



# ANNUAL REPORT | 2019–20



Industry Growth Centres







Our mission is to grow  
Australia's cyber security  
sector, to support the  
development of a vibrant  
and globally competitive  
Australian cyber  
security sector

# CONTENTS

Chairs foreword	2	<b>APPENDIX B</b>	<b>14</b>
<b>1 OVERVIEW</b>	<b>4</b>	Subcontractors engaged in the 2019–20 financial year	14
Our mission	4	<b>APPENDIX C</b>	<b>16</b>
<b>2 OPERATIONAL ACTIVITIES</b>	<b>6</b>	Public speaking engagements (excludes AustCyber hosted events)	16
Financial activity	6	<b>APPENDIX D</b>	<b>19</b>
Growth Centre members	6	General Purpose Financial Report for the year ended 30 June 2020	19
Expenditure	6	<b>APPENDIX E</b>	<b>52</b>
Subcontractors	6	BDO Annual Completion Report	52
<b>3 COMMUNICATION AND ENGAGEMENT</b>	<b>8</b>		
Digital media engagement	8		
Publications	10		
Public speaking engagements	10		
<b>APPENDIX A</b>	<b>12</b>		
Status of activities from the 2019–20 Business Plan	12		
Objective 1	12		
Objective 2	12		
Objective 3	13		
Objective 4	13		



## CHAIRS FOREWORD

AustCyber continued to make great strides against its mission domestically and internationally in 2019–20, working with over 300 Australian cyber security companies.

The 2019 update to Australia's Cyber Security Sector Competitiveness Plan (SCP) provided vital insights into the current state of the sector, and we partnered with CISO Lens on an inaugural public version of the third annual CISO Lens Benchmark, released and promoted as a companion report to the SCP.

The final round of the AustCyber Projects Fund commenced in support of Australian cyber security innovation, bringing the total direct cash contribution from industry and AustCyber to the Australian economy for both rounds to over \$32 million to the Australian economy.

AustCyber maintained an active schedule during the year, continuing to grow the Australian cyber security ecosystem with Cyber Security Innovation Nodes being launched in the ACT and Tasmania.

We consulted on, contributed to and participated in multiple national events and strategies, including the Independent National Security Legislation Monitor's review of the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (also known as the TOLA Act), the Government's public consultation on the development of the national Cyber Security Strategy 2020 and the ASEAN Women in Innovation Leadership Dialogue. We also partnered with METS Ignited (the mining equipment, technologies and services Industry Growth Centre) to release a report on the cyber readiness of mining companies.

Furthering our goal of exporting Australia's cyber security to the world, AustCyber partnered with Austrade to deliver our fourth trade mission to the USA as part of the RSA Conference in San Francisco in February 2020. AustCyber and Austrade also signed a Collaboration Agreement, the first to be signed by Austrade with a non-government entity and published a market insights report to support companies considering export and expansion in ASEAN countries.

Our CEO led a small delegation of cyber security companies to the UK in July 2019, attended the Australia/New Zealand Leadership Dialogue in September 2019 and provided a briefing to MITRE Corporation's Executive Board and separately their cyber security strategy team in the USA in December 2019. She also accompanied two cyber security companies to the 2019 Export Awards in December 2019, the first year that our companies have reached the national finals for this award series, convened by Austrade.

AustCyber staff attended the Asia Pacific and Japan 2019 RSA Conference in Singapore with 15 Australian cyber security companies. In November 2019, AustCyber's Chief of Ecosystem Development Prerana Mehta spoke on two panels at the World Economic Forum Annual Meeting on Cybersecurity held in Geneva Switzerland, on ecosystem growth and workforce development, and on a panel at the Organisation for Economic Co-operation and Development's annual Data Security Summit in London, on cyber innovation.

AustCyber contributed to many educational outcomes, including the shaping of initiatives that will deliver on the government's \$50 million commitment to cyber security skilling. AustCyber also participated in the Global Forum for Cybersecurity Expertise's Asia Pacific regional conference in Melbourne in February 2020.

We worked with the Australian Computer Society and Australian Information Security Association to put forward a proposal for delivery of the Government's \$20 million Skills Organisation pilot for cyber and digital skilling, an outcome of the Joyce Review of Vocational Education and Training announced in the 2019 Budget.

Together with the Canberra Institute of Technology and Fifth Domain, AustCyber attended the Australian Training Awards in November 2019 as a finalist for the Industry Collaboration Award, having won the category at the ACT's awards.

Our CEO and the AustCyber team also provided direct support to industry during the initial lockdown period caused by the COVID-19 pandemic and supported Australian governments in their efforts to make sense of the once-in-a-generation global crisis that, like many others across the economy, has placed increased pressure on our industry.

While the economy and community works to rebuild from successive crises from 2019 through 2020 and likely beyond, the Australian cyber security industry has responded and is at the ready to continue to support Australians to defend against malicious cyber attacks and deepen trust in our digital infrastructures and data as a result.

Operationally, the 2019–20 year saw AustCyber transition to a new business model, adopting the Objectives and Key Results (OKR) project management methodology to support the remaining two phases of our three phase strategic timeline for enabling and supporting sector growth. A snapshot of the OKR methodology together with progress against our strategic activities is included in Appendix A.

Although not widespread in Australia, the OKR methodology being employed by technology companies globally was chosen as a means for us to continue to drive our strategy forward, while being more responsive to the changing demands of the near and medium terms.

This is but a snapshot of our achievements in building knowledge infrastructure to support sustained growth in Australia's cyber security industry, deepen export pathways and help make Australia the leading centre for cyber security education.



**Doug Elix AO and Adrian Turner**  
Co-Chairs of AustCyber


# 1 OVERVIEW

## Our mission

AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector and support the development of a vibrant and globally competitive Australian cyber security sector. In doing so, our activities enhance Australia's future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation's economy and community.

We form a part of:

- the Australian Government's Industry Growth Centres Initiative, established through the 2015 National Innovation and Science Agenda, in sectors of competitive strength and strategic priority to boost innovation and science in Australia. Industry Growth Centres are required under contract with the government to achieve for their sector:
  - increased R&D coordination and collaboration leading to improved commercialisation outcomes;
  - improved management and workforce skills of businesses;
  - more businesses, including small and medium enterprises, integrated into global supply chains leading to increased export income;
  - a reduction in the cost of business through regulatory reform; and
  - additional or indirect (spillover) outcomes.
- Australia's 2016 Cyber Security Strategy. It was through the industry consultation and development of this strategy that the concept for AustCyber was first conceived.



The majority of funding for AustCyber comes from federal government grants – funding for operations and programs, and for the AU\$15 million AustCyber Projects Fund which provides matched funding to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber’s National Network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market ‘hot spots’ around the world.



# 2 OPERATIONAL ACTIVITIES

## Financial activity

As per the independently audited General Purpose Financial Report for the year ended 30 June 2020 (see Appendix D), AustCyber had a closing cash balance of \$11,565,691.

The auditor's completion report is at Appendix E.

## Commonwealth funding

AustCyber received a total of \$5,447,285 (excluding GST) from grant revenue through its funding arrangements with the Department of Industry, Science, Energy and Resources, broken down as follows:

Funding source	Amount (ex GST)
Operating funds	\$3,680,000
Project funds	\$5,000,000
Other revenue	\$143,767

## AustCyber participant contributions

The organisation received \$510,424 in state government contributions towards the national roll-out and implementation of AustCyber's National Network of Cyber Security Innovation Nodes.

## AustCyber's Projects Fund

In 2019–20, AustCyber was at the end of funding ten projects as part of round 1 and commencing 17 projects as part of round 2, details of which can be found on

AustCyber's website<sup>1</sup>. During the 2019–20 financial year, AustCyber paid \$1,867,102 to grant and Projects Fund expenses against agreed milestone deliverables.

## Growth Centre members

AustCyber did not have members during the 2019–20 financial year and therefore did not receive any associated contributions.

## Expenditure

AustCyber's operating expenses for the period was \$5,591,052.

## Subcontractors

AustCyber engaged the services of 48 subcontractors to support the delivery of its programs during the 2019–20 financial year. These services included, but were not limited to:

- Office accommodation
- Corporate travel administration
- Consultancy and research
- Legal services
- Editing
- Graphic design and printing
- Information and communication technology related services.

A full list of subcontractors engaged during the period is at Appendix B.

<sup>1</sup> AustCyber's Projects Fund: <https://austcyber.com/grow/projects-fund>





# 3 COMMUNICATION AND ENGAGEMENT

## Digital media engagement

### Social media

AustCyber has seen significant growth in audience engagement through its company Twitter handle, @AustCyber, which grew by 40.7% from 4,607 followers in July 2019 to 6,481 followers in June 2020. 533 Tweets were published over the period, which appeared more than one million times (impressions) in user feeds. There were close to 20,000 engagements with the Tweets over the period – which included retweets, replies, follows, likes and clicks on links, hashtags and embedded media. Further engagement was achieved through the supporting handles of @Cyber\_Roo, @NswCyber and @CBRNode.

AustCyber leveraged its LinkedIn presence, growing the number of followers by 154.3% from 4,515 in July 2019 to 11,482 in June 2020. 402 posts were published over the period, garnering more than 500,000 impressions and 160,000 engagements. Further engagement was achieved through the supporting LinkedIn pages of the NSW and Canberra Cyber Security Innovation Nodes.

### 'Friend of the network' list

AustCyber engages with the ecosystem through its 'Friend of the network' newsletter and mailing list. AustCyber published 63 campaigns sent to 73,602 emails, with an open rate of 33.7% and an unsubscribe rate of only 0.2% (166 unsubscribed users) over the reporting period.

### Website

AustCyber matured its web presence with a 136.7% increase in users (58,514) and 115.1% increase in sessions (83,142) over the period. There were 182,314 page views in total, with an average duration of 2 minutes and 12 seconds.

The majority of users visiting the website were from Australia (50.9%) and the United States of America (37.1%), with the majority of users visiting the website directly (32,913 users) versus other means such as organic searchers (21,896 users) and social media referrals (3,705 users).






### The top five most viewed pages on the company website were:

1. **Homepage** – 43,839 page views
2. **About us** – 6,660 page views
3. **About us: our team** – 5,927 page views
4. **Educate: career paths and opportunities** – 5,002 page views
5. **AustCyber's Projects Fund** – 5,728 page views.

### The top six most viewed articles were:

1. **'NSW Cyber Security Innovation Node and TAFE NSW launch cutting-edge online cyber security skills training'** – 812 page views
  2. **'AustCyber boosts cyber security innovation with almost A\$8.5 million for industry-led projects'** – 686 page views
  3. **'AustCyber is hiring'** – 675 page views
  4. **'Adelaide team wins Australia's first hackathon to find national missing persons'** – 642 page views
  5. **'Registration open for 'Australia House' program in San Francisco on 24 February'** – 638 page views
  6. **Projects Fund Round 1 recipients** – 213 page views.
- 

## News media

AustCyber was referenced in Australian online news media through 510 unique articles (an increase of 141%), which had a potential reach of 136.02 million people. AustCyber was referenced in global online news media through 666 unique articles (an increase of 115%), which had a potential reach of 179.56 million people.

The top Australian sources referencing AustCyber were:

Source	Number of Articles referencing AustCyber
Mirage News	13
National Tribune	13
Itwire	12
CSO	10
Technology decisions	8
ACS information age	8
Australian Cyber Security Magazine	8
InnovationAUS	7
Defence Connect	7
Computerworld Australia	6

AustCyber executives were interviewed for 20 podcasts and 45 radio segments.

Over the reporting period, AustCyber's share of voice (when referenced in comparison to fellow Industry Growth Centres) was 56.8%.

