



Australian Government
Department of Industry, Science,
Energy and Resources

Industry Growth Centres



ANNUAL REPORT | 2018–19





“

Cyber security
is emerging as
one of Australia's
most promising
growth sectors

CONTENTS

CEO overview	2	APPENDIX A	12
1 OVERVIEW	4	Status of activities from the 2018–19 Business Plan	12
Our mission	4	APPENDIX B	15
2 OPERATIONAL ACTIVITIES	6	Financial report for the year ended 30 June 2019	15
Progress on strategic activities	6	APPENDIX C	39
Financial activity	7	BDO Annual Completion Report	39
Growth Centre members	8	APPENDIX D	61
Expenditure	8	AustCyber's subcontractors	61
Subcontractors	8	APPENDIX E	62
3 COMMUNICATION AND ENGAGEMENT	9	Communication and media	62
Media engagement	9		
Publications	10		
Public speaking engagements	10		

CEO OVERVIEW

The 2018–19 financial year saw AustCyber cement its position within the Australian cyber security ecosystem.

Grow

Establishing a National Network of Cyber Security Innovation Nodes continued to be a high priority for the organisation – with the aim of delivering a coordinated, national approach to commercialisation opportunities. In November 2018, the SA Node officially launched alongside the Adelaide JCSC and the NSW Node was announced. In early 2019, Node Managers were employed in the ACT and WA.

The 2018 Update to Australia's Cyber Security Sector Competitiveness Plan was delivered in September 2018, including a deep dive into the skills shortage in Australia; and a framework for the Australian Cyber Security Capability Map was developed and circulated with stakeholders ahead of publication.

Another successful Australian Cyber Week delivered follow-up engagement for several companies. Similar results were achieved during two AustCyber pitching events conducted during the year; and we supported the graduation of the second cohort of the CyRise cyber security accelerator through two Demo Days in Melbourne and Sydney.

We co-sponsored a 'State of Play' survey with METS Ignited, examining the cyber awareness and maturity of the global mining sector. This work delivered on elements of the Cyber Industry Roadmap released by AustCyber and CSIRO Futures in 2018.

The Minister for Industry, Science and Technology, the Hon Karen Andrews MP, announced the launch of the 2019 round of AustCyber's Projects Fund in June 2019. The Projects Fund was supported by a new and more robust guidance and governance framework.

Export

A MOU with the Australian British Chamber of Commerce was successfully executed. This MOU will facilitate greater market insights and connectivity between Australian cyber security companies and the United Kingdom through both domestic and international activities.

Austrade announced the eighth cohort for its Singapore Landing Pad in May 2019. Partnering with Austrade, we financially supported the cyber security companies participating in this initiative.

Educate

The CyberTaipan Pilot qualifying rounds were completed, and the ten top teams were invited to Canberra for a finals event in March 2019. AustCyber secured sponsorship from three corporate entities to support the delivery of this project.

We also submitted a final impact report on the delivery of the CyberTaipan Pilot, working with Northrup Grumman on options for national scaling of the program. This work was conducted alongside the Schools Cyber Security Challenges package being delivered by the Australian Computing Academy under an AustCyber Projects Fund grant.

AustCyber presented at the CyberSmart Summit 2019 in Canada with significant outcomes. The US National Institute for Science and Technology, which operates the National Initiative for Cybersecurity Education (NICE), formally invited AustCyber to lead Australian engagement in the 2020 update to the NICE Framework which will, for the first time, encompass international input.

We also led a workshop and delivered several presentations at the 2018 National Initiative for Cybersecurity Education (NICE) Conference and Expo, in the USA in November 2018.

We continued to be involved in the ICT Industry Reference Committee (ICT IRC) as part of PwC Skills for Australia's work in developing specific units of competency in cyber security across vocational education training packages in Australia.

Policy and advocacy

AustCyber engaged the Australian Strategic Policy Institute (ASPI) to survey industry views on the economic implications of the Assistance and Access Bill 2018 (AABill). We also accepted an invitation from the Department of Home Affairs to participate in its consultation forum to inform development of the industry guidelines that will underpin the legislation's implementation.

Operations

AustCyber's Canberra office was successfully relocated to Manuka in November 2018 and the Sydney office relocated to the Sydney JCSC. We focused on maturing our corporate tools and workflows as we scaled our operations with a larger team and more mature service offering.



Michelle Price
CEO of AustCyber

1 OVERVIEW

Our mission

The Australian Cyber Security Growth Network Ltd (trading as AustCyber) – the Cyber Security Growth Centre under the Australian Government’s Industry Growth Centres Initiative – supports the development of a vibrant and globally competitive Australian cyber security sector and in doing so, enhances Australia’s future economic growth in a digitally enabled global economy.

AustCyber was born out of the Australian Government’s 2015 Cyber Security Review (and later described as a national network of innovation nodes in the ‘Growth and Innovation’ chapter of Australia’s Cyber Security Strategy launched on 21 April 2016). The organisation was announced as part of the government’s National Innovation and Science Agenda, through an expansion of the Industry Growth Centres Initiative. Its Co-Chairs were announced in July 2016 and AustCyber commenced operations on 1 January 2017.

AustCyber is one of six industry-led, non profit Industry Growth Centres established in sectors of competitive strength and strategic priority to boost innovation and science in Australia and deliver sustained economic benefit.

AustCyber works to align and scale Australian cyber security research and innovation related activities in the private sector, research community and across Australian governments. Charged with building infrastructure to support the growth of a sector (supply of innovative Australian cyber security solutions and capability), the organisation works collaboratively across the Australian economy to support a range of other government initiatives related to Australia’s cyber security readiness and resilience (demand for solutions and capability).

Beyond our shores, AustCyber also works internationally with a range of partners to develop sustained export pathways for Australian solutions and capability. This further enables the rapidly growing Australian cyber security sector to tap into global hubs located within cyber security ‘hotspots’ around the world.

The domestic and international focuses in AustCyber’s programs support a more cohesive and vibrant Australian cyber security ecosystem.



In delivering its mission, AustCyber's programs, initiatives and deliverables are aligned to three strategic objectives, outlined in Australia's Cyber Security Sector Competitiveness Plan published by AustCyber:



1. Grow an Australian cyber security ecosystem



2. Export Australia's cyber security capabilities to the world



3. Make Australia the leading centre for cyber education.



Underpinning implementation of activities across AustCyber's program of activities are **five strategic themes**:

- Demonstrate leadership and coherence
- Drive industry collaboration and coordination
- Accelerate commercialisation
- Facilitate talent growth
- Pursue policy advocacy and reform

This Annual Report details outcomes of activities and business operations arising from AustCyber's programs and initiatives for 2019–20.



2 OPERATIONAL ACTIVITIES

Progress on strategic activities

AustCyber is delivering against its mission domestically and abroad, in partnership with industry, academia and governments.

We made significant progress towards our operational objectives during the 2018–19 financial year: working with industry to create new jobs, enhancing talent pipelines to meet future workforce demands, opening up new international markets, and making Australia a leading destination for cyber security investment.

AustCyber's international engagement for 2018–19 had a more matured focus to:

- solidify Australia's growing reputation as a capable, credible cyber security partner in the Asia-Pacific and a source of world-leading cyber security solutions among international enterprise customers, research partners, potential investors and allies;
- support Australian companies to develop more scalable business models for growth domestically and internationally; and
- work with government/s to deepen the understanding of export opportunities. Collaborating with partners including Austrade, the Department of Foreign Affairs and Trade, and the Australian British Chamber of Commerce, AustCyber delivered several international delegations in priority export markets: ASEAN, USA and UK. These delegations are critical in opening up export markets to Australian companies that are scaling and growing their operations.

