

Business Impact Analysis

**Pauline Finlay** **B00107945**

**Declan McGuire B00107907**

**David Mulhall B00107874**

***Department of Informatics***

***School of Informatics & Engineering***

***Technological University Dublin, Blanchardstown***

***Dublin 15.***

**Word Limit for Assignment: 3000 Actual Word Count: 5810**

**BSc (Hons) in Computing in Digital Forensics & Cyber Security**

**DFCS H4019 Business Continuity Management & Cloud Security**

**9th November 2020**

**Plagiarism Declaration**

We hereby certify that this material, which we are submitting for assessment for the course title of BSc. (Hons) In Computing in Digital Forensics and Cyber Security is our own work and that we have:

* Clearly referenced/listed all sources as appropriate
* Given the sources of all pictures, data etc. that is not our own
* Any work of any other student(s) either past or present is clearly referenced
* Not submitted for assessment work previously submitted for any other course, degree or qualification
* Not incorporated any text acquired from external agencies other than extracts from attributed sources (including online facilities)
* Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
* My work may be electronically checked for plagiarism, including, but not exclusively, by the use of plagiarism detection software and stored for future comparison
* Any false claim for this work will be penalised in accordance with the College’s regulations

**Signed:** Pauline Finlay **Date:** 09/11/2020

**Signed:** Declan McGuire **Date:** 09/11/2020

**Signed:** David Mulhall **Date:** 09/11/2020

**Abstract**

DDP Architects commissioned this Business Impact Analysis (BIA) report to assess the ability of the company to contend with a range of possible disruptions to normal business operations.

This analysis categorises identified risks to business functions in terms of minor to mission-critical and quantifies the impacts of those risks. In addition, a fiscal review was undertaken, and a cost model derived to determine the financial impacts relative to the remediation costs.

Recovery time requirements were analysed by business function with particular focus on the mission critical elements. Some deficiencies were identified and will be addressed.

The Information Systems/Information Technology (IS/IT) business function was determined to be the most critical and the most vulnerable.

Table of Contents

[1 Executive Summary 6](#_Toc55725226)

[2 System Description 7](#_Toc55725227)

[2.1 System Overview 7](#_Toc55725228)

[2.1.1 Electrical system 7](#_Toc55725229)

[2.1.2 HVAC & Fire Suppression 7](#_Toc55725230)

[2.1.3 Internet connectivity 8](#_Toc55725231)

[2.1.4 Network switching and WiFi 8](#_Toc55725232)

[2.1.5 Physical Servers 8](#_Toc55725233)

[2.1.6 Power backup 8](#_Toc55725234)

[2.1.7 End user devices 8](#_Toc55725235)

[2.1.8 Fixed line telephony 8](#_Toc55725236)

[2.1.9 Alarm system, access and egress. 8](#_Toc55725237)

[2.1.10 Data Backup 9](#_Toc55725238)

[2.1.11 Endpoint protection 9](#_Toc55725239)

[2.1.12 Collaboration suite 9](#_Toc55725240)

[2.1.13 System Management 9](#_Toc55725241)

[2.2 Financial Overview 9](#_Toc55725242)

[2.2.1 Fiscal review 9](#_Toc55725243)

[2.2.2 Nominal cost assessment 9](#_Toc55725244)

[3 Business Process & Recovery Criticality Ranking 10](#_Toc55725245)

[3.1 Determine Process and System Criticality 11](#_Toc55725246)

[3.1.1 Identify Outage Impacts and Estimated Downtime 12](#_Toc55725247)

[3.2 Identify Resource Requirements 15](#_Toc55725248)

[3.3 Identify Recovery Priorities for System Resources 16](#_Toc55725249)

[3.4 Identify Threats 17](#_Toc55725250)

[3.5 Calculate risks 18](#_Toc55725251)

[3.6 Identify backup solutions 19](#_Toc55725252)

[4 Additional Findings 19](#_Toc55725253)

[5 Action Plan 20](#_Toc55725254)

[6 Conclusion 21](#_Toc55725255)

[7 Supporting Information 22](#_Toc55725256)

[7.1 Accounts Department Questionnaires 23](#_Toc55725257)

[7.2 Architectural Questionnaires 26](#_Toc55725258)

[7.3 IT Questionnaires 29](#_Toc55725259)

[8 References 32](#_Toc55725260)

**Table of Tables**

[Table 1: DDP Architects Business Processes 11](#_Toc55725280)

[Table 2: Outage Impact Costs 12](#_Toc55725281)

[Table 3: Outage Impact Severity Rating 13](#_Toc55725282)

[Table 4: Business Process MTD, RTO and RPO Table 14](#_Toc55725283)

[Table 5: Company Resources 15](#_Toc55725284)

[Table 6: RTO Priority 16](#_Toc55725285)

[Table 7: Threat Identification Table 17](#_Toc55725286)

[Table 8: Threat Risk Score 18](#_Toc55725287)

[Table 9: Threat Contingency/Mitigation 19](#_Toc55725288)

[Table 10: Accounting Questionnaire – Accounts Payable 23](#_Toc55725289)

[Table 11: Accounting Questionnaire – Accounts Receivable 24](#_Toc55725290)

[Table 12: Accounting Questionnaire – Payroll 25](#_Toc55725291)

[Table 13: Architectural Questionnaire - Client Details 26](#_Toc55725292)

[Table 14: Architectural Questionnaire – Architectural/Project Drawings 27](#_Toc55725293)

[Table 15: Architectural Questionnaire – Project Correspondence 28](#_Toc55725294)

[Table 16: IT Questionnaire - Backups 29](#_Toc55725295)

[Table 17: IT Questionnaire - Hardware 30](#_Toc55725296)

[Table 18: IT Questionnaire - Software 31](#_Toc55725297)

**Table of Figures**

[Figure 1: IT System Architecture 7](#_Toc55725279)

# Executive Summary

This Business Impact Analysis (BIA) has been developed as part of the contingency planning process for DDP Architects*.* It was prepared on the 9th November 2020.

