CYBER OPPORTUNITY PROJECT ADVISORY BOARD

BUILDING OPPORTUNITY

PATHWAYS TO CYBER ASSURANCE

ADVISORY
BOARD
CENTRE

CONTENTS

ABOUT THE REPORT

The Cyber Opportunity Special Interest Forum was formed by the Advisory Board Centre as a project based Advisory Board to provide balance to the traditional risk focus and explore the opportunities for organisations to confidently explore and embrace digitisation and technology. Commencing in August 2020, the Project Advisory Board included living research gathered from 38 Advisors with global expertise and industry consultation with Captains of Industry.

The Cyber Opportunity Advisory Board report, *Building Opportunity - Pathways to Cyber Assurance*, captures the key outcomes of the research and its importance for businesses, the advisory community who support them and the wider collaboration ecosystem.

REPORT USAGE

The true value of research is realised when it is used to stimulate fresh thinking, robust discussion and informed action. We encourage you to use the report content to build conversations that are meaningful for you. The report is designed to provide value to key stakeholder groups with an interest in cyber including:

- The global professional advisory community supporting organisations with strategic insight and foresight at a board level.
- The support ecosystem to understand the importance of their role in collaboration including:
  - Funders and Investors
  - Education & Institutions
  - Technology Providers
  - Advisors & Directors
  - Industry Groups & Associations
  - Stakeholders & Community
  - Government

FOREWARD

Louise Broekman
Founder & CEO
Advisory Board Centre

As a global society that runs largely on technology, we are dependent on its availability and ability to safeguard our information. Amidst the disruption and uncertainty of the global COVID-19 pandemic technology has been both an enabler and a creator of economic impact.

The pandemic accelerated internal decision making around technology investment and implementation which has led to a pressing need for businesses and governments to not only adopt but also to adapt.

Just as technology brings increasing threats, it also brings increasing opportunities to grow businesses and create positive impact. Finding the balance between risk and reward requires collaboration and co-creation. Cybersecurity is not optional, but it must service the organisation's strategic plan.

As interconnected global citizens, the reality of living in a less secure time means that we must integrate awareness and protection into our personal and professional lives. The risk of cyber threat through loss and disruption is such an event that must be met head on with business minds to weave awareness and resilience into our commercial and social fabric.

To be led by fear misses out on the opportunity of taking control and deriving opportunity from a more confident and vigilant approach. Businesses can continue to grow and prosper, learning how to maintain and deepen trust by treating cyber risk as an opportunity to increase resilience and trust.

Trust is the currency that binds customers through confidence and assurance – cyber assurance. For companies to be able to protect their trust reputations, board must embrace cyber risk into their roles and practices.

As the professional body for the global advisory community, the Advisory Board Centre recognises the valuable role of strategic Advisors to provide independent advice and drive critical thinking at a board level to support executives, business owners and directors. I want to thank our community for lending their voice and their deep expertise to advance this important discussion.

EXECUTIVE SUMMARY

In this year alone we have seen social and economic changes that have affected us all personally and professionally. Across the globe we have witnessed both a willingness to adapt quickly to change and an almost equal resistance to the pervasive nature of modern technology. For our business interests we must deal with a heightened level of cyber risk.

Company and Advisory Boards that provide advice on Cybersecurity and Cyber Resilience need to be able to articulate the essential aspects of how Cyber Opportunity, through its relationship with service assurance, can enable strategic business objectives and be embodied into operations, processes and reporting.

The desired outcome is for the Board of Directors to understand that cybersecurity is a business responsibility, not a technological one, and relates to an organisation's ability to influence the positive aspects of uncertainty (opportunities), rather than focus investment on fear and negative uncertainty (threats).

The primary challenge for Advisory Boards and Advisors is to work in collaboration with the Board and Directors to integrate cyber risk into corporate governance and business growth.

Through initiatives like the Cyber Opportunity Project Advisory Board, the Advisory Board Centre and global professional community is prepared to support and enable this through solid frameworks, guidelines and methodologies that will empower the strategic ambitions of the organisations they serve.

Peter Day
Certified Chair
Cyber Opportunity
Project Advisory Board

Daniel Brewer
Certified Chair
Cyber Opportunity
Project Advisory Board

CYBER OPPORTUNITY PROJECT ADVISORY BOARD

> In the world of Cyberspace, there are few differentiators more critical than Cyber Assurance. This requires the building of trust through service availability, integrity, confidentiality and resilience. This is the culture of Cyber Opportunity.

PETER DAY
CERTIFIED CHAIR

PRINCIPLES FOR ADVISORS TO CONSIDER

Below are specific insights identified from the Advisory Community as principles for Directors and Advisors to consider.

Security by Design: products and services that are conceived, designed with security in mind and released cyber secure will enforce reputational trust.

