BINGO CAPITAL FUND

Bingo Capital Fund Pty Limited

Information Technology Capacity Statement & Risk Management Plan

Version 4.0 21 January 2024

Contents

Document Control

Document Owner

Document Owner:	Ray Trevisan
Document Classification:	Commercial-in-Confidence
Document ID:	BingoCap IT Compliance 0001

Template History

Version	Date	Author	Summary of Changes	Authorised by
0.1	24/08/2020	Ray Trevisan	Initial draft	Ray Trevisan
1.0	21/09/2020	Ray Trevisan	Finalised	Ray Trevisan

Version Control

Version	Date	Section	Description	Author	Checked
0.1	24/08/2020		Initial Draft	RT	PO
1.0	21/09/2020		Final	RT	RT
2.0	30/01/2023		Update	RT	RT
3.0	24/11/2023		Update details from DA to BingoCap	RT	RT
4.0	21/01/2024		Update BingoCap AFSL attainment and addition of more apps into structure	RT	RT

Purpose

The purpose of this document is to outline Bingo Capital Fund Pty Limited's (***BingoCap***) Information Technology Capability Statement and the company's Risk Management Plan as it pertains to all matter's information technology. This will cover aspects of:

1. Website
2. Data storage
3. Communications (email, fax, mobile and landline telephony)
4. Physical and network security (referred to as cyber security)

This Statement & Plan was initially developed to align with the February 2020 version of the ISM (Information Security Manual) and updated to align with the updated version of the ISM in December 2022.

Cyber Security Principles

The cyber security principles provide guidance on how to protect systems and information from cyber threats in light of the requirements outlined in ASICs Report 429, dated 19 March 2015, and ASICs Regulatory Guide 3 – AFS Licensing Kit: Part 3, specifically.

B5 proof: Information Technology Capacity Statement, and
B7 proof: Risk Management System Statement

The cyber security principles consist of the following activities:

- Govern – Identifying and managing security risks;
- Protect – Implementing security controls to reduce security risks;
- Detect – Detecting and understanding cyber security events;
- Respond – Responding to and recovering from cyber security incidents.

Scope

The scope of this paper covers the requirements outlined in ASICs rep429 and RG3.

System Overview

BingoCap's IT architecture will comprise primarily of a cloud based, *"internet always on"* environment that facilitates BingoCap staff and interested authorised parties to access the cloud-based infrastructure wherever and whenever they wish as long as sufficient internet access is available.

High Level Diagram

A high-level design diagram can be found at Annex B.

System Type / Description

Given BingoCap's system is cloud based, all intelligence, data and mission critical applications will all operate within approved, hardened internet environments presently utilised by all major financial and business institutions worldwide. There will be no restrictions on hard device access thereby providing maximum flexibility to BingoCap, its partners, clients, and all regulatory bodies as required.

System Description

BingoCap will leverage a business suite from Zoho Corporation together with a combination of additional computing and IT resources that cater to specific end user requirements for day-to-day business operations, including Microsoft Office[1] productivity suite, Registry Direct[2] for online Unit Trust management and Xero[3] accounting software. ZohoOne is an internet-based business suite that will provide the following primary functions including:

- **CRM** (Customer Relationship Management) – management of all client information / interactions
- **Sites** – a Content Management System (CMS) for designing and publishing websites
- **SalesIQ** – an interactive customer facing tool to chat and communicate with website visitors
- **Mail** – an email client
- **Bookings** – an appointment setting application
- **Books** – an accounting application
- **Meetings** – an online video meeting/audio conferencing application similar to Skype & Zoom
- **Sheet**, **Show**, **Writer** – Zoho equivalents of GSuite, MS Office – general office applications for word processing, spreadsheets, and presentation slides
- **Contracts –** an online contracts management systems that provides for agreements management
- **Signature**, automated digital signatures that are blockchain enabled

- **CPD –** BingoCap's Continual Professional Development (CPD) will be a "white-label" commercial system provided by Aspire[4], through the company's membership of the AIOFP[5]. As the AFSLs RM, Bingo Capital Fund through it's principal, Ray Trevisan, will administer and monitor the ongoing CPD program for the company and its CAR/ARs.