Over 2018–19, AustCyber's National Network of Cyber Security Innovation Nodes has continued to grow and deliver exciting new initiatives and events. Most Nodes have a well-established Industry Advisory Group that has provided direction on the Nodes' workplans.

AustCyber is actively working with Tasmania to establish an Industry Advisory Group there, and recently the Tasmanian Government allocated an additional person to work on the Node. Work continues on establishing a Queensland Node and further engagement is underway to cement the Victorian Node.

Notable initiatives and events held include the Western Australian Node working with Horizon Power to deliver cyber security training in the remote Karratha region; the South Australian Node working with the University of Adelaide to take students to Cyber Security Research Bootcamp in Estonia.

Education and training underpins the Australian workforce. For cyber security, the worker demand is acute. AustCyber continues to work across the education and training sector to ensure the economy has access to a sustained pipeline of cyber security professionals with a range of strategic activities aimed to introduce and build cyber security capability in students from schools, Vocational Education and Training (VET) institutes and universities.

Examples of this over the course of 2018–19 include AustCyber delivering a pilot of the CyberTaipan cyber competition for high school aged students; and AustCyber's work with PwC Skills for Australia, which developed eight units of competency in cyber security for general use across all VET training packages.

Further sector growth will be realised through outcomes of AustCyber's first two rounds of the Projects Fund. Over the reporting period, AustCyber funded ten projects worth more than \$12 million of industry and matched AustCyber funding. Two projects have already been completed, with the remaining eight to be finalised in the 2019–20 financial year.

These successes only represent a small portion of AustCyber's programs, which also include complementing federal government initiatives such as the Joint Cyber Security Centres, the Cyber Security Cooperative Research Centre, the Academic Centres for Cyber Security Excellence and others.

A summary of AustCyber's progress on its strategic activities is at Appendix A.

Financial activity

As per the independently audited General Purpose Financial Report for the year ended 30 June 2019 (see Appendix B), AustCyber had a closing cash balance of \$8,908,580.

The auditor's completion report is at Appendix C.

Commonwealth funding

AustCyber received a total of \$10,650,000 (excluding GST) through its funding arrangements with the Department of Industry, Innovation and Science.

Funding source	Amount (ex GST)
Operating funds	\$3,500,000
Project funds	\$7,000,000
Industry Growth Network grant	\$180,000

AustCyber participant contributions

The organisation received \$450,000 in state and territory government contributions towards the national rollout and implementation of AustCyber's Network of Nodes.

Government	Contribution (ex GST)
New South Wales	\$50,000
Australian Capital Territory	\$200,000*
South Australia	\$50,000
Tasmania	\$100,000^
Western Australia	\$50,000

* Includes staffing costs for the Canberra Node Manager, employed by AustCyber under the agreement between the ACT Government and AustCyber.

^ Includes the previous year's contribution under the MoU between AustCyber and the Tasmanian government.

AustCyber's Projects Fund

In 2017–18, AustCyber announced ten projects to be funded under its Projects Fund, details of which can be found on the company website. The projects have a combined value of \$12,202,063 – with industry contributing \$6,131,778 and AustCyber allocating matched funding of \$6,070,285. During the 2018–19 financial year, AustCyber paid \$4,822,718.10 against agreed milestone deliverables.

Two projects were completed during the reporting period, with the remaining eight projects expected to be finalised in the first half of the 2019–20 financial year.



Growth Centre members

AustCyber did not have members during the 2018–19 financial year and therefore did not receive any associated contributions.

Expenditure

AustCyber's operating expenses for the period were \$4,017,208.

Subcontractors

AustCyber engaged the services of 42 subcontractors to support the delivery of its programs during the 2018–19 financial year. These services included, but were not limited to:

- Office accommodation
- Corporate travel administration
- Consultancy and research
- Legal services
- Graphic design and printing
- ICT related services

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

3 COMMUNICATION AND ENGAGEMENT

Media engagement

Social media

AustCyber has seen significant growth in audience engagement through its company Twitter handle, @AustCyber, which grew from 3,574 followers in July 2018, to 4,607 followers in June 2019. The company published 589 Tweets over the period which appeared more than one million number of times (impressions) in user timeline or search result. There were close to 18,000 engagements with the Tweets over the period.

AustCyber grew its LinkedIn followers from 809 in July 2019 to 4,515 in June 2019. The company published 260 posts over the period garnering more than 250,00 impressions with total engagements reaching close to 80,000.

'Friend of the network' list

AustCyber engages with the ecosystem through its, 'Friend of the network', newsletter and mailing list. AustCyber published 106 campaigns sent to 33,162 emails with an open rate of 40.5 per cent and an unsubscribe rate of only 0.3 per cent (84 unsubscribed users) over the reporting period.

Website

AustCyber matured its web presence with the launch its new website in November 2018. Over the financial year, the website had a total of 38,054 sessions, with an average duration of two minutes and 45 seconds.

The majority of users visiting the website were from Australia (50.4 per cent) and the United States of America (37.5 per cent), with the majority of users visiting the website directly (19,863 users) versus other means such as organic searchers (3,537 users) and social media referrals (1,337 users).

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

1. **Homepage** – 22,521 page views
2. **Sector Competitiveness Plan** – 3,892 page views
3. **Projects Fund** – 3,656 page views
4. **About us** – 3,364 pageviews
5. **Our team** – 3,153 page views

The company published 44 articles on the website over the period. The five most viewed articles were:

1. **AustCyber Sessions is launching on 7 February!** – 345 page views
2. **AustCyber's year in review by Michelle Price** – 320 page views
3. **AABill economic context** – Part 1: key perceptions about the economic implications of the legislation – 277 page views
4. **AustCyber's year ahead by Michelle Price** – 243 page views
5. **Projects Fund Round 1 recipients** – 213 page views.

News media

AustCyber was referenced in Australian and global online news media through 342 unique articles that had a potential reach of almost 450 million people. The ten outlets which published the most articles referencing AustCyber were:

No. of articles referencing AustCyber:	
CSO	20
ITWire	14
InnovationAus	13
Computerworld Australia	10
ZDNet	9
Australian Cyber Security Magazine	9
Lexisnexis Online News (print edition)	8
ACS Information Age	8
The Australian	7
Technology Decisions	7

The top ten English-language articles referencing AustCyber which had the greatest reach are listed in Table 1 at Appendix E.

Of the top 20 articles, four articles were rated as having a positive sentiment, and 16 having neutral sentiment. AustCyber was not featured negatively in any of the articles.

AustCyber executives were interviewed for 15 podcasts and 20 radio segments. Podcasts included interviews that resulted out of a partnership agreement with MySecurityMedia and can be streamed and downloaded from the AustCyberⁱ and MySecurityMediaⁱⁱ websites.

Publications

AustCyber launched the 2018 update to Australia's Cyber Security Sector Competitiveness Plan (SCP)ⁱⁱⁱ in November 2018. The Plan indicates strong growth against the data outlined in the first iteration, released in April 2017, reflecting the rapid evolution of this dynamic sector. The Plan draws on extensive industry consultation and research to provide a fresh picture of the global outlook, challenges, and opportunities and priority actions needed to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth. It also provides a deep dive into the skills and workforce gap, which is one of the key issues impacting the sector's growth.

