-Placeholder for Company Logo-

-Dental Equipment Supplies Example-

«Business Continuity Plan»

Version 01

-12 Jan 2010-

enisa
European Network
and Information
Security Agency

Part of the deliverable IT Business Continuity Management “An Approach for SMEs”

© European Network and Information Security Agency (ENISA), 2010

Document Information

Approval

Version	Approval Authority #1	Approval Authority #2
1.0	Company Owner	

Document Owner

Position	Title	Department	Date Assigned
Technician1	-Insert Owner's Corporate Title e.g. Business Continuity Manager-	-Insert the department that the owner is assigned to- e.g. Business Continuity Planning Unit, Environmental Services Department	5/10/2009

Document History

Version	Date	Reason / Description of Change	Page	Comments
1.0	12-01-2010	First release of company BCP		Checked and approved

Document Distribution List

Guideline:*-A Letter from the CEO demonstrating management support for the Business Continuity Plan (BCP) should be included in the distribution of the plan. Management commitment to the safety and protection of employees and the public should be reflected in this section.*

Copy No	Department / Unit	Responsible Party /
BCP1	**- Expedited Service Contract Fulfillment -**	**Technician1**
BCP2	**- Customer Relationship Management -**	**Company Owner**
BCP3	**-Finance-**	**Company Owner**
BCP4		
BCP5		

Incident Control & Handling

In case of an incident detection the organization should be able to respond rapidly by gaining the control (management) of the incident, thus preventing it from escalating to a disaster.

Incidents can be divided into two distinct categories: (a) life-threatening incidents and (b) non life-threatening incidents. When an incident is detected, it has to be evaluated and classified to identify the appropriate response. If the incident is a life-threatening one, responsible parties must execute the corresponding emergency procedures (see Annex C- Emergency Procedures).

A non life-threatening incident may affect several parts of an organization. Information technology and telecommunication assets, as an example, can suffer interruption, loss or destruction.

According to the incident type, different skills, expertise and practices need to be applied for an effective response:

- Life threatening incidents require emergency procedures (e.g. evacuation, firefighting, etc.) and usually involvement of the emergency services.
- Non-life threatening events related to IT and telecommunication require IT expertise and incident response tools, as well evidence collection and assessment capability.
- Non-life threatening events not related to IT require deep knowledge of the core business of the company and senior management skills to respond and manage the incident.

Regardless of the event type, investigation may reveal that the incident has seriously disrupted the organization’s critical business functions, leading thus to an unavailability of organization’s business.

In this case, the event should be escalated to a “Business Continuity Incident” triggering numerous actions from the available Business Continuity Plan. Following this, the organization’s business continuity team takes over the control of the incident which will be handled in accordance with the Business Continuity Plan.

This is the only way the organization can respond timely and recover from or avoid loss of availability. Therefore, escalations are a crucial part of the BCM process. The person responsible for assessing the criticality of an incident and escalating to a BCM incident needs to keep in mind the recovery priorities of the critical business functions.

These recovery priorities are available in the scope section of this document. Evaluation of the ability to meet the critical business functions recovery priorities using standard incident response and management practices will determine the need for activation of the Business Continuity Plan.

The following diagram describes an incident’s timeline with a possible escalation to a “business continuity incident”.

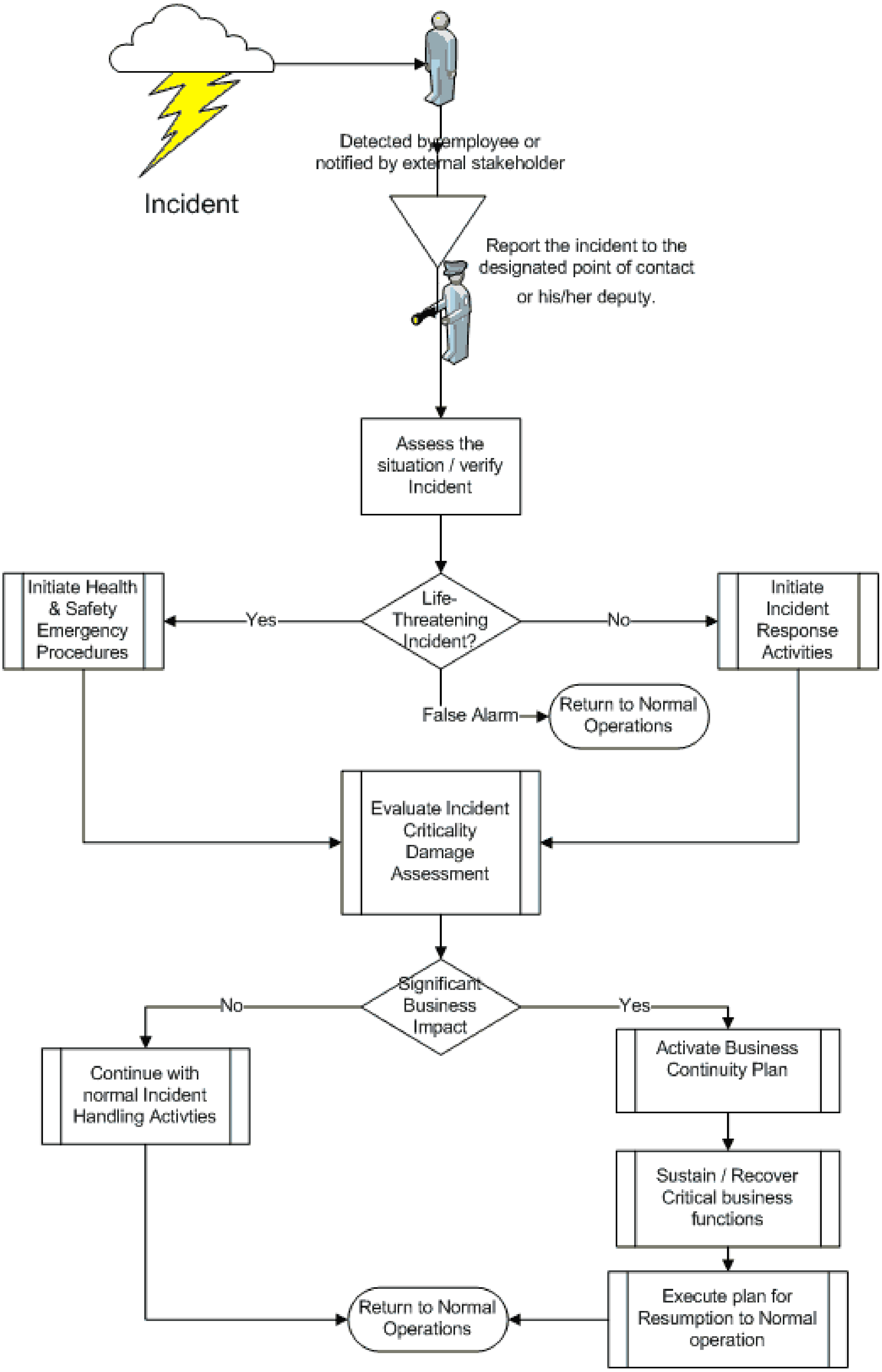

Incident
Detected by employee or notified by external stakeholder
Report the incident to the designated point of contact or his/her deputy.
Assess the situation / verify Incident
Life-Threatening Incident?
Yes
No
Initiate Health & Safety Emergency Procedures
Initiate Incident Response Activities
False Alarm
Return to Normal Operations
Evaluate Incident Criticality Damage Assessment
Significant Business Impact
No
Yes
Continue with normal Incident Handling Activties
Activate Business Continuity Plan
Sustain / Recover Critical business functions
Execute plan for Resumption to Normal operation
Return to Normal Operations

