RIVERROCK

DATED: JAN 2020

RIVERROCK SECURITIES
BUSINESS CONTINUITY PLAN
&
DISASTER RECOVERY PLAN

Contents

Introduction

The Information Technology continuity plan supports the overall business continuity plan (BCP) of an organisation. BCP seeks to ensure RiverRock Securities (RRS) processes are protected from disruptions and that RRS is able to respond positively and effectively when disruption occurs. RRS sets out its BCP priorities, and it is within this context that IT continuity plan activities take place. IT continuity plan ensures that the required information and communications technology and services are resilient and can be recovered to predetermined levels within timescales required by and agreed with directors of RRS. Thus, effective BCP depends on IT continuity plan to ensure that RRS can meet its objectives at all times, particularly during times of disruption. To be successful, both BCP and IT continuity plans have to be embedded within the culture of RiverRock.

IT Continuity Policy

RR IT strategy currently relies on the online services which store all data and email services across several datacentres.

IT continuity plan is an important strategy to protect the shareholders of RRS, including customer service, profitability and jobs.

The scope of the IT continuity plan covers

- File Servers, emails and attachments, calendars, network resources, security (active directory), telephone system, archiving

The person in charge of the adherence to the IT continuity policy is the BCP Manager and he or she is responsible for ensuring that the policy is continued to be carried out and that any changes in the IT strategy are implemented within IT continuity management.

The policy is to be reviewed periodically including the scope of service covered as part of a continuous improvement strategy. It will also be reviewed for its integration into the wider Business Continuity Plan or the rest of the business and amended accordingly for any changes in the business activity or identified risk.

IT Requirements

The IT services for RRS have been individually identified and linked to the services which support them. RRS have undergone a review of each service and identified the maximum Return Time Objective (RTO) and Recovery Point Objective (RPO) for each, which can be tolerated by RRS before a material impact on profitability, customer service and shareholder value would be incurred by the business.

RTO – the time taken to get a system fully tested and available to all users to useful work from the point of the disruption (including any decision time)

RPO – the time difference between point of the disruption and the point when the latest useable backup data is able to be recovered.

The current expected and tested RTO and RPO are as follows:-

Priority	Service Name	Service/Product Supported	Server Names	RTO	RPO
1	Email	Microsoft Office 365	Microsoft Cloud Servers	30mins	0
2	File sharing	Onsite Server Windows NAS Box	RRSVRFP01 RRSVRDC01 RRSVRDC02 RRSVRFP02 NAS Box	2 – 3 hrs	30mins
3	Security (Active directory)	Microsoft Windows Server	RRSVRDC01 RRSVRDC02 RRSVRFP01 RRSVRFP02	1hr	0
4	Network resources	Cisco Firewall Cisco Switches Cisco Umbrella	N/A	30mins	0
5	Phone system	Avaya Phone System – BT SIP Trunk	Avaya IP Office 500	20mins	0
6	Archiving	Mimecast	N/A	0	0

The Disaster Recovery Plan (DRP) is structured to ensure that the most important or time critical business processes are tackled first, with other processes being brought back as time permits. In general, the following priority list is correct:

- Service Delivery
- Financial Services
- Human Resources

This plan details the 2 main scenarios that RR believe are most likely. Other scenarios will be added as part of the review process and principle of continuous improvement.

Below is a list of services we use and how they work as part of our infrastructure: -

Microsoft Online Services

Microsoft Exchange Online

All emails are being hosted with Microsoft Exchange Online, which is a hosted messaging application that provides RiverRock with access to the full-features version of having an Exchange Server (Mail Server). It includes access to email, calendars, contacts and tasks for any endpoint devices. Exchange Online services are accessible globally via internet connectivity with Firefox, Safari, Internet Explorer and Chrome. It also has the compatibility with Apple iPhones and iPad, Microsoft Windows Phone and Android mobile devices.

With Microsoft Exchange Online there is a commitment of a 99.9% uptime provided by Microsoft with a continuous data backup between their global redundant data centres and round the clock intrusion monitoring and detection.