Business Inclusive: critical business functions and processes achieve strategic intent not technology. Boards must integrate cyber and business risk.

Internal Support: maintaining a program of awareness and education about cyber risk keeps people and culture updated and doesn't stifle innovation.

Return on Security Investment: evaluate how an investment in security controls contributes to the achievement of strategic objectives. Boards need to integrate cyber risk into business thinking.

Reinvestment: assets, whether physical, people, or technology require reinvestment to maintain their currency and availability. Cyber risk is another dimension of business investment and planning.

The following are specific definitions noted from the advisory community as important for Boards and Directors to understand:

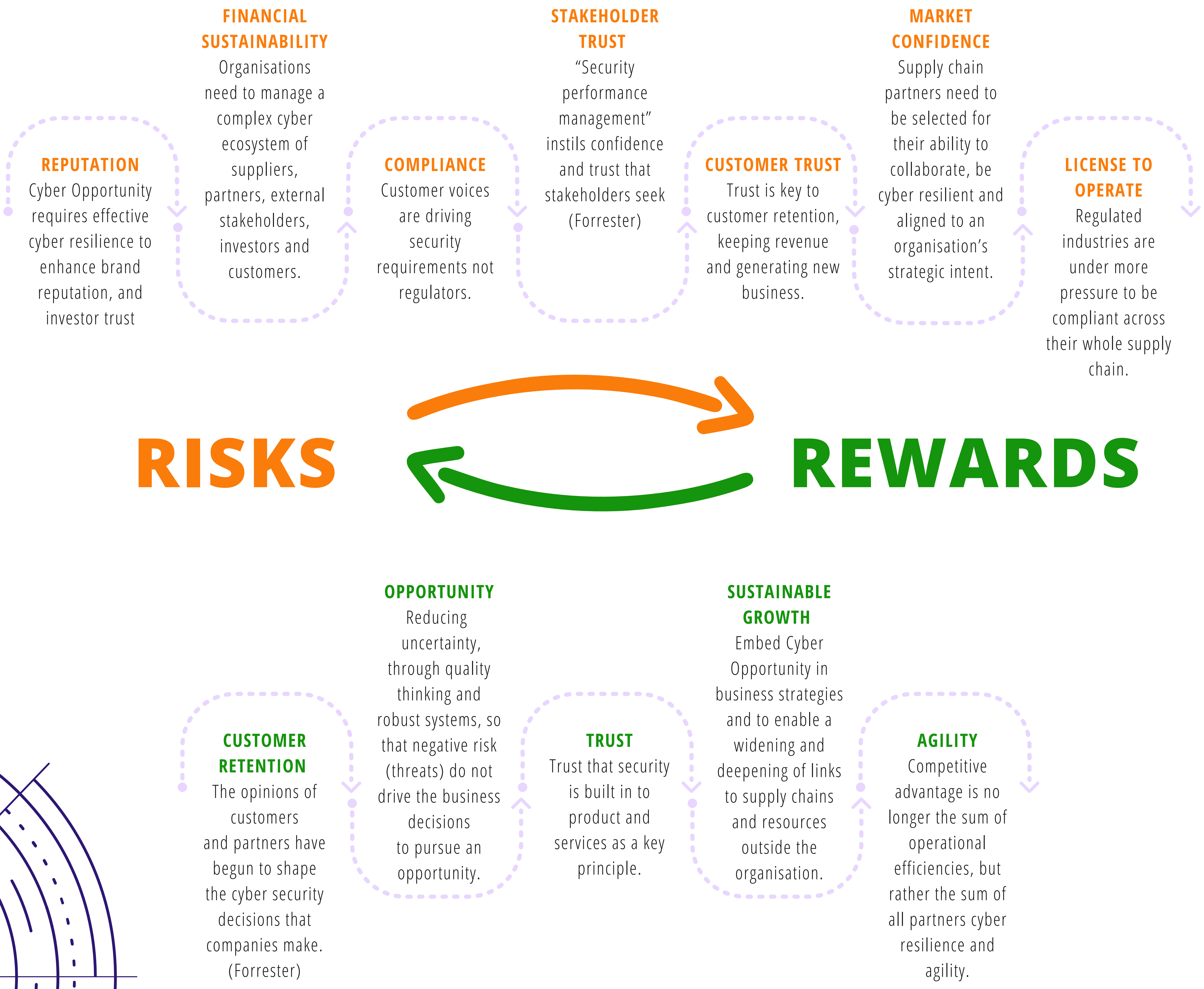
Security by Design: products and services are born cyber secure and are optimized for a higher risk economy.

Cyber Assurance: manages components of service assurance that are exposed to cyber risk and quantifies it into tangible measurements for the board.

Information Security: facilitates the protection and resilience of the critical data that enables critical business functions and processes, protecting the business, informing the board via cyber assurance.