Figure 1: Incident Control & Handling

© European Network and Information Security Agency (ENISA), 2010

Contents

1. Introduction

1.1 Purpose

Purpose of the Business Continuity Plan (BCP) is to prepare– Dental Equipment Supplies - to cope with the effects of an emergency. The objectives of the BCP are:

- To define and prioritize the Critical Functions of the business minimizing the organizational impact from their interruption
- To address the emergency risks to the business in the case the first are realized
- To detail the agreed response of the – Dental Equipment Supplies - to an emergency
- To identify Key Contacts during an emergency

1.2 Scope and Critical business Functions recovery Priority

The – Dental Equipment Supplies - BCP ensures the continuity of the business critical function(s) described in Table 1[1], protecting the customer base business products and / or services.

Critical Business Function Identification – Business Continuity Plan Scope		
Critical Business Function	**Rationale for Selection**	**Recovery Priority (High, Medium, Low)**
Production / Expedited service contracts fulfilment	Provide expedited equipment repair to customers that have purchased the expedited repair service. The repairs must be performed next business day when no spare parts are required. When spare parts need to be ordered then four business days is the defined maximum time to repair.	High
Customer relationships	Receive communication and service requests of existing customer base. This may range of new product information, equipment demonstrations, and requests for maintenance or repair at normal service level.	Medium
Finance	This function is used to manage, store and process financial data generated by the commerce of medical equipment and services. The function is	Medium

[1] The table derives from Phase 2, Step 1 of the BCM Assessment

<table>
<tr><th colspan="3">Critical Business Function Identification – Business Continuity Plan Scope</th></tr>
<tr><th>Critical Business Function</th><th>Rationale for Selection</th><th>Recovery Priority (High, Medium, Low)</th></tr>
<tr><td></td><td>essential for the business as it represents the most important element of accounting information regarding purchase, invoicing and delivery of medical equipment.</td><td></td></tr>
</table>

Table 1: Critical Business Function Identification – Business Continuity Plan Scope

1.3 Emergency Command Centre

Primary Site: Office of company owner

Guideline:*-The primary site where the team will initially meet to review and plan their activities. Address and telephone number(s) of the location and detailed instructions on how to get there should be provided and distributed to the Business Continuity Team-*

Secondary Site: Home of Company Owner

Guideline:*-In the event that the primary site is unavailable, –* Dental Equipment Supplies - Business Continuity *Team will meet to review and plan their activities in a designated alternate site. Address and telephone number(s) of the location and detailed instructions on how to get there should be provided and distributed to the Business Continuity Team-*

1.4 BCP Team Contact List

If a major incident/disaster occurs, the BCP team will be convened and the situation assessed. It will be the responsibility of this team to decide whether or not to implement the Business Continuity Plans and for which business functions.

Due to the small size of the company the BCP Team Leader has the full control and authority over the activities. The business continuity manager is assigned as a deputy leader and the two of them should collaborate closely.

It is the BCP Team Leader’s responsibility to contact all team members or their alternates and ensure that they convene at the Emergency Operations Centre as defined in this plan.

The BCP Team Leader is responsible for the successful implementation of this plan.

BCP Team Contact List	
Employee 1 (Team Leader)	
Employee Name	Company Owner
Department	Finance, Customer Relationships
Employee Title	Company Owner
Employee Office Telephone	+44 (0)12341234
FAX	+44 (0)12341234
Employee Mobile	+44 (0)123412345
E-mail	owner@dent-equip.foo
Team Member 1 (Team Leader Deputy)	
Employee Name	Technician1
Department	Expedited service fulfillment, Technical department
Employee Title	Technician1
Employee Office Telephone	+44 (0)12341234
FAX	+44 (0)12341234
Employee Mobile	+44 (0)123412346
E-mail	tech1@dent-equip.foo
Team Member 2	

BCP Team Contact List	
Employee Name	SalesMan1
Department	Customer Relationships
Employee Title	SalesMan1
Employee Office Telephone	+44 (0)12341234
FAX	+44 (0)12341234
Employee Mobile	+44 (0)123412347
E-mail	Sales1@dent-equip.foo
Team Member 3	
Employee Name	Warehouse man
Department	Finance
Employee Title	Warehouse man
Employee Office Telephone	+44 (0)12341234
FAX	+44 (0)12341234
Employee Mobile	+44 (0)123412348
E-mail	warehouseman1@dent-equip.foo
Team Member 4	
Employee Name	SalesMan2
Department	Customer Relationships
Employee Title	SalesMan2
Employee Office Telephone	+44 (0)12341234
FAX	+44 (0)12341234
Employee Mobile	+44 (0)123412349
E-mail	sales2@dent-equip.foo
Team Member 5	
Employee Name	**Van Driver**
Department	**Finance**
Employee Title	**Van Driver**
Employee Office Telephone	+44 (0)12341234
FAX	+44 (0)12341234
Employee Mobile	+44 (0)123412349
E-mail	driver@dent-equip.foo
Team Member 6 (External)	
Employee Name	Accountant (external)
Department	Finance
Employee Title	
Employee Office Telephone	+44 (0)45671234
FAX	+44 (0)45671235
Employee Mobile	+44 (0)45671238
E-mail	accountant@accounts-help.foo

Table 2: BCP Team Contact List

1.4.1 BC Team Responsibility matrix & Deputies

On activation of the Business Continuity Plan the BC Team members must assume their responsibilities as soon as possible for an effective management and recovery from the incident. The table below lists the key responsibilities and the team member assigned to each of them. Control P.1.2.3.Key Personnel Deputies demands identifying and training deputies for the BC duties.