The SCP is the premier source of information and data on Australia's cyber security ecosystem and the opportunities and challenges to its growth. Over the period the SCP has been referenced 80 times in unique articles published by global new media (not including syndicated publications) and is referenced at least once on a daily basis.

Released alongside the 2018 update to the SCP, the Australian Cyber Security Industry Roadmap^{iv}, brings together the expertise and networks of CSIRO Futures and AustCyber to identify a common vision and map out the road to success in the cyber security sector. World-class scientific and technological expertise is applied to steer business, government and society through the challenges we must navigate over the medium to long term, to seize opportunities across all Australian growth industries.

Public speaking engagements

The AustCyber executive took part in 43 speaking engagements at various forums throughout the year, which are detailed at Appendix E.

i AustCyber podcasts: <https://www.austcyber.com/news-events/podcasts>

ii Cyber Security Weekly Podcast: <https://blubrry.com/mysecurity/archive/>

iii 2018 Update to Australia's Cyber Security Sector Competitiveness Plan: <https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2018>

iv Australian Cyber Security Industry Roadmap: <https://www.austcyber.com/resources/industryroadmap>



APPENDIX **A**

Status of activities from the 2018–19 Business Plan

■ Completed ■ Work underway ■ Deferred or overtaken by events

Cyber security sector strategic outlook

Objective: Deliver a Cyber Security Sector Competitiveness Plan (SCP) and publish updates as required (at least annually), including an assessment of progress on delivery of the Plan's recommended actions assigned to AustCyber, and implement a Cyber Security Industry Roadmap (Roadmap) in partnership with CSIRO.

Key performance indicator	Status	Comments
The delivery of a second update to the SCP before end of June 2019.	Completed	An update to the SCP was delivered in September 2018, including a deep dive into the skills shortage in Australia.
Key stakeholders in growth sectors demonstrate an understanding of the economic development implications of a cyber resilient economy, as described in the SCP and Roadmap.	Completed	Ongoing engagement from AustCyber and the Node Network has revealed a maturing understanding among key stakeholders across other growth sectors, especially resources and advanced manufacturing.
Tracked data is available to demonstrate stakeholder engagement with AustCyber's communication on the SCP and Roadmap.	Work underway	AustCyber has made significant progress in developing these metrics, including implementing a CRM and engaging a consultancy.
Evidence of successful engagement with other responsible parties to the SCP's actions and can report on their implementation progress.	Work underway	AustCyber has made significant progress in developing these metrics, including implementing a CRM and engaging a consultancy.

Australian cyber security capability map

Objective: Map the capabilities of the Australian cyber security ecosystem and associated programs to provide a global resource for investment, trade, research and innovation activities.

Key performance indicator	Status	Comments
A categorisation of capability types is agreed and repeatable.		A framework has been developed and is now being circulated with stakeholders ahead of publication.
Release of a beta form of an online capability map through AustCyber's website.		A concept has been developed by AustCyber. Release is dependent on funding availability. Current status is the development of a position paper to seek funding from DIIS and Austrade.
A clear picture of what and where Australian cyber security capability exists.		Refer above.

Australian Cyber Week

Objective: Deliver Australian Cyber Week 2018, ensuring it is complementary to other key Australian cyber security events such as the ACSC Conference, AISA Conference and AusCERT Conference.

Key performance indicator	Status	Comments
Pitching companies at Sky's the Limit achieve follow up engagement with potential customers.		There was follow up engagement with some companies.
Pitching employers at the jobs speed dating event are successful in attracting and employing skilled students.		AustCyber delivered several events with Ribit. A follow-up survey showed that skilled students were attracted to the event and some were employed as a result.

Measuring ecosystem growth

Objective: Address gaps and inconsistencies in the Australian cyber security sector's approach to measuring its ecosystem growth and the impact of this growth on the broader Australian economy.

Key performance indicator	Status	Comments
Clear understanding of repeatable growth metrics common to other technology-based industries and gaps in available metrics unique to cyber security.		AustCyber engaged AlphaBeta to complete a body of work that achieved all these KPIs. The outcomes will be released through the 2019 update to the SCP.
A roadmap for developing missing metrics.		
A draft framework of growth measurement.		
A roadmap for undertaking a national measurement of ecosystem growth, applying the draft framework.		

National Network of Cyber Security Innovation Nodes

Objective: Establish and mature a national National Network of Nodes which brings together cyber security research and innovation activities into co-located facilities to foster collaboration, information sharing and commercialisation pathways.

Key performance indicator	Status	Comments
Node capability strengths/clusters are being leveraged by stakeholders to derive greater impact in how problems are solved.		Each Node is working to purposefully different, but complementary, priorities. For example, the WA Node is working extensively with securing infrastructure in the resources sector; the VIC Node designate is working on security in Internet of Things and Operational Technologies with application for the resources sector; the SA Node is focused on operational cyber security in the defence and space industries; and the Canberra Node is focused on the policy and research aspects of cyber security in the defence and space industries.
A coordinated, national approach to commercialisation opportunities.		Through Node Manager strategy meetings and nationally consistent communication tools, the Nodes are aligned in their approach to commercialisation opportunities.

National incubation, acceleration and export infrastructure

Objective: Build national infrastructure that supports cyber security sectoral capability development, from ideation and research and development through to incubation, acceleration and export.

Key performance indicator	Status	Comments
The model is developed, benchmarked against international best practice and supported by key stakeholders.		Mapping is currently being conducted to understand the existing infrastructure. A model will be developed as the next step.
MoUs and/or contracts are signed with strategic partners.		MOUs have been signed with CyRise, Austrade and the ABCC. Other MOUs identified and in development with Australia Indonesia Business Council and the Australia Singapore Business Chamber.
Non cyber incubators, accelerators and venture funds domestically and internationally are proactively engaging with the model and pilot.		Mapping is currently being conducted to understand the major contributors to this ecosystem, to determine how they might engage.
Attendance and deal flow at community building events meet targets.		AustCyber is not positioned to deliver against this KPI and is in discussions with its partners on how to measure this activity. Any outcomes will be reflected as part of work on the Node Network.
Gaps in the Australian technology transfer process are identified and possible solutions developed.		AustCyber is leveraging the process within its Projects Fund and its developing relationship with the Cyber Security CRC to better assess effective ways to address this KPI.
The AustCyber Angels Network is operational and has participation.		AustCyber has postponed delivery of this initiative until other elements of the infrastructure are more mature.
A roadmap for national rollout of the infrastructure is delivered off the back of a successful entrepreneurs bootcamp.		AustCyber has supported CyRise to conduct bootcamps across Australia in a more independent fashion.

APPENDIX **B**

Financial report for the year ended 30 June 2019

**AUSTRALIAN CYBER SECURITY
GROWTH NETWORK LIMITED**

ABN 73 616 231 451



Director's Report

The directors present this report on the company for the financial year ended 30 June 2019.

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
- Mr Michael Paul Burgess
- Ms Heather May Ridout AO

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) 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.

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.

- **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 Adviser 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 channels, which accounted for worldwide sales of all IBM products and services of some \$95 billion.

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 organization 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 11th 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 Turner is the CEO of Data61 at CSIRO. Data61 is creating our data-driven future.

Adrian is a successful and influential Australian technology entrepreneur who has spent 18 years in Silicon Valley. Most recently he was Managing Director and Co-Founder of Borondi Group, a holding company focused on the intersection of pervasive computing, platform economics and traditionally conservative industries. Prior to this, Adrian was co-founder and CEO of smart phone and Internet of Things security company 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. Mocana was named a Technology Pioneer by the World Economic Forum in 2012, one of 11 global IT companies selected from over 800 global nominations. Adrian was recently named co-Chair of the Cyber Security Growth Centre, is a member of the Board of the Australian eHealth Research Centre and is also a member of the UTS: Business School Advisory Board.

