Community Centres SA Board Governance

Participant Reference Notes

Topic: Why Boards Matter – Advanced Governance Training

Board Responsibilities -

Core Board Functions:

- Make decisions in the centre's best interest, aligned to the strategic plan
- Maintain strong financial management through diligent budgeting processes and regular oversight
- Ensure professional legal compliance and meet all legal obligations
- Manage and declare conflicts of interest appropriately
- Protect confidential information and maintain security
- Focus on high-level business decisions rather than operational details
- Recruit board members strategically using the Board Skills Matrix

---

Board Effectiveness Principles

Essential Practices for Effective Boards:

- **Be Prepared:** Read board papers thoroughly before meetings
- **Focus Strategically:** Concentrate on strategy and governance, not operations
- **Review Regularly:** Ensure policies and procedures are current and effective
- **Utilise Skills:** Understand and apply your unique skillset
- **Stay Organised:** Set priorities, maintain agenda focus, ensure one voice at a time

---

Essential Board Skills

Critical Skills Around the Board Table:

- **Financial Literacy:** Understanding budgets, financial reports, and fiscal oversight
- **Sector Knowledge:** Deep understanding of community services, local diversity, challenges, and impact opportunities
- **Strategic Planning:** Ability to create future-focused, sustainable plans
- **Risk Management:** Experience in identifying, assessing, and mitigating organisational risks
- **Legal/Governance:** Background in compliance, regulatory requirements, and governance frameworks
- **Technology & AI:** Understanding of digital transformation, cybersecurity, and artificial intelligence implications
- **Community Advocacy:** Skills to identify and respond effectively to local community needs

Note: Not every director needs all skills, but collective board appointments should comprehensively cover these areas.

Community Development Focus

Board Skills Matrix –

BOARD SKILLS MATRIX – Rank your skill level between 1 – 4 for each skill.
Skills Assessment Instructions
Please rate your proficiency in each skillset using the scale of 1-4, where 1 indicates no knowledge or skills in this area, and 4 represents high expertise and extensive experience. A strong board requires diverse skills around the table, so it's perfectly acceptable if some areas aren't relevant to your background. This assessment helps us identify both our collective strengths and potential gaps to address through targeted recruitment or professional development. Your honest self-evaluation is valuable for building a well-rounded board that can effectively govern our organisation.
4 = Skilled or Knowledgeable with experience (5+ years) 3 = Some knowledge with experience (0-5years) 2 = some knowledge without any experience 1 = No qualifications or experience

BOARD SKILL	SKILL DESCRIPTION	DIRECTOR 1	DIRECTOR 2	DIRECTOR 3	DIRECTOR 4
BRAND & MARKETING	Expertise in brand strategy, marketing communications, and public relations to guide organisational positioning and increase visibility and community engagement.				
COMMUNITY, ENGAGEMENT & NETWORKING	Skills in building relationships, engaging with stakeholders, and representing the organisation within the broader community to enhance its impact and reputation.				
CULTURAL & DIVERSITY	Experience with diverse communities across age, nationality, and religion, including knowledge of inclusion practices and ability to represent varied perspectives in decision-making and program development.				
DIGITAL, TECHNOLOGY & AI	Knowledge of digital transformation, cybersecurity, and emerging technologies to provide strategic guidance on tech investments and digital risk management.				
GOVERNANCE	Experience of governance through Board appointments at other organisations or through former senior management experience				
FINANCE AND ACCOUNTING	Finance and accounting experience with a recognised accounting qualification. Skills to chair the Audit, Finance and Risk committee.				
HUMAN RESOURCES	Experience in talent management, organisational development, and employment policies to guide staff development and create a healthy organisational culture.				
STRATEGY	Experience of strategic oversight, including the development and implementation of strategic plans.				

Purpose and Application: A board skills matrix assists in determining required skills and experience for optimal board composition by:

- Aligning board composition to organisational strategy and sector requirements
- Identifying skills deficits and gaps for succession planning
- Guiding professional development and training priorities
- Informing targeted recruitment for new board members

Assessment Approach:

- Skills categorised as 'Essential,' 'Desirable,' or 'Purchasable'
- Annual assessment of all directors against matrix criteria
- Gap analysis informs board development and recruitment strategies

Key Self-Assessment Questions

Financial Oversight:

- What financial metrics are most important for regular monitoring?
- How would you approach reviewing budget variances?