## Publications

AustCyber launched the 2019 update to the SCP<sup>2</sup> in December 2019. The SCP has been established as the premier source of information and data on Australia's cyber security ecosystem. Over the period, the 2019 SCP was referenced in global online news media (not including syndicated publications) through 95 unique articles. It is referenced at least once daily by Australian online news media.

Released as a companion document to the 2019 SCP, the CISO Lens Benchmark 2019<sup>3</sup> was launched in December 2019. It enables evidence-based decision making around cyber strategy and resource allocation and is founded on benchmarking completed by CISO Lens founder James Turner with cyber security executives to assess how their organisations respond to cyber risks.

## Public speaking engagements

The AustCyber executive participated in 52 speaking engagements at various forums throughout the year, which are detailed at Appendix C.

2 Australia's Cyber Security Sector Competitiveness Plan 2019: <https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019>  
3 CISO Lens Benchmark 2019: <https://www.austcyber.com/resource/ciso-lens-benchmark-2019>





# APPENDIX **A**

## Status of activities from the 2019–20 Business Plan

■ Target achieved   ■ Work underway to deliver target   ■ Not completed or shifting priorities

### Objective 1

Deliver scaled cyber security innovation superclusters, supported by a National Network of Nodes, providing the physical infrastructure underpinning sector growth.

Key Result	Status	Comments
1.1 Deliver the nodal stepping stones to pre-position for superclusters	■	Completed
1.2 Pilot the supercluster concept in at least one Australian location	■	Partially complete; carried over to 2020–21 due to shifts in partner priorities
1.3 Deliver a prioritised incubator/accelerator uplift action plan	■	Paused; carried over to 2020–21 due to internal capacity challenges in Q1 and Q2

### Objective 2

Implement sector knowledge infrastructure, supporting commercialisation and innovation from idea to exit/export.

Key Result	Status	Comments
2.1 Deliver a map of the Australian cyber security business operating environment	■	Partially complete; carried over to 2020–21 due to internal capacity challenges in Q3 and impacts of the pandemic on stakeholder information feeds
2.2 Deliver a compelling investment capability uplift program	■	Paused; carried over to 2020–21 due to internal capacity challenges in Q1 and Q2



## Objective 3

Establish robust export pathways to key markets for globally competitive Australian cyber security capabilities.

Key Result	Status	Comments
3.1 In partnership with others, deliver country/ region strategies and market insights & investment reports		Completed
3.2 Deliver the Australian cyber security industry capability map		Partially complete; carried over to 2020–21 due to greater than anticipated stakeholder interest in partnering on delivery and increased complexity in technical build than originally planned

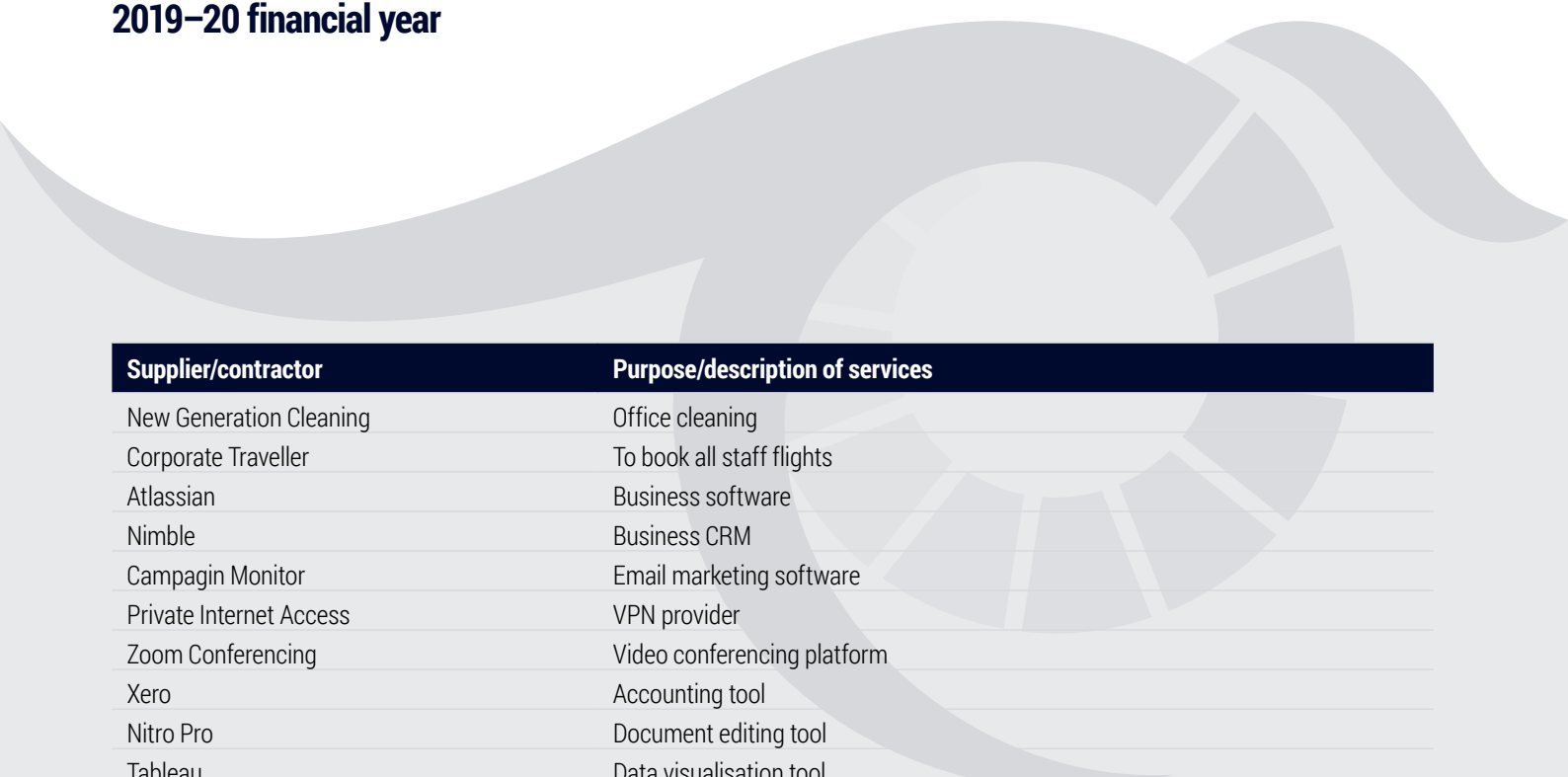
## Objective 4

Implement a national platform for measurable and scalable cyber security skills development and workforce growth.

Key Result	Status	Comments
4.1 Embed the US National Initiative for Cybersecurity Education (NICE) Framework for Workforce Development as the preferred approach to growing and sustaining a globally competitive cyber skilled workforce		Partially complete; carried over to 2020–21 as planned
4.2 Direct appropriate effort under the AustCyber Projects Fund to develop a national platform for skills development and workforce growth		Completed

# APPENDIX **B**

## Subcontractors engaged in the 2019–20 financial year



Supplier/contractor	Purpose/description of services
New Generation Cleaning	Office cleaning
Corporate Traveller	To book all staff flights
Atlassian	Business software
Nimble	Business CRM
Campaign Monitor	Email marketing software
Private Internet Access	VPN provider
Zoom Conferencing	Video conferencing platform
Xero	Accounting tool
Nitro Pro	Document editing tool
Tableau	Data visualisation tool
Adobe Export PDF	Adobe document export tool
ERP IT Canberra	Assist with delivering phase 1 of Jira Workflow Project
ForwardIT	IT managed services
Productivity HUB	Staff training for Mai Tran
Whitetower	Website hosting and related services
Brittany Fong	Specialist Tableau services to develop dashboards
Regus Sydney	Sydney office space contract
Servcorp Canberra	Canberra office space contract
Hyatt Regency Miami	The hiring of event facilities for a workshop
Momentum Dashboard	Google Chrome dashboard tool
Myer Vandenberg Lawyers	Legal services
Amazon Web Services	Cloud computing service for company website
Namecheap	Domain registrations
Microsoft Office Business	Microsoft license



Supplier/contractor	Purpose/description of services
Tripit	Travel itinerary manager and flight change alerts
Boomerang for Gmail	Email scheduling and productivity tool
Nuance	Dictation tool
ASPI	Policy research support
DocuSign	Electronic signature tool
Google G Suite	Productivity and collaboration tools
Security Colony	Website security
AlphaBeta	Measurement Project
Effective People PTY LTD	Recruitment services
LastPass	Password management tool
Qantas Business	Qantas rewards points
contentgroup	Retainer agreement for communications support
Datacom	CRM and business process tools
Kasada	Web security
SurveyMonkey	Online survey tool
Impress Design	Retainer agreement for website and graphic design services
Thinkplace	Business planning consultancy
Ambius Agreement	Servicing and provision of office plants
Meltwater	Media monitoring platform
LJ Hooker Commercial Canberra	Canberra office lease
TPG	Internet connection for Canberra office
Cosgrove Soutter	Accounting services
Synergy Group	Consultancy and strategic communication
IAG	Development of a digital ecosystem

# APPENDIX **C**

## Public speaking engagements (excludes AustCyber hosted events)

Event	Location	Date
Australian British Financial Services catalyst and multiple events this week	London	01/07/2019– 04/07/2019
Australian British Health catalyst and multiple events this week	London	08/07/2019– 11/07/2019
RSA APJ and multiple events this week	Singapore	16/07/2019– 18/07/2019
Digitize 2019	Brisbane	23/07/2019
2019 Public sector internal audit conference	Canberra	25/07/2019
SYD National Audit Office	Sydney	26/07/2019
Aura's State of play in Cyber' Media & analyst lunch	Sydney	30/07/2019
Reception to celebrate 54th National Day of the republic of Singapore	Sydney	01/08/2019
Blackhat and Defcon	United States	03/08/2019– 14/08/2019
14amf conference (industry 4.0 advanced manufacturing conference) held by the australian industry group (AIG)	Victoria	07/08/2019
D3 challenge finals	Western Australian	05/08/2019
Cyber session of the indo pacific – defence conference	Western Australia	05/08/2019
Lunch hosted by the american chamber of commerce	Sydney	08/08/2019
Australian national brand – shaping Australia's global reputation roundtable	Victoria	09/08/2019
Cyber affairs briefing to WA state office & other fed & state gov departments	Western Australia	13/08/2019

Event	Location	Date
Roundtable luncheon CEDS trustee: committee for economic development of Australia	Western Australia	13/08/2019
Ok RDY cyber edition mentoring launch	Canberra	15/08/2019
Cyber security CRC symposium 2019	Sydney	20/08/2019
Public sector network: cyber security series	Canberra	21/08/2019
National policing summit 2019	Victoria	27/08/2019
Eureka prizes	Sydney	29/08/2019
CSO women in security conference	Victoria	03/09/2019
ACA schools cyber security roadshow	Sydney	04/09/2019
ANZ13th Australia New Zealand leadership forum	Auckland	13/09/2019
Parliamentary reception with the British high commissioner	Canberra	16/09/2019
National roads and traffic expo 2019	Victoria	18/09/2019
MTAA Medtech 19 conference and dinner	Sydney	19/09/2019
My career lab breakfast forum	Sydney	25/09/2019
Insln town hall on Tola industry event	Canberra	26/09/2019
Australian defence industry awards	Canberra	26/09/2019
Tech series b'fast	Canberra	27/09/2019
Breakfast – CSRIO Australia-Singapore deep tech connection	Sydney	02/10/2019
D61+ live	Sydney	02/10/2019
National small business cyber summit	Canberra	14/10/2019
The prime minister's prizes for science	Canberra	16/10/2019
Amcham tech talk series breakfast	Sydney	17/10/2019
Press club lunch and address by the chairman of the German-Australian chamber of industry and commerce	Canberra	22/10/2019
Women in asean leadership dialogue	Victoria	14/11/2019
UBS 2019 conference	Sydney	18/11/2019
Cyrise bootcamp	Sydney	19/11/2019