The scope of this analysis examined three primary functions of the company, namely the Architectural Services, IT supports within the company and the Accounting Department. The goal of this analysis was to identity the key services and infrastructure required to conduct each of these functions and the impact on the business if they were unavailable. The analysis was conducted using the following steps:

**Determine business processes and recovery criticality -** Business processes and their interdependencies were identified, and the impact of their disruption was determined together with outage impacts and estimated downtime involved. The downtime is the maximum time the organization can tolerate while still operating.

**Identify resource requirements -** To make realistic recovery plans, a thorough evaluation of the resources required to restore business processes as quickly as possible was completed.  Resources identified included personnel, hardware, software, data files and system components.

**Identify recovery priorities for system resources –** Based on the outcomes of the previous activities the critical resources were clearly identified. Priority levels were assigned which determined the order for recovering resources and business activities.

In preparing this report interviews were conducted with the head of each of the three main departments and a questionnaire completed for each of their three main business processes.

Disruption to each of these resources was assessed qualitatively based on the knowledge and experience of the Department Managers and the outage impact categorised from 1-4 in terms of severity.

The findings of this BIA document will be used in building the Business Continuity and Disaster Recovery (BCDR) Plan for the company.

# System Description

DDP Architects provide architectural services for a variety of commercial and residential projects. There are 24 staff currently employed who are all based at their office in Athlone, a single office premises over two floors. The business is one of several located in a small business park.

The general breakdown of staff consists of 5 Architectural teams each headed by a lead architect supervising 3 technicians, Accounts manager, IT Manager and 2 reception/accounts assistants.

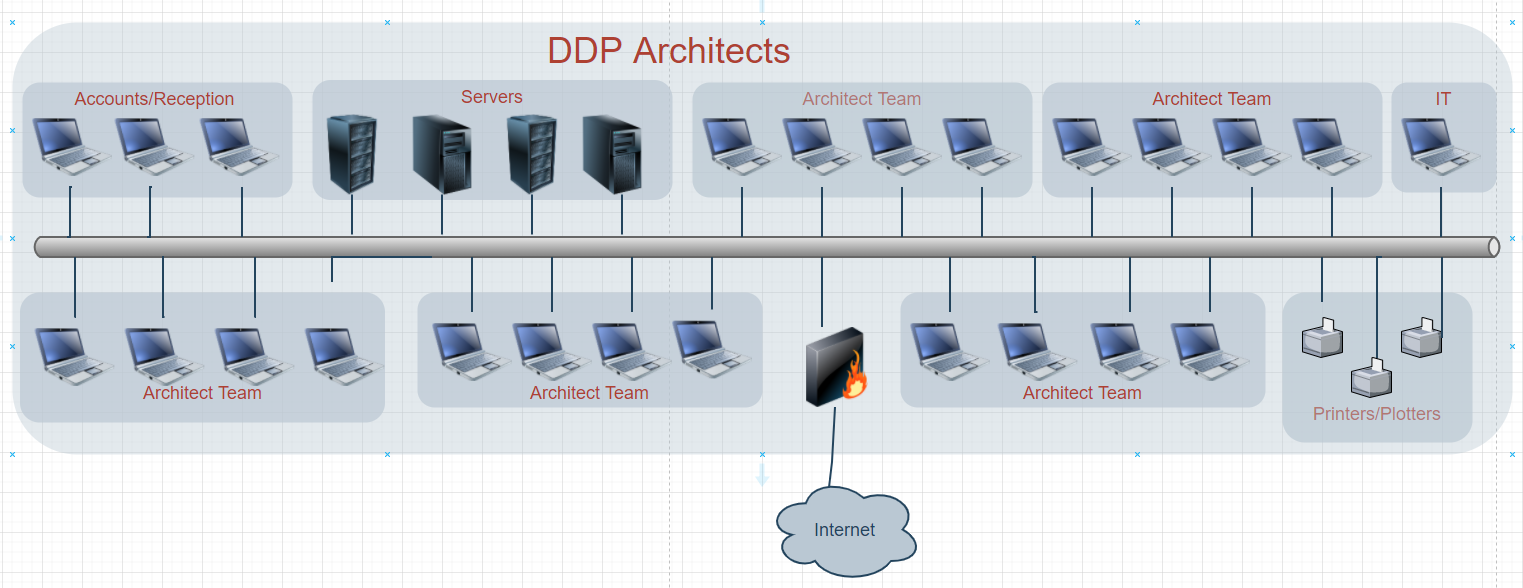


Figure 1: IT System Architecture

## System Overview

### Electrical system

The office premises has Cat6 structured cabling throughout. The comms cabinet is a 48U enclosed lockable rack securely housed in the electrical switch room. Power is three phase via a breaker from the landlord distribution board (MDB) to the sub distribution board (SDB). One phase is used for HVAC and the remaining two for small power and lighting with selectivity across both phases.

### HVAC & Fire Suppression

The HVAC system is controlled via a dedicated Building Management System (BMS) control panel situated in the electrical switch room. BMS sensors are hardwired to the BMS panel. Tenant controls are limited to thermostatic and timing adjustments. Maintenance by landlord via third party specialist.