There is a total of 50 Zoho business suite applications that additionally include HR, stock control, marketing and analytics. BingoCap will continue to deploy additional applications as the need arises. The software licensing is flexible enough to provide for this expansion.

Security Classification

All information stored by BingoCap will be classified "***Commercial-in-Confidence***", and within the remit and bounds of Australia's Privacy Act, our information, and data stores as well as data access protocols will adhere to these requirements.

Business Impact Level

The Business Impact Level has been determined to be mission critical to our daily and long-term business operations.

---

1 www.microsoft.com
2 www.registrydirect.com.au
3 www.xero.com.au
4 https://www.aspirecpd.com.au/
5 www.aiofp.net.au Association of Independently Owned Financial Professionals

System Status

BingoCap will not be engaging any bespoke code implementation all software and IT systems are "*off the shelf*" COTS (commercial off the shelf) environments. Hence our system status is operation/production from our first day of operations.

System Users

As BingoCap presently consists of the founder (Ray Trevisan) and a number of additional partners, contractors and freelance operators, there will be a strict limit to registered users of the system. As BingoCap grows, we intend having the following types of System Users:

1. **Super Admin.** Total control and access to all IT systems (RT only)
2. **Admin.** Control and access to all IT systems other than account control and the ability to change system access rights.
3. **User.** Control and access to normal worker/user rights for day to day operations within their stated job/operational role – this will usually be BingoCap permanent staff, contractors/labour hire/casuals under the direct supervision of BingoCap management. This may also include new directors / Responsible Managers, and support admin staff that are being brought into BingoCap as we grow.
4. **Guest.** Specific access granted for admin, guidance/counsel to assist BingoCap operations (accountant access to Books, IT specialist to programming/configuration rights etc.)
5. **Partner.** CRM specific access to partner information pertaining to their business relationship with BingoCap.

Guidelines for Cyber Security Roles

Chief Information Security Officer / System Owner

1. RT will be appointed the CISO and System Owner. The CISO within an organisation is typically responsible for providing strategic-level guidance for their organisation's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation

Guidelines for Cyber Security Incidents

Detecting cyber security incidents

A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

Managing cyber security incidents

A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Reporting cyber security incidents

The following table describes some of the data sources that organisations can use for detecting and investigating cyber security incidents.

Data Source	Description
Domain Name System logs	Can assist in identifying attempts to resolve malicious domains or Internet Protocol (IP) addresses which

	can indicate an exploitation attempt or successful compromise.
Email server logs	Can assist in identifying users targeted with spear-phishing emails. Can also assist in identifying the initial vector of a compromise.
Operating system event logs	Can assist in tracking process execution, file/registry/network activity, authentication events, operating system created security alerts and other activity.
Virtual Private Network and remote access logs	Can assist in identifying unusual source addresses, times of access and logon/logoff times associated with malicious activity.
Web proxy logs	Can assist in identifying Hypertext Transfer Protocol-based vectors and malware communication traffic.

These are all available from our cloud-based service providers on request. All our approved providers also provide a high level of cyber awareness, and inbuilt tools for combating and mitigating cyber security incidents.

Guidelines for Outsourcing

Information technology and cloud services

All IT and cloud services will be procured / secured through approved vendors via BingoCap senior management only.

Guidelines for IT/Security Documentation

Development and maintenance of security documentation (including system specific)

The CISO (RT) will be responsible for the development and maintenance of all IT related and security documentation. This includes system specific documentation.

Guidelines for Physical Security

Facilities and systems

BingoCap will not maintain any facilities or systems other than personal devices (PCs, laptops, notebooks & smart phones).