Legal Compliance:

- What regulatory requirements affect our organisation?
- How would you respond to potential compliance shortfalls?

Conflict Management:

- What constitutes a conflict of interest in our context?
- What's the proper process for declaring and managing conflicts?

Governance vs Operations:

- How do you distinguish governance matters from operational issues?
- What strategies prevent operational drift in board meetings?

Chair Selection and Responsibilities

Key Chair Functions:

- Balance operational oversight with mission-driven strategic focus
- Serve as primary liaison between board and executive leadership
- Provide clear direction based on board decisions
- Conduct regular CEO check-ins and performance evaluations
- Maintain healthy governance-operations boundaries
- Facilitate effective board-management communication
- Collaboratively set strategic meeting agendas

Selection Criteria:

- Leadership skills and relevant experience
- Ability to complement existing board strengths
- Transparent selection process based on organisational needs
- Capability to facilitate meetings and guide strategic direction

---

Staff Safety and Governance

Standing Requirements:

- Staff safety as standing agenda item for all board meetings
- Board review of all staff safety policies and procedures
- CEO maintenance of incident register with actions and outcomes

Key Oversight Policies:

- Social media guidelines
- Anti-bullying measures
- Harassment prevention protocols
- Psychosocial wellbeing programs

Board vs CEO Management Roles

Board Responsibilities (What & Why):

- Set strategic parameters and long-term direction
- Evaluate outcomes and provide oversight
- Approve resources and major decisions
- Ask strategic questions and think long-term
- Maintain confidential information security

CEO/Management Responsibilities (How & When):

- Work within board-established parameters
- Manage processes and daily operations
- Deploy approved resources effectively
- Provide detailed operational answers
- Handle short-term operational needs

Risk Management Framework

Risk Management Process:

- Establish formal risk register for identification, assessment, and monitoring
- Categorise risks: financial, operational, reputational, compliance, strategic
- Implement internal controls and mitigation strategies
- Assess risks by likelihood and potential impact
- Assign risk owners for accountability
- Review risk register quarterly or as circumstances require

Additional Considerations:

- Develop contingency plans for major risk scenarios
- Ensure adequate insurance coverage
- Consider reputational impacts in all decisions
- Document risk discussions in board minutes

Conflict of Interest Management

Declaration Requirements:

- Declare actual, potential, or perceived conflicts immediately when they arise
- Establish annual declaration process for ongoing conflicts
- Include conflicts as standing first agenda item in all meetings

- Provide clear definitions of what constitutes conflicts
- Ensure all directors understand legal disclosure obligations

Management Principles:

- Affected directors must abstain from voting on related matters
- Board determines appropriate participation levels during discussions
- Prevent undue influence over other board members
- Document all conflicts thoroughly in meeting minutes
- When in doubt, err on the side of disclosure

Strategic Planning Framework

Core Purpose: Strategic planning creates a clear 3-5 year roadmap, providing shared vision and aligned decision-making throughout the organisation.

AICD Five Critical Questions:

1. Why does this organisation exist?
2. What does this organisation do?
3. Who does this organisation benefit?
4. How will this organisation achieve its goals?
5. What does success look like for this organisation?

Vision, Mission, and Values

Vision Statement Characteristics:

- Inspirational and motivating
- Future-focused and aspirational
- Clear and easily understood
- Memorable without reference materials

Mission Statement Elements:

- Defines fundamental purpose and core activities
- Explains current identity and function
- Present-focused and practical
- Describes day-to-day organisational work

Strategic Values Purpose:

- Provide consistent decision-making framework
- Define organisational identity and culture
- Help prioritise competing options and resources
- Communicate commitments to stakeholders
- Establish evaluation criteria for strategies and behaviours

---

Strategic Implementation

Strategic Themes Examples:

- Community Connection: Bringing people together across diverse backgrounds
- Inclusive Programming: Meeting needs of all ages, cultures, and abilities
- Financial Resilience: Developing sustainable funding and efficient operations
- Space Optimisation: Maximising facility utilisation for community benefit
- Community Wellbeing: Promoting health, learning, and social support services

Strategic Initiatives: Specific, actionable projects with clear goals, timelines, resource requirements, and success measures that advance strategic themes.

