Portarlington NEIGHBOURHOOD HOUSE

Compliance & Risk Management Framework

- Risk Policy
- Risk Register
- CoM Annual Compliance & Risk Audit

1. Document Control

Version Number:	2
Date Adopted:	April 2024
Review Date:	March Annually as per CoM Annual Planning Calendar

This policy supersedes any prior policy on this subject matter.

2. Contents

3.

4. Document Purpose & Scope

The purpose of this document is:

1. to create a framework for identifying and managing risks to Portarlington Neighbourhood House (PNH) business sustainability and implementation of strategy;
2. to identify possible causes of those risks and the potential impacts;

3. to ensure there is a mitigation strategy, and contingency strategy, in place for those risks; and
4. to provide an audit procedure to ensure the Committee of Management (CoM) is confident that PNH is compliant with all legal and regulatory requirements, PNH Policy and requirements of the Risk Register.

For personal injury risks, refer to the OH&S Policy & Annual OH&S Audit.

For child safety risks, refer to the Child Safe Policy and Audit Procedure.

5. Risk Policy

4.1 PNH will endeavour to minimise the risk that foreseeable hazards (including physical, legal, financial, workplace, cyber and reputational hazards) pose to our organisation, our operations, our staff, our volunteers, our members or the general public.

4.2 PNH will maintain a Risk Register (Appendix 1) which will be reviewed annually by the CoM.

4.3 PNH will comply with its legal and regulatory requirements, and PNH Policy.

4.4 All PNH policy documents must have an attached audit checklist (for inclusion in this compliance audit).

4.5 A risk & compliance audit will be conducted annually (see Section 6. and Appendix 3).

4.6 This Compliance and Risk Management framework is aligned to ISO 31000 Risk Management (Summary in Appendix 4).

4.7 Risk Policy related to the insurance policy:

4.7.1 Cyber attack is not covered in insurance, PNH must have adequate back-up procedures

4.7.2 Contractors e.g. paid activity facilitators, must have their own insurance OR be associate members

4.7.3 Car-pooling - all cars used in a PNH activity or event for car-pooling must have comprehensive insurance (and PNH keeps records of car registration, and driver disclaimer signature, times and dates car is used for car-pooling)

4.7.4 All payment to activity facilitators MUST be made to the facilitator from the PNH account (no cash payments ANYTIME for any invoice)

4.7.5 All PNH generated invoices must be sent from PNH email address (via the Program Manager or Treasurer and not via private email addresses or postal addresses)

4.7.6 An asset register must be maintained. In accordance with DHHF service agreement, no 7, PNH needs DHHF consent to dispose of items over $5000.

4.8 A contingency fund will be kept aside for contingencies as per the Risk Register. The amount will be determined using the **Contingency Fund Analysis**, and this will be reviewed annually as part of financial risk management (Appendix 2).

4.9 **Security and Access Control**

4.9.1 The Program Manager must maintain a register of persons with:

- office keys (must be kept up to date, particularly how many keys are available)

- keys to front door (must be kept up to date, particularly how many keys are available)
- the access code to the 4 password key lock box (with key to front door)
- Zero access
- Bank account access
- Bank card holders
- PC access (office) and including access levels to Social Planet
- Access as official PNH contacts to any external organisations such as VMIA, ACNC, CAV etc.

4.9.2 The password for the 4 password key lock box (for front door) must change annually, and the access register updated.

4.9.3 The Program Manager must remove a person's access to financial accounts, IT systems and from official PNH-related access to external organisations immediately upon that person's cessation from any paid or volunteer role which required that access, and any keys, financial cards or other PNH equipment related to that role must also be returned immediately upon their cessation from the role.

4.9.4 Employees and volunteers will take all necessary measures to maintain the organisation's cyber security, including protecting passwords, securing access to computers and maintaining protective software.

