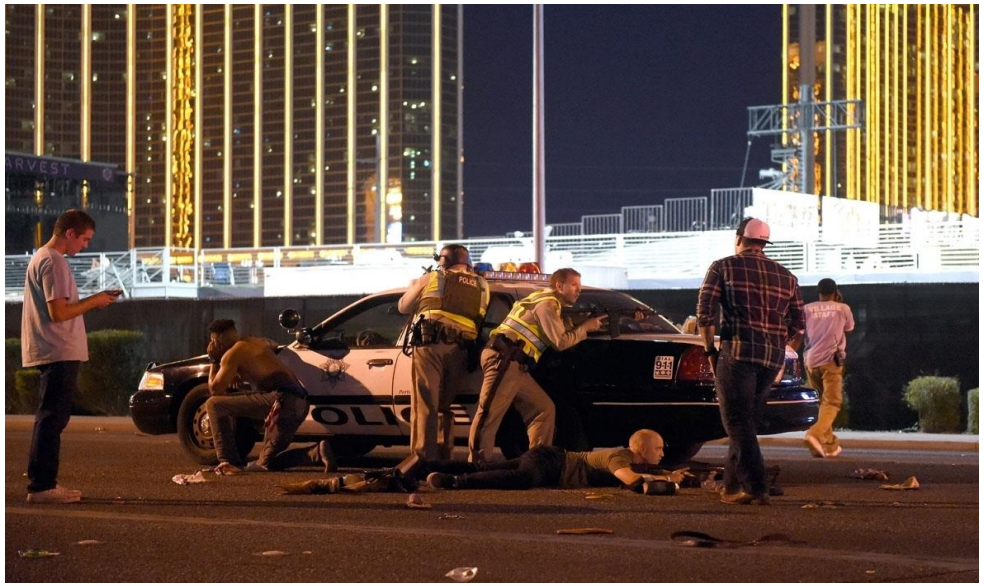


Risk Controls & Ownership: Guiding Principles

- For risk controls to be effective, **ownership and accountability** must be assigned to a responsible owner
- The risk control owner **may not** be the same person as the risk owner
- Risk Owner must understand how the control modifies risk & is responsible / accountable for monitoring and evaluating risk control effectiveness

Yesterday's Incident is Tomorrow's Risk™

A Guide to Active Shooter Risk Control Measures



Route 91 Harvest Festival, Las Vegas
10-01-2017

San Antonio Fiesta Festival sniper shooting
04-29-1979

The risk dread factor diminishes and is often forgotten over time… until it occurs again

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Case Study: Active Assailant Risk Control Measures

" A good solution applied with rigor is often better than a perfect solution applied 10 minutes later"
Patton

The following case study provides an example of mapping risk control measures (26) to an active assailant / marauding attacker 'risk event'. The risk controls matrix provides an integrated approach to mitigating the risk through identifying and documenting risk controls to reduce both the likelihood and the severity of consequences of the risk. The risk controls have also been aligned to the security-in-depth principles of "Deter, Detect, Delay, Respond (disrupt) and Recover ("D3R2").

It should be noted, that many of the identified risk controls in the active assailant matrix are also critivcal to mitigating other known event and organizational risks.

<u>Caveat:</u> This matrix is intended to provide guidance only

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Risk Mitigation Controls: Active Assailant

Preventative (Deter & Delay)*

1. Terms & conditions of entry - polices & procedures for no weapons & no bags etc
2. Staff training in hostile surveillance detection & workplace behavioral detection (change in behaviors)
3. Security screening to detect prohibited items & weapons
4. Security & police patrols in the "Last Mile" (outside the fence)
5. Perimeter fencing & signage
6. Security video surveillance systems
7. 24/7 controlled access & lockdown of event site from load-in to load-out
8. Counter sniper teams (Police)
9. Enhance liaison & coordination with external stakeholders
10. Background checks - staff, volunteers & contractors (insider threat)

Detective (Detect)

11. "See something, Say something" – threat reporting processes (unusual behavior)
12. Security video surveillance system (monitored)
13. Audits to assess effectiveness of security screening (detection) & access control
14. Controlled access & accreditation (for identity assurance)
15. Monitor social media for unusual posts / chatter
16. Conduct pre- event operational readiness & preparedness – test & validate plans through tabletop exercises, walkthroughs with all stakeholders & drills to validate ERPs, communications & decision-making protocols