Event	Location	Date
Australian training awards	Brisbane	21/11/2019
Science meets parliament gala dinner 2019	Canberra	26/11/2019
Export awards at parliament house	Canberra	03/12/2019
Innovation showcase at cbrin	Canberra	04/12/2019
Cyrise Melbourne bootcamp	Victoria	09/12/2019
Amcham – us bay area roundtable briefing	Sydney	05/02/2020
Cyrise mentor open office	Victoria	13/02/2020
2020 cyber security strategy – small business roundtable	Canberra	04/03/2020
International women's day cybercx event & launch of their women in cyber initiative	Sydney	12/03/2020
RSA conference and multiple events during this week	San Francisco	24/03/2020– 28/03/2020
Cyber industry roundtable – Covid tracing app	Online	27/04/2019
Future of work in the digital economy – developing skills for industry 4.0	Online	25/06/2020

# APPENDIX **D**

## **General Purpose Financial Report for the year ended 30 June 2020**

**AUSTRALIAN CYBER SECURITY  
GROWTH NETWORK LIMITED**

ABN 73 616 231 451



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**FINANCIAL REPORT**  
**FOR THE YEAR ENDED**  
**30 JUNE 2020**

**Liability limited by a scheme approved under  
Professional Standards Legislation**



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**CONTENTS**

Directors' Report	1
Auditors' Independence Declaration	8
Statement of Profit or Loss And Other Comprehensive Income	9
Statement of Financial Position	10
Statement of Changes in Equity	11
Statement of Cash Flows	12
Notes to the Financial Statements	13
Directors' Declaration	28
Auditors' Report	29
Compilation Report	31

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**DIRECTORS' REPORT**

The directors present their report on the company for the financial year ended 30 June 2020.

**Directors**

The names of each person who has been a director during the year and to the date of this report are:

Ms Michelle Clare Price  
Mr Douglas Thorne Elix AO  
Mr Adrian John Turner  
Mrs Michael Paul Burgess retired 29 September 2019  
Ms Heather May Ridout AO  
Ms Rachel Falk appointed 1 April 2020

Directors have been in office since the start of the financial year to the date of this report unless otherwise stated.

**Principal Activities**

AustCyber (The Australian Cyber Security Growth Network Limited) supports the development of a vibrant and globally competitive Australian cyber security industry enhancing Australia's future economic growth and helps protect Australia's interests online.

No significant change in the nature of the company's activity occurred during the financial year.

**Objectives**

The company's primary objective is to:

Support the development of a vibrant and globally competitive Australian cyber security industry that enhances Australia's future economic growth and helps protect Australia's interests online.

**Strategies**

- **Demonstrate leadership and coherence**

Create a national cyber security narrative and ensure cohesion across national cyber security programmes, leading to accelerated industry investment and more rapid scaling.

- **Drive industry collaboration and coordination**

Enable connectivity and information flow to promote high levels of collaboration for the industry. This will reduce wasteful duplication and therefore allow better leverage of resources and create increased productivity.

- **Accelerate commercialisation**

Accelerate the creation and adoption of Australian based cyber security products, services and best practices, domestically, regionally and globally.

- **Facilitate talent growth**

Rapidly build the quantity and professionalism of Australia's cyber security workforce to become globally competitive and respected.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**DIRECTORS' REPORT**

- **Pursue policy advocacy and reform**

Proactively recommend and support policy and regulatory reforms aimed specifically at the cyber security sector to foster an environment in which innovation and entrepreneurship can thrive.

**Information on Directors**

**Ms Michelle Price**

Position: Chief Executive Officer

Experience:

Michelle Price is the CEO for AustCyber. She was the inaugural Chief Operating Officer of AustCyber, joining the company in January 2017 and appointed as CEO in April 2018. Prior to joining AustCyber, Michelle was the first Senior Advisor for Cyber Security at the National Security College within The Australian National University, where she established an integrated approach to the College's cyber security program across executive and postgraduate education and policy engagement.

Before joining the ANU, Michelle was with the Australian Government Department of the Prime Minister and Cabinet (PM &C), where she was instrumental to the delivery of the Australian Government's 2015 Cyber Security Review and Cyber Security Strategy. In a previous role at PM&C, Michelle delivered the National Security Strategic Risk Framework (the first of its kind in the world) and Coordinated National Security Budget. Prior to PM&C, Michelle worked in several strategy and risk roles across Government, having moved to the public service from the communication and media sector and the food safety segment of Australia's food manufacturing sector.

**Special Responsibilities:**

Acting Company Secretary

**Mr Douglas Thorne Elix AO**

Position: Co-Chair

Experience:

Doug Elix retired from IBM in July 2008. From May 2004 to April 2008 he was senior vice president and group executive for IBM's worldwide sales and distribution operations, including revenue, profit and customer satisfaction in the 170 countries where IBM does business. In this role he led IBM's direct sales force, business partners and [ibm.com](http://ibm.com) channels, which accounted for worldwide sales of all IBM products and services of some \$95 billion.



## **AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**

**A.B.N 73 616 231 451**

### **DIRECTORS' REPORT**

Mr. Elix was named to that position in May 2004 after serving as senior vice president and group executive for IBM Global Services beginning in October 1999. In that role, he was responsible for the worldwide operation of IBM Global Services, the world's leading business and information technology services provider with approximately 170,000 professionals. IBM Global Services, which had grown annual revenues to \$43 billion in 2003, included IBM Business Consulting Services, the business unit formed through the combination of PwC Consulting and IBM's Business Innovation Services unit. By integrating IBM's broad range of capabilities in services, consulting, hardware, software and research, IBM Global Services helps companies of all sizes improve business performance through information technology. IBM Global Services today comprises Global Business Services (GBS) and Global Technology Services (GTS) with combined 2015 revenues of \$49 billion. In July 1998, Mr. Elix was named general manager, IBM Global Services, Americas, an organisation covering the U.S., Canada and Latin America. Prior to that, he was general manager, IBM Global Services, North America, beginning in December 1996. Earlier that year, he was appointed president and chief executive officer of Integrated Systems Solutions Corp. (ISSC), a wholly owned services subsidiary of IBM.

In 1994, he was named chief executive officer, IBM Australia Ltd, having been director of operations for IBM Australia/New Zealand since 1991. He was named director of the finance industry for IBM Asia Pacific in 1990. Since joining IBM in 1969, Mr. Elix has held a broad range of positions in systems engineering, marketing, marketing management and general management in Australia and Asia/Pacific prior to his transfer to the United States in 1996.

He has served on the Boards of IBM Australia Limited, the Australian Information Industries Association and the Australian Institute of Management. He was also a member of the Business Council of Australia, and a member of the Prime Minister's National Information Services Council (NISC). He was the leader of the IBM Corporate Operating Team and a member of the IBM Performance Team. He was a member of the Board of directors of the Royal Bank of Canada for 10 years until his retirement in March 2011.

Mr. Elix is Chairman of the Advance Global Advisory Council, Co-Chair of the Government's Cyber Security Growth Centre Initiative, Chairman of the Data61 Advisory Board, Chairman of the Board of the Australian Independent Schools USA Foundation, a member of the Advisory Committee of The Australian Centre of Excellence for Quantum Computation & Communication Technology, and a member of the Board of The Queen Elizabeth II September 11<sup>th</sup> Garden in New York.

In June 2006, Mr. Elix was awarded the rank of Officer of the Order of Australia (AO) for his service to the information technology and services industry internationally, to the business sector through facilitating the introduction of world's best technology in many companies, and as a mentor to industry professionals.

#### **Special Responsibilities:**

None

#### **Mr Adrian John Turner**

Position: Co-Chair

Experience:

Adrian is an experienced corporate leader and has a strong track record of building innovative companies and organisations that tackle complex challenges.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**DIRECTORS' REPORT**

At Minderoo Foundation, Adrian is CEO of the Fire Fund Initiative which was established in January 2020 with a \$70 million commitment from Andrew and Nicola Forrest. The collaborative initiative aims to see Australia become a global leader in fire and flood resilience by 2025. The initiative is also working with communities to help them respond and recover from the devastating 2019-20 Black Summer bushfires.

In addition to his responsibilities at the Minderoo Foundation Adrian co-chairs AustCyber, the national program to build a vibrant domestic cybersecurity industry.

Prior to joining the Minderoo Foundation, Adrian was the founding CEO of CSIRO's Data61, the data and digital specialist arm of Australia's national science agency.

He previously spent 18 years in Silicon Valley and was the co-founder of Borondi Group, co-founder and CEO of Mocana Corporation, had profit and loss responsibility for Philips Electronics connected devices infrastructure and was Chairman of the Board for Australia's expat network, [Advance.org](http://Advance.org).

Adrian is an avid reader and writer with deep interests in AI, data economics and biosecurity, as well being an artist. He graduated from UTS and completed the Executive Program for Managing Growth Companies at Stanford University and authored the book *BlueSky Mining - Building Australia's Next Billion Dollar Industries*.

**Special Responsibilities:**

None

**Mr Michael Paul Burgess**

Position: Director

Experience:

In December 2017, the Prime Minister announced Mr Mike Burgess as the Director-General Designate of ASD. Mr Burgess commenced his appointment on 4 January 2018. Mr Burgess became the first Director-General of ASD on 1 July 2018.

Prior to his appointment to ASD, Mr Burgess was an independent consultant specialising in strategic cyber security advice. In 2017, Mr Burgess was also a member of the Federal Government's naval shipbuilding advisory board, a member of the board of the Australian Cyber Security Growth Network and a non-executive director of SC8 Limited.

Mr Burgess was a member of the Prime Minister's expert panel for Australia's 2016 Cyber Security Strategy. Previously Mr Burgess was the Deputy Director for Cyber and Information Security at the Defence Signals Directorate (DSD) from 2008 to 2013.

Mr Burgess has a degree in electronics engineering from the South Australian Institute of Technology. He worked in private industry before joining the Defence Science and Technology Organisation in 1991 working in the field of imaging radar. Mr Burgess joined DSD as a collection engineer in 1995. During his career at DSD Mr Burgess held a variety of roles spanning the intelligence, security, capability development and

## **AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**

**A.B.N 73 616 231 451**

### **DIRECTORS' REPORT**

executive aspects of DSD's business. He left DSD in early 2013 to become Telstra's Chief Information Security Officer. He held this role until November 2016.

#### **Special Responsibilities:**

None

#### **Ms Heather May Ridout AO**

Position: Director

Experience:

Heather Ridout is a company director with a long history as a leading figure in the public policy debate in Australia. Heather is Chair of AustralianSuper- the largest industry fund in Australia; a Director of ASX Ltd; Director of Image Networks Holdings Pty Ltd and a Director of Sims Metal Management – the world's largest publicly listed recycling company. Her other appointments include member of the Boards of: the Australian Chamber Orchestra and the Advance Australia Advisory Board.

Up until 30 April 2012, Heather was Chief Executive of the Australian Industry Group- a major, national employer organisation representing a cross section of industry including manufacturing, defence, ICT and labour hire. Her previous appointments include: member of the Reserve Bank Board; member of the Henry Tax Review panel; board member of Infrastructure Australia; member of the Business Roundtable on Climate Change; member of the National Workplace Relations Consultative Committee; member of the Prime Minister's Taskforce on Manufacturing; co-Chair of the Australian-Canada Economic Leadership Dialogue and a delegate to the B20 which is the key business advisory body to the G20

In June 2013, Ms. Ridout was awarded the rank of Officer of the Order of Australia (AO) in the general division for distinguished service to business and industry through significant contributions to the development of economic and public policy.