4.10 **Committee of Management**

4.10.1 Prior to appointment, all members of the CoM will undergo a suitability screening check which will include a:

- national police records check
- Working with Children Check
- ASIC disqualified person's check
- ACNC disqualified person's check.

6. Legal Advice

Legal advice can be obtained from Not For Profit Law at Justice Connect
http://www.nfplaw.org.au/legaladvice

7. Audit Procedures

An annual Compliance & Risk Audit will be scheduled between May and June each year. The audit will include:

- The integrity of the Risk Register
- Implementation of Mitigation Strategies and Contingency Strategies for risks identified in the Risk Register
- Compliance to PNH's legal and regulatory requirements
- Compliance to PNH Policy and integrity of PNH Policy
- Compliance to PNH CoM Terms of Reference for subcommittees and other committee delegations
- A review of the audit process and checklist itself

The CoM may appoint a person or small team to carry out the Compliance & Risk Audit using the checklist in Appendix 3. The audit work can be divided and parts appointed to different auditors.

The audit is mostly desktop although evidence of compliance will be sought where appropriate. Any interviews with operational managers require at least two weeks' notice.

Any non-compliance items identified in the audit checklist will be placed in the **Risk Action Plan** and will become a regular part of the CoM monthly meetings until all compliance actions are completed.

8. Related Documents

PNH Strategic Plan
PNH Constitution
Code of Conduct
Performance Evaluation Framework
All Operational Handbooks (Policy & procedures documents)
Delegation of Authority
Financial Management Policy
Information & Communications Policy
OH&S Audit
Child Safe Policy

Appendix 1: PNH Risk Register

	Risk	Possible Causes	Potential Impact	Mitigation	Contingency
1.	Decline in membership, participation, and unable to broaden the membership demographics (as per strategic plan) (sustainability)	• Lack of good leadership from CoM • Negative **culture** (members not renewing) • Negative reputation (no new members) • Program not meeting need • **Program/facilitators/facilities** not suitable • Competition • Poor operations/administration • Strategic Plan not implemented, wrong plan, no 'buy-in' for plan • Lack of innovation • Lack of valid and reliable feedback from members/committee • Lack of advertising/marketing	• Reputation damage • Sustainability threatened	• Strong leadership & CoM • Attention to values / culture compliance • Focus on Quality Management, data, performance • Stakeholder Management • Member involvement & feedback processes, incl. complaints, regular open meetings • Continual improvement in processes • Clear transparency of all PNH activity from a financial and social responsibility • Targeted Marketing Plan	• Change Strategic Plan • Change leadership (consider change to Coordinator and/or Coordinator's supervisor) • Use contingency fund if required for change of personnel
2.	Loss of access to building /facilities /physical resources	• Damage to Facilities (fire, flood, or other natural disasters; impact by vehicles, planes, trees or other objects; failure of essential services - electricity, gas or water supply) • Unable to lease suitable facilities • Access restrictions due to landlord or legal restrictions e.g. COVID	• Potential OH&S issues • Impact to building security • Temporary close of Program (and income)	• (Insurance is a landlord responsibility)	• Find alternate facilities • Use contingency fund if required for venues
3.	Loss of revenue due to external circumstances	• economic downturn • competition • loss of DFFH funding	• sustainability threatened	• Good financial forecasting and budgeting • **Compliance & Risk Audit**	• Use contingency fund to continue until funding is restored or change is managed
4.	Loss of revenue due to internal circumstances	• Fraudulent activity / theft /corruption • Non-compliance to funding body requirements • Lack of control of budgets & cash flows	• sustainability threatened	**Finance Management Policy** • Control finance processes & checking mechanisms • Police Checks for office personnel • Insurance	• Discipline procedures • Deal with the immediate, then review policies • Review any relevant documents, implement change • Use adequate contingency fund if required
5.	Loss of communication, IT, records	• Cybersecurity attack or breach of security	• Loss of records • Loss of access to business systems	**Information & Communications Policy** • Security & Access control • Cybersecurity protection • Back-up records	• Check compliance to policies > update technology & procedures • Engage IT specialist to renew system • Ensure adequate contingency funds
6.	Human resource risk	Sudden loss, poor performance, wrong internal structure • Program Manager, Office/administration personnel • activity & event facilitators • key CoM members	• sustainability threatened • reputation damage	• Handover processes • Succession Planning for all key positions • PNH - HR Assist (for advice re setting up HR) • Pre-engagement suitability checking of all staff, volunteers and CoM members • Adequate training of all staff and volunteers in their role and in PNH Policy requirements	• Implement succession plans • Change model/structure • Use contingency fund if required for personnel
7.	Legal risk	• Non-compliance to laws, regulations • Serious complaint against staff member or PNH member	• sustainability threatened • loss of funding • reputation damage	• Integrity of operational polity & procedures • **Regulatory Compliance Audit** • Incident reporting procedures, complaint procedures • Good supervision practices	• Discipline procedures • Deal with the immediate, then review policies • If required, involve police
8.	Injury to persons	Refer to Hazards Register, **OH&S Framework, Child Safe Policy**	• Harm to person	• OH&S Audit & Child Safe audit annually • Public Liability Insurance/Workcover	• As above, emergency procedures check list in OH&S checklist & Child Safe checklist