Fire suppression is provided by a sprinkler system integrated in the building fabric (landlord domain). Tenant fire alarm panel (FAP) is situated adjacent to the BMS panel in the electrical switch room and is connected to the upstream landlord FAP via mineral insulated metal sheathed (MIMS) cable.

Carbon monoxide and smoke detection is integral to the fire suppression system.

### Internet connectivity

The primary Internet Service Provider (ISP), Eir provides a gigabit fibre FTTP connection, while a backup provider (Netcomm) providing a 50 Mbit fixed wireless access (FWA) connection for failover purposes.

The connections terminate on ISP supplied routers which are bridged to a Ubiquiti Unifi firewall appliance providing failover WAN connectivity.

### Network switching and WiFi

The core switch is a 48 port Ubiquiti Unifi PoE managed switch. There is an unused superseded Ubiquiti 24 port Edgeswitch mounted also. Ubiquiti Unifi WiFi access points are managed from a Ubiquiti controller on the core Switch.

### Physical Servers

Servers consist of a pair of Dell R620 rackmount units running Windows Server 2016 Hyper-V with Server 2016 VMs for Domain controller, software licensing services, payroll and finance, print server and file server.

A rackmount shelf holds a CCTV DVR.

### Power backup

A 5000VA UPS unit is rack mounted providing electrical supply to the active equipment.

### End user devices

Primary end user devices are a mix of laptops and high-performance workstations used for architectural modelling. All have company issue mobile phones. The firm has two Océ wide format plotter/scanners, alongside three departmental multifunction printers.

### Fixed line telephony

Fixed line telephony is provided on contract through a VoIP service provider via a managed cloud based PABX with 3 incoming lines configured in a hunt group. VoIP desk phones are provided.

### Alarm system, access and egress.

The burglar alarm system is connected to the monitoring centre via a dedicated analogue telephone line. A separate GSM module is fitted to the alarm system for failover. A second analogue line supports the lift emergency communication requirement. Disabled refuge is connected to the LAN via the primary switch.

### Data Backup

Periodic backup of the on-premises server file shares is provided by Backup-as-a-Service (BaaS) provider Saveitall.ie via backup agent software. Fileserver shares are backed up on a 4-hour window with a GFS (full/differential/incremental) scheme. Backups are retained for 3 years.

Email and online data in OneDrive and Sharepoint is backed up via a Spanning Backup cloud service subscription. This is a snapshot backup taken daily at 0100 hours GMT. Backups are held indefinitely.

### Endpoint protection

Endpoint protection is provided by Webroot on all end user and server devices and centrally managed in the cloud.

### Collaboration suite

The email and productivity suite is Microsoft 365 Business Standard (formerly Office 365).

### System Management

DDP Architects employs an IT manager who has overall responsibility for the day to day maintenance of IT and communications systems, servers, software, backup and end user support.

## Financial Overview

### Fiscal review

A financial review was conducted to assess the cost of potential downtime. The overall figures were as follows:

* Annual turnover: €2.5m
* Profit last fiscal year: €203,600
* Nominal operational cost: €10,000/working day. (staff x 24, utilities and overheads)
* Nominal cost of downtime => €10k divided by 8 hours = €1,250 hour approx.

### Nominal cost assessment

For the purposes of this BIA document, the organisation has settled on a figure of €1,250 per hour of downtime for failure which prevents normal business operations across all business areas.

# Business Process & Recovery Criticality Ranking

Analysing the data collected from interview questionnaires with the department heads showed that each depended on the Information System/Information Technology (IS/IT) infrastructure.

IS/IT was identified as critical to the operation of all other resources. This interdependency prioritises the recovery of the IS/IT infrastructure first and only by doing so can other business processes be brought back online.

## Determine Process and System Criticality

The key processes identified in the operation of DDP Architects, together with a brief description of what each entails, are outlined in the table below.

Table 1: DDP Architects Business Processes

| **Business Process** | **Description** |
| --- | --- |
| *Accounts Payable* | *The ledger management of all amounts owed to external vendors and suppliers – entering invoices, issuing payment and payment confirmation* |
| *Accounts Receivable* | *The ledger management of all amounts owing to company by clients – calculating invoice using employee timesheets, resources used and professional fees per contract* |
| *Payroll* | *Payment of junior employees on a fortnightly basis and managers/senior employees on a monthly basis.* |
| *Project Management* | *The recording of client name, contact phone number and email address, project location, contractor details and any relevant project notes* |
| *Project Architectural /Engineering Drawings* | *The detailed project drawings including measurements & co-ordinates* |
| *Project Correspondence* | *Correspondence relating to the project including initial consultation notes, contract, planning authority correspondence, correspondence from outside agencies, contractors, suppliers etc* |
| *Information Systems (IS/IT)* | *Systems administration, backup, compliance, IT security, IT service management, end user support and associated activities.* |
| *Hardware asset management* | *Lifecycle asset management of IT hardware assets.* |
| *Software asset management* | *Lifecycle asset management of software assets across the organisation.* |
| *Sales and marketing* | *Sales and marketing. Management of bids, proposals and quotations by the Business Development Team.* |
| *HR & Recruitment* | *Management of HR & recruitment activities, retention & incentives, CPD & training.* |

### Identify Outage Impacts and Estimated Downtime

DDP Architects has examined all aspects of the business processes to identify the potential impacts of an outage from a localised failure affecting a single end user to possible regional, national and even global events. This approach seeks to quantify and cost the impacts from minor to critical in broad terms.