ICT equipment and media

BingoCap will not be responsible for, nor maintain any ICT equipment or storage media. BingoCap will adhere to a strict BOYD (bring your own device) operations model, in which all data and smart software is contained in cloud systems.

Wireless devices and Radio Frequency transmitters

See ICT equipment and media.

Guidelines for Personnel Security

Cyber security awareness raising and training

All BingoCap personnel including senior management will be trained in relation to IT policy, cyber security both physical and virtual. The personnel / HR vetting process will include an onboarding procedure that will include familiarisation of all IT security protocols. These will be supplemented with yearly audits / refreshers to ensure compliance/adherence to the latest updates and local conditions / requirements.

This training will be extended through to Bingo Capital Fund's ecosystem of CAR/ARs.

Access to systems and their resources

All cloud-based solutions will be accessed only via two step authentications as prescribed by our cloud service provides.

Guidelines for Communications Infrastructure & Systems

As BingoCap will be a BYOD office, this is not applicable. Personnel will be encouraged to engage with the necessary PCs, smartphones, landlines and other communications devices as required to perform their duties. BingoCap will not prescribe any specific vendor or technology, other than the ability to effectively and efficiently interact with our selected cloud-based support systems and processes.

Guidelines for ICT Equipment Management

Being a BYOD office, this will require personal responsibility only. BingoCap will provide guidelines only as to equipment ICT equipment selection, operation & maintenance etc. The use of local media storage will be permitted for limited storage and backup. Mainstay client and company files must never be solely stored on stand alone media unless specifically required by BingoCap senior management. All data stores must be backed up in cloud-based stores at all times.

Guidelines for System Management

System administration, patching, change management, data backup and restoration

To be led and aligned with our cloud-based vendors.

Guidelines for Software Development

Application development / Web application development

Any application or bespoke development of any type will only be undertaken after approval of the entire board / senior management of BingoCap.

Guidelines for Database Systems, Email, Network Management

To be outsourced and managed, by our selection cloud-based service provider.

Guidelines for Network/Gateway Management

COTS (commercial-off-the-shelf) services will be engaged by BingoCap personnel as part of the overall BYOD implementation.

BingoCap's website, content, implementation, management and operation will remain the responsibility of RT/CISO, in conjunction with BingoCap's selected cloud-based service provider.

Risk Management

CISO will be responsible for maintenance and day to day Risk Management of the ICT Capacity of BingoCap. In the execution of his role, RT will ensure:

Education / Awareness

All BingoCap personnel will be made aware of and be kept up to date at least on an annual basis of the IT Capacity and Risk Management requirements. This will also include all elements of cyber security awareness, internet safety and potential risks / breaches.

Risk Management Register

CISO will maintain a Risk Management Register that includes recording, analysis, handling of cyber threats including malicious code infections, rectifications/remediations and post incident analysis. If appropriate, any breaches will then be reported through to government authorities as required. Further information on reporting cyber security incidents to the ACSC is available at https://www.cyber.gov.au/report .

Guidelines for Outsourcing

IT / Cloud / Gateway Services

All services selected by BingoCap will undergo regular security and commercial assessments to determine their security posture and security risks associated with their use.

As BingoCap does not envisage the handling of secure information per se, the storage/data sovereignty is not of primary concern unless access to our overseas data stores are for any unforeseen circumstances compromised/curtailed. We also do not envisage dealing with in any manner, countries that are presently nominated by Australian and allied security services as "at risk" destinations.

Appendix A – Approvals

System Owner

Based on the information provided, I have assessed that the implementation of the system provides adequate controls for the protection of information classified up to and including **COMMERCIAL-IN-CONFIDENCE**.

I have determined that the risk to BingoCap operations and assets operating in the environment is **Low** and is acceptable given the overarching need to place the system into operation.

System Owner	
Signature	
Name	Ray Trevisan
Date	

Appendix B – High Level Design