He is regarded as a thought leader on entrepreneurialism, Internet of Things security and the impact of network connectivity on business economics. He authored the eBook BlueSky Mining – Building Australia's Next Billion Dollar Industries. Adrian is a UTS graduate and has completed the Executive Programme for Managing Growth Companies at Stanford University.

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 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

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 2019 the measures related to the company delivering: quarterly financial reports, a 2018-19 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, 4 meetings of directors were held (25 October 2018, 31 January 2019, 5 April 2019, 20 June 2019). Attendances by each director were as follows:

Directors' Meetings		
	Number eligible to attend	Number attended
Ms Michelle Clare Price	4	4
Mr Douglas Thorne Elix	4	4
Mr Adrian John Turner	4	4
Mr Michael Paul Burgess	4	2
Ms Heather May Ridout	4	3

The company is incorporated under the *Corporations Act 2001* and is a company limited by guarantee.

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.

Auditor's independence declaration

A copy of the auditor's independence declaration as required under Section 307C of the *Corporations Act 2001* is set out on page 8.

Signed in accordance with a resolution of the directors.



Director

Sydney, 11 October 2019

Auditors Independence Declaration



Tel: +61 2 9251 4100
Fax: +61 2 9240 9821
www.bdo.com.au

Level 11, 1 Margaret St
Sydney NSW 2000
Australia

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

As lead auditor of Australian Cyber Growth Network Ltd for the year ended 30 June 2019, 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.

A handwritten signature in black ink, appearing to read 'Gillian Shea', with a long, horizontal flourish extending to the right.

Gillian Shea
Partner

BDO East Coast Partnership

Sydney, 11 October 2019

Statement of Profit or Loss and Other Comprehensive Income

FOR THE YEAR ENDED 30 JUNE 2019

	Note	2019 \$	2018 \$
Revenue	2	8,791,162	4,473,769
Other income	2	23,464	40,358
Employee benefits expense		(1,823,518)	(1,554,484)
Depreciation and amortisation expense	3	(8,129)	(3,131)
Advertising and marketing expense		(779,041)	(277,595)
Professional and consultancy expense		(346,741)	(539,118)
Rent expense		(201,362)	(270,333)
Subscriptions, reference and licences expense		(73,735)	(169,846)
Travel expense		(367,777)	(587,738)
Grant and project funding expense		(4,797,418)	(506,279)
Recruitment expense		(29,835)	(24,892)
Conference expense		(22,038)	(174,155)
Research expense		-	(122,394)
Training expense		(36,843)	(37,500)
Other expenses		(328,189)	(246,662)
Surplus before income tax		-	-
Income tax expense		-	-
Surplus for the year		-	-
Total comprehensive income for the year		-	-
Surplus attributable to members of the entity		-	-
Total comprehensive income attributable to members of the entity		-	-

The accompanying notes form part of these financial statements.

Statement of Financial Position

AS AT 30 JUNE 2019

	Note	2019 \$	2018 \$
ASSETS			
CURRENT ASSETS			
Cash and cash equivalents	5	8,098,580	5,206,240
Trade and other receivables		9,733	10,977
Other current assets	6	187,570	29,646
TOTAL CURRENT ASSETS		8,295,883	5,246,863
NON-CURRENT ASSETS			
Property, plant and equipment	7	31,737	17,828
TOTAL NON-CURRENT ASSETS		31,737	17,828
TOTAL ASSETS		8,327,620	5,264,691
LIABILITIES			
CURRENT LIABILITIES			
Trade and other payables	8	624,766	76,089
Deferred Revenue		7,615,591	5,144,204
Employee benefits provision		87,263	44,398
TOTAL CURRENT LIABILITIES		8,327,620	5,264,691
TOTAL LIABILITIES		8,327,620	5,264,691
NET ASSETS		-	-
EQUITY			
Retained surplus		-	-
TOTAL EQUITY		-	-

The accompanying notes form part of these financial statements.

Statement of Changes in Equity

FOR THE YEAR ENDED 30 JUNE 2019

	Note	Retained Surplus \$	Total \$
Balance at 01 July 2017			
Surplus for the period		-	-
Other comprehensive income		-	-
Total comprehensive income attributable to members of the entity for the year		-	-
Balance at 30 June 2018		-	-
Balance at 01 July 2018		-	-
Surplus for the year		-	-
Other comprehensive income			
Total comprehensive income attributable to members of the entity for the year		-	-
Balance at 30 June 2019		-	-

The accompanying notes form part of these financial statements.

Statement of Cash Flow

FOR THE YEAR ENDED 30 JUNE 2019

	Note	2019 \$	2018 \$
CASH FLOWS FROM OPERATING ACTIVITIES			
Receipt of grants		14,851,474	6,961,750
Receipts from customers		132,550	-
Payments to suppliers and employees		(12,093,110)	(4,710,843)
Interest received		8,757	23,033
Other income		14,707	17,325
		<hr/>	<hr/>
Net cash generated from operating activities		2,914,378	2,291,265
		<hr/>	<hr/>
CASH FLOWS FROM INVESTING ACTIVITIES			
Payment for property, plant and equipment		(22,038)	(15,992)
		<hr/>	<hr/>
Net cash used in investing activities		(22,038)	(15,992)
		<hr/>	<hr/>
Net increase in cash held		2,892,340	2,275,273
		<hr/>	<hr/>
Cash and cash equivalents at start of financial period		5,206,240	2,930,967
		<hr/>	<hr/>
Cash and cash equivalents at end of financial year	5	8,098,580	5,206,240
		<hr/>	<hr/>

The accompanying notes form part of these financial statements.

Notes to the Financial Statements

FOR THE YEAR ENDED 30 JUNE 2019

NOTE 1: SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

Basis of Preparation

Australian Cyber Security Growth Network Limited is a not-for-profit company limited by guarantee, incorporated and domiciled in Australia.

The financial statements are general purpose financial statements that have been prepared in accordance with 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 11 October 2019.

Significant Accounting Policies

New or 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.

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

The following Accounting Standards and Interpretations are most relevant to the company:

AASB 9 Financial Instruments

The Company has adopted AASB 9 from 1 July 2018. The Company has receivables at year end and under the standard there are new impairment requirements which use an 'expected credit loss' ('ECL') model to recognise an allowance. Impairment is measured using a 12-month ECL method unless the credit risk on a financial asset has increased significantly since initial recognition in which case the lifetime ECL method is adopted. For receivables, a simplified approach to measuring expected credit losses using a lifetime expected loss allowance is available and has been used..

NOTE 1: SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTINUED)

Impact of adoption

The adoption of new Accounting Standards and Interpretations did not have an impact on the financial performance or position of the Company as at 30 June 2019 or on opening retained earnings as at 1 July 2018.

a. Revenue

Revenue comprises revenue from the government grants and other income. Revenue from major products and services is shown in Note 2.

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. Where a grant may be required to be repaid if certain conditions are not satisfied, 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.

Interest income

Interest income is recognised on an accrual basis using the effective interest method. Dividend income are recognised at the time the right to receive payment is established.

All revenue is stated net of the amount of goods and services tax.

NOTE 1: SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTINUED)

Plant and other 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.