#### **Outage Impacts**

In categorising the impact on the business due to an outage we assess the damage under 4 headings:

* Critical
* Vital
* Important
* Minor

The costs associated with each are calculated in terms of the impact on staffing, financial penalties, and losses. The table below illustrates how each of these break down and the maximum financial impact to the company.

Table 2: Outage Impact Costs

|  |  |  |
| --- | --- | --- |
| **Category** | **Impact** | **Financial Cost** |
| Critical | Staff overtime, Temporary Staffing, Contractual Penalties, Company reputation, supplies | >€100,000 |
| Vital | Staff overtime, Contractual Penalties, supplies | €10,001-€99,999 |
| Important | Staff overtime, supplies | €1,001 - €10,000 |
| Minor | Supplies | <€1,000 |

The table below determines the impact severity of an outage on the business process if unavailable for a given period of time.

Table 3: Outage Impact Severity Rating

| **Business Process** | **1 0-1 day** | **2 2-4 days** | **3** **5-10 Days** | **4** **>2 wks** | **Impact** |
| --- | --- | --- | --- | --- | --- |
| Accounts Payable |  |  | **X** |  | **Minor** |
| Accounts Receivable |  |  | **X** |  | **Minor** |
| Payroll |  | **X** |  |  | **Vital** |
| Project Management | **X** |  |  |  | **Critical** |
| Project Architectural /Engineering Drawings | **X** |  |  |  | **Critical** |
| Project Correspondence | **X** |  |  |  | **Critical** |
| Information Systems (IS/IT) incl. Backups | **X** |  |  |  | **Critical** |
| Hardware asset management |  |  | **X** |  | **Important** |
| Software Asset Management | **X** |  |  |  | **Critical** |
| Sales and marketing |  |  | **X** |  | **Minor** |
| HR & Recruitment |  |  |  | **X** | **Minor** |

#### **Estimated Downtime**

Working directly with business management and staff, estimate the downtime factors for consideration because of a disruptive event.

* **Maximum Tolerable Downtime (MTD).**  This is the total amount of time management is willing to accept for a business process outage or disruption and includes all impact considerations. MTD is important for continuity planners in the selection of (1) appropriate recovery methods, and (2) the level of detail required to develop recovery procedures, including their scope and content.
* **Recovery Time Objective (RTO).** This is the maximum amount of time that a system resource can remain inoperable before there is serious impact on any other system resource, supported business process, or the MTD. The determination of the information system resource RTO is necessary for the selection of appropriate technologies best suited for achieving the MTD.
* **Recovery Point Objective (RPO).** The point in time before disruption or system outage, to where the business process data must be restored (using the most recent backup copy of data) after the disruption. The measure of time for how often backups need to be performed.

The table below identifies the MTD, RTO, and RPO for the critical business processes identified by the Department Managers during interviews.

Table 4: Business Process MTD, RTO and RPO Table

| **Business Process** | **MTD** | **RTO** | **RPO** |
| --- | --- | --- | --- |
| *Accounts Payable - Pay vendor invoice* | *72 hours* | *168 hours* | *12 hours (last backup)* |
| *Accounts Receivable - Issue Client Invoice* | *48 hours* | *120 hours* | *12 hours (last backup)* |
| *Payroll* | *48 hours* | *72 hours* | *12 hours (last backup)* |
| *Project Management* | *5 hours* | *24 hours* | *4 hours (last backup)* |
| Project Architectural/Engineering Drawings | *5 hours* | *24 hours* | *4 hours (last backup)* |
| *Project Correspondence* | *5 hours* | *24 hours* | *4 hours (last backup)* |
| *Backups (file shares or VMs)* | *4 hours* | *24 hours* | *4 hours (last backup)* |
| *Hardware Asset Management* | *72 hours* | *168 hours* | *24 hours* |
| *Software Asset Management* | *24 hours* | *24 hours* | *24 hours* |

**Objectives**

With regard to MTD, RTO and RPO the timeframe will be determined by the nature of the specific failure or incident. In all cases the objective will be to achieve the minimum possible downtime by ensuring internal procedures and resources are applied in accordance with the proposed business continuity and disaster recovery plan. Where outages are the result of circumstances beyond the control of the organisation such as regional or national events, the objective will be to position the organisation to recover as soon as possible after civic services/utilities are restored.

## Identify Resource Requirements

The table below is a list of the company resources essential to the operation of DDP Architects and the business processes identified in 3.1.

Table 5: Company Resources

|  |  |  |
| --- | --- | --- |
| **System Resource/Component** | **Platform/OS/Version (as applicable)** | **Description** |
| Hardware | | |
| Cabinet | Netshelter | 48U 600mm Wide x 1070mm deep enclosure, sheet steel sides, perforated steel doors, lockable. |
| ISP Router, Eir | Eir F2000 | ISP supplied router, primary connection |
| ISP Router, Netcomm | Draytek | ISP supplied router, secondary connection |
| UPS | American Power Conversion | 5000VA In line single phase UPS, supports active equipment in cabinet. |
| PDU | MK | 8 way rackmount PDU, 2 No. |
| Firewall/Gateway | Ubiquiti Unifi USG Pro | LAN gateway and firewall |
| Switch, 48 port | Ubiquiti Unifi USW-48-PoE | Core network switch, managed, PoE |
| Switch, 24 port | Ubiquiti Edgeswitch 24 | Spare switch, unused |
| WiFi Conntroller | Ubiquiti Cloud Key | PoE WiFi network controller, main switch |
| CCTV DVR | Hikvision | CCTV DVR |
| Physical Server | Dell R620 | Virtualisation Server (Hyper-V), 2 No. |
|  |  |  |
| PC Workstation | HP EliteDesk | Design workstation, 5 No. |
| PC Workstation | Dell Precision 3630 | Design workstation, 2 No. |
| PC Workstation | HP EliteDesk 400 mini | Reception PC |
| Laptop | HP ZBook 15 | Design Laptop, 4 No. |
| Laptop | HP Elitebook 840 G3 | Spare laptop, 3 No. |
| Laptop | HP Elitebook 840 G5 | Staff laptop, 8 No. |
| Laptop | HP Elitebook 840 G7 | Staff laptop, 5 No. |
|  |  |  |
| Canon Plotter | Prograf TX Series | Wide format plotter, 2 No. |
| Workgroup printer | Konica Minolta MFP | Workgroup printer, 3 No. |
| Non hardware | | |
| Virtual server 1 of 4 | Windows Server 2016 | Active directory domain controller, Radius server, Azure AD connect endpoint. |
| Virtual server 2 of 4 | Windows Server 2016 | License server for AutoDesk products |
| Virtual server 3 of 4 | Windows Server 2016 | Sage accounts and payroll server |
| Virtual server 4 of 4 | Windows Server 2016 | File and print services |
|  |  |  |