Strategic Milestones: Measurable achievements marking significant progress, serving as checkpoints for evaluation, course correction, and momentum maintenance.

Board Succession Planning

Key Elements:

- Plan for director departures and strategic recruitment
- Identify current skill gaps using skills matrix
- Support comprehensive induction of new directors
- Consider appropriate term limits for fresh perspectives
- Pursue ongoing training and professional development
- Document key processes for organisational continuity

Effective Governance Practices

Essential Components:

- Clear board charter defining roles and responsibilities
- Regular meetings with structured, strategic agendas
- Comprehensive governance policies and procedures
- Proper onboarding and orientation for new members
- Clear distinction between operational and strategic roles
- Diversity and inclusion considerations in recruitment
- Annual board performance reviews and evaluations
- Appropriate tenure considerations for board positions

Decision-Making Excellence

Decision-Making Framework:

- Align all decisions with mission and strategic plan
- Encourage constructive debate and diverse perspectives
- Avoid groupthink and confirmation bias
- Use data and evidence whenever possible
- Allow adequate time for complex decisions
- Ensure information is provided in advance

- Consider impacts on all stakeholders
- Reflect organisational values in all choices

Industry Knowledge Application: Strong governance requires thoughtful decision-making grounded in community services expertise, with every choice supporting the core mission and strategic direction.

Compliance Management

Compliance Framework:

- Establish compliance calendar for regulatory requirements
- Conduct regular compliance audits and assessments
- Stay informed about relevant legislative changes
- Ensure proper financial controls are implemented
- Review policies regularly to maintain ongoing compliance
- Document compliance discussions and decisions

Technology, Cybersecurity & AI Governance

Understanding the Basics: Why This Matters for Community Centres

What is Cybersecurity? Cybersecurity is protecting your organisation's digital information, systems, and operations from online threats. Think of it as digital security - just like you lock your building, you need to protect your computers, data, and online services.

What is Artificial Intelligence (AI)? AI refers to computer systems that can perform tasks that typically require human intelligence - like understanding language, recognising patterns, or making decisions. Examples include chatbots that answer questions, systems that recommend services to community members, or tools that help with scheduling and administration.

Why Community Centres Are Targets:

- You hold personal information about community members
- You handle financial transactions and donations
- You often have limited IT security resources
- Staff and volunteers may not have technical security training
- Your services are essential to the community, making disruption impactful

Board Oversight Framework

Governance and Accountability:

- Designate a board member or committee to oversee cyber/AI risks (this doesn't require technical expertise - focus on asking the right questions)
- Integrate cyber and AI risks into your organisation's existing risk management framework
- Define clear risk appetite and tolerance levels for cyber and AI-related exposures
- Focus on policy approval and risk tolerance setting, not day-to-day technical implementation

Cybersecurity Essentials - What Boards Need to Know

Understanding Common Cyber Threats

Phishing Attacks:

- **What it is:** Fake emails that trick people into clicking malicious links or sharing passwords
- **Example:** An email that looks like it's from your bank asking you to "verify your account"
- **Impact:** Can lead to stolen passwords, compromised accounts, or malware installation

Ransomware:

- **What it is:** Malicious software that locks all your computer files and demands payment to unlock them
- **Example:** Staff arrive to find they can't access any files, bookings systems, or member databases
- **Impact:** Can shut down all operations for days or weeks

Data Breaches:

- **What it is:** Unauthorised access to personal information you store about community members
- **Example:** Hackers accessing member contact details, medical information, or financial records
- **Impact:** Legal liability, fines, loss of community trust, notification requirements

Social Engineering:

- **What it is:** Manipulating people to reveal confidential information or perform actions
- **Example:** Someone calling pretending to be from IT support asking for passwords
- **Impact:** Can bypass all technical security measures through human manipulation