#### **Special Responsibilities:**

None

#### **Ms Rachael Falk**

Position: Director

Experience:

Rachael Falk is one of Australia's foremost cyber security experts and commentators.

As Chief Executive Officer of the Cyber Security Cooperative Research Centre, Rachael leads a cutting-edge program of cyber security research collaboration between government, industry and research institutions.

The aim is impact, lifting Australia's cyber security capacity and capability and creating innovative solutions for the ever-evolving problems of our interconnected world.

Rachael was Telstra's first General Manager of Cyber Influence and has a background in commercial law and cyber security, practising as a lawyer at top-tier firms in Australia and the UK and in-house for Telstra.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**DIRECTORS' REPORT**

She holds an Advanced Masters in National Security Policy (Hons) from the National Security College (ANU), Bachelor of Laws (Hons) (UTS) and Bachelor of Arts (ANU).

**Special Responsibilities:**

None

**Key Performance Measures**

The company measures its own performance through the use of both quantitative and qualitative benchmarks, that include meeting key milestone deliverable articulated in the funding agreement between the company and the Commonwealth. The benchmarks are used by the directors and the Commonwealth to assess the financial sustainability of the company and whether the company's short-term and long-term objectives are being achieved.

For 2020 the measures related to the company delivering: quarterly financial reports, a 2019-20 Annual Report, and update to the Cyber Security Sector Competitiveness Plan, and a Business Plan for the 2019-20 Financial Year.

The delivery of these key milestones was achieved for the reporting period.

**Meetings of Directors**

During the financial year, 3 meetings of directors were held (11 October 2019, 29 January 2020 and 1 April 2020). Attendances by each director were as follows:

<b>Directors' Meetings</b>		
	<b>Number eligible to attend</b>	<b>Number attended</b>
Ms Michelle Clare Price	3	3
Mr Douglas Thorne Elix	3	3
Mr Adrian John Turner	3	3
Mr Michael Paul Burgess	0	0
Ms Heather May Ridout	3	3
Ms Rachel Falk	1	1

**Impact of Covid-19**

Australian Cyber Security Growth Network Limited has determined that there are no going concern risks arising from the impact of the COVID-19 outbreak. The Directors have determined that Australian Cyber Security Growth Network Limited remains in a healthy financial position.

It is not possible to reliably estimate the duration and severity of the impact of COVID-19, as well as the impact on the financial position and results of Australian Cyber Security Growth Network Limited for future periods. However, based on analysis of the financial performance and position the financial statements have been prepared on a going concern basis. Australian Cyber Security Growth Network Limited believes at this



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**DIRECTORS' REPORT**

point in time that there is no significant doubt about Australian Cyber Security Growth Network Limited's ability to continue as a going concern.

**Contributions on Winding up**


In the event of the company being wound up, ordinary members are required to contribute a maximum of \$10 each. Honorary members are not required to contribute. The total amount that members of the company are liable to contribute if the company is wound up is \$20 based on 2 members.

**Auditors' Independence Declaration**

The lead auditors' independence declaration in accordance with section 307C of the Corporations Act 2001, for the year ended 30 June 2020 has been received and can be found on page 8.

Signed in accordance with a resolution of the Board of Directors:

**Director:**

 DOUGLAS ELIX

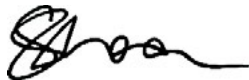
**Dated this**

11th day of November, 2020

**DECLARATION OF INDEPENDENCE BY GILLIAN SHEA TO THE DIRECTORS OF AUSTRALIAN CYBER  
SECURITY GROWTH NETWORK LTD**

As lead auditor of Australian Cyber Growth Network Ltd for the year ended 30 June 2020, I declare that, to the best of my knowledge and belief, there have been:

1. No contraventions of the auditor independence requirements of the *Corporations Act 2001* in relation to the audit; and
2. No contraventions of any applicable code of professional conduct in relation to the audit.



Gillian Shea  
Director

**BDO AUDIT PTY LTD**

Sydney, 11 November 2020

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**STATEMENT OF PROFIT OR LOSS AND OTHER COMPREHENSIVE INCOME**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	Note	2020 \$	2019 \$
<b>Income</b>			
Grant revenue	3	5,447,285	8,658,612
Other revenue	3	143,767	156,015
<b>Expenditure</b>			
Accountancy expenses		(61,925)	(59,795)
Advertising expenses		(594,181)	(779,041)
Auditors' remuneration	4	(15,500)	(15,000)
Conference expenses		-	(22,038)
Depreciation and Amortisation expenses		(65,855)	(8,129)
Employee Benefits expenses		(1,938,866)	(1,823,518)
Finance costs		(1,952)	-
Grant and Project Funding expenses		(1,867,102)	(4,797,418)
Professional and Consultancy expenses		(473,935)	(326,465)
Recruitment expenses		(104,243)	(29,835)
Rent expenses		-	(201,362)
Subscriptions, Reference & Licenses expenses		(80,720)	(73,735)
Training expenses		(30,594)	(36,843)
Travel expenses		(210,712)	(367,777)
Other expenses		(145,467)	(273,671)
		-	-
<b>Profit for the year</b>	5	-	-
		-	-
<b>Total comprehensive income for the year</b>		-	-

The company has initially applied AASB 16 using the cumulative effect method and has not restated comparatives. The comparatives have been prepared using AASB 117 and related interpretations.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**STATEMENT OF FINANCIAL POSITION**  
**AS AT 30 JUNE 2020**

	Note	2020 \$	2019 \$
<b>ASSETS</b>			
<b>CURRENT ASSETS</b>			
Cash and cash equivalents	6	11,565,691	8,098,580
Trade and other receivables	7	205,000	9,733
Other current assets	8	189,577	187,570
Right of use asset	9	18,293	-
<b>TOTAL CURRENT ASSETS</b>		<u>11,978,561</u>	<u>8,295,883</u>
<b>NON-CURRENT ASSETS</b>			
Property, plant and equipment	10	33,532	31,737
<b>TOTAL NON-CURRENT ASSETS</b>		<u>33,532</u>	<u>31,737</u>
<b>TOTAL ASSETS</b>		<u>12,012,093</u>	<u>8,327,620</u>
<b>LIABILITIES</b>			
<b>CURRENT LIABILITIES</b>			
Trade and other payables	11	523,132	624,766
Lease liabilities	12	16,065	-
Employee benefits		104,166	87,263
Provisions	13	10,000	-
Deferred Revenue		11,358,730	7,615,591
<b>TOTAL CURRENT LIABILITIES</b>		<u>12,012,093</u>	<u>8,327,620</u>
<b>TOTAL LIABILITIES</b>		<u>12,012,093</u>	<u>8,327,620</u>
<b>NET ASSETS</b>		<u>-</u>	<u>-</u>
<b>EQUITY</b>			
<b>TOTAL EQUITY</b>		<u>-</u>	<u>-</u>

The company has initially applied AASB 16 using the cumulative effect method and has not restated comparatives. The comparatives have been prepared using AASB 117 and related interpretations.



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**STATEMENT OF CHANGES IN EQUITY**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	Note	Retained Surplus \$	Total \$
<b>Balance at 01 July 2018</b>			
Surplus for the period		-	-
Other comprehensive income		-	-
<b>Total comprehensive income attributable to members of the entity for the year</b>		-	-
<b>Balance at 30 June 2019</b>		-	-
<b>Balance at 01 July 2019</b>		-	-
Surplus for the year		-	-
Other comprehensive income			
<b>Total comprehensive income attributable to members of the entity for the year</b>		-	-
<b>Balance at 30 June 2020</b>		-	-

The accompanying notes form part of these financial statements.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**STATEMENT OF CASH FLOWS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	2020 \$	2019 \$
<b>CASH FLOWS FROM OPERATING ACTIVITIES</b>		
Receipts of grants	9,866,924	14,851,474
Receipts from customers	77,212	132,550
Payments to suppliers and employees	(6,475,040)	(12,093,110)
Interest received	(171)	8,757
Interest paid on lease liability	(1,895)	-
Other Income	59,960	14,707
<b>Net cash used in operating activities</b>	<u>3,526,990</u>	<u>2,914,378</u>
<b>CASH FLOWS FROM INVESTING ACTIVITIES</b>		
Payment for property, plant and equipment	(12,771)	(22,038)
<b>Net cash used in investing activities</b>	<u>(12,771)</u>	<u>(22,038)</u>
<b>CASH FLOWS FROM FINANCING ACTIVITIES</b>		
Repayment of lease liability	(47,108)	-
<b>Net cash provided by financing activities</b>	<u>(47,108)</u>	<u>-</u>
Net increase (decrease) in cash held	3,467,111	2,892,340
Cash at beginning of financial year	8,098,580	5,206,240
Cash at end of financial year <b>6</b>	<u>11,565,691</u>	<u>8,098,580</u>

The company has initially applied AASB 16 using the cumulative effect method and has not restated comparatives. The comparatives have been prepared using AASB 117 and related interpretations.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

The financial reports cover Australian Cyber Security Growth Network Limited as an individual entity. Australian Cyber Security Growth Network Limited is a not-for-profit company limited by guarantee, incorporated and domiciled in Australia.

Comparatives are consistent with prior years, unless otherwise stated.

**1 Basis of Preparation**

The financial statements are general purpose financial statements that have been prepared in accordance with the Australian Accounting Standards – Reduced Disclosure Requirements of the Australian Accounting Standards Board (AASB) and the Corporations Act 2001. The company is a not-for-profit entity for financial reporting purposes under Australian Accounting Standards.

Australian Accounting Standards set out accounting policies that the AASB has concluded would result in financial statements containing relevant and reliable information about transactions, events and conditions. Material accounting policies adopted in the preparation of these financial statements are presented below and have been consistently applied unless stated otherwise. The financial report is presented in Australian Dollars, which is the company's functional and presentation currency.

The financial statements, except for the cash flow information, have been prepared on an accruals basis and are based on historical costs, modified, where applicable, by the measurement at fair value of selected non-current assets, financial assets and financial liabilities. The amounts presented in the financial statements have been rounded to the nearest dollar.

The financial statements have been prepared on a going concern basis, which assumes continuity of normal business activities and realisation of assets and liabilities in the ordinary course of business.

The preparation of the financial statements requires the use of certain critical accounting estimates. It also requires management to exercise its judgement in the process of applying the company's accounting policies. There are no areas involving a higher degree of judgement or complexity, or areas where assumptions and estimates are significant to the financial statements.

The financial report was authorised for issue in accordance with a resolution of the Board of Directors on 15 October 2020.

**2 Summary of Significant Accounting Policies**

**Property, Plant and Equipment**

Plant and other equipment (comprising fittings and furniture) are initially recognised at acquisition cost or manufacturing cost, including any costs directly attributable to bringing the assets to the location and condition necessary for it to be capable of operating in the manner intended by the Company's management.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

Plant and other equipment are subsequently measured using the cost model, cost less subsequent depreciation and impairment losses.

Depreciation is recognised on a straight-line basis to write down the cost less estimated residual value of buildings, plant and other equipment. The following useful lives are applied:

- computer hardware: 3-7 years
- office furniture and equipment: 3-7 years

Material residual value estimates and estimates of useful life are updated as required, but at least annually.

Low value assets are assessed based on useful life and fully written off on acquisition.

Gains or losses arising on the disposal of property, plant and equipment are determined as the difference between the disposal proceeds and the carrying amount of the assets and are recognised in profit or loss within other income or other expenses. Each class of property, plant and equipment is carried at cost less, where applicable, any accumulated depreciation and impairment of losses.