BC Team Responsibility matrix		
Responsibility	**Responsible**	**Deputy**
Operational Responsibilities (Incident Response and Recovery)		
Receive Incident notification, classify incident (False Alarm, Life Threatening, Non-Life Threatening) and notify relevant people/teams to initiate incident response and management **(SP2.8)**	BC Team Leader	Team Leader Deputy
Order evacuation incident site - During the initial phases of the response	Warehouseman	Company owner
Perform Damage assessment and provide situational awareness to the decision maker(s)	Warehouseman	Salesman1
Salvage Assets from incident site	Van driver	Technician2
Establish arrangements for Relocation of personnel	Van driver	Warehouseman
Procurement of replacement assets and supplies	Salesman2	Salesman1
Expedited service contracts fulfilment Recovery Leader	Technician1	Technician2
Customer relationships Recovery Leader	Salesman1	Salesman2
Finance Recovery Leader	Company owner	External (accountant)
Tactical Responsibilities (Incident Management)		
Declare BCM Incident and Initiate BCP	BC Team Leader	Team Leader Deputy
Stand-down BCP	BC Team Leader	Team Leader Deputy
Authorize spending	Company owner	Technician1
Periodical assessment of situation and corrective actions	Technician1	Company owner

BC Team Responsibility matrix		
Responsibility	**Responsible**	**Deputy**
Decide on the need to relocate business functions, Initiate disaster recovery	Technician1	Company owner
Ensure incident site physical security	Warehouseman	Get external support
Co-ordinate Original Site restoration	Technician1	Salesman2
Recovery coordination - Ensure critical business functions recovery activities are in progress. Monitor for failing dependencies / recovery objectives and indentify counter measures	Technician1	Salesman2
Monitor staff shifts and arrange for water and refreshments		
Strategic Responsibilities		
Planning and decisions for resumption	Company owner	Technician1
Communications with media	Salesman2	Company owner
Communications with stakeholders - Decide on an appropriate communication for customers that request a service or more information.	Salesman2	Salesman1
Maintain cash flow / funding for recovery and resumption	Company owner	External(accountant)

Table 3: BC Team Responsibility matrix

2. – Business Function “Finance”

The business function -Finance - has to be able to manage, store and process financial data generated by the commerce of medical equipment and services. The function is essential for the business as it represents the most important element of accounting information regarding purchase, invoicing and delivery of medical equipment. Most of the functions activities can be performed manually or delayed until information systems are available. Ordering spare parts required for the expedited service contracts fulfillment.

Guideline:*-Provide a brief description of the business function to resume/recover.*

2.1 Business Function Dependencies and Damage Assessment Form

The table below lists the key personnel and external contractors that have an active role in the recovery of the business function; as such they are a critical dependency. Use this table to track the availability of these key personnel to implement this function’s restoration activities. A deputy should be available for each person that falls under the control P.1.2.3 Key Personnel Deputies.

Key Personnel Availability list		
Name	Contact established? / Expected Availability for duty?	Deputy
External IT expert,		
Financial control software supplier		
Technician2		
PBX supplier		
Technician1		
Secretary		
Warehouse man		
Company-Owner		

Table 4: Key Personnel Availability list

The table[2] below list the dependencies of the -Finance- business function in terms of the underpinning assets used to provide and / or support the corporate business function. The damage assessment table will allow the function owner to have an overall picture of the assets' status. Upon this information alternative methods for asset and service recovery can be decided.

Damage Assessment of Assets			
Function Name	Finance	Who controls the function (Owner)	Company owner
Supporting IT Assets		**Damage Sustained (include assessor name and time/date)**	**Suggested Action (Salvage, Repair, Restore, Procure)**
Facilities	Company offices		
Hardware	Secretary Desktop PC, Owner Laptop, Accountant Computer(in accountants office premises), Financial control application server		
Network	Office Ethernet switch, Internet router		
Back Office Application	Financial control, Email		
Client Facing Applications	office productivity applications Internet Service provisioning Company fixed-line phone FAX		
Data	Corporate Financial Data, supplier agreements and contact information, funding agreements, order progress tracking		

Table 5: Damage Assessment of Assets

[2] The table derives from Phase 2, Step 2 of our approach

2.2 Business Function Protection Strategy

–Dental Equipment Supplies- has in place certain continuity controls described into the table[3] below, in order to protect and consequently achieve the continuity of the services provided by -Finance- business function and its key IT related assets. The information present in the column "**Control Implementation and usage information"** will provide the detailed information needed to implement the recovery action listed in the recovery strategy section.

Hardware Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
HN.1.1.1	Office Ethernet switch	**H**	IT Infrastructure Documentation There is an up-to-date and detailed IT infrastructure diagram including network and hardware components.	Annex IT Infrastructure Diagrams
	Office PBX	**H**		
	Secretary Desktop PC	**M**		
	Owner Laptop	**M**		
	Accountant Computer	**M**		
	Financial control application server	**M**		
HN.1.1.5	Office Ethernet switch	**H**	Disaster Recovery Cross Training No critical hardware or network component depends on an individual person for restoration in a disaster.	Annex – Disaster Recovery Cross Training Matrix
	Office PBX	**H**		
HN.1.1.7	Office Ethernet switch	**H**	Information Systems Hardening Control requires that all systems are up to date with respect to revisions, patches, and recommendations in security advisories.	
	Office PBX	**H**		
HN.1.2.1	Office Ethernet switch	**H**	Information Systems Backup Control requires that there is a documented backup procedure and backup plan that is: routinely updated, periodically tested, that calls for	Annex - Backup Plans
	Office PBX	**H**		

[3] The table derives from the assessment Phase 3, Step 3 and Phase 4, Step 2 of the BCM approach. The results produced as a consequence of the plan in Phase 4, step 2 will provide the input for the column "Control Implementation and usage information".

Hardware Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
	Secretary Desktop PC	**M**	regularly scheduled backups of software and configurations and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup (image) of the information systems / network equipment operating system, configuration files and any other modules provided by the information system / network component. More than one past backup sets is archived to make possible reverting to a well known working setup in case a system failure is also present in the most recent back. If a combination of full and incremental backups is used then the latest full backup and all the later incremental backups must be stored as a one backup set and must be retained in good working condition.	
	Owner Laptop	**M**		
	Accountant Computer	**M**		
	Financial control application server	**M**		
HN.1.2.5	Office Ethernet switch	**H**	Staff Training Control requires that all staff understand and is able to carry out their responsibilities under the backup plans.	
	Office PBX	**H**		
HN.1.3.3	Office Ethernet switch	**H**	Vendors SLAs The control requires that the organization maintains a list which includes hardware and network components vendors / suppliers and that a documented agreement exists between the two parties for the urgent provisioning of the required equipment within a predefined timeframe.	See Business Function Suppliers List and Annex Vendor SLAs
	Office PBX	**H**		

Table 6: Hardware Asset Based Continuity Controls

Applications Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
A.1.1.1	Email	**H**	Application Documentation. The control requires the organization to identify and collect documents required to install and operate the application. This includes information on the environment (OS version, external libraries, etc) for the execution of the application. This documentation has to be verified and	See annex Critical Application reference documentation index. Use the index to locate the documentation you need.
	office productivity applications	**H**		

