VMA

VENUE MANAGEMENT ASSOCIATION
(ASIA AND PACIFIC) LIMITED

VENUE
MANAGEMENT
SCHOOL

BUSINESS RISK & RESILIENCE COURSE NOTES

These course notes have been provided by the Venue Management Association and are provided free of charge to assist VMA members and the venue management industry manage their business during the COVID-19 crisis.

Venue Management School

The world-renowned, Australian based, Venue Management School has been cultivating the next generation of venue professionals for over 25 years and is ideal for middle to senior managers.

VMS combines the ultimate venue industry networking experience with a two-year program featuring workshops, discussions and presentations to explore 35 topics essential to the venue industry.

Executive-level venue managers with years of experience and endless industry connections, instruct each session with ready-to-implement strategies for venues of all sizes and sectors!

The Venue Management School is a program of the Venue Management Association (Asia and Pacific).

VMA
VENUE MANAGEMENT ASSOCIATION
(ASIA AND PACIFIC) LIMITED

Venue Management Association

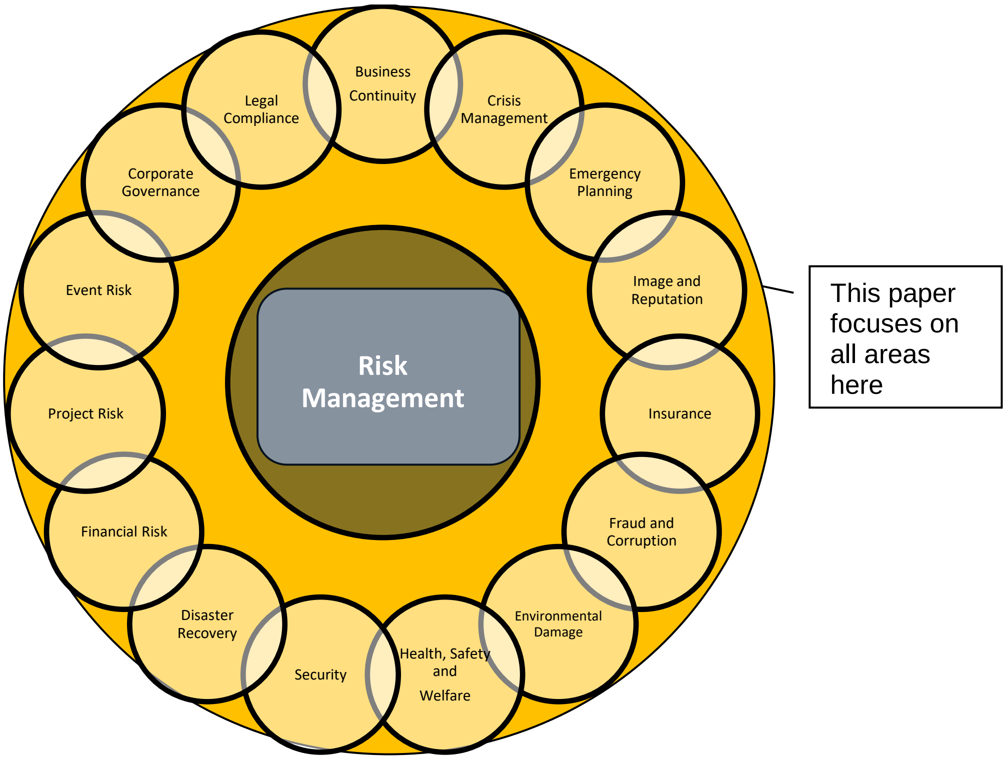
www.vma.org.au

Introduction

This session extends the knowledge of students beyond the basics of risk assessment and insurance covered in VMS Year 1 and takes a more holistic approach to understanding and dealing with risk.

There is an element of risk in everything we do; without risk, we would be unable to operate our organisations and would be unlikely to achieve our business goals. Risk relates to future uncertainty and risk management is a tool to help make good decisions based upon relevant information available to balance risk and reward.