Cyber Opportunity: the culture of leveraging benefits of cyber security to achieve strategic intent through positive risk management and determining value through strategy for the company's prosperity.

Attack Surface: points of entry, where an unauthorized entity can try to interrupt, disclose, modify, and or destroy data within the business environment. Quantifying the dimensions of the business at risk to the board.



REPUTATION
Cyber Opportunity requires effective cyber resilience to enhance brand reputation, and investor trust

FINANCIAL SUSTAINABILITY
Organisations need to manage a complex cyber ecosystem of suppliers, partners, external stakeholders, investors and customers.

COMPLIANCE
Customer voices are driving security requirements not regulators.

STAKEHOLDER TRUST
"Security performance management" instils confidence and trust that stakeholders seek (Forrester)

CUSTOMER TRUST
Trust is key to customer retention, keeping revenue and generating new business.

MARKET CONFIDENCE
Supply chain partners need to be selected for their ability to collaborate, be cyber resilient and aligned to an organisation's strategic intent.

LICENSE TO OPERATE
Regulated industries are under more pressure to be compliant across their whole supply chain.

RISKS

REWARDS

CUSTOMER RETENTION
The opinions of customers and partners have begun to shape the cyber security decisions that companies make. (Forrester)

OPPORTUNITY
Reducing uncertainty, through quality thinking and robust systems, so that negative risk (threats) do not drive the business decisions to pursue an opportunity.

TRUST
Trust that security is built in to product and services as a key principle.

SUSTAINABLE GROWTH
Embed Cyber Opportunity in business strategies and to enable a widening and deepening of links to supply chains and resources outside the organisation.

AGILITY
Competitive advantage is no longer the sum of operational efficiencies, but rather the sum of all partners cyber resilience and agility.

FORESIGHT

PRACTICAL APPLICATION FOR ADVISORY BOARD PROFESSIONALS

RISK

Risk is simply an uncertainty- not something to be feared. Whether in its negative form (threat) or its positive form (opportunity) it still needs to be understood in context to its impact to an organisation's strategic intent.

Investment in reducing an uncertainty needs to have a corresponding benefit, not just appease someone's fear; this is done with business alignment. (Gartner)

REWARDS

Rewards are positive outcomes for those who take the Risk, embrace the uncertainty and control it through collaboration, co-creation and investment in cyber opportunity as a business principle.

When outcomes are clearly defined and employees are given the opportunity to use their unique strengths and talents to accomplish, companies can trade on its trust protection to achieve growth and keep its customers.

INSIGHTS

David X Martin
Risk Management and
Cybersecurity Expert

> *"Most people assume the main function of cybersecurity is to reduce operational risk by eliminating the dangers posed by viruses and hackers. But it's time to reposition cybersecurity and for management and boards to see it for what it really is: a growth enabler as opposed to a growth inhibitor."*

MANAGEMENT CONSIDERATIONS

INSIGHTS

Cyber Opportunity, and the security principles and processes that underpin it, is a management discipline - not just a technical one. Boards and Executives will benefit from applying both curiosity and critical thinking to effectively consider risks and rewards.

PLANNING

- Security by Design
- Business inclusive
- Internal Support
- Return on Security Investment
- Reinvestment

FRAMEWORKS

- Incorporated into Enterprise Risk
- Integration into existing management capability
- Monitoring
- Governance
- External subject matter experts as support

FORESIGHT

PRACTICAL APPLICATION FOR ADVISORY BOARD PROFESSIONALS

PLANNING FOR BOARDS AND ADVISORS

- Establish a cyber language and framework that is clear and in business terms, tune it for the board operations
- Explore risk and uncertainty in terms of impacts to critical services and assets
- Do health checks on cyber knowledge, planning and education to improve awareness
- Use industry stories to educate, illustrate and evaluate cyber events, threats and risks
- Frame cyber risk in positive terms, identify the protections required for critical services and trust
- Being able to respond and recover to cyber threats is a prerequisite and assumption for service continuity and growth in trust.

MANAGEMENT FRAMEWORKS

- Cyber risk is a business risk, a board responsibility, they need to sponsor, evaluate and mitigate it within their roles and responsibilities
- Understanding requires a definition of what cyber risk is and what is means to a business' trust and operations
- By integrating cyber risk into enterprise risk, threats specific to critical assets/services can monitored and measured up through to the board
- Board members will benefit from incorporating cyber planning, evaluation and mitigation into the fabric of their governance processes
- Advisory boards are instrumental in providing the research, planning and communication for the cyber investigation boards and directors require.