Appendix 2: Contingency Fund Analysis

A contingency fund is required for managing risk (as per the Risk Register).

This is an analysis of funds required for contingency.

	Serious Risk	Resource Requirements	Expected Recovery Time	Contingency Fund
1.	Decline in membership, participation, and unable to broaden the membership demographics (as per strategic plan) (sustainability)	May need contingency fund to implement change of personnel		$10,000
2.	Serious loss of human resources (e.g. sudden resignation of program manager)	[cost of interim personnel, recruitment procedures]	4 - 6 months	$50,000
3.	Serious loss of facilities (e.g. due to fire or loss of lease)	[cost of local venues to move operations for next year]	4 -6 weeks to find venues and get established	$10,000
4.	Serious loss of revenue (e.g. loss of DFFH funding)	[cost of running the program until funding can be restored]	-program can keep running -12 months to restore DFFH funding (with emergency reduction of operational costs)	$65,000
5.	Loss of revenue due to internal circumstances, e.g. fraud	Ensure adequate contingency funds		$20,000
6.	Serious loss of communications, IT, records	[cost of getting system back up]	1 -2 week	$10,000
7.	Legal risk	N/A		
8.	Injury to persons	N/A		
				Total $165,000

Committee decided that the contingency fund will be at least one year equivalent to the operational expenses = $120K (to be reviewed annually)

Appendix 3: Annual Compliance & Risk Audit Checklist

Auditors:	Date of audit

		Items to check for compliance	Audit notes	✓
1.	Contingency Fund Analysis	• Reviewed annually		

2.	Insurance requirements	• Our public liability insurance requires that:
		  • Must have risk management system and use it in decision making (Risk Management - AS/NZS ISO 3100:2009)
		  • Contractors must have their own insurance OR it must be covered in the agreement with PNH (Activity Facilitator agreement)
		  • Car-pooling - all cars must have comprehensive insurance (Risk Management Policy)
		  • All payment to activity facilitators MUST be made to the facilitator from PNH (not activity participants) DFFH agreement
		  • Must have an asset register as per policy rule 6 this document
		• Cyber security - Cyber attack not covered by public liability - covered by adequate back up procedures/practices. Back-up security?
		• Is all insurance adequate?
		• WorkCover under Fair Work Act/Employees - in place		

3.	CAV - regulatory processes	• Annual reporting complies with regulations		
4.	ATO	• Reporting requirements completed		
5.	ACNC (charity)	• Reporting requirements completed		
6.	DFFH Reporting & meeting agreement requirements	• Regulated by reporting requirements - completed satisfactorily • IT Policy - eBusiness Access doc page 7 of 11		
7.	Barwon Network of Neighbourhood Centres, & Neighbourhood Houses Victoria	• Reporting requirements completed • Contract requirements met		
8.	CoGG	• Lease contract requirements met • Reporting? • Other?		
9.	Any other contracts/partnership agreements?	• Film Society Partnership Agreement - obligations met		