Mimecast

Mimecast is a service provider of unified email management services, which covers the four main bases outside messaging: Archiving and discovery, continuity, email security and email policy. Mimecast is cloud-based, geographically dispersed servers, they provide a 100% service availability SLA (Service Level Agreement) for their solution.

Mimecast has been set up to work alongside with Microsoft Exchange Online. The configuration is set up so that outbound and inbound emails are to go through Mimecast. Mimecast's Secure Email Gateway provides protection and scanning of both incoming and outgoing email for any spam, malware, phishing and more. As part of the services they provide a SLA that offers 100% viral protection and 98% spam protection.

Phone Lines and Phone System

Our phone systems is using Hays phones infrastructure.

User Accounts

All user account details are stored on our onsite server. This server controls the way the user profile is set up for RiverRock. All user details are then linked with Microsoft Azure Active Directory and then these user details are pushed out to Microsoft Office 365. Every 15mins all user account details at our on-premises server get synchronised to the Microsoft Azure Active Directory. Any changes to user accounts, such as passwords, will take up to 15mins to update (unless IT force the changes across, which effectively take less time).

Internet Lines

RRS is currently using Hays Internet line provided by Foliateam which is the Primary Internet line along with a secondary backup line in place.

UpdateYou - Additional IT Support

Where RiverRock IT Support is not available, UpdateYou will be contacted to provide additional IT assistance.

IT Continuity Management

Responsibilities

The Business Continuity Plan Forum (BCP Forum) has overall responsibility for the maintenance of the Disaster Recovery Plan (DRP) and the Business Continuity Plan should there already be one in

place. Within the Forum, individual members have responsibility for ensuring that the DRP adequately protects the IT Services that are within their control. Currently, the individual owners are as follows:

Owner	**Processes**
Ben Chadwick	Finance, Payroll
Diamandis Karamagias	Chief Operating Officer and Chief Financial Officer
Oliver Allan	Associate General Counsel and Group Compliance Officer
John Meager	Head of Operations
Simon Lam	Head of IT

BCP Forum

The BCP Forum will meet at least every 3 months to review and identify any new risks and to monitor any outstanding actions necessary as part of the continuous improvement policy. Standard agenda items are:

- Testing timetable,
- Identified Risks,
- RRS reports,
- IT Incidents,
- Staff Communication/Training.

Testing Schedule

Testing will take place on a 6-monthly basis. Q4 testing will be a full-scale walkthrough, simulating one of the major failure scenarios. Q2 testing will be a smaller scale, 'table-top' walkthrough. In addition, many smaller scale tests are done on a regular basis. All documents should be refreshed for any changes of contact details or new relationships.

Revision Plan

The Disaster Recovery Plan (DRP) and the risk assessment will be formally reviewed on a 6-monthly basis, timed to incorporate lessons learned from the most recent test. In response to this, the plan will be re-evaluated, and revised versions of it distributed to all employees with explicit roles and responsibilities in a DR scenario **Principle Recovery Mechanisms and Invocation Procedures**

Appendix A contains lists of personnel and their responsibilities within the BCP. These people have specific, assigned roles in a DR situation, and are required as part of their role to be familiar with the DRP and their part within the various scenarios that might be invoked.

Server Recovery

Invocation of the Plan is a significant event and carrying out many of the scenarios will involve both significant capital expenditure and large amounts of effort by employees. As a result, it is not a process to invoke lightly.

RiverRock Securities IT systems and security perimeter may be invoked onto the RiverRock Rescue Platform within 90 minutes. Invocation is activated by contacting the RiverRock invocation Manager, Simon Lam, and appropriate authorisation being given to commence the invocation.

Once the invocation has successfully been completed secure access to RRS IT systems at London office and Milan, if London office goes down, via any internet connection using a VPN. All normal security and access rights will remain the same. The Invocation Procedure can be found in Appendix D including an 'end users' access to the service guide. See Appendix E.

Authorisations are reviewed and checked that they are up to date on a monthly basis by the BCP Manager.