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.

c. **Impairment of Assets**

At the end of each reporting year, the entity assesses whether there is any indication that an asset may be impaired. If such an indication exists, an impairment test is carried out on the asset by comparing the recoverable amount of the asset, being the higher of the asset's fair value less costs of disposal and value in use, to the asset's carrying amount. Any excess of the asset's carrying amount over its recoverable amount is recognised immediately in profit or loss.

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.

d. **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.

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

NOTE 1: SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTINUED)

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.

e. Cash and Cash Equivalents

Cash and cash equivalents include cash on hand, deposits held at call with banks, other short-term highly liquid investments with original maturities of three months or less.

f. 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.

g. Provisions

Provisions are recognised when the entity 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.

h. Comparative Figures

When required by Accounting Standards, comparative figures have been adjusted to conform changes in presentation for the current financial year.

When the company applies an accounting policy retrospectively, makes a retrospective restatement or reclassifies items in its financial statements, a statement of financial position as at the beginning of the earliest comparative year will be presented.

i. 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.

NOTE 1: SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTINUED)

j. **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.

k. **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.

l. **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.

NOTE 1: SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES (CONTINUED)

Fair Value of Assets and Liabilities (continued)

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.

m. Trade and other receivables

Other receivables are recognised at amortised cost, less any allowance for expected credit losses

New Accounting Standards and Interpretations not yet mandatory or early adopted

Australian Accounting Standards and Interpretations that have recently been issued or amended but are not yet mandatory, have not been early adopted by the company for the annual reporting period ended 30 June 2019. Currently the Company is in process of evaluating the impact of AASB 15 Revenue with the Customers, AASB 1058 Income of Non-for Profit entities and AASB 16 Leases

NOTE 2: REVENUE AND OTHER INCOME

	2019	2018
	\$	\$
Revenue		
Revenue from (non-reciprocal) government grants and other grants:		
Grants received from:		
– state/federal government grants	3,680,000	3,777,273
– project funding - dept	7,000,000	3,000,000
– state government contribution	450,000	195,455
– grants deferred	(2,471,388)	(2,498,959)
Grants revenue recognised	8,658,612	4,473,769
Sponsorship Income		
– corporate sponsorship	127,459	-
Other revenue:		
– interest received on financial assets not at fair value through profit or loss	8,757	2,853
– challenge registrations	5,091	-
– other income	14,707	17,325
	28,555	40,358
Total revenue	8,814,626	4,514,127

NOTE 3: PROFIT FOR THE YEAR

a. Expenses		
Employee benefits expense:		
– provision for annual leave	42,864	25,711
– contributions to defined contribution superannuation funds	140,733	130,004
Depreciation and amortisation:		
– computer and equipment	8,129	3,131
Lease Payments:		
– Rent Expenses	201,362	270,333

NOTE 4: AUDITOR'S REMUNERATION

Audit fees	15,000	15,000
------------	--------	--------

AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED

ABN 73 616 231 451

FINANCIAL REPORT FOR THE YEAR ENDED 30 JUNE 2019

FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2019

	2019	2018
	\$	\$
NOTE 5: CASH AND CASH EQUIVALENTS		
CURRENT		
Cash at bank	8,908,580	5,206,240
	<u>8,908,580</u>	<u>5,206,240</u>

NOTE 6: OTHER ASSETS

CURRENT		
Prepayments	20,659	-
Deposits & Bonds	41,258	29,325
Other assets	125,653	321
	<u>187,570</u>	<u>29,646</u>

NOTE 7: PROPERTY, PLANT AND EQUIPMENT

Plant and Equipment

Computer equipment:

At cost	29,367	21,479
Less accumulated depreciation	(9,619)	(3,651)
	<u>19,748</u>	<u>17,828</u>

Office furniture & equipment:

At cost	14,150	-
Less accumulated depreciation	(2,161)	-
	<u>11,989</u>	<u>-</u>

Movements in Carrying Amounts

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

FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2019

	Computer Equipment	Office furniture & equipment	Total
	\$	\$	\$
2018			
Balance at the beginning of the period	4,967	-	4,967
Additions at cost	15,992	-	15,992
Immediate write-off	-	-	-
Depreciation expense	(3,131)	-	(3,131)
Carrying amount at the end of the period	17,828	-	17,828
2019			
Balance at the beginning of the year	17,828	-	17,828
Additions at cost	7,888	14,150	22,038
Immediate write-off	-	-	-
Depreciation expense	(5,968)	(2,161)	(8,129)
Carrying amount at the end of the year	19,748	11,989	31,737

NOTE 8: TRADE AND OTHER PAYABLES

	2019	2018
	\$	\$
CURRENT		
Trade payables	511,673	45,052
Accrued expenses	44,852	15,000
Other payables	68,241	16,037
	<u>624,766</u>	<u>76,089</u>

NOTE 9: COMMITMENTS

Operating lease

Within one year	47,730	40,528
One year or later and no later than five years	16,457	-

<u>64,277</u>	<u>40,528</u>
---------------	---------------

NOTE 10: CONTINGENT LIABILITIES

The company had no contingent liabilities as at 30 June 2019 and 30 June 2018.

FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2019

NOTE 10: EVENTS AFTER THE REPORTING YEAR

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

NOTE 11: KEY MANAGEMENT PERSONNEL COMPENSATION

Any person(s) having authority and responsibility for planning, directing and controlling the activities of the entity, directly or indirectly, including any director (whether executive or otherwise) of that entity is considered key management personnel (KMP).

The totals of remuneration paid to KMP of the company during the year are as follows:

KMP compensation – short term benefits	384,445	787,434
--	---------	---------

NOTE 12: RELATED PARTY TRANSACTIONS

Key management personnel

Disclosures relating to key management personnel are set out in note 11.

Transactions with related parties

There were no transactions with related parties during the current and previous financial year.

Receivable from and payable to related parties

There were no trade receivables from or trade payables to related parties at the current and previous reporting date.

Loans to/from related parties

There were no loans to or from related parties at the current and previous reporting date.

Director's Declaration

In accordance with a resolution of the directors of Australian Cyber Security Growth Network Limited the directors of the company declare that:

1. The financial statements and notes, as set out on pages 10 to 23, 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 2019 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.



(Chair)

Dated this 11 day of October 2019

Independent Audit Report



Tel: +61 2 9251 4100
Fax: +61 2 9240 9821
www.bdo.com.au

Level 11, 1 Margaret St
Sydney NSW 2000
Australia

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 2019, the statement of profit or loss and other comprehensive income, the statement of changes in equity and the statement of cash flows for the period 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* (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.

BDO East Coast Partnership ABN 83 236 985 726 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 East Coast Partnership 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.

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

This description forms part of our auditor's report.