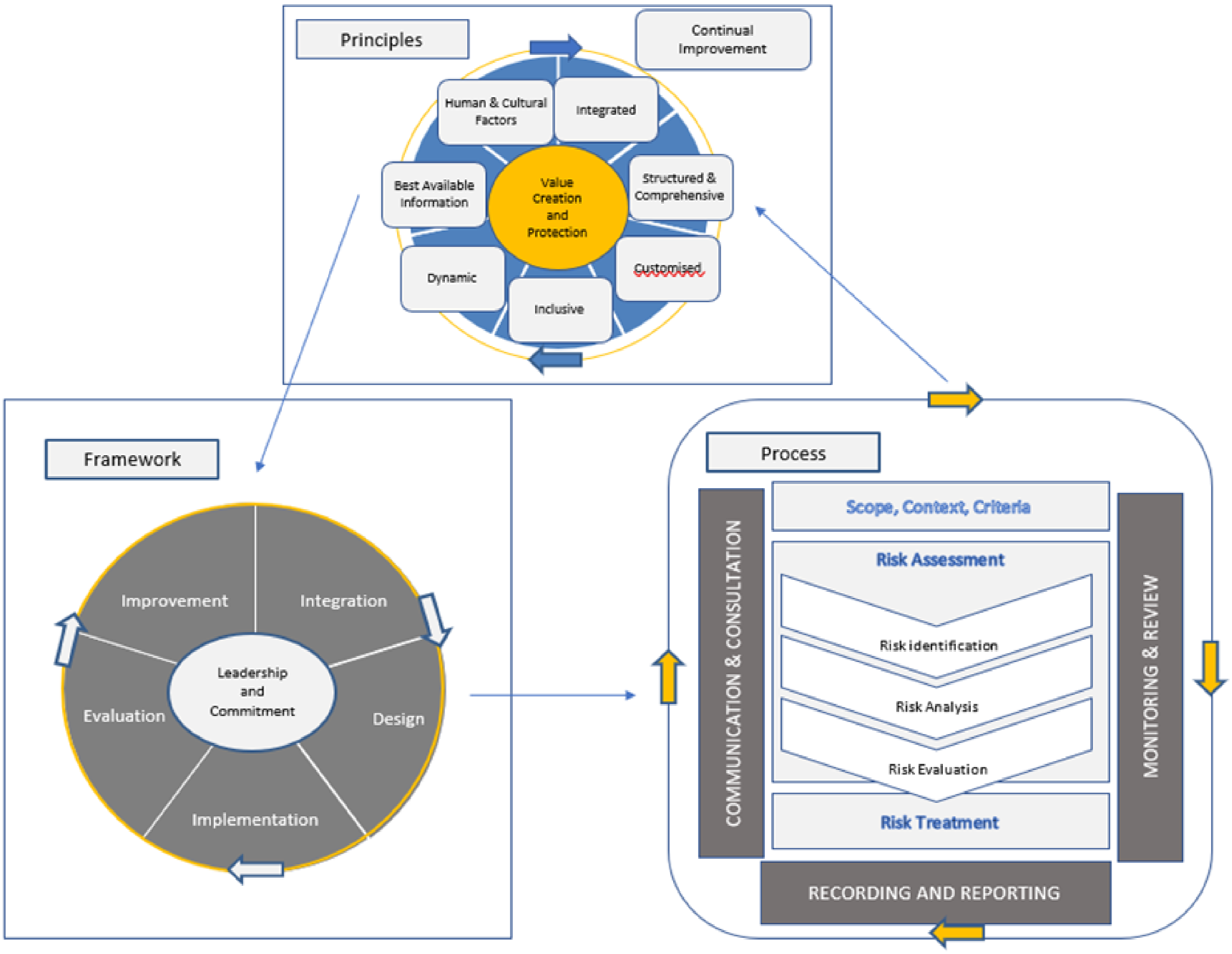
Unlike some other functions in business, risk management is far-reaching and crosses over into many other disciplines. Each function has its own unique set of risks and mitigation strategies and in some cases is governed by specific compliance and industry standards. Each of the following sub-disciplines of risk management affects organisations within the venues industry in different ways.



Risk Management is a discipline applied across many facets of Venue Management.

Risk Management Principles, Framework and Process

The following diagram is adapted from the ISO31000:2018 Risk Management Guidelines to explain what Risk Management involves:



Given Risk Management 1 at VMS focussed heavily on the ‘Process’ of risk management, this paper will largely consider the ‘Principles’ and ‘Framework’ sections.

In particular:

- Risk Management Principles of success,
- Enterprise-wide risk management and Risk Management Frameworks,
- Crisis management; and
- Business continuity.

Risk Management Principles

The Figure above shows the link between Principles, Framework and Process. The Process section sets out a practical guide on how to complete a risk assessment, while the Framework section explains how senior management can incorporate risk management into a continuous improvement cycle. The Principles, however, set out the recognised elements of success. These are aspirational goals that should be considered if risk management is to become embedded within an organisation.

These are explored briefly below:

Creates and protects value

Risk management must add value and not simply be an administrative process for process sake. Many organisations in the venues industry fail to achieve this principle. To achieve value risk management must be recognised and promoted across the organisation as helping the business achieve its goals and helping individual managers and employees focus their time and effort on the threats that reduce their potential for achieving objectives.

Is an integral part of organisational processes

Risk management should not sit out by itself. It is a discipline affecting all other disciplines so it needs to be integrated into other business planning, reporting and communication processes as just 'part of the things we do.'

Is systematic, structured and timely

Organisations that successfully embed risk management usually systemise risk assessment, treatment monitoring and risk reporting, so the risk-related information flowing up to management is regular, timely and accurate.

Is Customised

The Risk Management Framework, the definitions and terminology used, the roles and responsibilities, workflows, methods and business rules that support risk management, must be customised to meet the needs of the organisation. One size does not fit all!

Is transparent and inclusive

Risk management should involve everyone across the organisation, but be designed so it is specific to individual job roles.

Is dynamic, iterative and responsive to change

The nature and environment of most organisations can change rapidly. The speed at which the global financial crisis took hold in 2008 can demonstrate this, and the organisations that failed to respond to the deteriorating economic conditions in some cases risked their own survival. The rapid changing nature of the security threat in places of mass gatherings is another. The risk management system needs to be responsive so it remains a relevant tool for the organisation's decision-makers.

Is based upon the best available information

Updating of risk registers, and the decisions that flow from risk assessment must be based upon the best available information, and not from old data that does not reflect the changing nature of the organisation.

Takes human and cultural factors into account

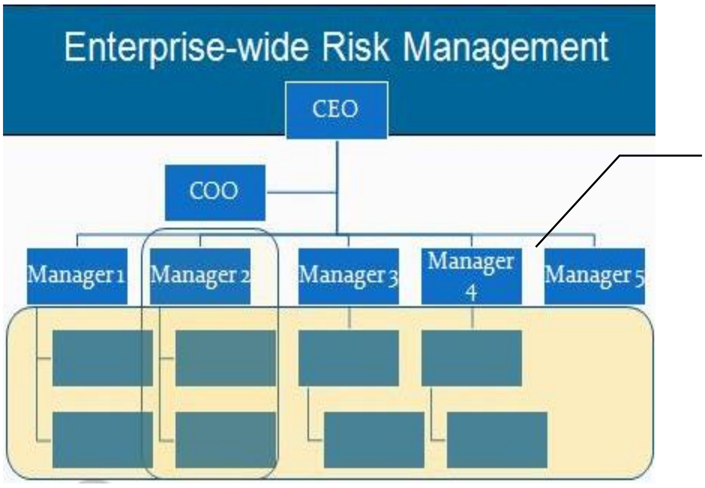
The culture of the organisation should not be underestimated. Where senior management encourage and reward risk taking behaviour, it can be assumed without stringent controls, more risks can often mean a bigger threat of losses.