## Identify Recovery Priorities for System Resources

In restoring business operations the following key resources are listed in order of priority and the Recovery Time Objective (time before their disruption has a significant impact on the business) is given.

Table 6: RTO Priority

| **Priority** | **System Resource/Component** | **Recovery Time Objective (RTO)** |
| --- | --- | --- |
| Mains Electrical Supply | Power | 30 mins |
| Internet connectivity | Communications | 1 hour |
| Virtual Server | Computing | 4 hours |
| ISP Router | Communications | 1 Day |
| Firewall/Gateway | Communications/Network | 1 Day (No alternate, long lead times) |
| Switch, 48 port | Network | 1 Day (No alternate, long lead times) |
| Physical Server | Computing | 1 Day |
| UPS | Power | 5 Days |
| PDU | Power | 5 Days |
| PDU | Power | 5 Days |
| WiFi Conntroller | Network | 5 Days |
| PC Workstation | Computing | 5 Days |
| Laptop | Computing | 5 Days |
| Plotter | Computing | 14 Days |
| Workgroup Printer | Computing | 14 Days |
| CCTV DVR | Security | 14 Days |
| Switch, 24 port (spare) | Network | 14 Days |

## Identify Threats

Table 7: Threat Identification Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat/Risk** | **Likelihood** | **Criticality (RTO)** | **Consequence of Occurrence** |
| Utility Outage - Electrical | Low | 1 hour | Moderate to High |
| Utility Outage - Internet | Low | 1 hour | Moderate (loss of primary) to High (loss of primary & secondary) |
| Utility Outage - Water | Low | 4 hours | Low to Moderate |
| Failure, HVAC | Low | Varies | Low to Moderate |
| Failure, Fire suppression | Low | 0 Hours | High |
| Failure, Telephone system | Low | 24 Hours | Low to Moderate |
| Failure, Firewall/Gateway | Low | 1 hour | High (replacement has long lead time) |
| Failure, Core Switch | Low | 1 Hour | High (replacement has long lead time) |
| Failure, Physical Server | Low | 2 Hours | High (NBDOS Warranty in effect) |
| Failure, PC/Laptop | Low | 3 Days | Low, considered expendable |
| Loss, Virtual server | Low | 1 hour | Medium, restore backup |
| Data Breach/Cyber Attack | Medium | 4 hours | Moderate to High depending on nature and scope of attack/breach |
| Damage to Premises, Accidental or Intentional | Low | ?? | Low to High depending on the nature and scope of the incident. |
| Pandemic | Low | ?? | Low to moderate |
| Disruption to Supply Chain | Medium | Hours to days | Low to High depending on vector |
| Employee Disputes | Low | ?? | Low to moderate |
| Natural Disasters/Extreme weather events | Low | Hours to days | Low to Moderate |
|  |  |  |  |

## Calculate risks

Risk is calculated in terms of the Probability of an Occurrence (PO) and the Business Impact (BI) that would have.

Probability of Occurrence (PO) is the number of estimated occurrences in a year ranging from 1 (low) to 10 (high).

Business Impact is the measure of how the business would be affected by a process or system failure. That impact can be either:

* **Quantitative** – estimates based on revenue streams and known costs
* **Qualitive** – estimates based on the knowledge of employees or consultants

Business Impact is measured on a scale of 1 (low) to 10 (high) where 10 represents the business ceasing to exist.

Table 8: Threat Risk Score

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat/Risk** | **Probability of occurrence (PO)** | **Business Impact (BI)** | **Risk Score** |
| Utility Outage - Electrical | 2 | 9 | 18 |
| Utility Outage - Internet | 3 | 9 | 27 |
| Utility Outage - Water | 2 | 3 | 3 |
| Failure, HVAC | 2 | 2 | 4 |
| Failure, Fire suppression | 2 | 8 | 16 |
| Failure, Telephone system | 2 | 3 | 6 |
| Failure, Firewall/Gateway | 2 | 4 | 8 |
| Failure, Core Switch | 3 | 6 | 18 |
| Failure, Physical Server | 2 | 6 | 18 |
| Failure, PC/Laptop | 2 | 2 | 4 |
| Loss, Virtual server | 3 | 8 | 24 |
| Data Breach/Cyber Attack | 5 | 5 | 25 |
| Damage to Premises, Accidental or Intentional | 2 | 3 | 6 |
| Pandemic | 2 | 4 | 8 |
| Disruption to Supply Chain | 3 | 5 | 15 |
| Employee Disputes | 2 | 2 | 4 |
| Natural Disasters/Extreme weather events | 3 | 4 | 12 |