The following personnel currently have the authority to invoke the DRP:

1. Diamandis Karamagias
2. Simon Lam

Disaster Recovery Strategies

After the invocation of disaster, the key element would be to access the data and emails via internet connection details are given at Appendix E.

Disaster Recovery Plan

Scenarios, Risks and Mitigants

This section outlines a number of the most predictable business continuity scenarios resulting in business disruption. Inevitably, the list cannot be complete, but any incident not covered is likely to be similar to one (or more) of those listed below and decisions can be taken accordingly.

1. **Large Area Explosion**

A large area explosion is one that would destroy/seriously damage the office premises and other significant structures, for example, transport infrastructure and/or staff residential buildings. This could arise through, for example, a bomb explosion (possibly as a terrorist attack) or a major bombing raid in the event of war (see below). While this scenario is, one hopes, unlikely, it is nevertheless possible. Risk mitigation really comes down to pre-emptively vacating the premises should a government agency so advise/instruct in the event of a warning.

2. **Localised Explosion**

A localised explosion is one that seriously damages or destroys the office building and its immediate vicinity. Risk mitigation would include pre-emptive evacuation, as above, together with measures to reduce the effects of an explosion on the building (for example, applying adhesive film to the windows to hinder glass fragmentation).

3. **Explosion in Vicinity**

An explosion in the vicinity is one that damages nearby infrastructure (for example, transport or utilities) and/or staff residential buildings – but not the office itself. However, a local police cordon could include the office building thus preventing staff from attending the office or forcing an evacuation. Mitigation would include invoking some of the general BCP provisions (for example, operate remotely).

4. **Radiological Bomb**

A radiological bomb (often known as a “Dirty” bomb) involves a small-scale explosion but the release of a large amount of radioactive fall-out, forcing the evacuation of large areas. While there is some risk to human health, dependent on the prevailing wind, the epicentre of the explosion and the extent of the radioactivity, the largest impact would be economic – for example, large parts of central London could become uninhabitable so critically damaging the financial services industry and the broader economy. While this threat may seem unlikely, it is one taken very seriously by security services.

5. **War, Civil Unrest**

War or civil unrest covers a very broad range of scenarios and would almost certainly require a high degree of flexibility in response as the outcomes could cover one or several of the BCP outcomes listed.

6. **Security Alert**

This would arise due to a bomb threat or similar. The likely impact would be the evacuation of the building and/or non-admittance for a period likely to be less than one day.

7. **Gas Leak**

This may have a similar impact to a Security Alert (see 6) although there is no Gas supply in the building.

8. **Earthquake**

The likelihood of a significant earthquake is highly correlated to the geological conditions of the office location. Therefore, the attention paid to this risk in planning would vary from extensive to none. For these purposes, an earthquake impact could be like a wide-area explosion.

9. **Fire**

A relevant statistic is that a fire permanently closes 44% of the businesses affected. This is an area where effective business continuity arrangements will make a critical difference. The impact of a fire could involve damage, to a greater or lesser extent, to the office – at the minimum forcing an evacuation and likely seriously damaging the IT and telecoms infrastructure. It is also possible that the building could be left structurally unsound so preventing both the reoccupation of the premises and the retrieval of key documents etc. In most countries, mitigation of fire risk is embedded in relevant legislation.

10. **Flooding**

As for an earthquake, risks vary considerably depending on the office location – and the floor level of the building in which an office is located. Floods can range from a tsunami, to the sea or a river bursting its banks, to a burst water pipe and therefore the commensurate damage can range from total destruction to a minor inconvenience. Water damage can also occur through, for example, plumbing issues on higher floors (although currently RR occupies the top floor) and as a secondary consequence of a significant fire where water is used as an extinguishant by the fire service. This would be likely to exacerbate damage to the organisation's office and infrastructure.