Critical Protection Areas for Community Centres

Financial Systems Protection:

- **Why it matters:** Community centres handle memberships, donations, grants, and program fees
- **Key actions:** Implement strong banking controls, require multiple approvals for transfers, consider cyber insurance
- **Board oversight:** Review financial access controls and approval processes regularly

Member Data Protection:

- **Why it matters:** You're legally required to protect personal information; breaches can result in fines and lawsuits
- **Key actions:** Only collect necessary information, store securely, have proper data handling policies
- **Board oversight:** Ensure data privacy policies exist and staff are trained on them

Operational Continuity:

- **Why it matters:** Cyber attacks can shut down booking systems, communications, and access controls
- **Key actions:** Maintain offline backups, have manual backup procedures, test recovery plans
- **Board oversight:** Ensure business continuity plans include cyber incident scenarios

Staff and Volunteer Training:

- **Why it matters:** 95% of cyber breaches involve human error - clicked links, weak passwords, social engineering
- **Key actions:** Regular practical training on recognising threats, strong password practices, reporting procedures
- **Board oversight:** Monitor training completion rates and effectiveness

Essential Security Measures (What to Ask Management)

Authentication and Access:

- Are we using strong, unique passwords for all systems?
- Do we have two-factor authentication (requiring both password and phone verification) on important accounts?
- Do we regularly review who has access to what systems?

Backups and Recovery:

- Do we have recent, tested backups of all important data?
- Are backups stored separately from our main systems?
- How quickly can we restore operations if our systems are compromised?

Software and Systems:

- Are all our computers and software kept up-to-date with security patches?
- Do we have antivirus software on all devices?
- Are we monitoring our systems for unusual activity?

Vendor and Third-Party Management:

- Do we understand what security measures our IT providers and software vendors have?
- Are we clear on what they protect versus what we're responsible for?
- Do we have contracts that address security requirements and incident response?

AI Governance Framework - A Beginner's Guide

Understanding AI in Community Centres

Current AI Uses You Might Already Have:

- Website chatbots that answer basic questions
- Email spam filters
- Online booking systems that suggest times
- Social media algorithms that determine who sees your posts
- Translation tools for multilingual communications

Emerging AI Applications:

- Virtual assistants for member services
- Automated program recommendations based on member interests
- Predictive analytics for resource planning
- Automated scheduling and resource allocation
- Content creation for newsletters and social media

Key AI Risks and Considerations

AI Bias and Fairness:

- **What it means:** AI systems can inadvertently discriminate against certain groups
- **Example:** An AI booking system that consistently prioritises certain types of programs over others
- **Board oversight:** Ensure AI decisions are regularly reviewed for fairness and bias

Data Privacy and AI:

- **What it means:** AI systems often require large amounts of data to function
- **Example:** An AI system analysing member behaviour patterns to improve services
- **Board oversight:** Ensure AI systems comply with privacy laws and only use necessary data

Transparency and Explainability:

- **What it means:** Understanding how AI systems make decisions
- **Example:** If AI recommends program cuts, can management explain why?
- **Board oversight:** Require that AI decisions affecting operations can be explained in plain language

Human Oversight and Control:

- **What it means:** Ensuring humans can override AI decisions when needed
- **Example:** Always having staff available to help members who can't use automated systems
- **Board oversight:** Ensure human alternatives exist for all AI-powered services

AI Governance Questions for Boards to Ask Management

Strategy and Planning:

- What AI tools are we currently using, and who approved their adoption?
- What's our strategy for evaluating new AI tools?
- How do we ensure AI supports rather than replaces our community-focused mission?

Risk Management:

- How do we test AI systems for bias, especially against vulnerable community members?
- What happens when AI systems make mistakes or cause problems?
- How do we protect member data when using AI tools?
- Do we have clear policies about which AI tools staff can and cannot use?

Community Impact:

- Are we creating barriers for less tech-savvy community members?
- Do members know when they're interacting with AI versus humans?
- How do we measure whether AI is actually improving our services?
- Are we maintaining personal, human-centred service options?