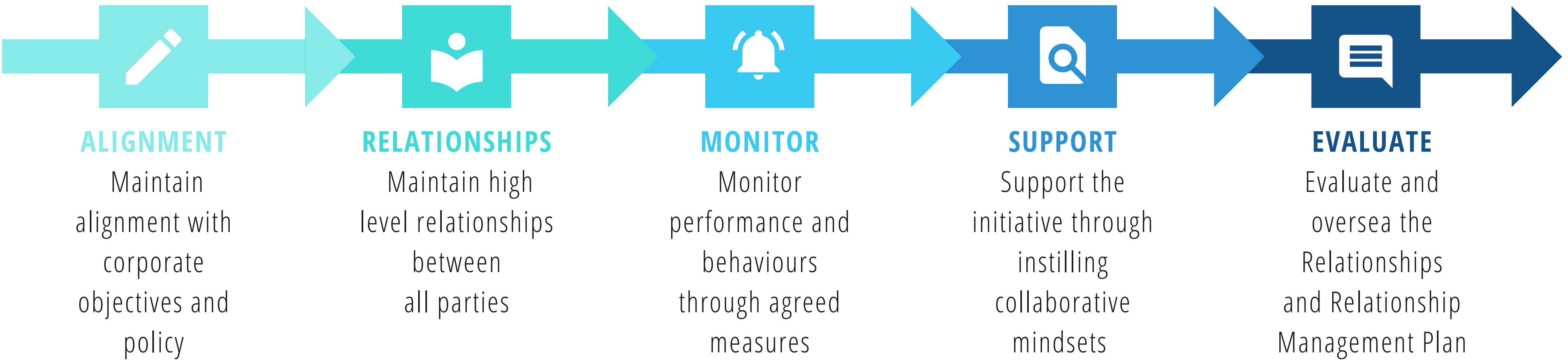
THE ROLE OF COLLABORATORS

Competitive advantage is no longer the sum of all efficiencies but rather the sum of all stakeholders (Forrester). Cyber Opportunity leverages collaboration to implement appropriate controls to manage risk to bring about a positive risk experience and allow collaborators to achieve their collective objectives. Collaborative Standards - ISO Standard 4401: 2017 provides a foundation for collaboration and co-creation.

ACHEIVING STRATEGIC INTENT THROUGH COLLABORATION

COLLABORATION is an association of two or more groups with the objective of participating in a common activity or pooling their resources for achieving a common goal.

COLLABORATORS focus on:



ALIGNMENT
Maintain alignment with corporate objectives and policy

RELATIONSHIPS
Maintain high level relationships between all parties

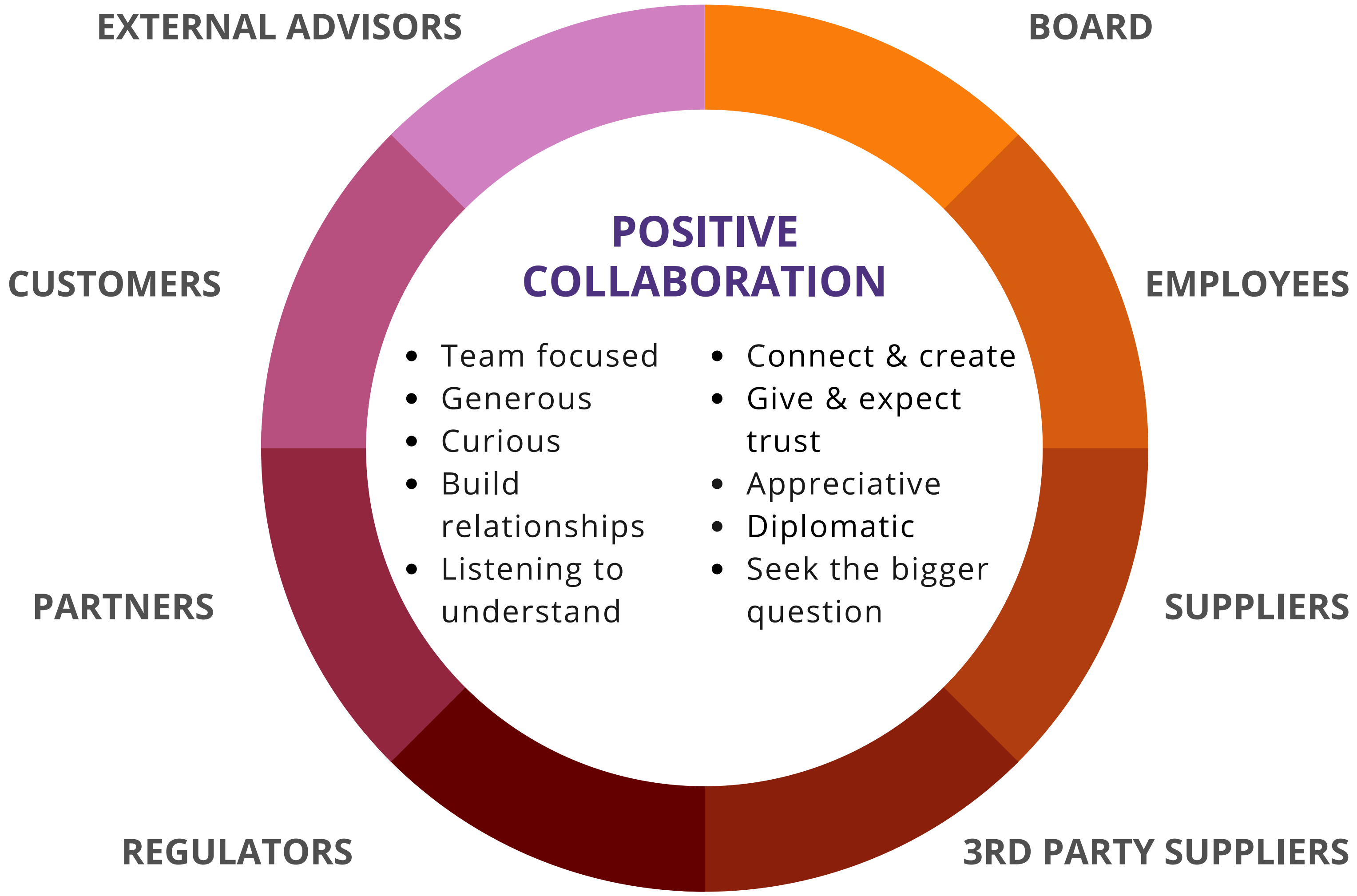
MONITOR
Monitor performance and behaviours through agreed measures