11. **Pandemic**

A pandemic is an epidemic of infectious disease that spreads through human populations across a large region, for example, a continent, or even worldwide. This is a serious risk, partly because the consequences are so unpredictable. Firstly, there is the possibility of staff becoming sick. Then there is the possibility of such a high proportion of the general population becoming sick that essential services start to break down (for example, transportation, power generation, food supplies etc.). It should also be noted that staff who are otherwise healthy may have to care for sick relatives and/or focus on securing essential food supplies and would therefore be unable to work. It is also likely that some, or all, service providers would be similarly impacted. In this environment it is likely that staff would wish to (or even be forced to) work from home – however their effectiveness is likely to be limited due to the reasons noted above. Mitigation would include acquiring a stockpile of surgical masks – and trying to secure supplies of any vaccine and/or drugs (assuming availability).

12. **Extreme Weather**

Very extreme weather could include a hurricane (for example, 1987 in London), very low temperatures, very high temperatures and torrential rain. This would be unlikely to impact the operation of the office directly – but would be very likely to disrupt staff transportation.

13. **Transport Disruption**

Commuter transport (and business trips) could be disrupted by adverse weather (see above), a strike, an explosion (see above) or technical failure. This could hinder a varying subset of staff's ability to get to (and from) the office. Mitigants could include booking hotel rooms near the office in the run up to, or during, a disruption.

14. **Accident**

An accident, whether in or outside the office, could result in the death or serious injury of one or more staff. Partial mitigants include life insurance policies for all staff, and key man insurance for senior executives. Nevertheless, if a scarce skill set becomes unavailable at short notice, this may cause disruption. This risk can be partially mitigated through cross training (as for other Loss of Staff issues – see below). However, the emotional impact on the colleagues of casualties is hard to mitigate for in the short-term.

15. **Electrocution**

This is really a subset of "Accident" above – but may also have the side-effect of damaging the IT Infrastructure and so it is included for completeness.

16. **General Power Outage**

A general power outage would be the failure of the national or local grid resulting in a power cut across a broad area, impacting both the office and local transportation – and conceivably the organisation's backup data centre, if any. Mitigation includes Uninterrupted Power Supply (UPS) – both desk and server-based. This will allow for an orderly shut-down of work and a head-start for the fail-over process, including backup generators. The biggest issue here is likely to be when to commence fail-over given that it is likely to be hard to get information on the expected duration of the outage. Diesel generators may provide a medium-term solution.

17. **Localised Power Outage**

A local power outage is one that just impacts the building or, at worse, the local area. Therefore, the impact is similar to the above other than it is unlikely to impact a backup data centre or transportation. Mitigation steps are therefore also similar to above.

18. **Circuit/Terminal Failure**

In the event of an individual PC failing, the damage should be confined to the loss of part of a day's work only, assuming that all files have been regularly backed up. Most firms should have a spare PC, already built to a basic configuration, which can be quickly substituted.

19. **Hardware Failure**

Computer hardware support arrangements should be in place, and a certain degree of resilience should be built into most systems.

20. **Virus/Hackers**

IT security should be treated as a significant priority and sensible precautions taken in conjunction with the IT Infrastructure Service Provider (ISP). Professional security firms may also be engaged to attempt to penetrate IT security measures as part of a broader security audit.

21. **Theft/Sabotage**

This issue is also tied in with security – and ensuring that intruders cannot easily obtain access to office premises.

22. **Telecom Utility Exchange/Line Failure**

This includes lines that permit data feeds and internet access. Mitigation would include separate circuits and/or fail-over to mobile network(s).

23. **Telecoms Hardware Failure**

This should be covered by the telecoms service provider. Mitigation options include failing over to a mobile network(s).

24. **Local Mobile Network Failure**

Finally, there is the possibility of one or more mobile networks failing. There is a fair likelihood that this could happen at the same time as a major incident (for example, the London tube bombings). Mitigating options include using more than one provider.

Outcomes

While it is very unlikely that any given crisis event can be accurately predicted beforehand, most events will feature a combination of one or more outcomes:

- timing;
- loss of building access;
- loss of staff;
- loss of IT; and
- loss of telecoms.