To foster a culture of acceptable behaviour stems from the communications and actions of the Board, the CEO and Senior Managers. If they 'walk the talk' then staff are more likely to respect their wishes and adopt the culture set by the leaders. If the organisation's leaders articulate the risk management expectations and ensure accountability systems are in place, staff should embrace this culture and hopefully take fewer risks; if that is the desired objective.

Continuous Improvement of the organisation

Through the organisational planning cycle, venues should systematically seek ways to review and improve how they manage risk and learn from their mistakes; or the mistakes of others.

Enterprise-wide Risk Management



Risks affecting individual functional areas

Risk affecting all functional areas

Examples of risks that have enterprise-wide consequences might include a major long-term loss of utilities or denial of access to a venue or office area within a venue. These can have impacts on event operations, revenues, public relations and loss of other services. All of these impacts require each functional area affected to develop treatments in consideration of their impact on their stakeholders. Under a normal operational approach to this risk, traditional risk management may have largely seen this risk as the responsibility of just site management, rather than considering its impact across the organisation.

An ERM approach to risk management requires a higher level of risk monitoring and oversight. This usually needs some type of risk information management system (software) to allow multiple risk owners to measure and control risks within their portfolio, while providing a means of reporting to the Board, Risk Committee or Senior Management on significant risks and effectiveness of controls.

In some cases, significant risks may have a potential high impact upon the business and therefore should be included within Crisis and Business Continuity Planning.

Risk Management Framework

Most organisations within the venues industry have some documented process for how they view, assess, tolerate and manage risk. This is known as a Risk Management Framework. Every organisation is different and therefore every Framework should be different; based upon the organisation’s context (not just copied from the Risk Management Standard).

As was covered in Year 1, under that International Risk Management Standard: ISO31000:2018, the organisation should establish its own risk management context based upon its appetite for risk (i.e. are they risk takers or risk averse), and risk tolerance levels (i.e. how much risk will the organisation tolerate before it is unacceptable).

A Framework is typically designed to assist the organisation’s workforce to manage their own risks by defining a structured approach. It may include:

- A company-wide risk management policy.
- A standardised process for risk assessment.
- A set of defined terminologies.
- Risk appetite statements – stating how much and types of risk the organisation will and will not accept.
- Setting out how risk management systems are integrated within an event, other non-event operations and strategic business planning.

- Articulating the accountabilities and responsibilities for risk oversight and reporting throughout the organisation; and
- Defining the organisation's risk evaluation criteria and tolerance levels.

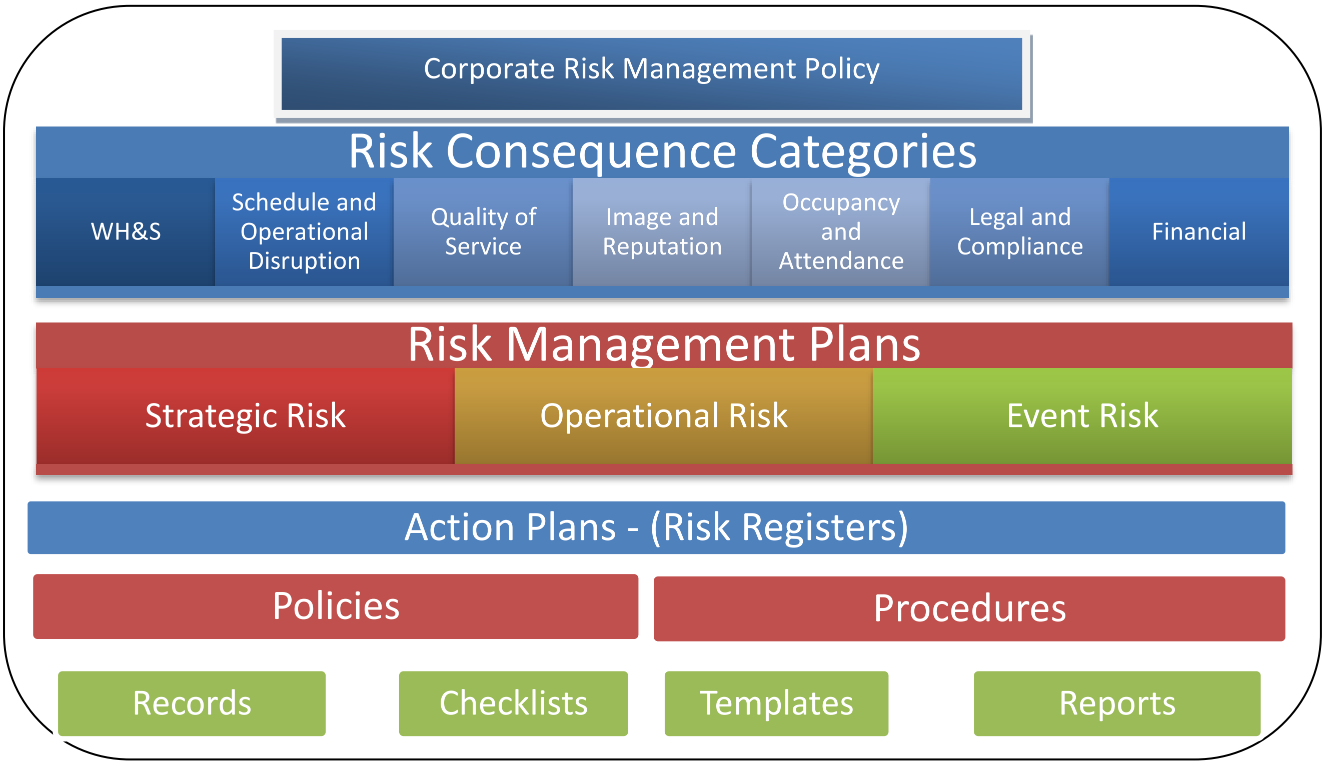
The following section provides an overview of suggested contents of a Risk Management Framework. (Refer to diagram over page)

Company-wide Risk Management Policy
Similar to a company Health and Safety Policy, an organisation's Risk Management Policy articulates management's commitment to managing its risk. The Policy should set out the organisation's key risk management focus areas. It is usually about one or two pages and is signed by either the CEO or the Chairman of the Board.