Compliance and Legal:

- Are we complying with privacy laws when using AI?
- Do we understand our legal liability if AI systems cause harm?
- Are we transparent with members about how we use AI?

Community Impact and Inclusion

Ensuring Technology Serves Everyone:

- **Digital Divide Considerations:** Not all community members have equal access to or comfort with technology
- **Accessibility Requirements:** AI and digital systems must work for people with disabilities
- **Cultural Sensitivity:** Technology should respect diverse cultural backgrounds and languages
- **Alternative Options:** Always maintain non-digital ways to access services

Questions to Ask:

- Will this technology exclude or disadvantage any community groups?
- Are we providing adequate support and training for less tech-savvy members?
- Do our AI systems understand and respect cultural differences?
- Can members opt out of AI-powered services if they prefer human interaction?

Personal Security for Board Directors

Why Board Members Are Targets

Board members are attractive targets because you have:

- Access to financial information and decision-making authority
- Personal details of other board members and staff
- Strategic information about the organisation
- Often limited cybersecurity training but significant access privileges

Essential Personal Security Practices

Password and Account Security:

- **Use unique passwords:** Never reuse passwords between different accounts
- **Use a password manager:** Tools like Bitwarden or LastPass generate and store secure passwords
- **Enable two-factor authentication:** Require both password and phone verification for important accounts
- **Examples:** Your board email, banking access, cloud storage accounts

Safe Communication Practices:

- **Use organisation email only:** Never conduct board business through personal email accounts
- **Verify unusual requests:** If someone asks you to transfer money or change banking details, verify through a separate communication method
- **Be cautious with attachments:** Don't open unexpected attachments, even from people you know

Document and Data Security:

- **Use approved platforms only:** Store board documents only in organisation-approved cloud storage or secure devices
- **Avoid public WiFi:** Don't access sensitive board materials on public WiFi networks
- **Lock your devices:** Use passcodes/passwords on phones, tablets, and laptops

AI Tool Usage Guidelines:

- **Never input confidential information:** Don't put board meeting notes, financial data, or member information into public AI tools like ChatGPT
- **Understand data retention:** Many AI tools store and learn from your inputs
- **Use organisation-approved tools only:** If the organisation provides AI tools, use those instead of public ones
- **Be transparent:** If you use AI to help draft documents, disclose this when appropriate

Recognising Social Engineering Attacks

Common Tactics Targeting Board Members:

- **Urgency pressure:** "This needs to be done immediately, or we'll lose funding"
- **Authority impersonation:** Someone pretending to be the CEO, bank, or government agency
- **Familiar relationship abuse:** Using knowledge about your colleagues or organisation to seem legitimate
- **Bypass requests:** "Can you approve this quickly to avoid the usual process?"

Red Flags to Watch For:

- Urgent requests for financial information or transfers
- Unexpected requests to change banking details or payment methods
- Pressure to bypass normal approval processes
- Communications that seem unusual for the sender
- Requests to click links or download files unexpectedly

Financial and Strategic Considerations

Understanding Cyber Risk Costs

Direct Financial Impacts:

- **Business interruption:** Lost revenue while systems are down
- **Recovery costs:** IT support, system rebuilding, data recovery
- **Regulatory fines:** Penalties for data breaches or privacy violations
- **Legal costs:** Lawsuits from affected community members or partners

Indirect Costs:

- **Reputation damage:** Loss of community trust and member confidence
- **Increased insurance premiums:** Higher costs for cyber insurance
- **Staff time:** Significant staff hours dealing with incident response
- **Member impact:** Disrupted services affecting community relationships

Budget Considerations for Small Organisations

High-Impact, Low-Cost Security Measures:

- **Staff training:** Regular cybersecurity awareness training (often available free online)
- **Strong authentication:** Two-factor authentication and password managers
- **Backup systems:** Cloud-based backup services
- **Basic security software:** Antivirus and anti-malware protection

Medium-Cost Investments:

- **Cyber insurance:** Coverage for breach response and liability
- **Professional IT support:** Regular security assessments and maintenance
- **Secure communication tools:** Encrypted email and messaging platforms

Questions for Budget Planning:

- What would it cost us if we couldn't operate for a week?
- How much would it cost to rebuild all our systems and data?
- What's the potential fine if we have a data breach?
- How does this compare to the cost of prevention measures?