While not explicitly listed, attention should also be paid to the duration of transient events since brief events may require little action (although it is not always clear at the time of the event how long a transient event may last at the time – for example, a security alert). Previous experience has shown that organisations which pro-actively address disruptions – at the very least actively investigating and monitoring their status – have superior outcomes to those that adopt a more reactive posture. Therefore, the chairman of the crisis management team should be advised as soon as any incident occurs where the duration is uncertain.

The final scenario to be considered is the failure of a key supplier – this is addressed separately.

1. **Timing**

This is a reflection of whether the event arises during or outside office hours (office hours defined for these purposes as when the building contains staff – which may be significantly beyond core hours).

2. **Loss of Building Access**

Loss of building access means that all staff within the building at the time of the incident must evacuate and all staff not within the premises will be refused entrance (this would include IT or telecoms contractors attempting to fix problems). In the event of a catastrophic failure (for example, an explosion) there is also likely to be a loss of staff.

3. **Loss of Staff**

This covers all of injury, illness, death and inability to get to the office (or potentially get home) for staff and key contractors. More specifically, awareness of key man dependency is important. The other key factor to be aware of is that if the loss of staff includes fatalities or serious injury it is likely to have a very adverse impact on morale amongst the remaining staff – people who have lost a close colleague and/or are concerned about the safety of their families are unlikely to be in the right frame of mind to commence recovery and their duties will need to be re-assigned to less impacted colleagues. Longer-term, the provision of counselling and support for affected staff (perhaps all) should be offered.

4. **Loss of IT Infrastructure**

This includes partial or complete failure of the IT network, including hardware and operating software. The key factor here is to involve service providers at an as early stage as possible to instigate the IT fail-over to backup systems.

5. **Loss of Telecoms Infrastructure**

This includes partial or complete failure of the telecoms network (including equipment, land lines, mobile networks and the internet). In general, the contingency would be to use mobile networks if the land lines fail and vice-versa. If both fail, then it is likely that the organisation's e-mail/internet would also fail.

Scenario/Outcome Mappings

The following table works through all combinations of the five variables listed above (variables which are extremely unlikely to arise, or which are not feasible have been deleted). Examples of the types of scenario that may result in these outcomes are also listed. Details of actions to take in the event of these outcome combinations are detailed under Crisis Management.

Business Disruption Combinations																	
During Office Hours?	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N
Access to Office Lost?	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N
Loss of Staff?	Y	Y	N	N	Y	Y	N	N	N	Y	Y	N	N	Y	N	N	N
On-Site IT Servers Fail?	Y	N	Y	N	Y	N	Y	Y	N	Y	N	Y	N	N	Y	Y	N
Telecoms Fail?	Y	N	Y	N	N	N	Y	N	Y	Y	N	Y	N	N	Y	N	Y
Examples of Incident	Large Area Explosion	Explosion in vicinity	General Power Outage	Security Alert	Electro cution	Transport Disruption	Localised Power Outage	Circuit/ Terminal Failure	Telecoms Exchange/ Line Failure	Large Area Explosion	Explosion In Vicinity	General Power Outage	Security Alert	Transport Disruption	Localised Power Outage	Circuit/ Terminal Failure	Telecoms Exchange Failure
	Fire		Fire	Gas Leak		War, Civil unrest	Virus/ Hackers	Hardware Failure	Telecom Hardware Failure		Radiological* Dirty Bomb	Fire	Gas Leak	War, Civil Unrest	Technical Failure	Hardware Failure	Telecoms Hardware Failure
	Flooding		Flooding			Accident	Theft/ Sabotage	Virus/ Hackers	Local Network Failure			Flooding		Accident	Virus/ Hackers	Virus/ Hackers	Local Network Failure
	Extreme weather					Pandemic		Theft/ Sabotage	Theft/ Sabotage			Extreme Weather		Pandemic	Theft/ Sabotage	Theft/ Sabotage	Theft/ Sabotage

Approach

Delivering the Disaster Recovery Plan (DRP) is a high priority in order to ensure appropriate RiverRock staff resume access to key business processes supported by IT systems. This will help deliver core services to clients, it will enable full service levels to be resumed and then normal business operations across the business. This will require the IT team to consider issues including:

- Implementing alternative working practices, such as remote working
- Identifying and equipping temporary premises or branch offices
- Monitoring the progress of the reinstatement work at the damaged premises, ensuring that this goes to plan and that office equipment is ordered and delivered at the appropriate time
- Keeping a disaster recovery log up to date by recording details of the actions, losses identified, and expenses incurred

The plans are broken down into a number of smaller action plans for differing scenarios (in this example there are three), each designed to be run in isolation and to restore normal business processes.