It might also include:

- A preamble – An overview of the policy.
- Important definitions – Defining risk, risk assessment and risk management.
- A policy statement - Balancing risk and reward and establishing the right risk aware culture.
- Policy objectives – With references to decision-making, risk appetite and compliance.
- Risk registers and reporting – How risk will be measured and reported.
- Senior management responsibility – Key entities responsible for risk oversight (I.e. Risk Manager, Senior Management Team and Audit & Risk Committee).
- Monitoring and reporting – Annual business reporting as well as the role of internal and external audit.

The Framework aims to deliver the intent of the organisation's Risk Management Policy.



Risk Consequence Categories
The Framework should aim to explain what risk consequence categories are important to the organisation. The Framework may include some or all of the following consequence categories:

- Workplace Health and Safety – Personal injury and health and safety to the public, players, performers, staff, contractors or other stakeholders under its control.
- Event Schedule Disruption - Impact upon event schedule from a temporary closure or operational delay at the venue.
- Operational Disruption – Business continuity risks affecting capacity to operate.
- Image and Reputation – Public scrutiny and brand erosion measured by the degree of media attention.
- Spectator Attendance – Impacts that affect attendances of the public at events.
- Legal and Compliance – Potential fines and prosecutions resulting from legislative, common law and/or compliance breaches.
- Financial– Positive or negative financial impacts upon revenue or costs to the venue.

Risk Management Tools
The Framework might be supported by a series of tools to assist people throughout the organisation manage risk in their area. These may include Risk Management Plans, Action Plans, Risk Registers, as well as policies, procedures, records, templates, checklists and reports that together help ensure consistent documentation of risk assessment and risk control.

Risk Management Plans
Some venues or larger events may require the development of a Risk Management Plan. This document may cover any range of risk management activities but should not be confused with a Risk Assessment (normally contained in a Risk Register). It may be an addendum to the Risk Management Plan or as a standalone document of risks and risk controls. A Risk Management Plan is a far more detailed document whereas a Risk Assessment is a list of risks that have been identified, analysed and risk mitigating controls documented.

In venues, such documents may be produced by:

- the venue for their internal purposes
- an event organiser and verified by the venue
- a supplier and verified by the venue or event organiser
- the venue and verified by local police; or
- the venue manager and verified by the venue owner (if they are different organisations)

An Event Risk Management Plan might include the following topics:

- Senior Management's Commitment to Risk
- Terms of Reference
- Definition of Risk
- Event Objective
- Reference Sources
- Risk Categories
- Relevant Policies and Procedures
- Event & Venue Management Roles and Responsibilities
- Key External Stakeholders
- Key Internal Stakeholders
- Communications Plans
- Event Details
- Location
- Event Activities
- Event Regulatory Compliance

  - Place of Public Entertainment Licence
  - Health & Safety Regulations
  - Food Safety Act
  - Liquor Licence
  - Sound Management
  - Major Events (legislation if relevant)
- Contractor Management
  - Contractor Safety
  - Contractor Supervision
- Insurance
  - Public Liability Insurance
  - Workers Compensation
  - Insurance Certificates
- Inductions
- Medical
- Emergency Management
- Incident Reporting and Investigation
  - Incident Reporting
  - Incident Management
  - Control Room Communications
- Operational Risk Monitoring
- Pre-Event Readiness
- Event Risk Register

Risk Register

The Risk Register is a repository for risks affecting, identified by, or managed by the organisation or its individual business units. They may contain strategic, operational or event-related risks.

They may live in document form, a spreadsheet, a risk database or in software (a risk information management system). They typically contain risks identified, their corresponding assessment, agreed controls, action plans and accountabilities.

Action Plans

Action plans are generated at the completion of the Risk Assessment. They define specific actions, activities, policies, procedures or other controls required to mitigate risk. The action plans nominate a person responsible for implementing the action and can relate to:

- Pre-Event Checklists.
- Ongoing business risk controls.

Policies

Risk management policies provide a point of reference for the organisation’s management, staff and contractors on the guiding principles for managing:

- Specific hazardous activities.
- Specific risks that threaten objectives; and
- Systems and processes that mitigate a variety of risks.

Procedures

Risk-related procedures articulate how to implement the guiding principles contained within risk policies.

Records

Risk management records are documents completed by the organisation's workforce as evidence that risk-related activities have occurred. Examples might include training records, meeting minutes, etc.

Checklists

Checklists can provide a useful tool to either:

- Prompt the user toward a particular activity or risk
- Verify that a particular activity or risk exists and has been addressed.

Examples might include pre-event readiness checklists, safety inspection checklists, vehicle maintenance checklists, etc.

Templates

Templates may be used to guide the user in a pre-defined format or structure. Completed templates become useful records evidencing risk-related activities. Examples of risk-related templates used might include:

- Operational Plans.
- Policy and procedure templates.
- Contract templates.
- Scope of services templates.

Reports

Various reports are used to assist in data collection and continuous improvement of risk management. Key risk reports include:

- Risk assessment reports.
- Audit reports.
- Incident reports; and
- Post-event debriefs.