BDO East Coast Partnership

BDO



Gillian Shea
Partner

Sydney, 11 October 2019

APPENDIX **C**

BDO Annual Completion Report



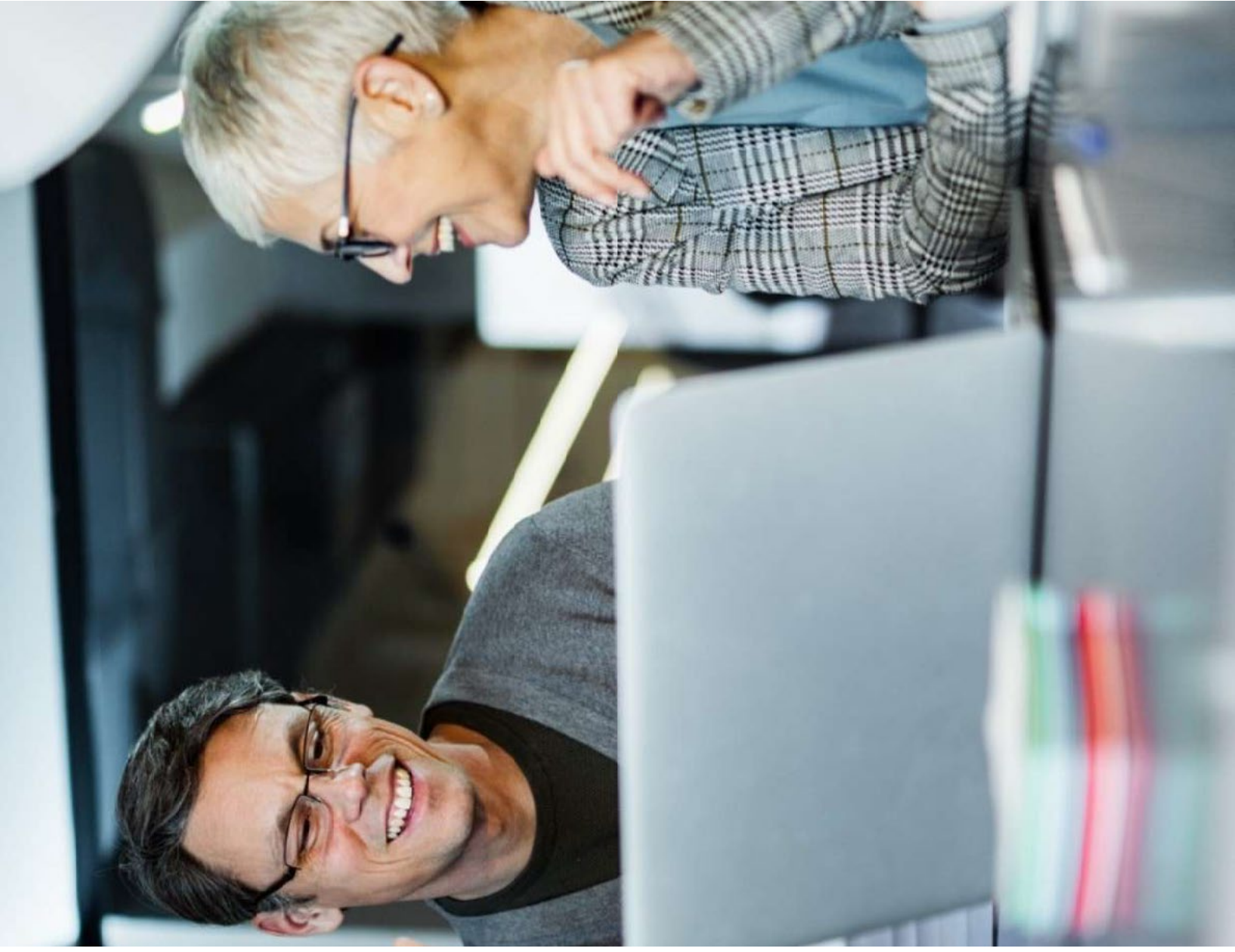


AUSTRALIAN CYBER SECURITY GROWTH NETWORK LIMITED

Annual completion report

CONTENTS

Executive Summary	4
Areas of audit focus	5
areas of audit focus	6
Internal control	9
Other reporting requirements	14
Appendix 1 Proposed audit report	15
Appendix 2 Auditor independence declaration	17
Appendix 3 New developments	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 2019 annual audit.

As at the date of this report, we have substantially completed our audit and subject to the satisfactory resolution of the matters detailed 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 11 October 2019 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 666.

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 2019.

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:

- ▶ Signing of the management representation letter (BDO to provide);
- ▶ Approval and signing of the annual financial report;
- ▶ Review of subsequent events up to the date of signing.

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 2019.

AREAS OF AUDIT FOCUS

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

- ▶ Management Override of Controls
- ▶ Revenue Recognition

Refer to the next [section](#) of this report for further details on the significant risk areas and other areas focused on during the audit.



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.

We set out below the areas that were considered significant risks of material misstatement along with an outline of the work performed and a summary of findings.

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

Revenue Recognition for not-for-Profits		
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">• The entity will comply with the conditions attaching to them; and• The grants will be received.	<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">• Reviewed revenue recognition policies and ensure compliance with Australian Accounting Standards;• Tested a sample of grant revenue and expense transactions throughout the year, and vouched to relevant supporting documentation; and• Reviewed deferred revenue as at 30 June 2019 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.	<ul style="list-style-type: none">• No material exceptions were observed from the audit procedures performed. We consider that revenue recognised for the year has not been materially misstated. We consider it reasonable that deferred revenue has been recognised on the unspent portion of grant funding received.



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 **\$7,900**. 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
1. Being accrual of the salaries and wages for last 10 days in June 2019, paid subsequently	-	(64,454)	-	64,454
Net effect of uncorrected misstatements	-	(64,454)	-	64,454



SUMMARY OF MISSTATEMENTS

CORRECTED MISSTATEMENTS

There are no corrected misstatements for the period ended 30 June 2019



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.

The matters being reported are limited to those deficiencies that we have identified during the course of our audit and that we have concluded are of sufficient importance to merit being reported to the Directors.

CURRENT PERIOD

Significant deficiency in internal control	Potential effects	Recommendation	Management comments
1 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.	Inadequate review of payments. It is recommended that Bank accounts should have at least two authorised signatories.	Authorised signatory listings should be updated on a timely basis, with the responsibility assigned to more than one existing employee.	Management is aware that it is not the best practise to have only one assigned signatory. It has been the intention to add another signatory when a new COO is recruited. There is a gap between when Belinda left the company and when the COO comes on board, expected to be in November.

INTERNAL CONTROL CONTINUED



Other deficiencies in internal control		Potential effects	Recommendation	Management comments
1	Audit Trail for Closed Accounts Bank statements could not be obtained for accounts that were active as of 30 June 2019 but closed post year end.	Cash at bank balances may be inaccurate or incomplete if not matched to Bank statements at year end.	Bank statements should be obtained and maintained for all accounts held at year end.	These accounts were AustCyber's ANZ Bank accounts, which was a self-identified matter prior to the audit commencing. AustCyber appreciates the circumstances of the actual closure were such that statements were not obtained. AustCyber is working with one of its Directors who was the remaining signatory on these accounts to release the statements needed.
2	Review of cut-off for accruals There was no review of the cut-off for payroll-related accruals (FBT payable and salaries and wages payable) relating to June 2019.	Accruals may be misstated at year end.	A review of the cut-off of all accruals should be undertaken at year end to ensure expenses have been recorded in the correct period.	AustCyber relies on Enspira (Bookkeeper) to undertake FBT and Payroll functions as part of the service agreement with them. This error has been oversighted. In future management will ensure that all cut off process has been followed properly by bookkeeper's team and sign off by AustCyber management. .

INTERNAL CONTROL CONTINUED

Other deficiencies in internal control	Potential effects	Recommendation	Management comments
3 No reconciliation is undertaken of GST on supplier invoices BDO noted two invoices on which GST had not been correctly accounted for.	There is a risk that expenses are not recorded correctly and the incorrect GST amount is recorded on the BAS.	We recommend a reconciliation of the GST payable is undertaken to ensure GST and expense amounts have been accurately recorded.	These two matters are a combination of human error. AustCyber will ensure its staff are reminded about correct processing of invoices received. This has been further incorporated into the agreement with Enspira.