SUPPORT
Support the initiative through instilling collaborative mindsets

EVALUATE
Evaluate and oversea the Relationships and Relationship Management Plan

Institute for Collaborative Working

Adapted from ISO 44001 : 2017



POSITIVE COLLABORATION

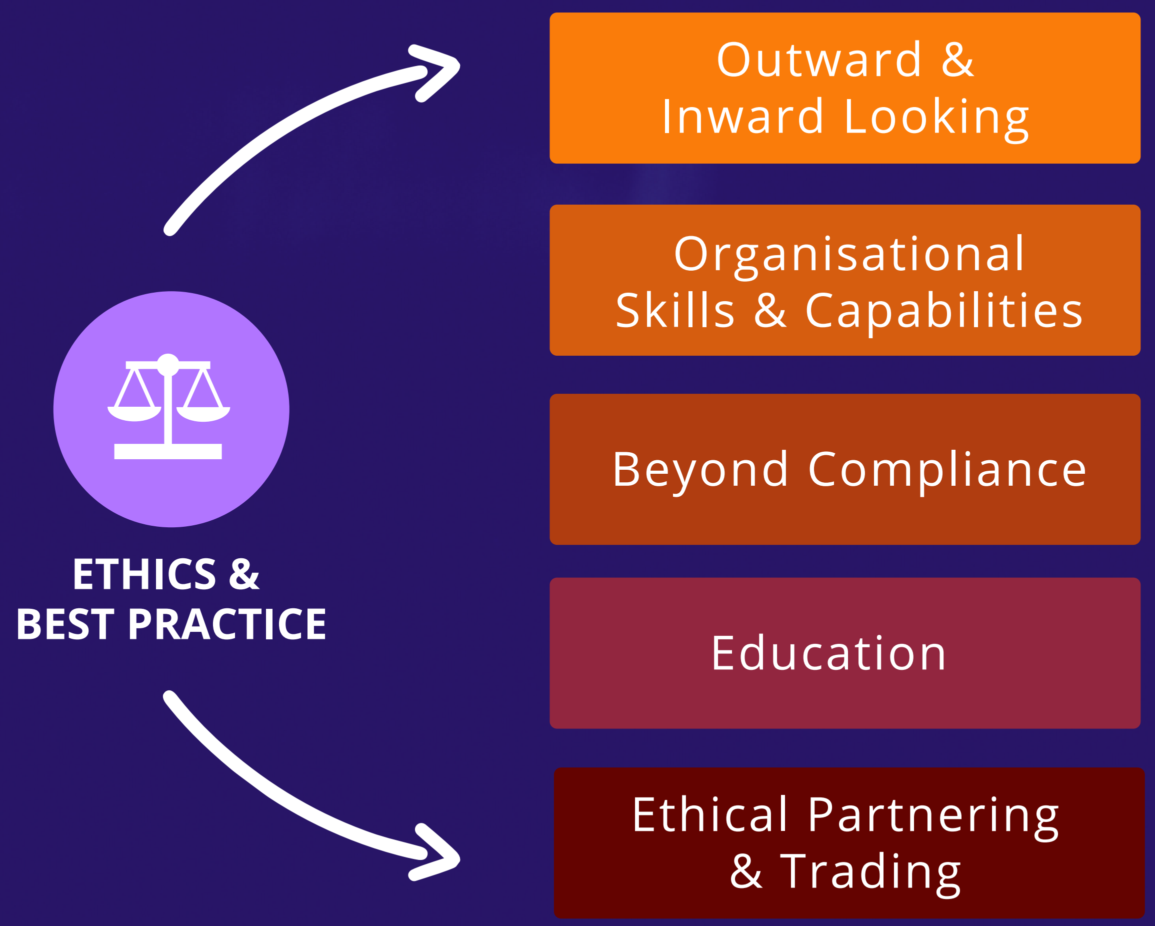
- Team focused
- Generous
- Curious
- Build relationships
- Listening to understand