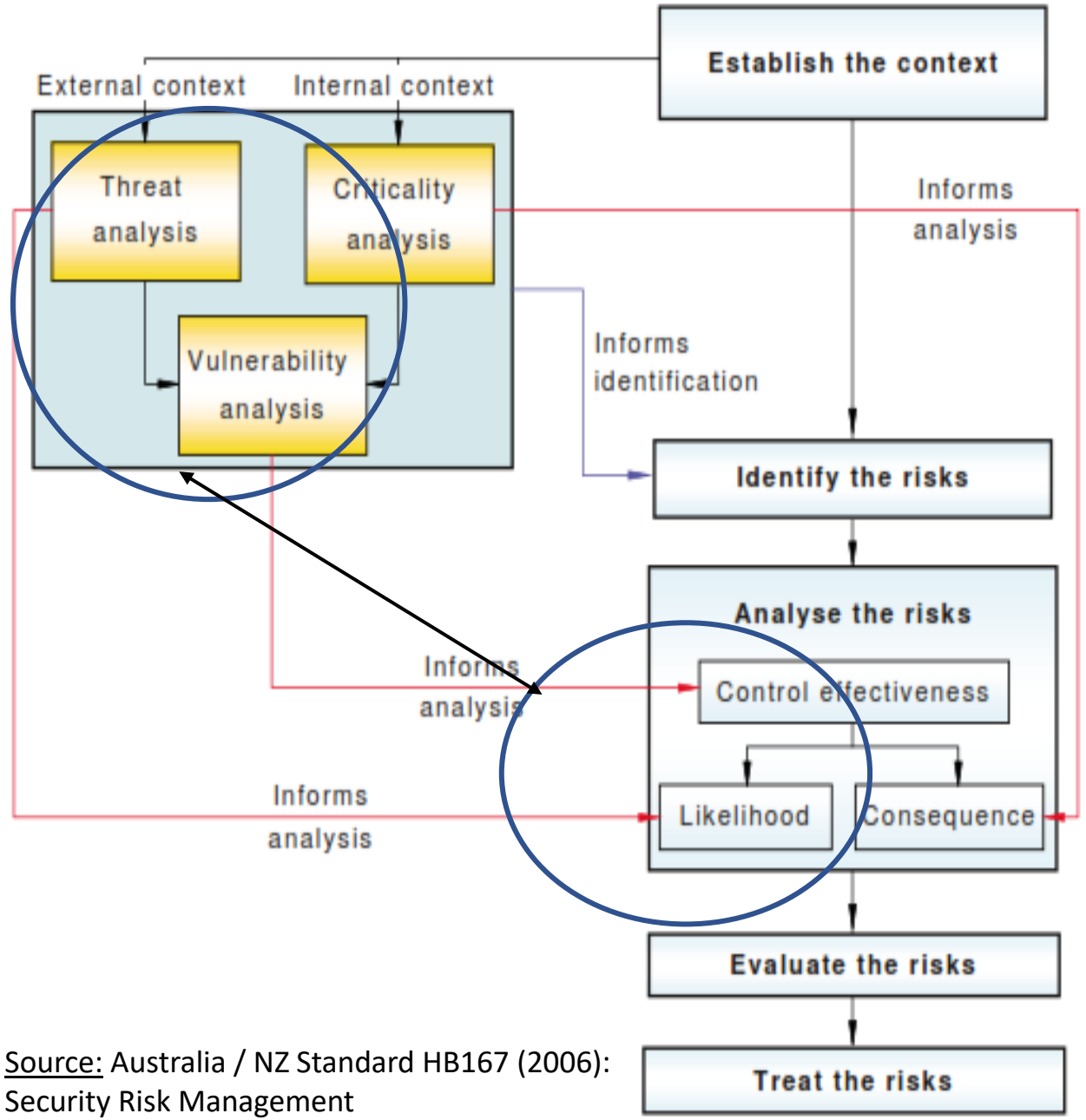
Reactive / Corrective (Respond & Recover)

17. Plans & Procedures: Event Security & Safety Management Plan & Emergency Response Procedures
18. Unified command center onsite (event ops, police & public safety)
19. Armed police response teams
20. Pre-event "just in time" team leader training – ERP drills / comms & radio tests (enhances response)
21. Front line staff trained in "stop the bleed" / bleed control kits onsite
22. EMT's onsite
23. Mass Casualty Incident Plan (led by City / Public Safety)
24. Event Insurance policies
25. Public address system / universal sound system
26. Mass notification / alert system to all staff & workforce

* Aligned to D3R2 – security principles aligned to threat design basis (TDB) methodology for security planning & design

The Relationship between Vulnerability, Control Effectiveness & Likelihood

- A direct correlation exists between likelihood of a risk event occurring and the effectiveness of existing risk control measures.
- Control measures should be audited ("trust but verify") to assess effectiveness and identify gaps.
- Audits and assessments provide insights into an organization's resilience to uncertainty; the ability to respond and manage the "unknowns".