Applications Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
	Company fixed-line phone	**H**	updated at least at every maintenance cycle of the BCP. Furthermore, if the application is custom the application code should be documented. The criticality of the application will dictate the level of documentation required.	
	Financial control App	**M**		
	FAX	**M**		
	Internet Service provisioning	**M**		
A.1.1.3	Email	**H**	Application Configuration Management A well defined configuration management procedure should be maintained, and changes to the application, its configuration and the running environment should be documented appropriately.	
	office productivity applications	**H**		
	Company fixed-line phone	**H**		
A.1.1.4	Email	**H**	Application Maintenance and Patching Vendor patches are applied via a documented patch management procedure and backups of critical systems are performed before and after updating the application.	Check backup plans for the latest backup set and the latest verified backup set.
	office productivity applications	**H**		
	Company fixed-line phone	**H**		
	Financial control App	**M**		
	FAX	**M**		
	Internet Service provisioning	**M**		
A.1.1.6	Email	**H**	Application Vendors & SLAs. The control requires that the organization maintains a list which includes the applications vendors / suppliers and that a documented	
	office productivity	**H**		

Applications Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
	applications		agreement exists between the two parties for technical support provisioning when required.	
	Company fixed-line phone	**H**		
A.1.2.1	Email	**H**	Application Backup Control requires that there is a documented backup procedure that is routinely updated, periodically tested, that calls for regularly scheduled backups of application software and requires periodic testing and verification of the ability to restore from backups. The control requires that the organization performs via the procedure a full Backup of the application files, database and any other available application modules.	Annex - Backup Plans
	office productivity applications	**H**		
	Company fixed-line phone	**H**		
	Financial control	**M**		
	FAX	**M**		
	Internet Service provisioning	**M**		
A.1.2.2	Email	**H**	Staff Training Control requires that all staff understand and are able to carry out their responsibilities under the backup plans.	See function recovery strategy responsibilities
	office productivity applications	**H**		
	Company fixed-line phone	**H**		
	Financial control	**M**		
	FAX	**M**		
	Internet Service provisioning	**M**		

Table 7: Applications Asset Based Continuity Controls

Data Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
D.1.1.5	Corporate Financial Data	**M**	Store Backup Media Offsite Backup media should be labeled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. A documented procedure should exist (part of the backup plan) to obtain the offsite backup media when required. Data storage continuity arrangements must assure the proper security levels (confidentiality, integrity, availability), while data are stored, in transit or at an off-site location.	See Backup Plan and recovery actions
	supplier agreements and contact information	**M**		
	funding agreements	**M**		
	order progress tracking	**M**		
D.1.2.1	Corporate Financial Data	**M**	Backup Rotation Schedules The control requires the enforcement of data backup via a documented, well-known backup rotation scheme such as Grand-Father-Son, Round Robin and Tower of Hanoi.	See Backup Plan and recovery actions
	supplier agreements and contact information	**M**		
	funding agreements	**M**		
	order progress tracking	**M**		
D.1.2.4	Corporate Financial Data	**M**	Internet Backup The control requires that workstation users (personnel) are allowed to back up data to a remote location over the Internet. Formal authorization is required prior to the execution of this backup method.	See Backup Plan and recovery actions
	supplier agreements and contact information	**M**		
	funding agreements	**M**		
	order progress	**M**		

Data Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
	tracking			
D.1.2.5	Corporate Financial Data	**M**	Data Backup Control requires that there is a documented data backup plan that is routinely updated, periodically tested, that calls for regularly scheduled backups of data and requires periodic testing and verification of the ability to restore from backups.	See Backup Plan and recovery actions
	supplier agreements and contact information	**M**		
	funding agreements	**M**		
	order progress tracking	**M**		

Table 8: Data Asset Based Continuity Controls

People Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
P.1.1.2	External IT expert PBX Supplier Technician1 Technician2	**H**	Physical Access Control Control requires that there are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where such information is stored. This includes employees, contractors, partners, collaborators, and personnel from third-party organizations, systems maintenance personnel, or facilities maintenance personnel.	

People Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
P.1.1.3	External IT expert PBX Supplier Technician1 Technician2	**H**	Clean Desk Policy A clean desk policy is in operation followed by all personnel, contactors and third parties	
P.1.2.1	External IT expert PBX Supplier Technician1 Technician2	**H**	Business Continuity Tool Set The control requires that staff has access and is trained to use a business continuity tool set which includes the appropriate material (software / hardware, documented guidelines and procedures) for responding after a security or business continuity incident.	See annex for toolset retrieval instructions
P.1.2.2	External IT expert PBX Supplier Technician1 Technician2	**H**	Business Continuity Tests Staff, have been trained and involved in business continuity tests.	
P.1.2.3	External IT expert PBX Supplier Technician1 Technician2	**H**	Key Personnel Deputies All executives, managers and designated critical staff participating into business continuity teams have trained deputies who can fulfill their duties / responsibilities.	See BC team responsibilities matrix.
P.1.2.4	External IT expert PBX Supplier Technician1 Technician2	**H**	Key IT Personnel Training The control requires that key IT personnel assigned with a key role into business continuity plans and procedures, are trained on a "business as usual" basis. The training ensures that such key position employees are fully capable of executing efficiently business continuity plans or procedures	See disaster recovery cross training matrix.

People Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
	Financial control software supplier	**M**		

Table 9: People Continuity Controls

Facilities Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
F.1.1.1	Company offices	**H**	IT Site Physical Access Physical access to IT Site is restricted by lock / combination lock and / or swiped cards or similar physical access control technologies.	
F.1.1.2	Company offices	**H**	IT Site Power Supply The power supply of the site equipment is protected with UPS and / or generators.	See Detailed Asset profiles
F.1.1.3	Company offices	**H**	IT Site Air-Conditioning IT site humidity, ventilation and air-conditioning are controlled.	
F.1.1.4	Company offices	**H**	IT Site Anti-fire Systems Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within the IT site.	
F.1.1.7	Company offices	**H**	IT Site Recovery Plan Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites.	Annex IT Site Recovery Plan
F.1.2.2	Company offices	**H**	Fire Fighting Equipment Fire detection (Fire Alarm Sensors) and suppression systems (water or gas suppression system, fire extinguishers) are installed within	

Facilities Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)
			corporate facilities	
F.1.2.3	Company offices	**H**	Air-conditioning The air-conditioning system installed into the corporate facilities has auto-shut-off if there is a fire, smoke detection or alert.	
F.1.2.4	Company offices	**H**	Anti-flood Equipment There are water detection systems and anti-flood techniques (raised floors, drop ceilings) in all vulnerable or high flood-risk areas of the corporate facilities.	
F.1.3.4	Company offices	**H**	Rooms and Areas Secure Access Physical access to critical areas and floors is restricted by guards' presence and /or individual swiped card or locked doors with keys only available to authorized personnel.	