- Connect & create
- Give & expect trust
- Appreciative
- Diplomatic
- Seek the bigger question

FORESIGHT
PRACTICAL APPLICATION FOR ADVISORY BOARD PROFESSIONALS

Facilitating the understanding and exploration of the collaborative role of the Cyber ecosystem is paramount for high quality, independent advisory. A strong **ETHICAL FRAMEWORK** must underpin the ecosystem to allow each part to contribute in a transparent and independent manner to achieve optimal outcomes for individual businesses and the sector as a whole.

ETHICAL CONSIDERATIONS FOR COLLABORATION



ETHICS & BEST PRACTICE

Outward & Inward Looking

Organisational Skills & Capabilities

Beyond Compliance

Education

Ethical Partnering & Trading

ETHICAL COLLABORATION

- Shared risk and opportunity
- Conflicts of Interest
- Brand Reputation
- Corporate social responsibility
- Independence

FORESIGHT

PRACTICAL APPLICATION FOR ADVISORY BOARD PROFESSIONALS

SUPPORT

- Going beyond compliance means to derive measures and metrics for the board to assess the impact of cyber risk on business objectives, operations and performance. (Gartner)
- Establish a cyber language and framework that is clear and in business terms, tune it for the board operations
- Explore risk and uncertainty in terms of impacts to critical services and assets
- Do health checks on cyber knowledge, planning and education to improve awareness
- Use industry stories to educate, illustrate and evaluate cyber events, threats and risks
- Frame cyber risk in positive terms, identify the protections required for critical services and trust
- Ability to respond and recover to cyber threats is a prerequisite and assumption for service continuity and growth in trust.

ETHICAL ENGAGEMENTS

- Clarity in language and demystified jargon enables clear analysis and intention to be planned, executed and reported on. Cyber risk planning takes business collaboration and requires ethical intent.
- Education is the key to addressing and incorporating ethics and cyber issues and risks
- Advisors need to be aware of the consequences of organisations who may lack comprehension or misunderstanding of some advice (jargon)
- A board needs qualified experts to assess technology and business, the two must collaborate but have appropriate skills and experience.
- It's the advisor's role to be curious, to test the different options, to ask the questions about *what if*, *how*, & *what*

ELEVATED THINKING AT A BOARD LEVEL

The Project Advisory Board, supported by the Captains of Industry panel and wider industry consultation, advocated for Cyber Opportunity to be recognised as a strategic topic for boardroom table discussion. Executives and boards will benefit from accessing specialist knowledge and insights from independent Advisors to support critical thinking, robust discussion, ethical collaboration and informed decision making.

INSIGHTS

Christopher McNaughton
Director, SECMON1
Captains of Industry Panel

"The pandemic has seen an understandable prioritisation of survival over security. It's now time to adjust the balance to ensure we are operating safely in this risky cyber world."

INSIGHTS

KIm Scott
Chairman, Australian Cyber Collaboration Centre Pty Ltd
Captains of Industry Panel

"SMEs tend to be the soft underbelly of the supply chain with more than 60% suffering cyber breaches of some kind. Cyber security is a business risk that needs to be addressed at the Board level first, rather than assuming the IT department has it covered.""

FORESIGHT

PRACTICAL APPLICATION FOR ADVISORY BOARD PROFESSIONALS

CAPABILITY STATEMENT

The Advisory Board Centre State of the Market Report 2019 identified the growing trend of Advisory Board variations. In particular, the report highlights the widening of the Advisory Board sector as a thinking system to solve problems of the future.

Accessing capability is crucial in this approach where targeted conversations in an Advisory Board setting informs strategy and decision making of Directors as a result. The scope and context can vary.

Considerations for Advisory Board Composition include:

- Project Advisory Boards for commercialisation strategies, businesses expanding into new markets, seeking advisors on the ground
- Board of Directors seeking unbiased and expert opinions for a Technical Advisory Board to debate and problem solve in areas such as Manufacturing, Supply Chain, Cyber Opportunity.
- Consultative Advisory Board where organisations seek diverse market insight into Corporate Social Responsibility and Sustainability

The Advisory Board Centre in its independent capacity seeks to support organisations to gain clarity in their problem-solving framework and provide access to leading thinkers.