Source: Australia / NZ Standard HB167 (2006): Security Risk Management

ERMS EVENT RISK MANAGEMENT SOLUTIONS

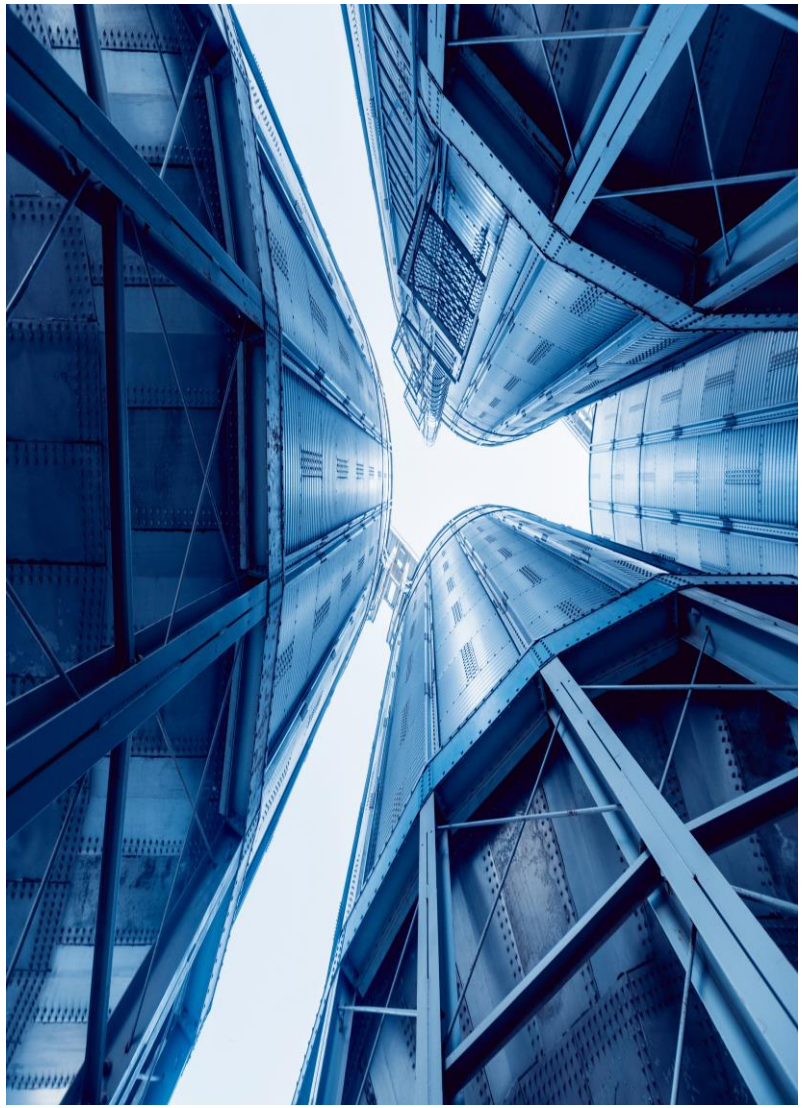
Assessing Risk Control Measure Effectiveness

Risk Control Self Assessment (RCSA) is a technique based on qualitative criteria to evaluate effectiveness of risk control measures.