Table 10: Facilities Asset Based Continuity Controls

2.3 Business Function Recovery Strategy

The following tables describe the recovery actions[4] that –Dental Equipment Supplies- should undertake for the recovery of the Finance Business Function in the case of an unexpected event that could cause the loss / destruction of the first or the interrupted access to the function of information stored.

Business Function Assets Recovery Actions			
Assets & Recovery Objective	**Recovery Actions** **(check the protection strategy for reference to implementation instructions and docs)**	**Responsible Party**	**Recovery Progress (Time and status, will we meet the objective?)**
People			
External IT expert **(High)**	RA.1.2.3 - Business Continuity Deputies take over the duties of the staff responsible with business continuity responsibilities.	Company Owner	
Technician1 **(High)**			
Technician2 **(High)**			
PBX Supplier **(High)**			
Facilities			
Company offices **(High)**	RA.1.1.1 - Once the emergency/incident is contained provide arrangements for the physical security of the incident site.	Warehouseman	
	RA.1.1.2 - Verify UPS / generators operate correctly and safely. Arrange adequate fuel supply. Extend you power autonomy by shutting down unnecessary loads. Communicate with the power company to establish	Warehouseman	

[4] Insert the immediate recovery actions derived by the implementation of the asset based controls (Annex B of the BCM approach document) used to protect the business function. Recovery actions should be expanded further to meet the recovery requirements of the business function; for each action listed in the summary list, provide all the details necessary to carry out this action-

	the nature of the problem, coordinated course of action and estimated time of utility resumption.		
	RA.1.1.3 - Verify air-conditioning operates normally. Make sure you can contact qualified technicians in case of failure.	Warehouseman	
	RA.1.1.4 - If the anti-fire systems were engaged make sure the site is safe for personnel (consult with the fire department) before attempting to salvage any equipment.	Warehouseman	
	RA.1.1.7 - On DR site activation implement the site recovery plan.	External IT Expert	
Hardware			
Office Ethernet switch **(High)**	RA.1.1.5 - establish the availability of the individuals or their backups, responsible for the disaster recovery of the individual components	Function owner	
	RA.1.2.1 - Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules	External IT Expert, Technician2	
	RA.1.3.3 - Switch to manual procedures and contact the equipment vendor / suppliers to provide the required equipment	External IT Expert, Technician2	
Office PBX **(High)**	ra.1.1.5 - establish the availability of the individuals or their backups, responsible for the disaster recovery of the individual components	Function owner	

	RA.1.2.1 - Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules	Secretary (PBX Supplier)[5]	
	RA.1.3.3 - Switch to manual procedures and contact the equipment vendor / suppliers to provide the required equipment	Secretary	
Secretary Desktop PC **(Medium)**	RA.1.2.1 - Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules	Secretary(External IT Expert), Technician2	
Owner Laptop **(Medium)**	RA.1.2.1 - Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules	Company Owner(External IT Expert), Technician2	
Accountant Computer **(Medium)**	RA.1.2.1 - Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules	Company Owner (Accountant)	
Financial control application server **(Medium)**	RA.1.2.1 - Initiate backup procedure to restore hardware and / or network component operating system / configuration file / software modules	Company Owner (External IT Expert)	
Applications			
Email **(High)**	RA.1.1.3 - Consult the application's configuration records to repair / reinstall the application	Technician1 (Email Hosting Services LTD)	
	RA.1.1.6 - Switch to manual procedures and contact the application	Technician1	

[5] When the maintainer is an external contractor his name is put in parenthesis following the asset owner's name(e.g. asset_owner(contracted asset_maintainer). The asset owner will supervise the recovery actions for his/her asset.

	vendor to provide the required technical support in order to restore the application.		
	RA.1.2.1 - Initiate backup procedure to restore the application software modules	Technician1 (Email Hosting Services LTD)	
office productivity applications **(High)**	RA.1.1.3 - Consult the application's configuration records to repair / reinstall the application	Technician2, Hardware asset owner(External IT Expert)	
	RA.1.1.6 - Switch to manual procedures and contact the application vendor to provide the required technical support in order to restore the application.	Technician2, Hardware asset owner	
	RA.1.2.1 - Initiate backup procedure to restore the application software modules	Technician2, Hardware asset owner(External IT Expert)	
Company fixed-line phone **(High)**	RA.1.1.3 - Consult the application's configuration records to repair / reinstall the application	Secretary (The telephone company)	
	RA.1.1.6 - Switch to manual procedures and contact the application vendor to provide the required technical support in order to restore the application.	Secretary	
Financial control **(Medium)**	RA.1.2.1 - Initiate backup procedure to restore the application software modules	Company Owner(Financial control software supplier)	
FAX **(Medium)**	RA.1.2.1 - Initiate backup procedure to restore the application software modules	Secretary (The telephone company)	
Internet	RA.1.2.1 - Call service	Company	

Service provisioning **(Medium)**	provider to restore service in good working order	Owner(The Internet Service Provider)	
Data			
Corporate Financial Data **(Medium)**	RA.1.1.5 - Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.	Company owner, Van driver (as defined in the backup plan)	
	RA.1.2.1 - Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.	Company owner (External IT Expert)	
	RA.1.2.5 - Initiate the backup plan to restore the damaged / lost data	Company owner (External IT Expert)	
supplier agreements and contact information **(Medium)**	RA.1.1.5 - Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.	Company owner, Van driver (as defined in the backup plan)	
	RA.1.2.1 - Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.	Company owner (External IT Expert)	
	RA.1.2.5 - Initiate the backup plan to restore the damaged / lost data	Company owner (External IT Expert)	
funding agreements **(Medium)**	RA.1.1.5 - Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the	Company owner, Van driver (as defined in the	

	organization's production information systems.	backup plan)	
	RA.1.2.1 - Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.	Company owner (External IT Expert)	
	RA.1.2.5 - Initiate the backup plan to restore the damaged / lost data	Company owner (External IT Expert)	
order progress tracking **(Medium)**	RA.1.1.5 - Initiate the procedure for obtaining the offsite backup media from the designated site and load backup data to the organization's production information systems.	Company owner, Van driver (as defined in the backup plan)	
	RA.1.2.1 - Identify the backup sets needed for effective restore. These may be the latest backup set available or some older copy if restoring to an older point in time is required.	Company owner (External IT Expert)	
	RA.1.2.5 - Initiate the backup plan to restore the damaged / lost data	Company owner (External IT Expert)	

Table 11: Business Function Assets Recovery Actions

2.4 Business Function Suppliers List

The following suppliers may need to be contacted in the event of a disaster towards the recovery of the -Finance- business function. Information from the implementation of controls HN.1.3.3 and A.1.1.6 will need to be included in this table.