## **Leases**

### **For comparative year**

Lease payments for operating leases, where substantially all of the risks and benefits remain with the lessor, are charged as expenses on a straight-line basis over the life of the lease term.

### **For current year**

At inception of a contract, the company assesses whether a lease exists i.e. does the contract convey the right to control the use of an identified asset for a period of time in exchange for consideration.

This involves an assessment of whether:

- The contract involves the use of an identified asset that may be explicitly or implicitly identified within the agreement. If the supplier has a substantive substitution right then there is no identified asset.
- The company has the right to obtain substantially all of the economic benefits from the use of the asset throughout the period of use.
- The company has the right to direct the use of the asset i.e. decision-making rights in relation to changing how and for what purpose the asset is used.



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

**Lessee accounting**

The non-lease components included in the lease agreement have been separated and are recognised as an expense as incurred.

At the lease commencement, the company recognises a right of use asset and associated lease liability for the lease term. The lease term includes extension periods where the company believes it is reasonably certain that the option will be exercised.

The right of use asset is measured using the cost model where cost on initial recognition comprises of the lease liability, initial direct costs, prepaid lease payments, estimated cost of removal and restoration less any lease incentives received.

The right of use asset is depreciated over the lease term on a straight-line basis and assessed for impairment in accordance with the impairment of assets accounting policy.

The lease liability is initially measured at the present value of the remaining lease payments at the commencement of the lease. The discount rate is the rate implicit in the lease, however where this cannot be readily determined then the company's incremental borrowing rate is used.

Subsequent to initial recognition, the lease liability is measured at amortised cost using the effective interest rate method. The lease liability is remeasured whether there is a lease modification, change in estimate of the lease term or index upon which the lease payments are based (e.g. CPI) or a change in the company's assessment of lease term.

Where the lease liability is remeasured, the right of use asset is adjusted to reflect the remeasurement or is recorded in profit or loss if the carrying amount of the right of use asset has been reduced to zero.

**Exceptions to lessee accounting**

The company has elected to apply the exceptions to lease accounting for both short term leases (i.e. leases with a term of less than or equal to 12 months) and leases of low value assets. The company recognises the payments associated with these leases as an expense on a straight line basis over the lease term.

**Impact of adoption**

The Company has applied AASB 16 using the modified retrospective approach. The cumulative effect of initially applying AASB 16 as an adjustment to the opening balance of retained earnings was not material, and as such, no adjustment has been made to retained earnings at the date of initial application. The comparative information presented in 2019 has not been restated and continues to be reported under AASB 117 and related interpretations as allowed by the transition provision in AASB 16.

The following table summarised the impact of transition to AASB 16 on the statement of financial position as of 30 June 2019 to that of 1 July 2019 as follows:

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	<b>Increase/ (decrease) AUD\$</b>
<b>Assets</b>	
Right-of-use assets	73,172
	<hr/>
<b>Total assets</b>	73,172
	<hr/>
<b>Liabilities</b>	
Lease liabilities – current	63,172
Make Good Provision – current	10,000
<b>Total liabilities</b>	73,172
	<hr/>
<b>Equity</b>	
Retained earnings	-
<b>Total equity</b>	-
	<hr/> <hr/>

### **Impairment of Assets**

Where it is not possible to estimate the recoverable amount of an individual asset, the entity estimates the recoverable amount of the cash-generating unit to which the asset belongs.

### **Employee Benefits**

#### **Short-term employee benefits**

Provision is made for the company's obligation for short-term employee benefits. Short-term employee benefits are benefits (other than termination benefits) that are expected to be settled wholly within 12 months after the end of the annual reporting year in which the employees render the related service, including wages, salaries and sick leave. The company classifies employees' annual leave entitlements as other short-term employee benefits as they are expected to be settled wholly within 12 months after the end of the annual reporting year in which the employees render the related service. Annual leave provision is based on accrued balances at the year end and on future salaries. Short-term employee benefits are measured at the (undiscounted) amounts expected to be paid when the obligation is settled.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

The company's obligations for short-term employee benefits such as wages, salaries and sick leave are recognised as a part of current trade and other payables in the statement of financial position. Accrued annual leave is recognised as a provision in the statement of financial position.

**Retirement benefit obligations**

*Defined contribution superannuation benefits*

All employees of the company receive defined contribution superannuation entitlements, for which the company pays the fixed superannuation guarantee contribution (currently 9.5% of the employee's average ordinary salary) to the employee's superannuation fund of choice. All contributions in respect of employees' defined contribution entitlements are recognised as an expense when they become payable. The company's obligation with respect to employees' defined contribution entitlements is limited to its obligation for any unpaid superannuation guarantee contributions at the end of the reporting year. All obligations for unpaid superannuation guarantee contributions are measured at the (undiscounted) amounts expected to be paid when the obligation is settled and are presented as current liabilities in the company's statement of financial position.

**Provisions**

Provisions are recognised when the company has a legal or constructive obligation, as a result of past events, for which it is probable that an outflow of economic benefits will result and that outflow can be reliably measured.

Provisions recognised represent the best estimate of the amounts required to settle the obligation at the end of the reporting year.

**Cash and Cash Equivalents**

Cash and cash equivalents comprises cash on hand, demand deposits and short-term investments which are readily convertible to known amounts of cash and which are subject to an insignificant risk of change in value.

**Goods and Services Tax (GST)**

Revenues, expenses and assets are recognised net of the amount of GST, except where the amount of GST incurred is not recoverable from the Australian Taxation Office (ATO). Receivables and payables are stated inclusive of the amount of GST receivable or payable. The net amount of GST recoverable from, or payable to, the ATO is included with other receivables or payables in the statement of financial position. Cash flows are presented on a gross basis. The GST components of cash flows arising from investing or financing activities which are recoverable from, or payable to, the ATO are presented as operating cash flows included in receipts from customers or payments to suppliers.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

**Revenue and Other Income**

Revenue comprises revenue from the government grants and other income revenue from major products and services is shown in Note 3.

Revenue is measured by reference to the fair value of consideration received or receivable by the Company for goods supplied and services provided, excluding sales taxes, rebates, and trade discounts.

Revenue is recognised when the amount of revenue can be measured reliably, collection is probable, the costs incurred or to be incurred can be measured reliably, and when the criteria for each of the Company's different activities have been met. Details of the activity-specific recognition criteria are described below.

**Government grants**

A number of the Company's programs are supported by grants received from the federal, state and local governments.

If conditions are attached to a grant which must be satisfied before the Company is eligible to receive the contribution, recognition of the grant as revenue is deferred until those conditions are satisfied.

Where a grant is received on the condition that specified services are delivered, to the grantor, this is considered a reciprocal transaction. Revenue is recognised as services are performed and at year-end until the service is delivered.

Revenue from a non-reciprocal grant that is not subject to conditions is recognised when the Company obtains control of the funds, economic benefits are probable, and the amount can be measured reliably.

Grant revenue is recognised to the Company's point of break even under AASB 15 and AASB 1058, a liability is recognised at year end to the extent that conditions remain unsatisfied.

Where the Company receives a non-reciprocal contribution of an asset from a government or other party for no or nominal consideration, the asset is recognised at fair value and a corresponding amount of revenue is recognised.

**Project Funds**

Included in cash and cash equivalents are project funds of \$7,565,598 (2019: \$4,856,654) which are specifically for project funding and are not available for general use.

**For current year**

The company has adopted AASB 15 from 1 July 2019. The standard provides a single comprehensive model for revenue recognition. The core principle of the standard is that an entity shall recognise revenue to depict the transfer of promised goods and services to customers at an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services. The standard introduced a new contract-based revenue recognition model with a measurement approach that is based on an allocation of the transaction price. This is



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

described further in the accounting policies below. Credit risk is presented separately as an expense rather than adjusted against revenue. Contracts with customers are presented in an entity's statement of financial position as a contract liability, a contract asset, or a receivable, depending on the relationship between the entity's performance and the customer's payment. Customer acquisition costs and costs to fulfil a contract can, subject to certain criteria, be capitalised as an asset and amortised over the contract period.

**AASB 1058 Income of Not-for-Profit Entities**

The company has adopted AASB 1058 from 1 July 2019. The standard replaces AASB 1004 'Contributions' in respect to income recognition requirements for not-for-profit entities. The timing of income recognition under AASB 1058 is dependent upon whether the transaction gives rise to a liability or other performance obligation at the time of receipt. Income under the standard is recognised where: an asset is received in a transaction, such as by way of grant, bequest or donation; there has either been no consideration transferred, or the consideration paid is significantly less than the asset's fair value; and where the intention is to principally enable the entity to further its objectives. For transfers of financial assets to the entity which enable it to acquire or construct a recognisable non-financial asset, the entity must recognise a liability amounting to the excess of the fair value of the transfer received over any related amounts recognised. Related amounts recognised may relate to contributions by owners, AASB 15 revenue or contract liability recognised, lease liabilities in accordance with AASB 16, financial instruments in accordance with AASB 9, or provisions in accordance with AASB 137. The liability is brought to account as income over the period in which the entity satisfies its performance obligation. If the transaction does not enable the entity to acquire or construct a recognisable non-financial asset to be controlled by the entity, then any excess of the initial carrying amount of the recognised asset over the related amounts is recognised as income immediately. Where the fair value of volunteer services received can be measured, a private sector not-for-profit entity can elect to recognise the value of those services as an asset where asset recognition criteria are met or otherwise recognise the value as an expense.

**Comparative Amounts**

Comparatives are consistent with prior years, unless otherwise stated.

Where a change in comparatives has also affected the opening retained earnings previously presented in a comparative period, an opening statement of financial position at the earliest date of the comparative period has been presented.

**Trade and Other Payables**

Trade and other payables represent the liabilities for goods and services received by the company during the reporting year that remain unpaid at the end of the reporting year. The balance is recognised as a current liability with the amounts normally paid within 30 days of recognition of the liability.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

**Significant Management Judgement in Applying Accounting Policies**

When preparing the financial statements, management undertakes a number of judgements, estimates and assumptions about the recognition and measurement of assets, liabilities, income and expenses.

**Estimation uncertainty**

Information about estimates and assumptions that have the most significant effect on recognition and measurement of assets, liabilities, income and expenses is provided below. Actual results may be substantially different.

**Useful lives of depreciable assets**

Management reviews its estimate of the useful lives of depreciable assets at each reporting date, based on the expected utility of the assets. Uncertainties in these estimates relate to technical obsolescence that may change the utility of certain software and IT equipment.

**Fair Value of Assets and Liabilities**

The company measures some of its assets and liabilities at fair value on either a recurring or non-recurring basis, depending on the requirements of the applicable Accounting Standard.

“Fair value” is the price the company would receive to sell an asset or would have to pay to transfer a liability in an orderly (ie unforced) transaction between independent, knowledgeable and willing market participants at the measurement date.

As fair value is a market-based measure, the closest equivalent observable market pricing information is used to determine fair value. Adjustments to market values may be made having regard to the characteristics of the specific asset or liability. The fair values of assets and liabilities that are not traded in an active market are determined using one or more valuation techniques. These valuation techniques maximise, to the extent possible, the use of observable market data.

To the extent possible, market information is extracted from the principal market for the asset or liability (ie the market with the greatest volume and level of activity for the asset or liability). In the absence of such a market, market information is extracted from the most advantageous market available to the entity at the end of the reporting year (ie the market that maximises the receipts from the sale of the asset or minimises the payments made to transfer the liability, after taking into account transaction costs and transport costs).