INEFFECTIVE	• The control has not been implemented or significant control gaps exist that result in the control not modifying either the likelihood or consequences of the risk • No Control Owner assigned
PARTIALLY EFFECTIVE	• Some control gaps (- that result in the control having limited influence on risk level (incidents or near misses recorded); some improvement or strengthening of the control is required • Control Owner has been assigned; monitoring and assessment of risk controls may be limited
EFFECTIVE	• No control gaps; assessed as effective in mitigating the risk. • Ongoing monitoring by Control Owner through risk control self assessment

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Trust but Verify: Risk Controls Assurance & Monitoring



Three Lines of Defense (LoD)

Without a cohesive, coordinated approach, limited risk and control resources may not be deployed effectively, and significant risks may not be identified or managed appropriately.
(The Institute of Internal Auditors, 2013)

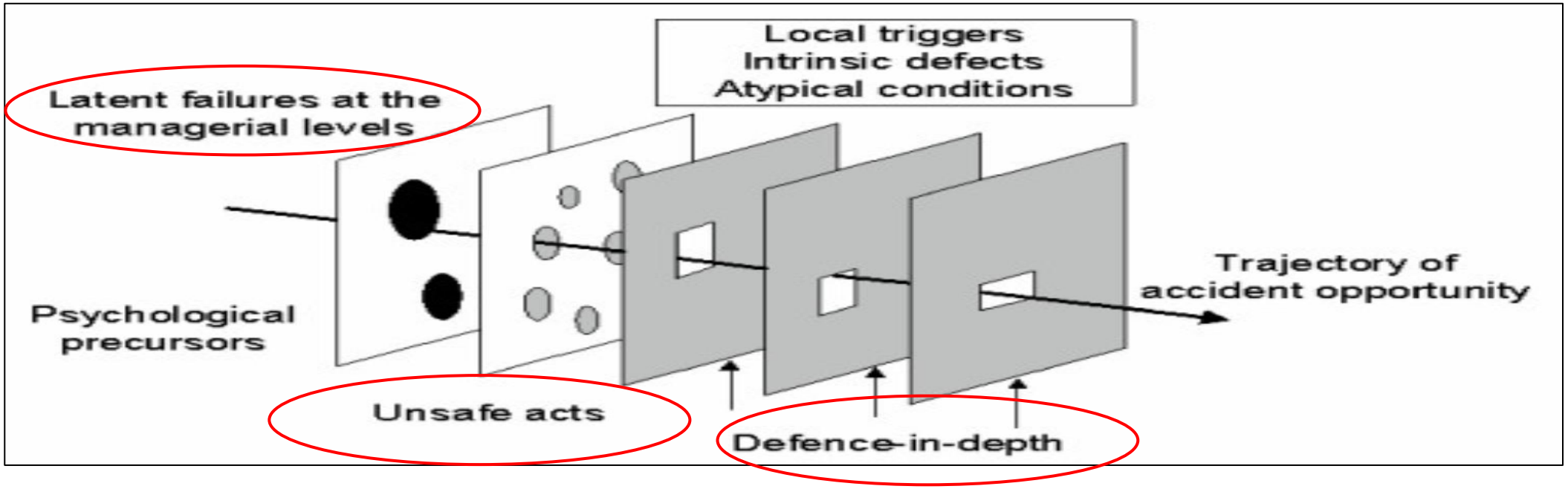
(1) **Risk Control Self-Assessment by Control Owner** to evaluate/assess effectiveness of controls, reported back to the Risk Owner

(2) **Internal review/audit by the Risk Owner –** reported to Risk Working Group/ Committee

(3) **External 3rd party** independent audits & assessment/evaluation of risk controls (most effective of the 3 LoD)

The Theory of Accident Causation: the Swiss Cheese Model

- **Multiple layers of defense (controls)** are required to prevent a single point of failure between the risk source (hazard or threat) and the "risk event"; provides redundancy and resilience to prevent a "risk event" from occurring, if one control fails or is flawed
- Incidents **rarely result from a single cause** but rather by **multiple failures of controls** that coincide and collectively result in an **exceptional event** with **catastrophic consequences**