The scenarios below, while not a comprehensive list, detail what is believed to be the most likely sub-set of disaster scenarios that may be encountered by RR.

Main Scenario 1: Complete Loss of Data file server Facility at RiverRock Securities.

Due to the nature of the service provided by RiverRock Securities and the dependency upon the main File Server, loss of this server would curtail RiverRock Securities activity to such an extent that business could not continue in its current form unless an alternative location running all critical processes was found quickly.

Likely effects

- RRS IT services would not operate.
- Loss of communication with customers

Effect upon core processes

Core business process would be curtailed:

- No access to files share drive ➔ all company processes are affected
- No security (active directory) validation ➔ all company processes are affected

Plan of action

If access to the RiverRock Securities space is likely to be denied for a prolonged period and service is lost or likely to be lost, actions should be taken are as follows:

- The RRS Disaster Recovery services should be invoked by an authorised person (See Appendix E)
- The Telephone diversion service will be activated by instructing Hays to invoke the Disaster Recovery Plan as appropriate if RRS landlines are affected. (See Appendix F)
- Test RiverRock Securities services and confirm running status
- Access latest version of the BCP on newly running server. Distribute as per BCP
- Advise staff of how to access IT services and time of last snapshot of data with newly issued access credentials
- Sales and marketing would halt or delay client expectations advising of Disaster but reassuring that service will be back to normal very shortly.

- Advise Insurance company of disaster and contact critical suppliers as per Appendix B
- Client Services would contact all existing clients affected by the disaster and set expectations of resumption of service and the plans in place to achieve these.
- Certain staff to work remotely using internet broadband or mobile internet
- Prepare/update and Execute plan for migration back to original newly repaired/prepared Data Server Facility
- Detail list of 'Lessons' learned to improve BCP Plan

Main Scenario 2: Complete Loss of Data file server Facility and Offices at RiverRock Address

Due to the nature of the service provided by RRS and the dependency upon the main file server Facility, loss of this facility would curtail RRS's activity to such an extent that business could not continue in its current form unless an alternative location running all critical was found quickly.

Likely effects

- RRS IT services would not operate at current location.
- Loss of communication to customers
- Staff would no longer be able to work, poor morale

Effect upon core processes

Core business process would be curtailed:

- Clients would no longer be given the service which they were paying for.

Plan of action

If access to the Paris office facility & Office space is likely to be for a prolonged period and service is lost or likely to be lost, actions should be taken are as follows:

- The RiverRock Securities Disaster Recovery services should be invoked by an authorised person (See Appendix E and J)
- The Telephone diversion service will be activated by instructing Hays to invoke the Disaster Recovery Plan as appropriate if RRS landlines are affected. (See Appendix F)
- Test RiverRock Securities services and confirm running status.
- Access latest version of the BCP on newly running server. Distribute as per BCP
- Advise staff of how to access IT services and time of last snapshot of data with newly issued access credentials
- Ability to access remotely via VPN the infrastructure of the London or Milan offices.
- Sales and marketing would halt or delay client expectations advising of Disaster but reassuring that service will be back to normal very shortly.
- Client Services would contact all existing clients affected by the disaster and set expectations of resumption of service and the plans in place to achieve these.
- Certain staff to work remotely using internet broadband or mobile internet
- Prepare/update and Execute plan for migration back to original newly repaired/prepared Data Facility and Offices

Main Scenario 3: Cyber Attack at RiverRock Securities IT Infrastructure

Due to the nature of the service provided by RRS and the dependency upon the main file server Facility, loss of this facility would curtail RRS's activity to such an extent that business could not continue in its current form unless an alternative location running all critical was found quickly.