For non-financial assets, the fair value measurement also takes into account a market participant's ability to use the asset in its highest and best use or to sell it to another market participant that would use the asset in its highest and best use.

The fair value of liabilities and the entity's own equity instruments (if any) may be valued, where there is no observable market price in relation to the transfer of such financial instrument, by reference to observable market information where such instruments are held as assets. Where this information is not available, other valuation techniques are adopted and, where significant, are detailed in the respective note to the financial statements.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

**Trade and other receivables**

Trade and other receivables are recognised at amortised cost, less any allowance for expected credit losses.

**New and Amended Accounting Standards and Interpretations Adopted**

The company has adopted all of the new or amended Accounting Standards and Interpretations issued by the Australian Accounting Standards Board ('AASB') that are mandatory for the current reporting period, including AASB 15, AASB 1058 and AASB16.

Any new or amended Accounting Standards or Interpretations that are not yet mandatory have not been early adopted.

The adoption of these Accounting Standards and Interpretations did not have any significant impact on the financial performance or position of the company.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	2020 \$	2019 \$
<b>3 Revenue and Other Income</b>		
<b>Revenue</b>		
Grants received from:		
State/Federal Government Grants	3,680,000	3,680,000
Project Funding	5,000,000	7,000,000
State Government Contribution	510,424	450,000
Grants Deferred	(3,743,139)	(2,471,388)
	<u>5,447,285</u>	<u>8,658,612</u>
Other revenue:		
Interest received	(171)	8,757
Sponsorship Income	70,202	127,459
Other revenue	73,736	19,799
	<u>143,767</u>	<u>156,015</u>
Total revenue	<u>5,591,052</u>	<u>8,814,627</u>
<b>4 Auditors' Remuneration</b>		
Auditor Fees	<u>15,500</u>	<u>15,000</u>
<b>5 Profit for the year</b>		
The result for the year was derived after charging / (crediting) the following items:		
<b>Expenses</b>		
Employee benefits expense:		
- movement in provision for annual leave	16,903	42,864
- contributions to defined contribution superannuation funds	142,033	140,734
Depreciation of property, plant and equipment	10,976	8,129
Depreciation of right of use asset	54,879	-
Interest on lease liability	1,895	-

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	2020 \$	2019 \$
<b>6 Cash and Cash Equivalents</b>		
Cash at Bank	11,565,691	8,098,580
	<u>11,565,691</u>	<u>8,098,580</u>
<b>7 Trade and Other Receivables</b>		
Trade Debtors	205,000	9,733
	<u>205,000</u>	<u>9,733</u>
The carrying value of trade receivables is considered a reasonable approximation of fair value due to the short term nature of the balances.		
<b>8 Other Assets</b>		
<b>Current</b>		
Deposits & Bonds	13,126	41,258
Other Assets	-	47,448
GST Receivable	102,029	78,205
Prepayments	68,206	20,659
FBT Refundable	4,186	-
Payroll Tax Refundable	2,030	-
	<u>189,577</u>	<u>187,570</u>
<b>9 Right of Use Assets</b>		
Property at Cost	73,172	-
Less Accumulated depreciation	<u>(54,879)</u>	<u>-</u>
Total Right of Use Asset at End of Year	<u>18,293</u>	<u>-</u>

The company leases a property for its operations. In determining the lease term and assessing the length of the non-cancellable period, the company applies the definition of a contract and determines the period for which the contract is enforceable. The discount rate applied to lease liabilities recognised in the statement of financial position as at 1 July 2019 is 3%. The company has a renewal option available at the end of October 2020, however the company has not yet taken up this option. The right of use asset includes a provision of \$10,000 for make good at the end of the lease term.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	2020 \$	2019 \$
<hr/>		
<b>10 Property, Plant and Equipment</b>		
<b>PLANT AND EQUIPMENT</b>		
<b>Plant and Equipment:</b>		
At cost	56,288	43,517
Accumulated depreciation	(22,756)	(11,780)
<b>Total Plant and Equipment</b>	<u>33,532</u>	<u>31,737</u>

**Movements in Carrying Amounts of Property, Plant and Equipment**

Movement in the carrying amounts for each class of property, plant and equipment between the beginning and the end of the current financial year.

	Computer Equipment \$	Office Furniture & Equipment \$	Total \$
Balance at 1 July 2018	17,828	-	17,828
Additions	7,888	14,150	22,038
Depreciation expense	(5,968)	(2,161)	(8,129)
Balance at 30 June 2019	<u>19,748</u>	<u>11,989</u>	<u>31,737</u>
Additions	6,946	5,825	12,771
Depreciation expense	(7,429)	(3,547)	(10,976)
Carrying amount at 30 June 2020	<u><u>19,265</u></u>	<u><u>14,267</u></u>	<u><u>33,532</u></u>



**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	2020 \$	2019 \$
<hr/>		
<b>11 Trade and Other Payables</b>		
<b>Current</b>		
NAB Credit Card	5,768	12,737
Trade Creditors	243,498	511,673
Accrued Expenses	146,725	44,852
PAYG Withholding Payable	62,894	55,422
Superannuation Payable	6,142	-
Other Payables	-	82
Wages & Super Accrual	58,105	-
	<hr/> 523,132	<hr/> 624,766

Trade and other payables are unsecured, non interest bearing and are normally settled within 30 days. The carrying value of trade and other payables is considered to be a reasonable approximation of fair value due to the short term nature of the balances.

**12 Lease Liabilities**

**Current**

Lease Liabilities	16,065	-
<b>Total Lease Liabilities</b>	<hr/> 16,065	<hr/> -

**13 Provisions**

Make Good Provision	<hr/> 10,000	<hr/> -
---------------------	--------------	---------

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	2020 \$	2019 \$
<b>14 Capital and Leasing Commitments</b>		
<b>Operating Lease Commitments</b>		
Non-cancellable operating leases contracted for but not capitalised in the financial statements:		
Payable - minimum lease payments		
Not later than 12 months	-	(47,730)
Between 12 months and five years	-	(16,457)
	<u>-</u>	<u>(64,187)</u>

**15 Contingent Liabilities**

The company had no contingent liabilities as at 30 June 2020 and 30 June 2019.

**16 Events After the Reporting Period**

The directors are not aware of any significant events since the end of the reporting year,

**17 Key Management Personnel**

**Short-term employee benefits**

KMP Compensation - short term benefits	528,337	384,445
<b>Total compensation</b>	<u>528,337</u>	<u>384,445</u>

**18 Related Party Transactions**

Transactions with related parties

- There were no transactions with related parties during the current and previous financial year.
- There were no trade receivables from or trade payables to related parties at the current and previous reporting date.
- There were no loans to or from related parties at the current and previous reporting date.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**NOTES TO THE FINANCIAL STATEMENTS**  
**FOR THE YEAR ENDED 30 JUNE 2020**

	<b>2020</b>	<b>2019</b>
	<b>\$</b>	<b>\$</b>

---

**19 Economic Dependence**

Australian Cyber Security Growth Network Limited is dependent on the Department of Industry, Innovation and Science for the majority of its revenue used to operate the business, which requires continuing compliance with the grant funding agreement. At the date of this report, the Board of Directors has no reason to believe the Department will not continue to support Australian Cyber Security Growth Network Limited.

**AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED**  
**A.B.N 73 616 231 451**

**DIRECTORS' DECLARATION**

The directors of the company declare that:

1. The financial statements and notes, as set out on pages 1 to 23, for the year ended 30 June 2020 are in accordance with the Corporations Act 2001 and:
  - (a) comply with Australian Accounting Standards - Reduced Disclosure Requirements; and
  - (b) give a true and fair view of the financial position of the company as at 30 June 2020 and of its performance for the year ended on that date.
2. In the directors' opinion, there are reasonable grounds to believe that the company will be able to pay its debts as and when they become due and payable.

This declaration is made in accordance with a resolution of the Board of Directors.

Director:  DOUGLAS ELIX

Dated this 11th day of November, 2020

## INDEPENDENT AUDITOR'S REPORT

To the members of Australian Cyber Security Growth Network Ltd (AustCyber).

### Report on the Audit of the Financial Report

#### Opinion

We have audited the financial report of Australian Cyber Security Growth Network Ltd (the Company), which comprises the statement of financial position as at 30 June 2020, the statement of profit or loss and other comprehensive income, the statement of changes in equity and the statement of cash flows for the year then ended, and notes to the financial report, including a summary of significant accounting policies, and the directors' declaration.

In our opinion the accompanying financial report of Australian Cyber Security Growth Network Ltd, is in accordance with the *Corporations Act 2001*, including:

- (i) Giving a true and fair view of the Company's financial position as at 30 June 2020 and of its financial performance for the year ended on that date; and
- (ii) Complying with Australian Accounting Standards - Reduced Disclosure Requirements and the *Corporations Regulations 2001*.

#### Basis for opinion

We conducted our audit in accordance with Australian Auditing Standards. Our responsibilities under those standards are further described in the *Auditor's responsibilities for the audit of the Financial Report* section of our report. We are independent of the Company in accordance with the *Corporations Act 2001* and the ethical requirements of the Accounting Professional and Ethical Standards Board's *APES 110 Code of Ethics for Professional Accountants (including Independence Standards)* (the Code) that are relevant to our audit of the financial report in Australia. We have also fulfilled our other ethical responsibilities in accordance with the Code.

We confirm that the independence declaration required by the *Corporations Act 2001*, which has been given to the directors of the Company, would be in the same terms if given to the directors as at the time of this auditor's report.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

### Other information

The directors are responsible for the other information. The other information obtained at the date of this auditor's report is information included in the Directors Report, but does not include the financial report and our auditor's report thereon.

Our opinion on the financial report does not cover the other information and accordingly we do not express any form of assurance conclusion thereon.

In connection with our audit of the financial report, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial report or our knowledge obtained in the audit, or otherwise appears to be materially misstated.

If, based on the work we have performed on the other information obtained prior to the date of this auditor's report, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

### Responsibilities of the directors for the Financial Report

The directors of the Company are responsible for the preparation of the financial report that gives a true and fair view in accordance with Australian Accounting Standards - Reduced Disclosure Requirements and the *Corporations Act 2001* and for such internal control as the directors determine is necessary to enable the preparation of the financial report that gives a true and fair view and is free from material misstatement, whether due to fraud or error.

In preparing the financial report, the directors are responsible for assessing the Company's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the directors either intend to liquidate the Company or to cease operations, or has no realistic alternative but to do so.

### Auditor's responsibilities for the audit of the Financial Report

Our objectives are to obtain reasonable assurance about whether the financial report as a whole is free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with the Australian Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of this financial report.

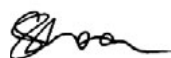
A further description of our responsibilities for the audit of the financial report is located at the Auditing and Assurance Standards Board website (<http://www.auasb.gov.au/Home.aspx>) at:

[http://www.auasb.gov.au/auditors\\_responsibilities/ar4.pdf](http://www.auasb.gov.au/auditors_responsibilities/ar4.pdf)

This description forms part of our auditor's report.

**BDO Audit Pty Ltd**

BDO



Gillian Shea  
Director

Sydney, 11 November 2020



# APPENDIX **E**

## **BDO Annual Completion Report**





# AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED

Annual completion report

YEAR ENDED 30 JUNE 2020

---

# CONTENTS

Executive Summary .....	4
Impact of COVID-19 .....	5
Areas of audit focus .....	6
Summary of misstatements .....	9
Internal control .....	10
Other reporting requirements .....	12
Appendix 1 Proposed audit report .....	13
Appendix 2 Auditor independence declaration .....	15
Appendix 3 New developments .....	16
Appendix 4 Responding to COVID-19 .....	18







---

Dear Directors

We are pleased to present this report to the Directors of Australian Cyber Security Growth Network Limited in relation to the 30 June 2020 annual audit.