INTERNAL CONTROL CONTINUED

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	Management comments
1 <u>Board minutes</u> Upon review of the board minutes it appears there is no evidence documented that the management accounts have been reviewed.	2018	Noted that the review of quarterly Management accounts was included in the Board Meeting minutes.	Agree notes against current status
2 <u>Grant income</u> Grant receivable in the year has been recorded within different bank accounts in the year.	2018	Noted that grants as per the main funding agreement were received through the NAB Main Account. Separate accounts have been opened in the current year for project funds and for state contributions relating to their respective Nodes.	Bank accounts are now in place for the Projects Fund and Nodes. All grant funding comes to AustCyber's day to day account, the Projects Fund funding is then transferred to the Projects Fund account. AustCyber provides the Node bank account details on its invoices to States and Territories for direct payment into those accounts.

INTERNAL CONTROL CONTINUED

Description of matter	Date previously communicated	Current status	Management comments
3 <u>Travel Expenses</u> Travel expenses have increased significantly during the year. Travel is mainly completed by Michelle, who also approves the expenditure, therefore there is a lack of segregation of duty for travel expenditure.	2018	The CEO still approves expenditures. It has however been noted that travel expenditures has decreased significantly in the current year and relates to multiple employees.	Travel has decreased for the current year. The CEO does still approve expenditure for travel, however as in 2018, all expenditures are approved in a two-step process



OTHER REPORTING REQUIREMENTS

INDEPENDENCE AND ETHICS

In conducting our audit, we have complied with the independence requirements of the *Corporations Act 2001* and s290 of APES 110 *Code of Ethics for Professional Accountants*.

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.

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 Limited

Report on the Audit of the Financial Report

Opinion

We have audited the financial report of Australian Cyber Security Growth Network Limited (the Company), which comprises the statement of financial position as at 30 June 2019, the statement of profit or loss and other comprehensive income, the statement of changes in equity and the statement of cash flows for the period 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 Limited, 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 (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 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.

APPENDIX 1 PROPOSED AUDIT REPORT CONTINUED

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

This description forms part of our auditor's report.

BDO East Coast Partnership

Gillian Shea

Partner

Sydney, 11 October 2019.

APPENDIX 2 AUDITOR INDEPENDENCE 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 2019, 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 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 16

The new leases standard, AASB 16 Leases is effective for annual periods beginning on or after 1 January 2019 and early adoption is permitted.

This new leases standard, which mainly impacts lessees, will therefore apply for the first time to your 30 June 2019 -year end and supersedes existing standard, AASB 117 Leases, as well as related Interpretations.

The core principle of AASB 16 is that all assets and liabilities arising under lease contracts are recognised in the statement of financial position as right-of-use assets, with a corresponding lease liability, and an annual expense reflecting depreciation on the leased asset and interest expense, which will vary from period to period, depending on the outstanding balance of the lease liability (i.e. front-end loaded expense).

Exceptions

There are optional exceptions for short-term leases (i.e. where lease term is for a period of less than 12 months, including extension options), and low value leases (i.e. where the value, as new, is less than approximately US \$5,000).

Main implications

- ▶ There is no longer a distinction made between ‘operating’ and ‘finance’ leases, and no more straight-line expense for operating leases
- ▶ Non-cancellable lease payments are included when measuring the right-of-use asset, as well as payments for option periods which the entity is reasonably certain to exercise
- ▶ Contingent rentals (e.g. those linked to sales) are not capitalised into the right-of-use asset but are expensed in profit or loss when incurred.

For more information, please refer to BDO’s [Need to know](#) and Accounting News [article](#), as well as to the ‘Leasing’ section of our [Issues and Trends](#) page.

Please contact Gillian Shea to discuss any specific implementation issues.

A photograph of a man and a woman smiling and looking towards the right. The man is in the foreground, wearing a blue checkered shirt, and the woman is slightly behind him, wearing a white top. They appear to be in a professional setting.

APPENDIX 3 NEW DEVELOPMENTS CONTINUED

AASB 15 AND AASB 1058

The new revenue standards AASB 15 revenue from contracts with customers and AASB 1058 Income of Not-for-Profit Entities, apply to annual reporting periods ending on or after 1 January 2019 and will supersede all current income recognition requirements for private sector NFPs, and most of the requirements for public sector NFPs currently contained in AASB 1004 *Contributions*

Income currently recognised as non-reciprocal contributions under AASB 1004 Contributions could instead result in revenue being recognised under AASB 1058. The objective of this standard is to establish principles for recognising income:

- On transactions where the consideration to acquire an asset is significantly less than fair value principally to enable a NFP to further its objectives, and
- For the receipt of volunteer services.

This means that AASB 1058 does not deal with situations where either consideration is not significantly less than fair value, or it is significantly less than fair value but the difference is not principally to enable the NFP to further its objectives.

In addition to grants, donations and contributions, many NFPs run business enterprises to supplement income, or as part of providing goods or services to clients in need. These are likely to comprise revenue from contracts with customers and therefore the new '5 step model' in AASB 15 must be applied. Depending on the circumstances, this could result in revenue being recognised either earlier or later, and could also result in a change to the quantum of revenue recognised.

Each 'income stream' needs to be evaluated on a contract-by-contract basis whether AASB 1058 or AASB 15 applies.

Please contact Gillian Shea to discuss any specific implementation issues

APPENDIX 3 NEW DEVELOPMENTS CONTINUED

WHISTLEBLOWING

As of 1 July 2019 Whistleblowing legislation has changed in Australia. Not only has the law been harmonised between the states but it has been augmented to provide greater protections for whistle-blowers.

Main implications:

- Expanded whistle-blower protections regarding all Australian companies and gives public and large proprietary Australian companies until 1 January 2020 to introduce a whistle-blower policy that is compliant with the new law, or else companies may face fines of up to \$12,600
- Increased penalties for breaches of whistle-blower protections, reaching up to \$10.5million
- Victimisation and compensation provisions apply to protected disclosures made at any time
- Disclosures may now be made anonymously
- Whistle-blower protection now expands to employees (current and former), officers, suppliers and their employees, an individual who is an associate of the entity, and family members of any of these eligible people.

PRIVACY, DATA PROTECTION AND CYBER SECURITY

The Australian Federal Government has announced a number of important amendments to the Privacy Act to be legislated later in 2019 which will significantly increase the potential penalties for serious or repeated breaches for all entities covered by the Act. The proposed changes follow in wake of the EU's introduction of the General Data Protection Regulation (GDPR) which became law in May 2018.