Guideline: *-The list is copied and retained in a secure place of the organization's premises as well in an off-site location-*

Suppliers Contact List HN.1.3.3			
Supplier 1			
Company Name	IT Valued Ltd.		
Street Address			
Phone	+44 4556 445545		
FAX	+44 4556 445546		
E-mail	expert@itvalue.co.uk		
Point of Contact	External IT Expert		
Material / Service Material (Asset supported and requirements set in the SLA)	Maintain most of the IT assets of the company (details in the assessment)		
Supplier has formal BCM requirements (SP5.2)	**Yes**	**BCM Capacity Verified (SP5.2)**	**No**
Agreed Procedure for recovery of outsourced services (SP5.1)	Special arrangement for BC incident. On call availability of 4 hours.		
Supplier 2			
Company Name	Financial control software supplier		
Street Address			
Phone	+44 (0) 2345 2345678		
FAX	+44 (0) 2345 2345679		
E-mail	support@fcss.foo		
Point of Contact	Jeremy Smith		
Material / Service Material (Asset supported and requirements set in the SLA)	Financial control software. Onsite support contract in two business days and business hours phone support.		
Supplier has formal BCM requirements (SP5.2)	**Yes**	**BCM Capacity Verified (SP5.2)**	**No**
Agreed Procedure for recovery of outsourced services (SP5.1)	A request has to be delivered through phone call. Depending on the assessment of the supplier remediation might be attempt through remote (phone) instructions. When possible screenshots showing the problem must be provided through email.		
Supplier 3			
Company Name	Email Hosting Services LTD.		
Street Address	12, Bread St, Ediburg		
Phone	+44 (0) 2345 2345679		
FAX	+44 (0) 2345 2345679		
E-mail	support@ehs.foo		

Point of Contact	John		
Material / Service Material **(Asset supported and requirements set in the SLA)**	Email Service provision. Availability in the SLA 99.9% annually		
Supplier has formal BCM requirements (SP5.2)	No	**BCM Capacity Verified (SP5.2)**	No
Agreed Procedure for recovery of outsourced services (SP5.1)	Call customer support, business hours		
Supplier 4			
Company Name	Telephone Company.		
Street Address			
Phone	+44 (0) 2345 2345679		
FAX	+44 (0) 2345 2345679		
E-mail	support@phonecompany.foo		
Point of Contact	John		
Material / Service Material **(Asset supported and requirements set in the SLA)**	Fixed Line telephone numbers and Internet service provisioning		
Supplier has formal BCM requirements (SP5.2)	No	**BCM Capacity Verified (SP5.2)**	No
Agreed Procedure for recovery of outsourced services (SP5.1)	Call customer support, business hours		
Supplier 5			
Company Name	Mobile phone company.		
Street Address			
Phone	+44 (0) 2345 2345679		
FAX	+44 (0) 2345 2345679		
E-mail	support@mobile.foo		
Point of Contact	John		
Material / Service Material **(Asset supported and requirements set in the SLA)**	Mobile telephony providers.		
Supplier has formal BCM requirements (SP5.2)	No	**BCM Capacity Verified (SP5.2)**	No
Agreed Procedure for recovery of outsourced services (SP5.1)	Call customer support, business hours. In case of lost or damaged SIM cards we can request sim replication at any of their stores. We must present an authorization of the company representative to get the new SIM module.		
Supplier 6			
Company Name	Internet service provider		
Street Address			
Phone	+44 (0) 2345 2345678		
FAX	+44 (0) 2345 2345679		
E-mail	support@isp.foo		

Point of Contact	Internet service provider		
Material / Service Material **(Asset supported and requirements set in the SLA)**	Standard ADSL service for business		
Supplier has formal BCM requirements (SP5.2)	No	**BCM Capacity Verified (SP5.2)**	No
Agreed Procedure for recovery of outsourced services (SP5.1)	Call customer support, 8:00 AM – 10:00 PM.		
Supplier 7			
Company Name	PBX Supplier		
Street Address			
Phone	+44 (0) 2345 2345678		
FAX	+44 (0) 2345 2345679		
E-mail	support@PBXSupp.foo		
Point of Contact	Jack		
Material / Service Material **(Asset supported and requirements set in the SLA)**	Next Business Day service support. Stock of spare parts.		
Supplier has formal BCM requirements (SP5.2)	Yes	**BCM Capacity Verified (SP5.2)**	Yes
Agreed Procedure for recovery of outsourced services (SP5.1)	Call customer support business hours.		

Table 12: Suppliers Contact List

3. – Business Function “Insert Function Name”

This chapter has been intentionally left blank in order to serve as template for prospective users of this BCM approach.

Guideline:*-Repeat all relevant steps for each identified critical business function*

3.1 Business Function Dependencies and Damage Assessment Form

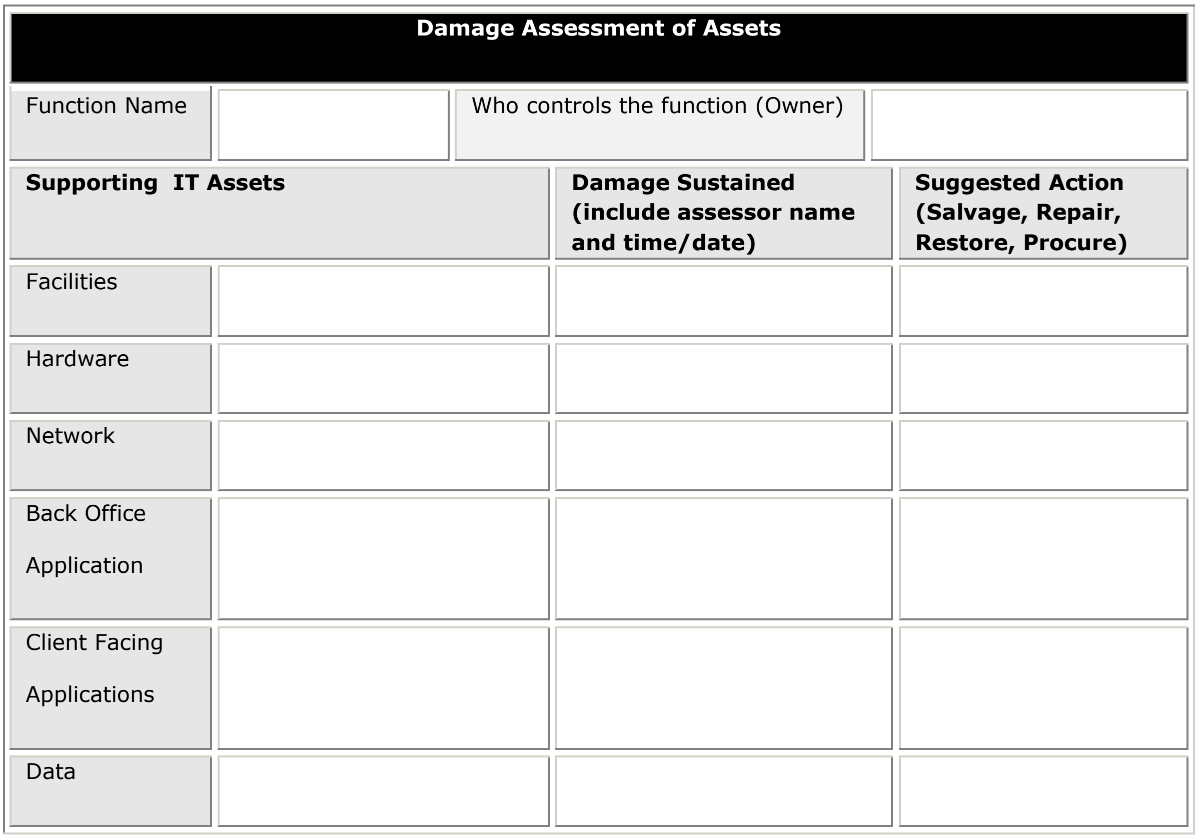
The table below lists the key personnel and external contractors that have an active role in the recovery of the business function; as such they are a critical dependency. Use this table to track the availability of these key personnel to implement this function’s restoration activities. A deputy should be available for each person that falls under the control P.1.2.3 Key Personnel Deputies.