As at the date of this report, we have substantially completed our audit and subject to the satisfactory resolution of the matters outlined in the Executive Summary, we expect to issue an unmodified audit report.

We have set out in this document the significant matters arising from our audit. This summary covers those matters we believe to be material in the context of our work.

We look forward to the Directors meeting on 15<sup>th</sup> October 2020 where we will have the opportunity to discuss this report.

Should you require clarification on any matter in this report before this date, please do not hesitate to contact me on +61 2 8264 6666.

We would like to take this opportunity to extend our appreciation to management for their assistance and cooperation throughout the course of our audit.

Yours faithfully,

**Gillian Shea**  
Engagement Partner



# EXECUTIVE SUMMARY

## PURPOSE

The purpose of this report is to communicate significant matters arising from our audit to the Directors. This report has been discussed with management.

## SCOPE

Our audit was conducted in accordance with Australian Auditing Standards and the *Corporations Act 2001* for the year ended 30 June 2020.

## STATUS OF THE AUDIT

Our audit of the financial report is substantially complete. We expect to issue an unmodified audit report, subject to satisfactory completion of the following:

- ▶ Signed Engagement Letters
- ▶ Signed Management Representation Letters
- ▶ Signed Financial Statements

A draft of the proposed audit report is included at [Appendix 1](#).

## SUMMARY OF MISSTATEMENTS

We have identified misstatements during our audit. The list of corrected and uncorrected misstatements is included in the respective [section](#) of this report.

We have not identified any uncorrected misstatements that, in our judgement, either individually or in aggregate, could have a material effect on the financial report for the year ended 30 June 2020.

## AREAS OF AUDIT FOCUS

In performing our audit, we have identified those matters that, in the auditor's judgement, were of the most significance in the audit of the financial report.

Our audit procedures also focused on areas that were considered to represent significant risks of material misstatement. These areas of focus are outlined below:

- ▶ Going Concern
- ▶ Management Override of Controls
- ▶ Revenue Recognition
- ▶ Leases

Refer to the relevant section for details on the key audit matters, significant risk areas and other areas focused on during the audit.



# IMPACT OF COVID-19

On 31 January 2020, the World Health Organisation (WHO) announced a global health emergency because of a new strain of coronavirus and the risks to the international community as the virus spreads globally beyond its point of origin. Because of the rapid increase in exposure globally, on 11 March 2020, the WHO classified the COVID-19 outbreak as a pandemic. Besides the serious public health threat that has arisen from the outbreak of COVID-19, it continues to have serious economic impacts on many businesses.

## COVID-19 AND THE FINANCIAL REPORT

The following table sets out the areas of the 30 June 2020 financial report/financial reporting process that were materially impacted by the COVID-19 pandemic and its associated measures. It also sets out our audit response to these impacts and our findings.

Area	Impact on the financial report	Audit response and summary of findings
Going Concern	<p>The full impact of the COVID-19 outbreak continues to evolve. There is therefore uncertainty as to the full impact that the pandemic will have on its financial condition, liquidity, and future results of operations during 2021. Management is actively monitoring the global situation and its impact on the Company's financial condition, liquidity, operations, suppliers, industry, and workforce. Although the Company cannot estimate the length or gravity of the impact of the COVID-19 outbreak at this time, if the pandemic continues, it may have an adverse effect on the Company's results of future operations, financial position, and liquidity in fiscal year 2021.</p>	<p>Our procedures to review the impact of COVID-19 included the following:</p> <ul style="list-style-type: none"><li>• Discussing with Management the impact of COVID-19 on AustCyber.</li><li>• Obtaining and reviewing cash flow forecasts for the next financial year, to ensure the application of the going concern assumption remains appropriate;</li><li>• Assessing the cash flow forecasts provided by management and challenging the assumptions therein to ensure consistency with management's stated business and operational objectives;</li><li>• Considering the potential impairment of assets, mainly Intangibles and Receivables.</li></ul> <p>There is no material uncertainty noted with regards to Going Concern as the company continues to be funded by the government. Grant income is set by the funding agreements in place, and has been agreed to by the government until the end of the agreement in February 2023. The pandemic has not had an impact on government funding and operations, nor is it considered to have impacted the recoverability of the Company's assets.</p>





## AREAS OF AUDIT FOCUS

We identified the risk areas as part of our risk assessment procedures undertaken during the planning phase and continued to be alert for risks during the course of the audit. Our audit procedures focused on areas that were considered to represent risks of material misstatement.

Management Override of Controls		
Description	Audit work performed	Summary of findings
Management override is considered a significant risk due to the inherent risk of fraud. Management is in a position to perpetuate fraudulent reporting by overriding established journals, or posting unauthorised or inappropriate journal entries. Management override is also a presumed fraud risk under Auditing Standards.	<p>The risk has been addressed by performing the audit procedures below:</p> <p>Reviewed general journal entries processed during the year and at year-end to ensure they were reasonable and appropriately authorised; and</p> <p>Reviewed significant estimate and judgement areas to ensure assumptions used by management were reasonable and in line with our expectations. The key areas of focus were in the useful lives of assets and employee leave provisions.</p>	No evidence of management override of controls was observed from the audit procedures performed.

## AREAS OF AUDIT FOCUS CONTINUED

Revenue Recognition		
Description	Audit work performed	Summary of findings
<p>Revenue recognition is considered a significant risk of material misstatement due to the inherent risk of fraud and it is a presumed fraud risk under Auditing Standards.</p> <p>AustCyber revenue is generated primarily from grants from the Department of Industry, Innovation and Science and is recognised based upon set milestones detailed in the funding agreement. There is a risk that the conditions of the agreement have not been met in order to recognise revenue.</p> <p>AASB 120 requires that revenue from government grants is only recognised when there is reasonable assurance that:</p> <ul style="list-style-type: none"> <li>The entity will comply with the conditions attaching to them; and</li> <li>The grants will be received.</li> </ul>	<p>We have performed the following audit procedures to ensure revenue recognised in the period is not materially misstated:</p> <ul style="list-style-type: none"> <li>Reviewed revenue recognition policies and ensure compliance with Australian Accounting Standards;</li> <li>Tested a sample of grant revenue and expense transactions throughout the year, and vouched to relevant supporting documentation; and</li> <li>Reviewed deferred revenue as at 30 June 2020 in conjunction with the grant funding agreement, ensuring that any unspent money has been recognised as a liability at year end in accordance with the funding agreement and Australian accounting standards (AASB115 AND AASB1058).</li> </ul>	<p>No material exceptions were observed from the audit procedures performed. We consider that revenue recognised for the year has been recognised in accordance with AASB 15 and AASB 1058 and is not materially misstated. We concur with the treatment of the deferred revenue that has been recognised on the unspent portion of grant funding received.</p>



## AREAS OF AUDIT FOCUS CONTINUED

LEASES		
Description	Audit work performed	Summary of findings
<p>AASB 16 Leases is a new accounting standard that became effective for the 30 June 2020 financial year.</p> <p>There is a risk that accounting policies have not been appropriately updated for changes required under the accounting standards and that transitional adjustments for prior year comparatives or new disclosures required in relation to these standards have not been appropriately reflected.</p>	<p>We reviewed management's assessment of the company's right-of-use asset and lease liability under the requirements of AASB 16 Leases.</p> <p>We reviewed the disclosures included in the financial statements to ensure these meet the requirements of the new standard.</p>	<p>We reviewed the calculations to account for the right-of-use assets and lease liabilities under the requirements of AASB 16. We also assessed the key judgement related to the incremental borrowing rate of each lease and we did not identify any significant variances, and consider the accounting for leases to be materiality correct.</p> <p>We reviewed the disclosure included in the financial statements and conclude that it appropriate in terms of the requirements of Australian Accounting Standards.</p>

A smiling man and woman are shown in a meeting setting. The man, on the left, is wearing glasses and a white shirt. The woman, on the right, is also smiling and wearing a red top. They are both looking towards the right side of the frame.

# SUMMARY OF MISSTATEMENTS

## UNCORRECTED MISSTATEMENTS

We detail below the uncorrected misstatements which we have identified during the audit, and that were determined by management to be immaterial, both individually and in aggregate to the financial report taken as a whole.

Misstatements have not been included if they are considered to be clearly trivial which we have set at **\$5,514**. Matters which are clearly trivial are regarded as clearly inconsequential when taken individually or in aggregate.

We will seek representation from management to acknowledge that:

- ▶ Uncorrected misstatements have been brought to their attention by us; and
- ▶ They have considered the effect of any uncorrected misstatements, aggregated during and pertaining to the latest period, on the financial report and consider the misstatements are immaterial individually and in aggregate to the financial report taken as a whole.

Description	Assets	(Liabilities)	Reserves	(Profit)/Loss
Understatement of expenses due to the reversal of GST on PY invoice against current year expenses.			(7,500)	7,500
Understatement of audit fees due to the reversal of PY over accrual against the current year expense.			(9,913)	9,913
Net effect of uncorrected misstatements	-	-	(17,143)	17,143





# INTERNAL CONTROL

## CURRENT YEAR

In accordance with ASA 265 *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management*, we are required to communicate in writing, significant deficiencies in internal control identified during the audit to those charged with governance on a timely basis.

The standard defines a deficiency in internal control as follows:

1. A control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial report on a timely basis; or
2. A control necessary to prevent, or detect and correct, misstatements in the financial report on a timely basis is missing.

Significant deficiency in internal control means a deficiency or combination of deficiencies in internal control that, in the auditor's professional judgement, is of sufficient importance to merit the attention of the Directors.

Our audit procedures did not identify any significant deficiencies that in our professional judgment are of sufficient importance to merit the attention of the Directors.

## FOLLOW UP ON PRIOR PERIOD FINDINGS

We have detailed below the current status of matters relating to internal control that have been raised in prior communications and are not referred to in the current period findings.

Description of matter		Date previously communicated	Current status
1	<b>Bank Signatories</b> Michelle Price is the only signatory on the NAB Bank Accounts. This is after the resignation of Belinda Newham who was previously the second authorised signed.	2019	Noted that Signatories were updated on 9/06/2020 to be Antony Stubbs and Michelle Price.
2	<b>Audit Trail for Closed Accounts</b>	2019	Issue was not encountered in the current year.



## INTERNAL CONTROL CONTINUED

Description of matter	Date previously communicated	Current status
Bank statements could not be obtained for accounts that were active as of 30 June 2019 but closed post year end.		
<b>3 Review of cut-off for accruals</b> There was no review of the cut-off for payroll-related accruals (FBT payable and salaries and wages payable) relating to June 2019.	<b>2019</b>	Noted that payroll related accruals were accounted for in the June 2020 Trial Balance.
<b>4 No reconciliation is undertaken of GST on supplier invoices</b> BDO noted two invoices on which GST had not been correctly accounted for.	<b>2019</b>	This error was not encountered in the current period audit.





## OTHER REPORTING REQUIREMENTS

### INDEPENDENCE AND ETHICS

In conducting our audit, we are required to comply with the independence requirements of the *Corporations Act 2001* and Part 4A of APES 110 *Code of Ethics for Professional Accountants* (including *Independence Standards*).

We have obtained independence declarations from all staff engaged in the audit.

We also have policies and procedures in place to identify any threats to our independence, and to appropriately deal with and if relevant mitigate those risks.

We have not become aware of any issue that would cause any member of the engagement team, BDO or any BDO network firm to contravene any ethical requirement or any regulatory requirement that applies to the audit engagement.

BDO has not provided any other services during the audit to Australian Cyber Security Growth Network Limited.