Health and Safety Program

The organisation's Health and Safety (H&S) Program can be an important part of the Framework. In some venues in Australia and New Zealand H&S and public safety represent a significant portion of the organisation's risk profile as well as its operational compliance obligations.

The organisation's Safety Management System (SMS) might be designed in accordance with ISO 45001:2018 Occupational health and safety management systems - Requirements with guidance for use. This supersedes the previously used:

- AS/NZS 4801:2001 across most states and Commonwealth employers in Australia and New Zealand,
- SafetyMap in Victoria, and
- OHSMS 18001 (international standard) in other countries.

In each case the SMS usually has an element requiring the management of risk.

Security Risk Management Program

The venue's security program also falls within this Framework. The entire program should be underpinned by sound risk management principles and consider important asset groups of: physical people, information and technology-based security risk.

Physical assets include tangible and intangible assets. Tangible assets include physical goods and property and intangible assets include financial assets and cash in the bank. People include all stakeholders who attend our venues and the potential harm that threat actors can bring to the safety and security of these stakeholders. Information assets include structural (such as intellectual property and commercially sensitive information), relational (such as contractual relationships with suppliers and licensing arrangements), and human categories (such as expertise and know how) of information. Information technology is an area of increasing importance with threats to cybersecurity and need to protect personal and commercially sensitive information having significant legal compliance and civil liability implications if not upheld.

The security risk management activities should seek to deter, delay, detect, respond and recover; assisting the organisation to achieve a level of resilience from security-based threats.

Crisis Management & Business Continuity Management

Introduction

While risk management is a discreet discipline that helps to measure, prioritise and prevent risk, it is also an important element of Crisis Management (CM) and Business Continuity Management (BCM). As an iterative process, risk management requires consultation with stakeholders and encourages risk controls in response to changing economic, legal, environmental, political and social conditions that affect a venue.

All venues operate with limited resources and have, amongst their many goals and objectives, to protect people, property and their reputation. They all seek the ability to be resilient against major unforeseen situations that can damage the business.

This section explores the interrelationships between risk management, CM and BCM.

Overview of Interrelationship between Crisis, Business Continuity and Risk

Like many areas in risk management, there is considerable confusion in the terminology used between CM, BCM and Risk Management. For example, some argue BCM is a subset of CM, and both are a subset of Risk Management. Others argue differing combinations of the three.

Regardless of the theoretical approach chosen, each term seeks to protect an organisation to help it achieve its objectives. CM and BCM help the response and recovery from unforeseen incidents or events that affect the organisation achieving its objectives using a risk -based approach.[1]

Despite different approaches, CM and BCM must be integrated across the Enterprise (i.e. an ERM approach). These are two intertwined disciplines. In some literature, the two are combined as one called Business Crisis and Continuity Management (BCCM).

Shaw and Harrald (2004) describe BCCM as, *"The business management practices that provide the focus and guidance for the decisions and actions necessary for a business to prevent, prepare for, respond to, resume, recover, restore and transition from a disruptive (crisis) event in a manner consistent with its strategic objectives."* [2]

CM and BCM are growing in importance due to numerous high-profile incidents that have a high disruptive consequence. These include any number of security and terrorism threats in places of mass gathering, the 2011 Queensland floods affecting Suncorp Stadium in Brisbane; and the 2011 Christchurch earthquake in New Zealand. As the operating environment becomes more complex and 'risky', venues need to be equipped to respond and recover quickly.

[1] Mitroff, I. (Mitroff and Pauchant 1992, Mitroff 2001) and Fink, S. (Fink 1986) cited in Business Crisis and Continuity Management Gregory L. Shaw, D.Sc., CBCP Senior Research Scientist, The George Washington University Institute for Crisis, Disaster, and Risk Management at http://www.gwu.edu/~icdrm/publications/ShawTextbook011105.pdf

[2] Shaw and Harrald *(2004)* cited in Business Crisis and Continuity Management Gregory L. Shaw, et al.

In a paper titled *The Core Competencies Required of Executive Level Business Crisis and Continuity Manager,* Shaw and Harrald (2004), provided a useful framework showing how ERM, CM and BCM interact against an incident timeline.

<table>
<tr><td colspan="3"><b>Enterprise-wide Risk Management (ERM)</b></td></tr>
<tr><td>Before an Incident or Loss Event</td><td>During an Incident or Loss Event</td><td>After an Incident or Loss Event</td></tr>
<tr><td colspan="3"><b>Crisis Management (CM)</b>
• Crisis communications</td></tr>
<tr><td></td><td>Knowledge Management</td><td></td></tr>
<tr><td><b>Risk Management</b>
• Risk-based decisions
• Compliance
• Risk assessment
• Business Impact Analysis</td><td></td><td></td></tr>
<tr><td></td><td>Emergency Management and Response</td><td></td></tr>
<tr><td></td><td colspan="2"><b>Business Continuity Management (BCM)</b>
• Response
• Recovery
• Resumption</td></tr>
<tr><td colspan="3">Time ⟶ ⟶</td></tr>
</table>

Under this model:

Risk Management – Is the analysis of risk (before an incident), including critical impact on an organisation. It also involves making risk-based choices for strategic and tactical decision-making in line with company goals and objectives.

Crisis Management – Coordinates efforts to bring an incident or loss event under control so the situation becomes consistent with goals and objectives of the organisation. This may include coordinating Crisis Communications with internal and external stakeholders (especially media), to assist in delivering clear and timely information.

Business Continuity Management – Involves developing a prioritised set of plans and nurturing an operational state of readiness to enable an organisation to respond, recover and resume operations to previous levels, (or beyond previous levels). BCM usually deals with longer-term incidents or situations than CM; ones which have escalated to the point of affecting critical business functions. They usually require a longer-term recovery and restoration process.