Key Personnel Availability list		
Name	Contact established? / Expected Availability for duty?	Deputy

Table 13: Key Personnel Availability list

The table[6] below list the dependencies of the -Finance- business function in terms of the underpinning assets used to provide and / or support the corporate business function. The damage assessment table will allow the function owner to have an overall picture of the assets’ status. Upon this information alternative methods for asset and service recovery can be decided.

[6] The table derives from Phase 2, Step 2 of our approach



Damage Assessment of Assets			
Function Name		Who controls the function (Owner)	
Supporting IT Assets		**Damage Sustained (include assessor name and time/date)**	**Suggested Action (Salvage, Repair, Restore, Procure)**
Facilities			
Hardware			
Network			
Back Office Application			
Client Facing Applications			
Data			

Table 14: Damage Assessment of Assets

3.2 Business Function Protection Strategy

–Insert Company Name- has in place certain continuity controls described in the table[7] below, in order to protect and consequently achieve the continuity of the services provided by - Customer Relationships - business function and its key IT related assets. The information present in the column "**Control Implementation and usage information"** will provide the detailed information needed to implement the recovery action listed in the recovery strategy section.

Hardware Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

[7] The table derives from the assessment Phase 3, Step 3 and Phase 4, Step 2 of the BCM approach. The results produced as a consequence of the plan in Phase 4, step 2 will provide the input for the column "Control Implementation and usage information".

Hardware Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Table 15: Hardware Asset Based Continuity Controls

Applications Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Applications Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Applications Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Table 16: Applications Asset Based Continuity Controls

Data Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Data Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Table 17: Data Asset Based Continuity Controls

People Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

People Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Table 18: People Continuity Controls

Facilities Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Facilities Asset Based Continuity Controls				
Control	**Respective Asset & Priority**		**Control Description**	**Control Implementation and usage information** (Short directions and /or pointer to documentation e.g. Annex F - backup plan)

Table 19: Facilities Asset Based Continuity Controls

3.3 Business Function Recovery Strategy

The following tables describe the recovery actions[8] that –Insert Company Name- should undertake for the recovery of the – Insert name of Business Function - Business Function in the case of an unexpected event that could cause the loss / destruction of the first or the interrupted access to the function of information stored.

Business Function Assets Recovery Actions			
Assets & Recovery Objective	**Recovery Actions** **(check the protection strategy for reference to implementation instructions and docs)**	**Responsible Party**	**Recovery Progress (Time and status, will we meet the objective?)**
People			
Facilities			
Hardware			

[8] Insert the immediate recovery actions derived by the implementation of the asset based controls (Annex B of the BCM approach document) used to protect the business function. Recovery actions should be expanded further to meet the recovery requirements of the business function; for each action listed in the summary list, provide all the details necessary to carry out this action-

Applications			
Data			

Table 20: Business Function Assets Recovery Actions

3.4 Business Function Suppliers

The following suppliers may need to be contacted in the event of a disaster towards the recovery of the -Insert name of Business Function - Business Function.

Guideline: *-The list is copied and retained in a secure place of the organization's premises a well in an off-site location-*

Suppliers Contact List HN.1.3.3			
Supplier 1			
Company Name			
Street Address			
Phone			
FAX			
E-mail			
Point of Contact			
Material / Service Material (Asset supported and requirements set in the SLA)			
Supplier has formal BCM requirements (SP5.2)		**BCM Capacity Verified (SP5.2)**	
Agreed Procedure for recovery of outsourced services (SP5.1)			
Supplier 2			
Company Name			
Street Address			
Phone			
FAX			
E-mail			
Point of Contact			
Material / Service Material **(Asset supported and requirements set in the SLA)**			
Supplier has formal BCM requirements (SP5.2)		**BCM Capacity Verified (SP5.2)**	
Agreed Procedure for recovery of outsourced services (SP5.1)			

Table 21: Supplier Contact List

4. BCP Maintenance

4.1 Change Management

The –Insert Company Name- responsible party for changes afterwards the finalization of the current document is the Document Owner. Proposals for improvement of the access management procedure are addressed to the document owner via the Document Change Management Form (see Annex A). The Document Owner evaluates all the submitted proposals and proceeds according to Change Management Process.

4.2 BCP Training

Training is provided at least annually; new staff who will have plan responsibilities receive training shortly after they are hired. –Insert Company Name- personnel is trained to the point that they are able to execute their respective business continuity responsibilities without the aid of the documents. Training encompasses:

- Purpose of the Business Continuity Plan
- Business Continuity team co-ordination and communication
- Reporting procedures
- Security arrangements
- Team specific processes
- Individual responsibilities

4.3 BCP Testing

Testing of the ability to recover critical business functions as intended is an essential component of effective business continuity management. Such testing is conducted periodically by the –Insert Company Name- with the scope and frequency determined by the criticality of the business functions, the –Insert Company Name- role in broader market operations, and material changes in the organization’s business or external environment. In addition, such testing identifies the need to modify the –Insert Company Name- Business Continuity Plan and other aspects of an organization’s business continuity management in response to changes in its business, responsibilities, systems, software, hardware, personnel, or facilities or the external environment. The following items are incorporated when planning an exercise:

- **Goal**. The part / business continuity function of the BCP to be tested.
- **Objectives**. The anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic and timely.
- **Scope**. Identifies the departments or organizations involved, the critical business function, the geographical area, and the test conditions and presentation.
- **Artificial aspects and assumptions**. Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability.
- **Participant Instructions**. Explains that the exercise provides an opportunity to test the BCP before an actual disaster.
- **Exercise Narrative.** Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time,

location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions.