## Identify backup solutions

Table 9: Threat Contingency/Mitigation

|  |  |
| --- | --- |
| **Threat/Risk** | **Contingency/Mitigation Action** |
| Utility Outage - Electrical | Subject to nature and duration, UPS for short duration <=30 mins, primary equipment only. Potential for generator hire to ensure key functions in prolonged outage. Look at generator procurement. |
| Utility Outage - Internet | Existing failover in situ, cannot mitigate regional/national outage. |
| Utility Outage - Water | Escalate via Landlord and Local Authority/Irish water contacts as necessary. Determine severity and ETA for restoration. |
| Failure, HVAC | Escalate via Landlord & service company contacts as required. ETA for restoration. |
| Failure, Fire suppression | Activate fire drill immediately. Escalate via Landlord and service company contacts as required. |
| Failure, Telephone system | Mobile phones. Escalate to service company |
| Failure, Firewall/Gateway | Use ISP modem as temporary gateway, Procure replacement or alternative firewall as a standby. |
| Failure, Core Switch | Needs a hot spare online, existing spare is 24 port non PoE unmanaged. New spare 48 port PoE to be purchased |
| Failure, Physical Server | Move VM if possible, Escalate under NBDOS warranty |
| Failure, PC/Laptop | Swap out with spare pending replacement |
| Loss, Virtual server | Restore from backup |
| Data Breach/Cyber Attack | Drop internet connectivity, assess & remediate |
| Damage to Premises, Accidental or Intentional | Subject to nature of damage. Advise landlord. Have contacts for repair services to hand. Engage builder to provide emergency remediation. |
| Pandemic | Test remote working procedures annually, move suitable services to cloud if possible. |
| Disruption to Supply Chain | Subject to nature of disruption, alternate supplier from approved suppliers list. Procure directly online. |
| Employee Disputes | Per company policy, escalate via HR, engage industry/statutory bodies as necessary. |
| Natural Disasters/Extreme weather events | Subject to severity. Advise employees in line with Govt. guidelines (Red warning = shelter in place/evacuate premises or stay at home mandate). |

# Additional Findings

DDP Architects has identified the need to draw up a formal incident response and disaster recovery plan and train staff members accordingly.

Cyber-attack/ransomware protection needs to be reviewed and documented.

# Action Plan

Analysis shows that the most significant predictable threats accrue from utility provider outages, notably power and communications.

**Power:** Cost/benefit analysis previously undertaken determined that the company would not see a return on the purchase of a generator owing to the infrequency and duration of outages which typically correlate to storm events. The existing UPS provision is deemed adequate.

**Communications:** There is a failover broadband connection in situ. Resilience could be further improved by a third connection option such as a 4G connection for emergency use. This option is to be costed within three months.

**CIRT:** DDP Architects has identified the need to formally nominate a Critical Incident Response Team (CIRT) to deal with critical outages. Team leaders will be the Director of Operations and the IT Manager. Each department lead will identify and triage their specific requirements and escalate to Director of Operations. The incident response team will be formalised at the next quarterly business review meeting.

A business continuity vulnerability has been identified in that there is no failover for the firewall and core switch infrastructure. The IT Department will address this deficiency, effective immediately.

The existing backup and restore procedures have been identified as a concern. There are three separate backup providers. The organisation will look to consolidate and streamline this situation within 12 months.

DDP Architects has decided to draft a formal incident response and disaster recovery plan and train staff members accordingly.

# Conclusion

DDP Architects has found room for improvement in systems, procedures and processes. Fiscal analysis shows that a significant outage will cost in the order of €1,250/hour. In addition, there is potential for:

* Delayed sales income.
* Activation of penalty clauses in contracts.
* Damage to the DDP brand reputation.
* Customer dissatisfaction.
* Loss of new or repeat business.
* Knock on impacts on other business processes

To better mitigate these risks, some steps have already been taken in line with actions identified in section 5.

DDP Architects will, within six months, develop a full Business Continuity and Disaster Recover (BCDR) plan utilising both internal and external resources.

# Supporting Information

This section contains the completed BIA Questionnaire for each business function.

## Accounts Department Questionnaires

Table 10: Accounting Questionnaire – Accounts Payable

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | Accounts | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Accounts Payable | | |
| **Process Description** | The ledger management of all amounts owed to external vendors and suppliers | | |
| **Process Participants** | Claudia McDonnell – Department Manager | | |
| **Process/Data Inputs**  *(who provides info to the process)* | Invoices are entered into the system upon receipt and allocated an automatic system reference number which is noted on the paper copy by team member Ann Marie | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | The Department manager oversees the Accounts Payable Ledger  countersigning payment authorisation with the General Manager monthly before payments are issued by Ann Marie | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | *Define in hours/days and provide explanation for the answer*  Due to the volume of items to be entered monthly the maximum down time for this process would be 1 week | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | SAGE Accounting | 2/3 Days |
| **Equipment** | | PC/Laptop, Backup Server |  |
| **Data** | | Last Saved Daily Backup |  |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A |  |
| **Paper/client records**  Client related documents not stored electronically | | Paper copies of the invoices if digital copy not available |  |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Username/Password for SAGE login |  |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A |  |
| **Critical Vendors/Service Providers** | | SAGE Accounting |  |
| **Physical Workspace** | | Terminal or laptop access to server |  |
| **Work from Home Capabilities** | | VPN connection to Server |  |