		Items to check for compliance	Audit notes	✓
10.	Liquor Licensing	• As per Activity and Event Management Policy (and as per legal requirement)		
11.	Privacy Act 1988, including Confidentiality & compliance to Health Records Act (Victoria) 2001	• Privacy & confidentiality **policy** is covered in CoM Handbook, Employee Handbook, Activity Facilitator Handbook, Office Policy & procedures documentation • Privacy & confidentiality responsibilities is covered in all **position descriptions** (CoM, Employees, Activity Facilitators, all volunteers) • Employees, Activity Facilitators (fee-for-service and volunteers), Office personnel - all sign an **engagement agreement with PNH** which contains compliance clause for privacy & confidentiality • Discussion with representatives from committee, office, activity facilitators and other operational personnel, to ensure policy is known and compliance strong		
12.	Discrimination & Harassment legislation (Code of Conduct)	Policy = Code of Conduct • Reporting non-compliance via OH&S incident or grievance procedures - clear procedures • Access & equity is a standard for activities & events - evaluated as part of operational performance evaluation framework • Member feedback opportunity - members survey and subsequent focus groups procedures working, suggestion box, access to Program Manager • Discussion with representatives from committee, office, activity facilitators and other operational personnel, to ensure legal requirements are known and compliance strong - our framework and procedures work? This section includes: Age Discrimination Act 2004 (Australia), Australian Human Rights Commission Act 1986, Disability Discrimination Act 1992 (Australia), Racial Discrimination Act 1975 (Australia) Sex Discrimination Act 1984 (Australia), Equal Opportunity Act 2010 (Victoria) Child Safe Standards (Victorian Government)		
13.	Fair Work Act	**Policy** in Employee Handbook • Employees comply with policies • CoM comply with employee management practices (in management of staff) • Workcover		
14.	WorkSafe	• OH&S Audit Checklist (for compliance to legal requirements) completed annually		
15.	Child care/safety regulations	• As part of OH&S Audit completed annually		
16.	Constitution	• Compliance with all rules • Membership rules - *Compliance to membership procedures (Act & Constitution) and rules for AGM & elections (Act & Constitution) should be part of Governance Committee*		

		Items to check for compliance	Audit notes	✓
17.	CoM	• Committee members comply to Code of Conduct as per Committee Member position descriptions (CoM Handbook) - Self regulated by CoM, self-assessment procedures (includes legal requirements) • Handover processes (Risk Management) satisfactory • Succession Planning for all key positions (Risk Management) satisfactory • PNH - HR Assist (for advice re setting up HR) (Risk Management) - satisfactory point for assistance (it costs us?) • All CoM members compliant with ACNC Governance Standard 5		
18.	CoM delegations	• Charter of Delegations - compliance to policy • TOR compliance		
19.	Activity & Event Management Policy	• Audit checklist in this document completed (including integration/alignment of policy)		
20.	Record Management Public records Act 1973 Vic	• Official PNH records (except finance) - 7 years electronic records (secure?) • Financial records 7 years (secure?) • **Security register - security & access controlled (as per Risk Policy)** • Asset register - assets controlled, note: DHHF service agreement, no 7, disposing of items over $5000 - need departments consent • Storage register is current • *Activity Register is current / other registers?*		
21.	PNH Information & Communications Policy	• *(to be added when policy is completed)*		
22.	PNH Compliance & Risk Management	• Mitigation Strategies and Contingency Strategies of Risk Management Framework adequate/reviewed annually • Police Checks for office personnel and CoM • Working with Children Checks for all staff/volunteers who have contact with children and for CoM members		
23.	PNH Finance Management Policy	• Secure money handling procedures documented and implemented • Good financial forecasting and budgeting (risk management) • **Contingency Fund Analysis completed and implemented in budget** • Contractors e.g. paid activity facilitators, must have their own insurance OR it must be covered in the agreement with PNH (insurance requirement) • All payment to activity facilitators MUST be made via PNH account (no cash payments) • Al invoices via Program Manager or Treasurer (non from personal email accounts) • *(to be added when policy is completed)*		
24.	Activity Facilitator Handbook	• Policies and procedure compliance (and aligned)		
25.	Reception Counter Handbook/Office Procedures	• Policies and procedure compliance • Clear processes for when Program Manager is absent		
26.	Complaints procedures	• Clear to members and visitors		