Crisis Management

Crisis Management involves dealing with incidents or situations that threaten the organisation and its reputation. Such situations are characterised by being unforeseen and occurring rapidly. They usually require quick decisions. These situations may not necessarily affect critical business functions but have the potential to threaten achievement of business objectives from brand erosion and reputational damage.

Often under a crisis, the image and reputation of the organisation is at stake with brand erosion as a genuine risk, if not handled carefully. The crisis may have occurred as a result of a real incident or loss event, or perceived risk that has invoked a degree of public outrage and media attention. Because of this outrage factor, crisis management has an important communication element where open, honest and consistent communications are needed throughout an organisation and with external stakeholders.

Types of Crisis

There are numerous types of crisis that can affect the organisation. These may include (but are not limited to):

- Natural disasters – fire, flood, earthquake
- Technological failure – loss of critical data
- Violence and confrontation – riots, picketing or blockades
- Deliberate malevolence –product tampering
- Management deception or misdeeds - deliberately deceiving customers, shareholders or the media
- Workplace violence or harassment – violence or harassment between workers
- Rumours – false information deliberately or inadvertently leaked

Why is Crisis Management Important?

Crisis Management is important because bad news travels fast. With globalisation and access to instant real time information through mainstream and social media, information about a crisis affecting an organisation can travel around the world very quickly. This is why being prepared is vital!

Getting Prepared for a Crisis

To prepare for a crisis an organisation might:

- Establish a CM Team
- Understand potential high impact risks that could create a crisis
- Develop a CM Plan
- Prepare for media interest
    - Designate a competent media spokesperson
    - Identify target audience
    - Prepare pre-scripted communications
- Respond appropriately
- Nurture goodwill and reputation
- Plan for the recovery

Establish a Crisis Management Team

Select the Crisis Management Team (CMT). Nominate an empowered senior manager as leader with appropriate decision-making authority and experience. This person may be required to drop other work commitments in a crisis so this circumstance must be taken into account during selection. Other members of the senior management team might also be required. Include representatives from functional areas such as security, marketing, ticketing, finance, site management and public relations.

Understand potential high impact risks that could create a crisis

The best way to deal with a crisis is by prevention. Use risk assessment to identify risks that have a high impact upon the organisation. Initiate risk prevention and mitigation measures to minimise the occurrence of high impact risks.

Develop a CM Plan

Establish a plan and prepare staff through training and instruction for their role in the plan. It should describe the elements of the company's image, brand and reputation that must be protected.

The plan should include:

- High impact foreseeable risks.
- Information about the CM Team
    - Roles and responsibilities.

  - Contact details.
- Action plans and checklists – including when the plan will be activated.
- A Crisis Communications Plan.
- Media contacts.
- Training and testing schedule.
- Pre-scripted media statements.

Prepare for media interest

CM requires an organisation to manage two priorities:

- Resolving the crisis.
- Dealing with media interest; i.e. minimise the damage to image, reputation and the brand.

Media communications must be clear, concise, honest and timely. The media needs information so maintain open communications with them.

Designate a competent media spokesperson

Nominate a competent person to represent the company in the media during the crisis. The organisation must maintain a clear and consistent voice.

Identify the target audience

The Crisis Communications Plan should identify the key target groups intended for company crisis communications, how best to reach them, and what the messaging contains. Vary the message based upon the high impact risks identified.

The target audience could include:

- Public
- Media
- Suppliers
- Promoters
- Staff
- Business owners
- Public transport providers

Prepare pre-scripted communications

Prepare clear and concise pre-scripted messages for the high impact risks identified.

Respond appropriately

In your initial release of information to the media, state that you have incomplete information but you should provide an assurance that further information will be forthcoming. Provide a brief explanation of your approach to the crisis but do not speculate on causes. Provide regular updates. If possible, describe actions you might take in future to prevent recurrences.

Nurture goodwill and reputation

Make efforts now (before a crisis) to build goodwill with important stakeholders. Goodwill and a strong reputation can help alleviate negative impacts to image, reputation and brand in a crisis.

Plan for the recovery

In preparation, consider the environment that you will be operating under after the incident, particularly in the mid- to long-term. Establish what information to communicate and whom it should be communicated to in order to regain public confidence in your organisation.

Business Continuity Management

BCM is a term that describes the integration of an organisation's planning and management processes to provide operational resilience. It encompasses areas previously known as contingency planning and disaster recovery and extends beyond just developing a Business Continuity Plan (BCP). It includes the notion of:

- The ongoing management of risk
- Building a resilient and sustainable business
- Achieving business goals and objectives

The BCP is a collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of an emergency, ongoing crisis or disaster. The BCP is part of BCM that addresses specific high impact circumstances that affect:

- People (workforce)
- Facilities and infrastructure
- Services and suppliers
- Information; and
- Resources

BCM Definition

Under the Australian / New Zealand Standard for Business Continuity, AS/NZS 5050:2010, the purpose of the Standard is:

> *"To assist organisations maintain continuity of their business through effective management of disruption-related risk. This will thereby enhance an organization's resilience and can create strategic and tactical advantage in uncertain and volatile environments."*

It is more than just having a plan, but rather it reflects an ongoing degree of readiness to respond to and recover from, unscheduled incidents or events. It is usually subject to some level of resource, time and capability restraints within which it must recover. Organisations need to accept that there is risk in every decision and that to recover from interruptions requires not only the right plan, but also the right culture, good communications and appropriate resources in recovery.