Likely effects

- RRS IT services with be at minimal capacity at current location.
- Loss of communication to customers
- Staff would no longer be able to work at full capacity, poor morale

Effect upon core processes

Core business process would be curtailed:

- Clients would no longer be given the service which they were paying for.
- No access to files share drive ➔ all company processes are affected
- No security (active directory) validation ➔ all company processes are affected

Plan of action

If a Cyber Attack occurred at our Paris office it is likely to be for a prolonged period and service is lost or likely to be lost. Actions should be taken are as follows: -

- The RiverRock Securities Disaster Recovery services should be invoked by an authorised person (See Appendix E and J)
- The Telephone diversion service will be activated by instructing Hays to invoke the Disaster Recovery Plan as appropriate if RRS landlines are affected. (See Appendix F)
- Communication with Hays Internet provider to alert them of Cyber Attack.
- Disconnect all internet activities.
- Shutdown all servers and workstations in the London office.
- Seek out the infected machine(s) and quarantine for further investigation.
- Reset all domain user passwords.
- Scan entire RRS IT Infrastructure for any further potential threats.
- Block all outside internet connection.
- Access latest version of the BCP on newly running server. Distribute as per BCP
- Advise staff of how to access IT services and time of last snapshot of data with newly issued access credentials
- Ability to access remotely via VPN the infrastructure of the London or Milan offices.
- Sales and marketing would halt or delay client expectations advising of Disaster but reassuring that service will be back to normal very shortly.
- Client Services would contact all existing clients affected by the disaster and set expectations of resumption of service and the plans in place to achieve these.
- Certain staff to work remotely using internet broadband or mobile internet
- Prepare/update and Execute plan for migration back to original newly repaired/prepared Data Facility and Offices.

Appendix A – Roles and Responsibilities (amend as appropriate)

This section contains details of all personnel who have general responsibilities in all Business Continuity Scenarios. Individual Scenarios require additional staff, and those are documented within their individual portions.

CFO/COO (Diamandis Karamagias)

Prime Responsibilities

1. To decide, based on the apparent risks to the business, whether the DRP should be invoked

2. To safeguard Customer and Staff Interests

3. To provide commercial assistance to the DRP

4. To have read and fully understood all relevant portions of the DRP

5. To manage expectations of all interested parties including staff, suppliers, customers, press

6. To authorise adequate resource to ensure that a smooth and predictable execution of the DRP and BCP can be achieved

Main Activities

1. To Coordinate Communication with Customers and Staff and ensure they are both kept up-to-date, and that expectations on recovery timescales are correctly set.

2. To handle all commercial aspects of the acquisition of required goods and services to implement the DRP.

Head of IT (Simon Lam)

Prime Responsibilities

1. To have read and fully understood all relevant portions of the DRP

2. To coordinate activity and ensure that the DRP is correctly carried out

Main Activities

1. To assist the CFO/COO in the implementation of the technical aspects of the DRP.

BCP Manager (Diamandis and Simon)

Prime Responsibilities

1. To have read and fully understood all relevant portions of the BCP

2. To manage and operate the BCP

3. To ensure that the business continues to review and mitigate risks to the business in line with the BCM Forum

Main Activities

1. To operate the BCP

2. To ensure that testing of the DRP and reviews of risks and improvements are carried out in line with the DRP policy

3. To ensure that the DRP continues to integrate within the overall BCP of the business

Appendix B – Contact Details

This section contains contact numbers for personnel and organisations who are required to successfully execute the BCP. It must be regularly checked, and details kept up to date.

Name or Organisation	Role		Contact Numb
Diamandis Karamagias	CFO/COO		02078427662
Simon Lam	Head of IT		02078427676
Hays IT	Hays Building Management		+33 (0)1 84 88
UpdateYou			07 69 72 10 34

Appendix C – Required Items

This section lists items which must be available in all scenarios in order to successfully execute the BCP. Each individual scenario contains a separate section of required items – this Appendix simply brings them together in one place to simplify audit.