Table 11: Accounting Questionnaire – Accounts Receivable

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | Accounts | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Accounts Receivable | | |
| **Process Description** | The ledger of all amounts owing to company by clients | | |
| **Process Participants** | Claudia McDonnell – Department Manager | | |
| **Process/Data Inputs**  *(who provides info to the process)* | Invoices are calculated using timesheets, resources used and professional fees per contract by team member Paula and entered into the system where they assigned an automatic reference number | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | The Department manager oversees the Accounts Receivable Ledger  checking invoices with the relevant Project Manager for the job on a daily basis before invoices are issued to the client | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | *Define in hours/days and provide explanation for the answer*  Due to the necessity for accurate and timely billing the maximum down time would be 2 days | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | SAGE Accounting | 1/2 Days |
| **Equipment** | | PC/Laptop, Backup Server |  |
| **Data** | | Last Saved Daily Backup |  |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A |  |
| **Paper/client records**  Client related documents not stored electronically | | Any diary notes for meetings, resources used, and contract details |  |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Username/Password for SAGE login |  |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A |  |
| **Critical Vendors/Service Providers** | | SAGE Accounting |  |
| **Physical Workspace** | | Terminal or laptop access to server |  |
| **Work from Home Capabilities** | | VPN connection to Server |  |

Table 12: Accounting Questionnaire – Payroll

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | Accounts | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Payroll | | |
| **Process Description** | Payment of employees on a fortnightly and monthly basis | | |
| **Process Participants** | Claudia McDonnell – Department Manager | | |
| **Process/Data Inputs**  *(who provides info to the process)* | Payments are made to junior employees on a fortnightly basis and senior employees/managers monthly by calculating basic pay, holiday pay, overtime, bonus etc. | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | Payroll calculations and payments are made by team member Paula, overseen and signed off on by Department Manager. This information is also reported to Revenue via ROS 2 days before payments are made. | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | *Define in hours/days and provide explanation for the answer*  Due to the necessity for accurate and timely payment of employees the maximum downtime is 2 days | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | Thesaurus Payroll Manager | 1/2 Days |
| **Equipment** | | PC/Laptop, Backup Server |  |
| **Data** | | Last Saved Daily Backup |  |
| **Desktop-related**  Items such as digital certificates for e-filing | | ROS Digital Certificate |  |
| **Paper/client records**  Client related documents not stored electronically | | Dairy entries for holidays/ overtime |  |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Username/Password for login to Thesaurus Payroll Manager |  |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | ROS Digital Certificate  Bank Login |  |
| **Critical Vendors/Service Providers** | | Thesaurus Payroll Manger |  |
| **Physical Workspace** | | Terminal or laptop access to server |  |
| **Work from Home Capabilities** | | VPN connection to Server |  |

## Architectural Questionnaires

Table 13: Architectural Questionnaire - Client Details

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | Architectural | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Project Management | | |
| **Process Description** | The recording of client name, contact phone number and email address, project location, contractor details and any relevant project notes | | |
| **Process Participants** | Patrick Wynne – Architect | | |
| **Process/Data Inputs**  *(who provides info to the process)* | Project Manager or appointed member of the design team | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | The lead Architect for the project and their design team of CAD technicians, engineers and surveyors | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | *Define in hours/days and provide explanation for the answer*  Due to the sensitive nature of data the maximum down time for access to client details is 4/5 hours | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | Streamline Project Management | 4/5 Hours |
| **Equipment** | | PC/Laptop, Backup Server |  |
| **Data** | | Last Saved Daily Backup |  |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A |  |
| **Paper/client records**  Client related documents not stored electronically | | Paper copies of initial contact form |  |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Username/Password for Streamline |  |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A |  |
| **Critical Vendors/Service Providers** | | Streamline |  |
| **Physical Workspace** | | Terminal or laptop access to server |  |
| **Work from Home Capabilities** | | VPN connection to Server |  |

Table 14: Architectural Questionnaire – Architectural/Project Drawings

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | Architectural | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Project Architectural/Engineering Drawings | | |
| **Process Description** | The detailed project drawings including measurements & co-ordinates | | |
| **Process Participants** | Patrick Wynne – Architect | | |
| **Process/Data Inputs**  *(who provides info to the process)* | Project Manager or members of the design team CAD technicians, engineers or surveyors | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | The lead Architect for the project and their design team of CAD technicians, engineers or surveyors, external contractors and planning authority | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | *Define in hours/days and provide explanation for the answer*  Due to the critical nature of data the maximum down time for access to client details is 4/5 hours | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | CAD Software | 4/5 Hours |
| **Equipment** | | PC/Laptop, Backup Server | 3 Days |
| **Data** | | Last Saved Daily Backup | 4 Hours |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A | N/A |
| **Paper/client records**  Client related documents not stored electronically | | Measurements or notes from design team |  |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Username/Password for CAD |  |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A |  |
| **Critical Vendors/Service Providers** | | AutoDesk | 4 Hours |
| **Physical Workspace** | | Terminal or laptop access to server, Plotter for printing | 3 Days |
| **Work from Home Capabilities** | | VPN connection to Server | 4 Hours |