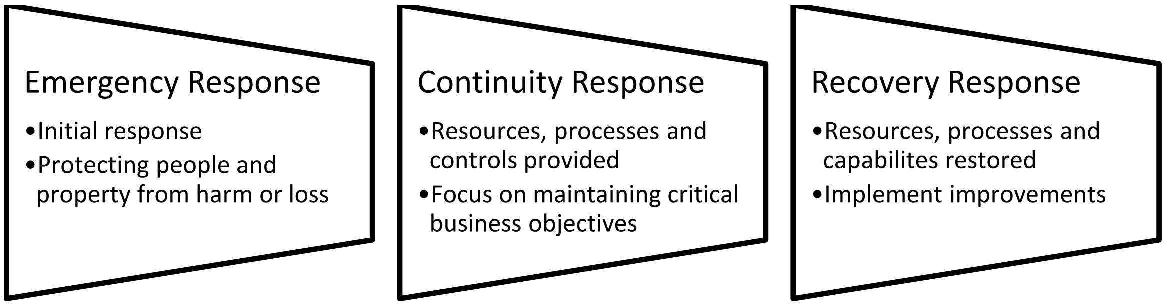
To achieve this an organisation must:

- Understand its critical objectives.
- Be aware of any risks to achieving its critical objectives.
- Analyse and test various control options to achieve an appropriate level of residual risk.
- Establish a means for ensuring critical objectives are maintained following an interruption.

BCM will help an organisation during a crisis to minimise its operational impact on critical functions, minimise damage to image and reputation, maintain market share and retain confidence with its stakeholders. BCM helps provide predictability in an unforeseen situation.

Three Responses of BCM

According to A Practitioner's Guide to Business Continuity Management (HB 292:2006), there are three phases of a business continuity response:



Emergency Response
- Initial response
- Protecting people and property from harm or loss

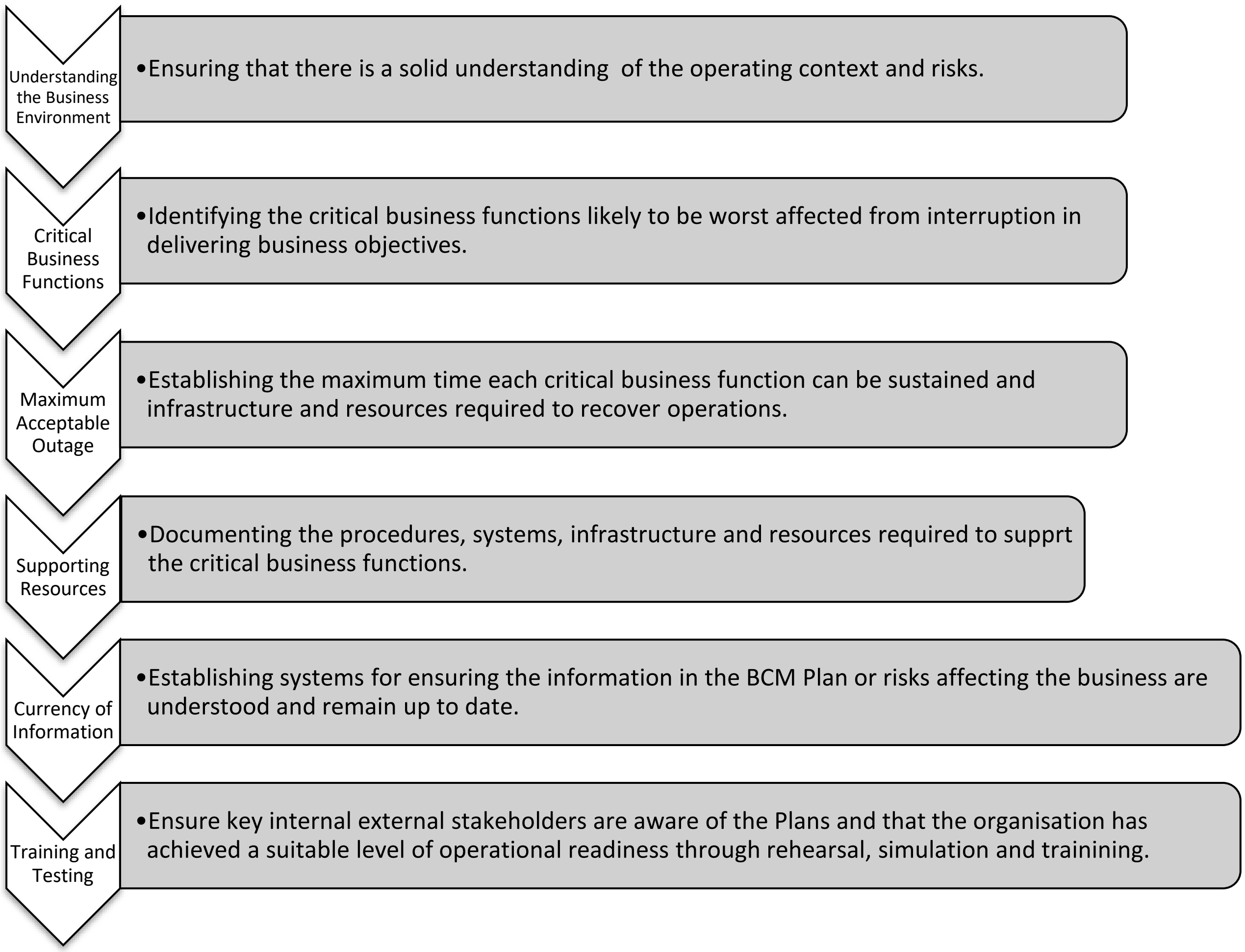
Continuity Response
- Resources, processes and controls provided
- Focus on maintaining critical business objectives

Recovery Response
- Resources, processes and capabilites restored
- Implement improvements

These response phases transition from one to the next dependent upon the severity and timeframe of the incident or loss event.

Six Key Elements to BCM

In readying an organisation to be resilient, a BCM program typically comprises of six key elements:



Understanding the Business Environment
- Ensuring that there is a solid understanding of the operating context and risks.