Item	**Storage Location**
Current Copies of DRP	At homes of all Personnel listed in Appendix A
Employee Addresses List (contains home and Mobile Phone numbers of all employees)	At home of all Personnel listed in Appendix A
Emergency employee contact details	At home of all Personnel listed in Appendix A
Software Licence details and activation keys	Held by Simon
Server technical documentation and builds	Held by Simon

Appendix D – RiverRock Invocation Guide

ACTION	**DONE**
Assess damage to the IT infrastructure.	
Determine the level of disruption to voice and data communications lines.	
Contact Hays, Hays as required to assist with the recovery process.	
Contact Directors and advise whether IT systems are currently accessible remotely, expected time for recovery and the date of the backup being restored.	
Once remote access to servers is available, notify Directors and provide support to staff as required.	
Recover telephony services.	
Replace desktop PC's and associated software if necessary.	
Maintain records of activities and actions taken and ensure relevant parties are kept informed of the current status.	

Appendix E – End User Access Guide

Please contact Simon Lam for these updated details which are under test phase

User Access Guide will be the Remote VPN Access for RiverRock Office.

Secondary access will be Office 365. (User Access Guide is still incomplete)

Phones will be diverted to the appropriate Disaster and Recovery Plan we have with BT Local Business. A spreadsheet has been produced to demonstrate this.

Appendix G – Microsoft Office 365 BCP

Microsoft has an understanding of how to deliver highly available service comes from years of experience in building enterprise-class solutions and running online services. They combine robust recovery-oriented design, continuous learning, and consistent communication to deliver high quality service and a great customer experience.

They also have a financially backed guarantee of 99.9% uptime, giving us peace of mind.

High availability design principles:

Redundancy

- Physical redundancy at server, data centre, and service levels
- Data redundancy with robust failover capabilities
- Functional redundancy with offline functionality

Resiliency

- Active load balancing
- Automated failover with human backup
- Recovery testing across failure domains

Distributed services

- Distributed component services like Exchange Online, SharePoint Online, and Lync Online limit scope and impact of any failures in a component
- Directory data replicated across component services insulates one service from another in any failure events
- Simplified operations and deployment

Monitoring

- Internal monitoring built to drive automatic recovery
- Outside-in monitoring raises alerts about incidents
- Extensive diagnostics provide logging, auditing, and granular tracing

Simplification

- Standardized hardware reduces issue isolation complexities
- Fully automated deployment models, making deployment easier than ever
- Standard built-in management mechanism

Human backup

- Automated recovery actions with 24/7 on-call support
- Team with diverse skills on the call provides rapid response and resolution
- Continuous improvement by learning from the on-call teams

Continuous learning

- If an incident occurs, regardless of the magnitude of impact we do a thorough post-incident review every time
- Our post-incident review consists of analysis of what happened, our response, and our plan to prevent it in the future

- In the event your organization was affected by a service incident, we share the post-incident review with you

Consistent communication

- Transparency requires consistent communication, especially when you are using the service
- We have a number of communication channels such as email, RSS feeds, and the very important and highly relevant Service Health Dashboard

The Office 365 Service Health Dashboard is the window into the health of the service for our specific organization. As an Office 365 customer, we get a detailed view into the availability of services that is relevant to our organization. Their service dashboard gives us full insight into our services by showing their current status and even lets us see when we need to renew licenses.

Appendix H – Mimecast BCP

Mimecast Email Continuity delivers always-on, seamless email availability through automatic service failover and failback in near real-time during an email outage. It integrates so seamlessly with Microsoft Outlook that your employees will just carry on using email safely and securely – whether the email outage is planned or not.

Appendix I – RiverRock Backup

All RiverRock Securities data run on a scheduled daily incremental, week end full and a month end full backup. All backup files are stored locally on a server and replicated over to our Network Attached Storage (NAS). We also have our data replicated over to our Microsoft Windows Azure Cloud Server and to our Paris Office Server.