ADVISORY BOARD METHODOLOGY

The Cyber Opportunity Project Advisory Board adopted the ABF101 Advisory Board Best Practice Framework™ and included the living research methods detailed below.

CLARITY OF SCOPE

Clearly articulated approach outlining purpose, roles and responsibilities, process, timing and boundaries
We established a Cyber Opportunity Project Advisory Board Charter, participant guideline and meeting structure to support the strategic priorities.

INDEPENDENCE

The Project Advisory Board has independent, diverse representation
Participation in the Project Advisory Board was sought via the Advisory Board Centre global community and included 38 participants over the 90 day period. We engaged in knowledge building through a living survey approach and collaborative thinking system for participants to evolve their thinking.

FIT FOR PURPOSE

Members are profiled and selected to fulfill the scope and meet the objectives
Collaborating with the Co-Chairs, member capability and experience, including currency of knowledge within the sector was mapped to established relevant experience and transferable skills to bring to the Project Advisory Board.

STRUCTURE AND DISCIPLINE

Structure is clearly outlined with protocols to establish, manage and review effectiveness
The Project Advisory Board structure had a clearly defined 90 Day Plan including structured and scheduled meetings enabling research findings to be explored, interpreted and challenged. Participants were supported with Participant Guides, Agendas and Meeting Preparation handouts to focus discussions. A continuous feedback loop was established via research and other communication channels to allow robust discussion while maintaining focus.

MEASUREMENT

Measured on an ongoing basis for impact and scope alignment
Final outcome to meet the objective of the project included Captains of Industry Panel to road test findings and explore critical thinking at a global scale and co-creation of the report with the Advisory Board Centre global community.

CONTRIBUTORS - CAPTAINS OF INDUSTRY PANEL

Louise Broekman, Advisory Board Centre Founder & CEO

Louise is an award winning Entrepreneur, researcher and business advisor. Louise has received recognition from Industry and Government at a local and national level for her contribution to the Australian business sector.

In 2004, Louise established an Advisory Board for her own business which has provided her with first hand experience in how a well run Advisory Board can positively impact CEOs. Since 2012, Louise has served as Chair for commercial Advisory Boards. She is an in-demand speaker and is regularly called upon as the leading voice for Advisory Boards in the Asia Pacific region.

Peter Day, Co-Chair - Cyber Opportunity Project Advisory Board

Peter works closely with Boards and Senior Executives to identify and implement innovative and disruptive strategies, across business and technology areas. This has included extensive experience leading major transformation and organisational change. Peter is adept at identifying areas of innovation across any sector and has extensive experience in researching and canvassing, including international assignments, examining disruptive processes and technologies, then developing concept papers and feasibility studies, as well as investment logic maps.

He has extensive experience across both ICT and Cyber Security. His roles and engagements include Security Architecture, Governance Risk and Compliance, Enterprise Architecture and Strategy, CISO, CIO, CTO and Project Director across Government (State and Federal), Education, Utilities, Telecommunications, Health, Not For Profit, Gaming, and Finance.

Daniel Brewer, Co-Chair - Cyber Opportunity Project Advisory Board

Daniel is an experienced executive and director whose advises on quantifying risk across cyber and law for businesses dependent on digital technologies. Defined by the experience of delivering over 200 online enterprise platforms, Daniel has become a leading law-tech expert and now specialises in defining legal and risk strategies for cyber threats for government, defence and private industry.

Recently completing a master's degree in law and focusing on international and trade law, Daniel has been determining strategies for limiting cyber risk and legal protection by aligning it through a company's culture. Daniel has actively promoted thought leadership into Government, Defence and Industry programs to rationalise how cyber and legal risk is identified and mitigated through IT planning and delivery.

Sandra Gamble, Chair, Non-Executive Director, Tribunal Member | Board Advisor

Sandra a non-executive director, chair & committee member with over two decades of board level experience as both a director and board advisor. She has worked across the public, private and not for profit sectors with particular experience in the utilities, infrastructure and the energy industries. Sandra is Board Member of the NZ Electricity Authority and a Tribunal Member with the Independent Pricing and Regulatory Tribunal of New South Wales.

Before that Sandra held senior executive roles at Sydney Water Corporation and Jemena Limited. Sandra holds a Master of Business Administration (Technology Management) and a Bachelor of Electrical Engineering with Honours. She is a Fellow of the Australian Institute of Company Directors and a Certified Advisory Board Chair.

Kim Scott, Chairman Australian Cyber Collaboration Centre Limited

Kim Scott is Principal Director and founder of his own consulting company, Three As One (TAO) Consulting, and has over 35 years' experience in defence technology in the electronic and land systems markets, including 7 years at the Defence Science and Technology Organisation, and 28 years in Defence Industry.