1300 138 991
www.bdo.com.au

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

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

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 East Coast Partnership ABN 83 236 985 726 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 East Coast Partnership 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

APPENDIX **D**

AustCyber's subcontractors

Supplier/contractor	Purpose/description of services
AlphaBeta	Consultancy and research services
Amazon Web Services	Cloud computing service for corporate website
Ambius Agreement	ACT office amenities
Australian Strategic Policy Institute	Consultancy and research services
Atlassian	Software services
Brittany Fong	Specialist software services
contentgroup	Communication and media services
Corporate Traveller	Corporate travel manager
Datacom	Software services
Effective People	Recruitment services
ERP IT Canberra	ICT consultancy
ForwardIT	ICT managed services
Google	Software productivity and collaboration tools
Impress Design	Graphic design and web hosting services
Kasada	Website and online presence security
LJ Hooker Commercial Canberra	ACT office lease
Mailguard	Email security services
Meltwater	Media monitoring platform
Microsoft Office Business	Software productivity and collaboration tools
Myer Vandenberg Lawyers	Legal services
New Generation Cleaning	ACT office cleaning
Nimble	Software CRM and collaboration tools
Regus Sydney	NSW office lease
Robert Holtsbaum Commercial Lawyer	Legal services
Servcorp Canberra	ACT office lease
ThinkPlace	Consultancy and research services
TPG	ICT services
Xero	Accounting tool

APPENDIX **E**

Communication and media

Top ten articles mentioning AustCyber

Title	Date of publication	Source	Average reach
How Australia could lose its next war without firing a shot	28 June 2019	Daily Mail	55 M
Did Australia poke a hole in your phone's security?	23 January 2019	The Indian Express	34 M
Australia is using AI to 'catch up' rather than to get ahead: Deloitte	7 May 2019	ZDNet	11 M
ACSC dumps annual conference, partners with AISA for cyber events	29 January 2019	ZDNet	11 M
Explosion in digital evidence coming thanks to IoT and 5G: Hancom GMD	2 January 2019	ZDNet	11 M
RMIT partners with NAB and Palo Alto Networks for new cybersecurity course	16 April 2019	ZDNet	11 M
Australia isn't buying local cyber and the rest of the world might soon follow	13 March 2019	ZDNet	10 M
Canberra's tech report provides obvious digital outcomes	21 December 2018	ZDNet	8 M
CISOs given cyber leadership role in Australia's new Information Security Manual	4 December 2018	ZDNet	8 M
Entersoft Security Announces the First Ever Brisbane Hackfest	24 May 2019	Business Standard	7 M

Public speaking engagements

Event	Role	Location	Date
SINET61 (part of 2018 Australian Cyber Week)	Panellist	Melbourne	1 July 2018
CyRise Roadshow Launch	Speaker	Melbourne	1 July 2018
Industry Partnership Masterclass	Event attendee	Sydney	6 July 2018
Siemens Digitalize 2018	Speaker	Melbourne	8 August 2018
2nd Annual ADM STEM in Defence Summit	Speaker	Canberra	21 August 2018
APAC Food Safety Conference	Speaker	Melbourne	23 August 2018
Cyber Security Internship Launch	Event attendee	Sydney	27 August 2018
CarbonCore Enex Carbon Launch	Speaker	Melbourne	28 August 2018
That Startup Show: ghost tech edition	Panellist	Melbourne	30 August 2018
ISACA Oceania CAC 2018 Conference	Speaker	Melbourne	3–4 September 2018
A Vision for Australia: GAP 9th Annual Economic Summit	Speaker	Sydney	6 September 2018
AmCham Cyber Security Lunch	Panellist	Sydney	11 September 2018
BlackBerry Security Summit	Speaker	London, UK	12 September 2018
United Nations Institute for Disarmament Research Cyber Stability Conference 2018	Speaker, Panellist	Geneva, Switzerland	26 September 2018
BlackBerry Security Summit	Speaker	New York, US	5 October 2018
Cyber Security Challenge Australia 2018 Awards	Speaker	Canberra	9 October 2018
AISA CyberCon 2018	Speaker, Panellist	Melbourne	9–10 October 2018
Australia-Singapore Cyber Security Dialogue	Speaker	Singapore	12 October 2018
Australia-Indonesia Cyber Security Workshop	Speaker	Jakarta, Indonesia	15 October 2018
Cyber Security for Startups	Speaker	Jakarta, Indonesia	17 October 2018
21st Victoria Prize for Science and Innovation	Event attendee	Melbourne	23 October 2018
Medical Technologies Association of Australia Annual Summit 2018	Speaker	Melbourne	8 November 2018
IoT IMPACT 2018	Speaker	Sydney	10 November 2018
Australia-Japan Cyber Security Dialogue	Panellist	Canberra	13 November 2018
Dtex Systems Briefing for Government: Risk-based Cyber Security	Speaker	Canberra	14 November 2018

Event	Role	Location	Date
Australian Technologies Competition Finals Showcase and Awards	Speaker	Sydney	15 November 2018
Home Affairs Cyber Security Summit	Panellist	Perth	22 November 2018
Joint Cyber Security Centre & AustCyber Node joint launch	Speaker	Adelaide	23 November 2018
Security Influence and Trust Summit 2018	Speaker	Melbourne	29 November 2018
ACT Innovation Showcase 2018	Event attendee	Canberra	4 December 2018
The Business of Events	Speaker	Sydney	7 February 2019
CyRise Showcase to Government	Speaker	Canberra	13 February 2019
Cyber Storm Policy Workshop	Workshop participant	Canberra	19 February 2019
Schools Cyber Security Challenges launch	Speaker	Sydney	19 February 2019
US Cyber Security Trade Delegation	Speaker (various)	New York, Washington DC, San Francisco	25 February – 8 March 2019
Innovation Expo: Industry 4.0 and IoT	Speaker	Geelong	7 March 2019
International Women's Day – Females in IT	Panellist	Melbourne	8 March 2019
International Women's Day – Females in IT	Speaker	Sydney	15 March 2019
Dean's Leaders Forum	Event attendee	Melbourne	19 March 2019
National Future Schools Expo	Speaker	Melbourne	20 March 2019
Mastering SAP	Speaker	Sydney	18–20 March 2019
Public Sector Innovation Show	Speaker	Canberra	26 March 2019
Australian British Chamber of Commerce: Finance, Fintech & Cyber Security breakfast seminar	Panellist	Melbourne	28 March 2019
Ai Group Industry Transformation Member Reference Group: Cyber Security Regulation	Panellist	Sydney	28 March 2019
National Security College Roundtable on the Future of Foreign Electoral Interference	Panellist	Canberra	4 April 2019
Research Innovation & Commercialisation Summit 2019	Speaker	Sydney	9–10 April 2019
Kasada Stop the Bots Report Launch	Speaker	Sydney	16 April 2019

Event	Role	Location	Date
ANU-Indiana University Collaboration Lecture	Speaker	Canberra	8 May 2019
CRN Pipeline	Speaker	Melbourne	9 May 2019
KPMG: Future of AI in Australia	Event attendee	Canberra	10 May 2019
CIT Cyber Tech Showcase	Speaker	Canberra	13 May 2019
ANU National Security College: Risk for national security practitioners course	Speaker	Canberra	15 May 2019
Privacy Awareness Week – DTA event	Speaker	Canberra	17 May 2019
CRN Pipeline	Speaker	Sydney	23 May 2019
Australian Computing Academy roadshow	Speaker	Melbourne	28 May 2019
CyberSMART 2019	Speaker	Fredericton, Canada	29–30 May 2019
Smart Cities 2019	Speaker	Melbourne	30 May 2019
Australian Davos Connection 2019 Leadership Summit	Panellist	Gold Coast	31 May 2019
AUSec 2019 Cyber Security Summit	Speaker	Melbourne	4–6 June 2019
Public Sector Fraud & Corruption Prevention Forum 2019	Speaker	Canberra	5 June 2019
EDUtech	Speaker	Sydney	7 June 2019
Brisbane Hackfest 2019	Speaker	Brisbane	7 June 2019
IMPACTfest Business and Educational Emerging Technology	Speaker	Sydney	14 June 2019
Research and Intelligence in Australia	Speaker	Canberra	18 June 2019



AustCyber's mission is to grow a vibrant and globally competitive cyber security sector that enhances Australia's future economic growth.

Contact

Email: info@austcyber.com

Phone: 0455 260 848

Website: www.austcyber.com

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