Table 15: Architectural Questionnaire – Project Correspondence

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | Architectural | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Project Correspondence | | |
| **Process Description** | Correspondence relating to the project including initial consultation notes, contract, planning authority correspondence, correspondence from outside agencies, contractors, suppliers etc | | |
| **Process Participants** | Patrick Wynne – Architect | | |
| **Process/Data Inputs**  *(who provides info to the process)* | Project Manager or members of the design team CAD technicians, engineers or surveyors, Planning authority, outside agencies, contractors and suppliers | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | The lead Architect for the project and their design team of CAD technicians, engineers or surveyors | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | Due to the critical nature of data the maximum down time for access to client details is 4/5 hours | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | Streamline Project Management | 4/5 Hours |
| **Equipment** | | PC/Laptop, Backup Server, Scanner |  |
| **Data** | | Last Saved Daily Backup |  |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A |  |
| **Paper/client records**  Client related documents not stored electronically | | Planning Application Docs, Planning authority correspondence |  |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Streamline username/password |  |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | Scanner |  |
| **Critical Vendors/Service Providers** | | Streamline |  |
| **Physical Workspace** | | Scanner to scan paper documents to digital project folder, PC/Laptop, Server |  |
| **Work from Home Capabilities** | | VPN connection to Server |  |

## IT Questionnaires

Table 16: IT Questionnaire - Backups

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | IT Department | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Backup and restore process | | |
| **Process Description** | The saving, storage and availability of all digital information | | |
| **Process Participants** | Mick McGovern – IT Manager | | |
| **Process/Data Inputs**  *(who provides info to the process)* | The IT Manager | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | All users with electronic access to any of the company systems | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | As all users and all activities of the company are reliant on access to the servers it is critical to restore services within 1-2 hours. | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | Veeam Backup  Veeam backup agent  Spanning Backup | <4 Hours |
| **Equipment** | | Physical server/VM | <4 Hours |
| **Data** | | Portal login credentials | <1 Hour |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A | N/A |
| **Paper/client records**  Client related documents not stored electronically | | N/A | N/A |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | Backup and Recovery procedure for Veeam.  Logins credentials for online management portals. | <1 Hour |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A | N/A |
| **Critical Vendors/Service Providers** | | Veeam | N/A |
| **Physical Workspace** | | Server Room Access | <1 Hour |
| **Work from Home Capabilities** | | VPN link | <1 Hour |

Table 17: IT Questionnaire - Hardware

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | IT Department | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Hardware Management | | |
| **Process Description** | Procurement, lifecycle maintenance and disposal of IT hardware assets | | |
| **Process Participants** | Mick McGovern – IT Manager | | |
| **Process/Data Inputs**  *(who provides info to the process)* | End users, Department heads, IT Manager. | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | IT Department | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | Low to moderate. Servers covered under Next Business Day on Site (NBDOS) warranties. Physical servers are available off the shelf from major vendors and resellers. Commodity hardware available next business day from multiple suppliers. IT Manager has overall ownership of and responsibility for this process. | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | N/A | N/A |
| **Equipment** | | Laptop | N/A |
| **Data** | | Internet connection | N/A |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A | N/A |
| **Paper/client records**  Client related documents not stored electronically | | N/A | N/A |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | N/A | N/A |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A | N/A |
| **Critical Vendors/Service Providers** | | HP (direct), Dell (direct), Ubiquiti (reseller), Canon and Konica Minolta (Print supplier). | N/A |
| **Physical Workspace** | | N/A | N/A |
| **Work from Home Capabilities** | | N/A | N/A |

Table 18: IT Questionnaire - Software

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact Analysis Survey** | | | |
| **Department Name** | IT | | |
| **Your Name** | Pauline Finlay | | |
| **Define the Business Function/Process** | | | |
| **Process/Function Name** | Software Asset Management | | |
| **Process Description** | Software Asset Management (SAM) | | |
| **Process Participants** | Mick McGovern – IT Manager | | |
| **Process/Data Inputs**  *(who provides info to the process)* | All staff, AutoDesk, Veeam. | | |
| **Recipients of Data/Process Output** *(who uses what is produced by the process)* | All staff. | | |
| **Process Criticality**  *How long can the Firm go without this process during a disaster?* | High. SAM ensures SaaS license renewals prior to subscription expiry. Expired software licenses for AutoDesk immediately locks out users and prevents access to design/modelling functions. Microsoft Office, Bluebeam PDF, and others require a live subscription to function. | | |
| **Supporting Requirements**  *What you need to complete the process, even during an emergency* | | | |
|  | | **Name**  (Be Specific) | **Desired Recovery Time**  (Hours/Days) |
| **Applications** | | AutoDesk AEC Suite  Microsoft 365  LAN Sweeper  Veeam | 1 Hour |
| **Equipment** | | Laptop | 4 Hours |
| **Data** | | Logins for service provider online portals. | <1 Hour |
| **Desktop-related**  Items such as digital certificates for e-filing | | N/A | N/A |
| **Paper/client records**  Client related documents not stored electronically | | N/A | N/A |
| **Forms or Documents**  Filing forms, passwords, cheat sheets, procedure manuals | | N/A | N/A |
| **Special Supplies**  Items such as security/key fob tokens for banking or efiling | | N/A | N/A |
| **Critical Vendors/Service Providers** | | AutoDesk, Microsoft, LAN Sweeper, Veeam |  |
| **Physical Workspace** | | N/A | N/A |
| **Work from Home Capabilities** | | N/A | N/A |

# References

BCMMETRICS. 2020. What Goes Into A Business Impact Analysis (BIA) Report?. [ONLINE] Available at: https://bcmmetrics.com/what-goes-into-business-impact-analysis-report/. [Accessed 03 November 2020].

CSRC | NIST. 2020. SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC. [ONLINE] Available at: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final. [Accessed 03 November 2020].

Ilta.personifycloud.com. 2020. [ONLINE] Available at: http://ilta.personifycloud.com/webfiles/productfiles/1367/BIAHomeSurvey.pdf. [Accessed 03 November 2020].