In addition to the audit, we have completed the following engagements during the year:

- ▶ AUP (Acquittals review)

None of these engagements have impaired our independence

The *Corporations Act 2001* requires the lead auditor to make a declaration to the directors regarding independence. We are in a position to make this declaration, a draft of which has been included at [Appendix 2](#).

### NON-COMPLIANCE WITH LAWS AND REGULATIONS

We have made enquiries in relation to any non-compliance with laws and regulations during the course of our audit. We have not identified any instances of non-compliance with laws and regulations as a result of our enquiries.

We would like to remind you that under s311 and 601 HG of the *Corporations Act 2001* we are obliged to notify ASIC about matters that we have reasonable grounds to suspect amount to a significant contravention of the *Corporations Act*. We have 28 days in which to report once we have identified or suspect a significant contravention.

We have not identified any reportable matters during the course of our audit.

### FRAUD

Management have confirmed that there were no matters of fraud identified for the period under audit, or subsequently. It should be noted that our audit is not designed to detect fraud however should instances of fraud come to our attention we will report them to you.

We have not identified any instances of fraud during the course of our audit.



## APPENDIX 1 PROPOSED AUDIT REPORT

### INDEPENDENT AUDITOR'S REPORT

To the members of Australian Cyber Security Growth Network Ltd (AustCyber).

#### Report on the Audit of the Financial Report

##### Opinion

We have audited the financial report of AustCyber (the Company), which comprises the statement of financial position as at 30 June 2020, the statement of profit or loss and other comprehensive income, the statement of changes in equity and the statement of cash flows for the year then ended, and notes to the financial report, including a summary of significant accounting policies, and the directors' declaration.

In our opinion the accompanying financial report of AustCyber, is in accordance with the Corporations Act 2001, including:

- (i) Giving a true and fair view of the Company's financial position as at 30 June 2019 and of its financial performance for the year ended on that date; and
- (ii) Complying with Australian Accounting Standards - Reduced Disclosure Requirements and the Corporations Regulations 2001.

##### Basis for opinion

We conducted our audit in accordance with Australian Auditing Standards. Our responsibilities under those standards are further described in the Auditor's responsibilities for the audit of the Financial Report section of our report. We are independent of the Company in accordance with the Corporations Act 2001 and the ethical requirements of the Accounting Professional and Ethical Standards Board's APES 110 Code of Ethics for Professional Accountants

(including Independence Standards) (the Code) that are relevant to our audit of the financial report in Australia. We have also fulfilled our other ethical responsibilities in accordance with the Code.

We confirm that the independence declaration required by the Corporations Act 2001, which has been given to the directors of the Company, would be in the same terms if given to the directors as at the time of this auditor's report.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

##### Other information

The directors are responsible for the other information. The other information obtained at the date of this auditor's report is information included in the Directors Report, but does not include the financial report and our auditor's report thereon.

Our opinion on the financial report does not cover the other information and accordingly we do not express any form of assurance conclusion thereon.

In connection with our audit of the financial report, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial report or our knowledge obtained in the audit, or otherwise appears to be materially misstated.

If, based on the work we have performed on the other information obtained prior to the date of this auditor's report, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

##### Responsibilities of the directors for the Financial Report

The directors of the Company are responsible for the preparation of the financial report that gives a true and fair view in accordance with Australian Accounting

# APPENDIX 1 PROPOSED AUDIT REPORT CONTINUED

Standards - Reduced Disclosure Requirements and the Corporations Act 2001 and for such internal control as the directors determine is necessary to enable the preparation of the financial report that gives a true and fair view and is free from material misstatement, whether due to fraud or error.	BDO Audit Pty Limited
In preparing the financial report, the directors are responsible for assessing the Company's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the directors either intend to liquidate the Company or to cease operations, or has no realistic alternative but to do so.	Gillian Shea
Auditor's responsibilities for the audit of the Financial Report	Director
Our objectives are to obtain reasonable assurance about whether the financial report as a whole is free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with the Australian Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of this financial report.	
A further description of our responsibilities for the audit of the financial report is located at the Auditing and Assurance Standards Board website ( <a href="http://www.auasb.gov.au/Home.aspx">http://www.auasb.gov.au/Home.aspx</a> ) at:  <a href="http://www.auasb.gov.au/auditors_responsibilities/ar4.pdf">http://www.auasb.gov.au/auditors_responsibilities/ar4.pdf</a>  This description forms part of our auditor's report.	



## APPENDIX 2 AUDITOR INDEPENDENCE DECLARATION

### Positive declaration

We set out below our draft Auditor independence declaration.

#### DECLARATION OF INDEPENDENCE BY GILLIAN SHEA TO DIRECTORS OF AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED

As lead auditor of Australian Cyber Security Growth Network Limited for the year ended 30 June 2020, I declare that, to the best of my knowledge and belief, there have been:

1. No contraventions of the auditor independence requirements of the *Corporations Act 2001* in relation to the audit; and
2. No contraventions of any applicable code of professional conduct in relation to the audit.

This declaration is in respect of Australian Cyber Security Growth Network Limited and the entities it controlled during the year.





## APPENDIX 3 NEW DEVELOPMENTS

We wish to bring to your attention some upcoming changes in financial reporting which may cause significant changes to your future reported financial position and performance. We have provided an overview of the major changes below and would be happy to discuss the impact on your business and assist with transition where applicable.

### AASB 2020-4 AMENDMENTS TO AUSTRALIAN ACCOUNTING STANDARDS - COVID-19 RELATED RENT CONCESSIONS

Effective for annual reporting periods beginning on or after 1 June 2020, this change introduces a practical expedient that permits lessees not to assess whether a rent concession that occurs as a direct consequence of the COVID-19 pandemic is a lease modification, provided all of the following criteria are met:

- ▶ Change in lease payments results in revised consideration for the lease that is substantially the same as, or less than, the consideration for the lease immediately prior to the change
- ▶ Any reduction in lease payments affects only payments originally due on or before 30 June 2021 (for example, a concession would meet this condition if it resulted in reduced lease payments on or before 30 June 2021 and increased lease payments that extend beyond 30 June 2021)
- ▶ There is no substantive change to other terms and conditions of the lease.

In such cases, the concessions are accounted for as if they were not a lease modification. On first time adoption for the year ended 30 June 2021, the cumulative effect of initially applying the amendment will be recognised as an adjustment to opening balances of retained earnings on 1 July 2020.

### AASB 2018-6 AMENDMENTS TO AUSTRALIAN ACCOUNTING STANDARDS - DEFINITION OF A BUSINESS

The nature of this amendment clarifies the definition of a 'business' in AASB 3 *Business Combinations* (AASB 3) to assist in determining whether a transaction should be accounted for as a business combination or as an asset acquisition. The main amendments include:

- ▶ Narrowing the definition of 'outputs' and a 'business' to focus on returns from selling goods and services to customers, rather than on cost reductions
- ▶ Amending guidance on inputs, processes and outputs to align with the new definition of a 'business'
- ▶ Clarifying that to be considered a 'business', an acquired set of activities and assets must include, as a minimum, an input and a substantive process, that together significantly contribute to the ability to create outputs.

There will be no impact on the financial statements when these amendments are first adopted because they apply prospectively to acquisitions occurring on or after the beginning of the first annual reporting period beginning on or after 1 January 2020, i.e. on or after 1 July 2020.



## APPENDIX 3 NEW DEVELOPMENTS CONTINUED

### AASB 2020-1 AMENDMENTS TO AUSTRALIAN ACCOUNTING STANDARDS - CLASSIFICATION OF LIABILITIES AS CURRENT OR NON-CURRENT

Effective for annual reporting periods beginning on or after 1 January 2022, there are four main changes to the classification requirements within AASB 101 *Presentation of financial statements*:

1. The requirement for an 'unconditional' right has been deleted from paragraph 69(d) because covenants in banking agreements would rarely result in unconditional rights.
2. The right to defer settlement must exist at the end of the reporting period. If the right to defer settlement is dependent upon the entity complying with specified conditions (covenants), the right to defer only exists at reporting date if the entity complies with those conditions at reporting date.
3. Classification is based on the right to defer settlement, and not intention (paragraph 73), and
4. If a liability could be settled by an entity transferring its own equity instruments prior to maturity (e.g. a convertible bond), classification is determined without considering the possibility of earlier settlement by conversion to equity, but only if the conversion feature is classified as equity under IAS 32.

As these amendments only apply for the first time to the 30 June 2023 balance sheet (and 30 June 2022 comparative balance sheet), companies are not yet able to make an assessment of the impacts regarding the right to defer settlement, compliance with bank covenants, and intention to settle.

## APPENDIX 4 RESPONDING TO COVID-19

### COVID-19 AND YOUR BUSINESS

The unprecedented COVID-19 crisis affecting the globe has directly and materially impacted economic activity in Australia and throughout the world. This has caused some otherwise healthy businesses to experience material reductions to revenue while overhead expenses have remained relatively fixed. This inevitably leads to a cash flow crisis and even solvency concerns.

If your business is in this situation, an immediate and robust business rescue plan is necessary to give you the best chance to ensure long-term viability. Being proactive is critical.

Clients facing this scenario can click on the icon opposite for a detailed business impact and risk response guide. This provides guidance on the following areas:

- ▶ People and leadership
- ▶ Sustainability
- ▶ Operations
- ▶ Supply chain
- ▶ Health and safety.

Download **Coronavirus (COVID-19) Business impact and risk response guide** ▶



There are a number of areas of a business that may continue to be impacted by the COVID-19 outbreak. BDO have therefore provided guidance on appropriate actions to mitigate the impact and manage associated risks to [‘Keep your business running’](#).

The Australian Government has also released a number of economic measures in response of COVID-19 and BDO can continue to help you navigate these stimulus measures. Please refer to BDO’s [‘Stimulus measures’](#) resource page where BDO advisers continue to provide expert commentary on these measures and how businesses can access them via a range of technical updates, webinars and articles.

### COVID-19 AND FUTURE REPORTING PERIODS

We understand that this changing environment may continue to create challenges from a financial reporting perspective and create risks that entities may not have encountered before. BDO will continue to work closely with management to ensure these challenges are addressed on a timely basis.

Please refer to BDO’s [IFRS Advisory Coronavirus](#) resource page which continues to be updated with financial reporting bulletins and accounting news articles which address ongoing financial reporting considerations for businesses.



1300 138 991  
[www.bdo.com.au](http://www.bdo.com.au)

NEW SOUTH WALES  
NORTHERN TERRITORY  
QUEENSLAND  
SOUTH AUSTRALIA  
TASMANIA  
VICTORIA  
WESTERN AUSTRALIA

Distinctively different - it's how we see you  
AUDIT • TAX • ADVISORY

We have prepared this report solely for the use of Australian Cyber Security Growth Network Limited. As you know, this report forms part of a continuing dialogue between the company and us and, therefore, it is not intended to include every matter, whether large or small, that has come to our attention. For this reason we believe that it would be inappropriate for this report to be made available to third parties and, if such a third party were to obtain a copy of this report without prior consent, we would not accept any responsibility for any reliance they may place on it.

BDO Audit Pty Limited ABN 236 985 726 is a member of a national association of independent entities which are all members of BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee. BDO Audit Pty Limited and BDO Australia Ltd are members of BDO International Ltd, a UK company limited by guarantee, and form part of the international BDO network of independent member firms. Liability limited by a scheme approved under Professional Standards Legislation.

[www.bdo.com.au](http://www.bdo.com.au)

## Contact

Email: [info@austcyber.com](mailto:info@austcyber.com)

Phone: 0455 260 848

Website: [www.austcyber.com](http://www.austcyber.com)

Twitter: [@AustCyber](https://twitter.com/AustCyber)