Compliance & Risk Action Plan post audit

Send this Risk Action Plan to Program Manager and to CoM

- include any recommendations to update PNH policy including identification of risks without adequate mitigation of contingency

	Item	Action	Reason for action
1			
2			
3			
4			

Suggested changes to this audit checklist

	Item	Suggested Change	Reason for change

Appendix 4: The Basics of ISO 31000 – Risk Management

This article will discuss the structure and key elements of ISO 31000 Risk Management.

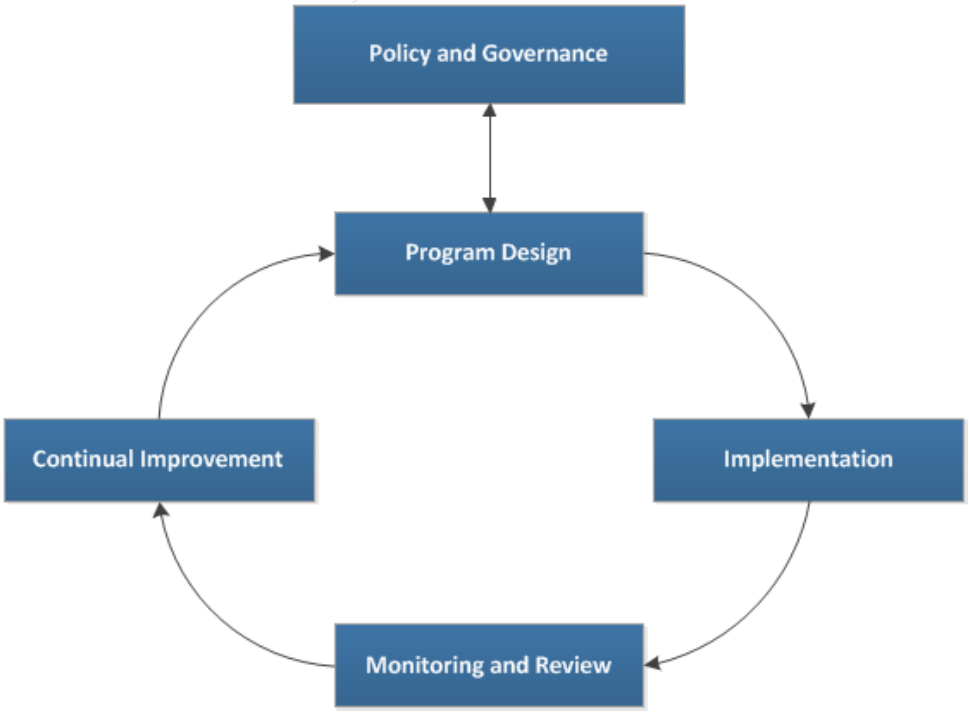
The two primary components of the ISO 31000 risk management process are:

- The Framework, which guides the overall structure and operation of risk management across an organization; and
- The Process, which describes the actual method of identifying, analyzing, and treating risks.

Framework
The ISO 31000 Framework mirrors the plan, do, check, act (PDCA) cycle, which is common to all management system designs. The standard states, however, that, "This Framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system". This statement should encourage organizations to be flexible in incorporating elements of the framework as needed.