Regulatory Compliance and Legal Responsibilities

Privacy and Data Protection

What You Need to Know:

- **Australian Privacy Principles:** Requirements for how you collect, store, and use personal information
- **Notifiable data breaches:** Legal requirement to report certain breaches to authorities and affected individuals
- **Consent requirements:** When and how you need permission to collect and use personal data

Board Responsibilities:

- Ensure privacy policies exist and are followed
- Understand notification requirements for data breaches
- Review contracts with service providers regarding data handling
- Monitor compliance with privacy training for staff

Emerging AI Regulations

Current Regulatory Landscape:

- AI regulations are rapidly evolving globally
- Australian government is developing AI governance frameworks
- Industry-specific regulations may apply to community services
- International regulations may affect organisations using global AI tools

Board Oversight Requirements:

- Stay informed about emerging AI regulations in your sector
- Ensure AI use complies with existing privacy and discrimination laws
- Review AI vendor contracts for compliance responsibilities
- Document AI decision-making processes for transparency

Board Reporting and Monitoring

Regular Reports Management Should Provide

Monthly Cyber Security Updates:

- Number and type of security incidents (attempted and successful)
- Status of security training completion
- Software update and patch status
- Backup testing results

Quarterly Risk Assessments:

- Review of risk register for cyber and AI risks
- Assessment of new threats or vulnerabilities
- Review of vendor security assessments
- Budget impact of security measures

Annual Comprehensive Reviews:

- Full cybersecurity assessment or audit
- Review of all AI tools and their governance
- Staff training effectiveness evaluation
- Insurance coverage adequacy review

Questions Boards Should Ask Regularly

About Cybersecurity:

- What cyber incidents have occurred since our last meeting?
- Are all staff completing required security training?
- When did we last test our backup and recovery procedures?
- Are we monitoring for new threats or vulnerabilities?

About AI Usage:

- What new AI tools are staff requesting or using?
- How are we ensuring AI systems are fair and unbiased?
- Are we complying with privacy requirements for AI use?
- How are we measuring the effectiveness of AI tools?

About Community Impact:

- Are any community members unable to access services due to technology barriers?
- How are we maintaining human alternatives to automated systems?
- What feedback are we receiving about our use of technology?

Action Steps for Boards

Immediate Actions (Next 30 Days)

1. **Designate responsibility:** Assign cyber and AI oversight to a board member or committee
2. **Request current status:** Ask management for inventory of current AI tools and recent cyber incidents
3. **Review policies:** Ensure basic cybersecurity and privacy policies exist
4. **Assess training:** Confirm staff are receiving regular cybersecurity awareness training

Short-term Actions (Next 90 Days)

1. **Risk assessment:** Conduct or commission a basic cybersecurity risk assessment
2. **Insurance review:** Evaluate current cyber insurance coverage
3. **Vendor assessment:** Review security practices of key IT vendors and service providers
4. **Policy development:** Develop basic AI governance policies and procedures

Ongoing Responsibilities

1. **Regular reporting:** Establish cyber and AI updates as a standing item on the board agenda
2. **Annual reviews:** Conduct comprehensive annual assessments of cyber and AI risks
3. **Stay informed:** Keep updated on emerging threats and regulations

Resources for Further Learning

Cybersecurity Resources:

- Australian Cyber Security Centre (ACSC) - cyber.gov.au
- Stay Smart Online - staysmartonline.gov.au
- Australian Privacy Commissioner - oaic.gov.au

AI Governance Resources:

- Australian Government AI Ethics Framework
- Responsible AI Network Australia
- Industry-specific AI guidelines for community services

Board Governance Resources:

- Australian Institute of Company Directors (AICD)
- Governance Institute of Australia
- Community sector governance resources

Remember: You don't need to become technical experts, but you do need to ask the right questions and ensure appropriate oversight of these critical risks.

These reference notes serve as your comprehensive guide to effective board governance for community centres.