He now conducts Independent Assurance Reviews for Defence projects within CASG, and facilitates Smart Buyer Workshops for Defence. In addition, he advises a number of innovative SME organisations operating in the Defence and Space markets. Kim is presently the Chair of the Australian Cyber Collaboration Centre (A3C) located at Lot Fourteen, Silentium Defence, the SA Node of AustCyber and Defence Innovations Partnerships (DIP). He is a Non Executive Director of TAE Aerospace and is also on the Advisory Board of Turbine Aeronautics, elmTEK, Redarc Defence Systems, Praxis Aeronautics, YourDC and the Australian Institute of Machine Learning (AIML).

Christopher McNaughton, Secmon1

Chris' career commenced in law enforcement where over 24 years he has investigated serious crime, including homicide, fraud and organised crime. Chris career culminated in his role as a senior computer forensic examiner & cybercrime expert.

In 2007 Chris moved to General Electric, where he was responsible globally for digital forensics, investigations, litigation support and insider threat. In 2014 Chris formed the SECMON1 which provides Cyber Security and Investigative services to Government and corporate sector.

CONTRIBUTORS - LIVING RESEARCH & CONSULTATION

The Cyber Opportunity Project Advisory Board included deeply experienced advisory professionals within the global advisory community. We thank them for their valuable contribution including participation in living research, robust discussions, meaningful collaboration and the supportive role they provide to organisations. The views and considerations in this report may or may not reflect the individual views, advisory perspectives and experiences of contributors. This demonstrates the value of an Advisory Board setting in regards to optionality, debate and diversity of views and experience.

ADVISORY BOARD CONTRIBUTORS

Jane Beaumont
Denis Brown
David Camus
Mike Christensen
Sharyn Csanki
Paul Davies
Kalum De Silva
Sandy Deans
Jan Easton
Penny Ellenger

Sandra Gamble
Rhyll Gardner
Carolyn Grant
Hemi Gur-Ary
Paul Guy
Lawrence Hilliker
Belinda Howell
Neil James
Renee Lahti
Lucy Lin

Lisa May
Nicky Mackie
Greg Magee
Paul MacRae
Ken Mahon
Vince Murdolo
David Nash
Joanna Nelson
Paul Nielsen
Kellie Penridge

Kylie Philippe
Daniel Ronai
Liz Smith
Beau Tydd
Michele Walls
Lyndon Walker
Ben Watson
Anthony Woodward
Bruce Wookey
Wenting Xu

PROFESSIONAL CREDENTIALS

Advisory Board Centre professional members obtain credentials to demonstrate their commitment to best practice, ethical enagements and currency in their professional development and market engagement. To learn more about the Advisory Board Centre credentials, visit www.advisoryboardcentre.com.

CERTIFIED
CHAIR

APPROVED
ADVISOR

RESEARCH REFERENCES

- MIT Sloan "Make Cybersecurity a Strategic Asset" : By elevating cybersecurity from an operational necessity to a source of opportunity, leaders can boost resilience and business advantage.
- Gartner “The Urgency to Treat Cybersecurity as a Business Decision”- A better way to address this standard is to approach security as a business problem and align it with business needs. Organisations need to understand the limitations of their current execution and change their approach.
- Forrester - “Better Security And Business Outcomes With Security Performance Management”: Security in business, match pace, can't stifle innovation, core change/fix/support processes need to be heightened.
- PWC Global Digital Trust Insights Survey 2021- One of our key jobs is to engage with our partners throughout the organisation that will help us achieve our objectives.
- David Martin - "Cyber Security as a business strategy", https://davidxmartin.com/cybersecurity-as-a-business-strategy/
- ISO 44001:2017 Collaborative business relationship management systems — Requirements and framework
- State of the Market Report 2019; Louise Broekman; Advisory Board Centre

HOW TO REFERENCE THIS REPORT

Building Opportunity: Pathways to Cyber Assurance - Cyber Opportunity Project Advisory Board, January 2021; Louise Broekman; Peter Day and Daniel Brewer, Advisory Board Centre

Advisory Board Centre Pty Ltd have used their best efforts in collecting the information published in this report. Advisory Board Centre Pty Ltd does not assume, and hereby disclaims, any liability for any loss or damage caused by errors or omissions in this report, whether such errors or omissions result from negligence, accident, or other causes.

Advisory Board Centre Pty Ltd
+61 408 477 165
www.advisoryboardcentre.com

ABOUT ADVISORY BOARD CENTRE

The Advisory Board Centre is the professional body for the global advisory sector. We provide research-based best practice training, certification and connection to support the professionalism, growth and impact of the advisory sector for professionals and the organisations they serve.

As the developers of the ABF101 Advisory Board Best Practice Framework™, the Advisory Board Centre is the sole organisation authorised to deliver authenticated education and resources for the ABF101 Advisory Board Best Practice Framework™ including the Certified Chair™ credential. Any unauthorised use of the ABF101 Framework is strictly prohibited.