Major elements of the Framework include:

- **Policy and Governance**
  Provides the mandate and demonstrates the commitment of the organization
- **Program Design**
  Design of the overall Framework for managing risk on an ongoing basis
- **Implementation**
  Implementing the risk management structure and program
- **Monitoring and Review**
  Oversight of the management system structure and performance
- **Continual Improvement**
  Improvements to the performance of the overall management system



Process design is an important step because the Framework provides the stability and continuity to assist in establishing a program as opposed to just executing a project.

Key elements that organizations should not overlook include:

- Establishing management commitment both during the implementation and on a long-term basis, including:
    - Development and approval of a formal policy
    - Identification and allocation of needed resources, including sufficient expertise and budget to sustain the program
    - Establishment of a regular review cycle to maintain program visibility to management and motivate all participants
- Developing a program that works within the organization, its culture and environment, including:
    - Understanding the external forces – industry trends, regulatory requirements, and expectations of key external stakeholders
    - Understanding the internal forces – existing governance, organizational structure, culture, and organizational capabilities

The extent to which an organization considers and implements any of these elements is dependent on the organizational purpose and needs. The goal is a visible, adequately-equipped program that is compatible with the organization's culture and objectives and sustainable for the long-term.

Process

After establishing the risk management Framework, an organization is ready to develop the Process. The Process, as defined by ISO 31000, is "multi-step and iterative; designed to identify and analyze risks in the organizational context."

Major elements of the Process, as seen in the diagram below, include:

- Active Communication
    - Communication and consultation with all stakeholders
- Process Execution
    - Establishing the context
    - Risk identification
    - Risk analysis
    - Risk evaluation
    - Risk treatment
- Oversight
    - Similar to the Framework, regular monitoring and review is required

The actual process of assessing risks first requires definition of what ISO 31000 calls the "context". The context is a combination of the external and internal environments, both viewed in relation to organizational objectives and strategies. The context setting process begins during the Framework phase with the examination of the organization's internal and external environments, but management should continue this assessment in greater detail here and focus on the scope of the particular risk management Process.

The remaining assessment steps involve developing techniques to identify, analyze, and evaluate specific risks. While multiple documented methods and techniques exist, all should include the following key elements:

- Risk Identification
    - Identification of the sources of a particular risk, areas of impacts, and potential events including their causes and consequences
    - Classification of the source as internal or external
- Risk Analysis
    - Identification of potential consequences and factors that affect the consequences
    - Assessment of the likelihood
    - Identification and evaluation of the controls currently in place
- Risk Evaluation
    - Comparison of the identified risks to the established rick criteria
    - Decisions made to treat or accept risks with consideration of internal, legal, regulatory and external party requirements

Overall, management should develop and implement risk treatments to reduce residual risks to levels acceptable to key stakeholders and monitor/adjust to ensure efficiency and effectiveness.

Relationship to ASIS SPC.1-2009 and Business Continuity

SPC.1 presents a somewhat more limited scope, defining Organizational Resilience in terms of security, preparedness and continuity while ISO 31000 maintains a broader – perhaps more strategic – focus. Regarding business continuity, it is just one of the many risk treatments that would comprise a more strategic risk management program espoused by ISO 31000. As a result, business continuity should be viewed a sub-component of the risk management program described in ISO 31000 because it addresses one specific risk (process, resource and technology availability).

Conclusions

Overall, the risk management principles and processes described in ISO 31000 and supported by the guidance of ISO/IEC 31010 provide a robust system that allows an organization to design and implement a repeatable, proactive and strategic program. The design of specific program elements is highly dependent on the goals, resource, and circumstances of the individual organization. Regardless of the level of implementation, management involvement in setting direction and regularly reviewing results should be a part of every program, which will not only elevate the management of risk, but also ensure an appropriate treatment of risk based on organizational objectives and long-term strategies.