Critical Business Functions
- Identifying the critical business functions likely to be worst affected from interruption in delivering business objectives.

Maximum Acceptable Outage
- Establishing the maximum time each critical business function can be sustained and infrastructure and resources required to recover operations.

Supporting Resources
- Documenting the procedures, systems, infrastructure and resources required to supprt the critical business functions.

Currency of Information
- Establishing systems for ensuring the information in the BCM Plan or risks affecting the business are understood and remain up to date.

Training and Testing
- Ensure key internal external stakeholders are aware of the Plans and that the organisation has achieved a suitable level of operational readiness through rehearsal, simulation and trainining.

Steps in BCM

There are nine recognised steps in the BCM process. These are set out below.

Step 1: Commencement

- Establishing the need – Defining the scope, objectives and outcomes of the BCM program.
- Management committment – Gaining committment from the CEO, senior management team and Board. Commitment includes ensuring adequate budget, scope and deliverables are agreed upon.
- Form the BCM team – Establish a team for designing and implementing the program.

Step 2: Conduct a risk and vulnerability analysis

- Analyse the environment – Consider the external and internal business environment and identify core business objectives and the functions that support it.
- Identify risks and vulnerability – Using risk analysis, identify risks that have a potential high impact upon critical business functions.

Step 3: Conduct a Business Impact Analysis

The Standard AS/NZS 5050:2010 prescribes the following steps to be completed as part of a Business Impact Analysis:

- Confirm business functions – Consider the technical, operational and finanical impacts of a disruption and decide which business functions will be further considered.
- Process review each function – Analyse each function to determine its processes and interdependencies so the full impact of disruption can be understood.
- Prepare an inventory of existing controls – Review all current controls.
- Determine the significance for how long the disruption could occur: the Maximum Acceptable Outage – Establish the maximum time that critical business functions can fail before their failure affects the entire operation (i.e. hours, days or weeks).
- Determine the effects of current controls – Effectiveness of current controls can be determined by assessing factors such as the time required after an incident for a control to start operating.

Step 4: Response strategies

- Emergency response – Develop emergency response plans and review against disruption scenarios.
- Continuity response – Establish the criteria for activation and deactivation of plan (ensuring minimum acceptable level of performance).
- Recovery response - Recovery to full performance capability or improved performance capability.
- Alignment – Align all response plans to identify any conflict. Assign oversight to Crisis Management Team.

Step 5: Develop resource and interdependency requirements

- Resource requirements – Confirm minimum resource requirements from Step 3.
- External interdependencies – Establish important contact details; confirm customer expectations; identify alternative locations, suppliers, etc.

Step 6: Developing continuity plans

- Specialist organisational plans – Establish continuity plans for specialist areas such as IT or unique critical business units.
- General continuity plans – Develop continuity plans that are comprehensive but simple.

  They might cover:

  - Business function or location.

- Response strategy.
- Actions and activities.
- Trigger points for plan activiation.
- Length of time for key activities.
- Alternate persons responsible.
- Important contact details.
- Information or data required (soft copy, hard copy).

Step 7: The communication strategy

- Scope - Set the scope for:
  - Who needs information?
  - What information needs to be communicated?
  - How can it be communicated?
  - What limitations exist for this communication?
- Message content – Establish pre-scripted messages.
- Channels – Establish the most appropriate means and frequency for information being provided.

Step 8: Training, maintaining and testing plans

- Plan testing – Conduct a test of the plan through a desktop exercise or simulation. Conduct a debrief to ensure lessons can be learned.
- Training – Provide basic training to all persons regarding their roles and responsibilities in the plan.
- Maintenance – Develop a periodic review and update of the plan.

Step 9: Activation and development of plans

- Plan activation – Activation of the plans should be done as documented.
- Governance issues – Ensure appropriate minimum standards of governance are maintained; these include regulatory compliance, document control and records management, audit trails, insurance providers notified, etc.

Why is BCM so Important?
The current security situation and the threat of terrorism in the region suggests that BCM should be taken seriously. In addition to this, our venues are often subjected to disasters resulting from weather, fire, or criminal activities. We are also potentially susceptable to the affects of loss of workforce from pandemics or sudden loss of critical suppliers, infrastructure, utilities or stakeholders. Having a robust approach to BCM can help build your organisation's resilience to such interruptions.

Finding more information on Crisis Management and Business Continuity Management

Standards

Standards Australia and New Zealand

- ISO 31000:2018 – Risk Management Guidelines
- AS/NZS 5050:2010 – Business continuity – Managing disruption-related risk
- HB 292-2006 – A practitioner's guide to business continuity management

- HB 293-2006 – Executive guide to business continuity management
- HB 167-2006 – Security risk management

Websites

- Standards New Zealand
  - http://www.standards.co.nz
- Standards Australia
  - http://www.standards.org.au
- Trusted Information Sharing Network for Critical Infrastructure Protection
  - http://agsearch.ag.gov.au/search/tisn
- Australian National Audit Office - Business Continuity Management – Keeping the Wheels in Motion
  - http://www.anao.gov.au/uploads/documents/Business_Continuity_Management.pdf
- Emergency Management Australia - Articles and Journals on Business Continuity Management. Australian Emergency Manuals
- http://www.ema.gov.au/www/emaweb/emaweb.nsf/Page/EMALibrary_OnlineResources_EMALibrarySubjectGuides_EMALibrarySubjectGuides-BusinessContinuity

Sample Exam Question

Question: The three main phases of business continuity are?

A ○ Emergency response, risk management, hazard monitoring

B ○ Calling 000, await direction from emergency services, collect photographic evidence

C ● Emergency response, continuity response, recovery response

D ○ Always have a plan B, test it occasionally, and document everything