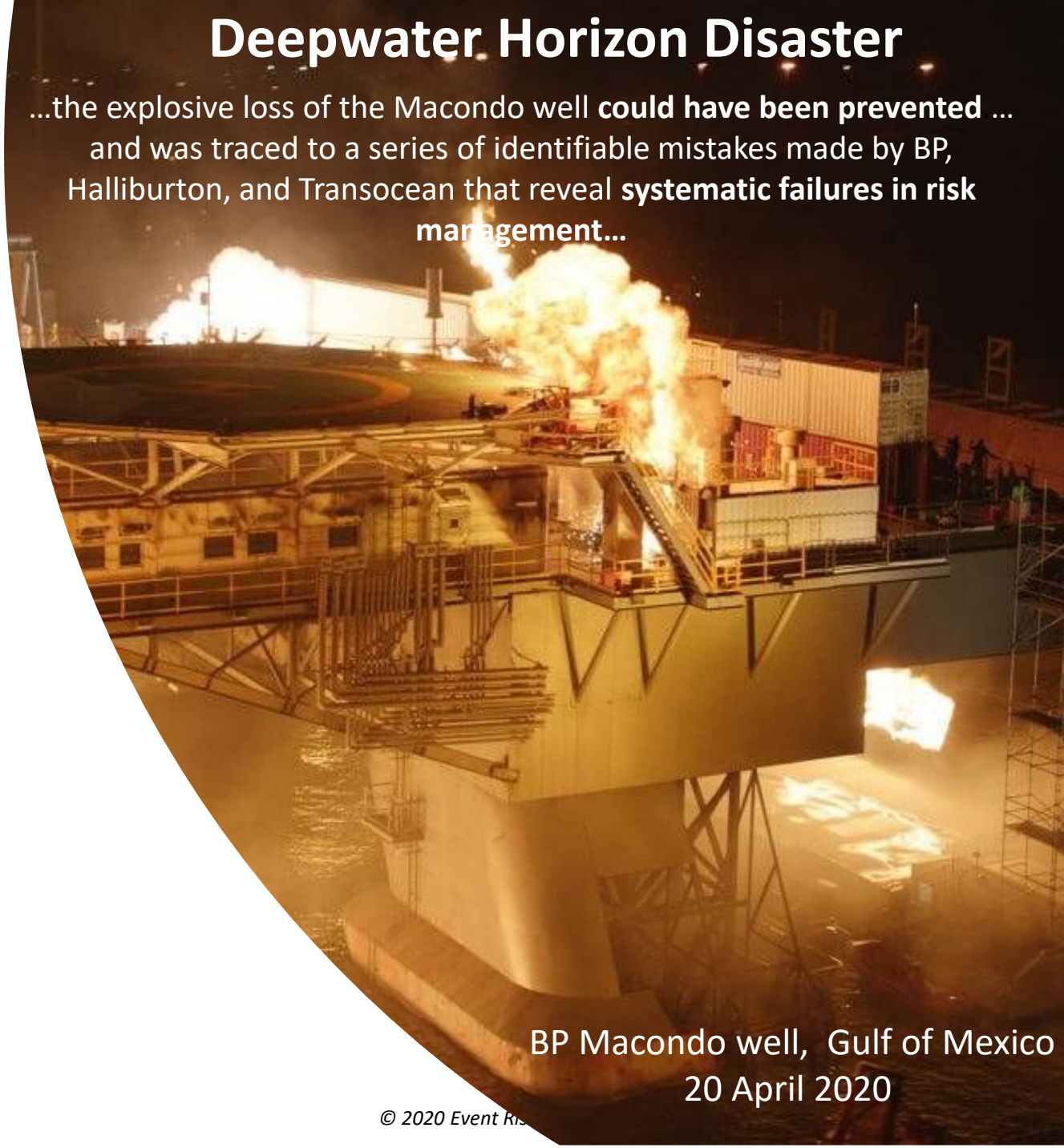


Source: Swiss Cheese Model of Accident Causation
James Reason (1990), University of Manchester

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Incidents or ‘risk events’ rarely occur because risk control measures were not identified or implemented, but rather designated risk control measures were ineffective or failed due to lack of managerial oversight (latent conditions)

(James Reason, 1997)



Reason, J. (1997) *Managing the Risks of Organizational Accidents.* Surrey: Ashgate Publishing Ltd.

Closing Summary

It is essential that cities, event organizers, venues and event professionals adopt a proactive approach to embedding risk management practices that inform risk-based decisions to prioritize efforts to enhance organizational resilience, delivery of a safe and secure guest experience, while protecting reputation and pursuing business opportunities within today's uncertain and complex global risk environment.

ERMS EVENT RISK MANAGEMENT SOLUTIONS

Yesterday's Incident is Tomorrow's Risk™

For more information on Enterprise Risk Management, Event Security & Organizational Resilience solutions, contact:

Peter Ashwin
Principal
peter.ashwin@ermsglobal.com
M:+1 617.396.0788

ERMS EVENT RISK MANAGEMENT SOLUTIONS