- **Testing and Post-Exercise Evaluation.** The exercise is monitored impartially to determine whether objectives were achieved. Participants' performance, including attitude, decisiveness, command, coordination, communication, and control are assessed. Debriefing is short, yet comprehensive; explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback should also be incorporated in the exercise evaluation.

The –Insert Company Name- Business Continuity Manager is responsible log the preparedness exercises of–Insert Company Name- BCP into the following table.

Guideline: *-Document the date and type of exercise as well any pertinent comments each time the plan is exercised-*

Exercise Log		
Date	**Type of Exercise**	**Comments**

4.4 BCP Review

Review of the plan and plan components are conducted annually. In addition the –Insert Company Name- Business Continuity Plan is re-evaluated when any of the following occur:

- Regulatory changes
- Resources or organizational structures change
- Funding or budget level changes
- When changes to the threat environment occur;
- When substantive changes to the organization’s IT infrastructure take place; and
- After an exercise to incorporate findings.

Annex A- Document Change Management

Document Change Management Form					
Document Title					
Document Version			**Date**		
Sender	Name / Surname: E-mail: Office Tel:			Department:	
Page(s) Interested			**Section(s) Interested**		
Description of Suggestions :					
Instructions: Please, fill out the above sections and Submit form to the document owner					
Document Owner Review of Suggestions:					
Instructions: Please, review the submitted suggestions and forward form to the **-Insert Approval Authority- e.g. Business Continuity Manager, Chief Information Security Officer, Chief Information Officer**					
Approved		**Not Approved**		**Signature**	
-Insert Approval Authority- Review of Suggestions::					
Instructions: Please, review suggestions and notify plan owner					

Approved		**Not Approved**		**Signature**	

Annex B- Emergency Contact List

–Insert Company Name- retains available the following emergency contact list for all employees in the event of an emergency.

Emergency Contact List		
	Contact Details	
	Telephone	Address
Local Police Department	-Insert Number-	-Insert Address-
Local Fire Department:	-Insert Number-	-Insert Address-
Ambulance Service:	-Insert Number-	-Insert Address-
Hospital:	-Insert Number-	-Insert Address-
Insurance Company:	-Insert Number-	-Insert Address-
Telephone Company:	-Insert Number-	-Insert Address-
Gas/Heat Company:	-Insert Number-	-Insert Address-
Electric Company	-Insert Number-	-Insert Address-
Local Newspapers:	-Insert Number-	-Insert Address-
Local Radio Stations:	-Insert Number-	-Insert Address-
Local TV Stations	-Insert Number-	-Insert Address-

Annex C- Emergency Procedures

Prior to developing a BCP the organization should have in place a set of emergency procedures describing the general measures that will be taken to protect employees, customers, visitors, etc. from the direct, indirect or potential effects of any incident or emergency (i.e. evacuation, shelter-in-place, area of refuge). It is beneficial to have these procedures attached in the BCP for quick reference.

Annex D – Disaster Recovery Cross-training Matrix

Prepare a disaster recovery cross-training matrix to satisfy controls HN.1.1.5 and P.1.2.4. Identify cross training opportunities by listing the asset maintainers that have responsibility of the recovery actions in the recovery strategy. For each category create pairs of asset maintainers that will be cross trained to the recovery actions of each other's assets. Modify the template given below for all Asset types and recovery actions that apply to your BCP. If not enough maintainers for the same recovery action can be identified try to identify matches in similar recovery actions or identify externals (consultants) that can provide the required backup. Note that the recovery actions may need to be amended changed according to the implementation of your business continuity controls.

Asset Type	Recovery Actions	Asset Maintainers	Cross training Pairs
	Hardware		
Server	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Laptop	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Workstation	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Storage	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Security Devices (firewall, IDS / IPS, anti-spam etc)	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
	Network		
Routers	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		

	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Gateways	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Switches	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Wireless Access Points	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Network Segment (e.g. cabling and equipment between two computers)	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		
Other (SAT, Laser)	RA.1.1.2		
	RA.1.1.5		
	RA.1.2.1		
	RA.1.2.4		
	RA.1.3.1		
	RA.1.3.2		
	RA.1.3.3		

Annex E - Backup Plans

This plan shall include implementation of the backup related controls like:

- Information Systems Backup Plan (HN.1.2.1)
- Backup Media redundancy (HN.1.2.3)
- Backup Fail-over (HN.1.2.4)
- Applications Backup Plan (A1.2.1)
- Data Backup Plan (D.1.2.5)
- Data Backup Controls Implementation (D.1.2.x)
- Store Backup Media offsite (D.1.1.5)
- Secure Remote Backup Storage (D.1.1.3)

Example Backup plan for Dental Equipment Supplies is provided in the following Annex.

Dental Equipment Supplies Backup Plan

The Company Dental Equipment Supplies has implemented the backup plan described in this document in order to protect their information assets from loss or destruction. The backup plan will be implemented following the schedule[9] described in Table 1 below. The backup system that is used for the implementation has adequate capacity to hold the backup of all systems, applications and data in a single tape. The systems, application and data covered by this backup plan are listed in Table 23.

Backup System Operation

Every weekday morning the backup system logs must be reviewed for errors during the backup process. If everything worked as expected then the backup tape must be ejected, labeled and prepared for shipping to off-site location. The next tape in the schedule should be loaded in the tape drive.

If problems are detected they must be investigated and resolved. The backup job must be repeated to maintain the correctness of the backup schedule.

Offsite Location

The Offsite Location is set to: Corporate-Owner Home, Full Address.

Responsible for transportation of media is: Corporate-Owner

Alternate Responsible for transportation of media is: Van Driver

Essential Configuration Parameters

The backup system must be configured to verify the content of the tapes after completing the backup creation process.

Backup Restore Tests

Once a month test restore of one of the assets will be performed. The asset to be restored can be selected randomly but no asset can be test restored twice before all other assets have been tested at least once.

Activity Logging

The backup system produces logs of its operation. In addition the backup operators must fill the activity log provided at the end of this plan to keep track of activities like off-site storage, tape rotation and restore testing.

Backup System Implementation

This section should provide information on the architecture of the backup solution and pointers to the vendor's documentation

[9] Backup system software may automatically produce such a schedule and allow printing it.

Sample Backup Schedule – Tapes 12 – 3 Weeks full backup retention, daily incremental 1 week retention							
Weekly Schedule	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Backup Type		Incremental	Incremental	Incremental	Incremental	Full	
Week1	(Bootstrap – Tape 12 Full)	Tape1 Off-site (Tape12)	Tape2 Off-site (Tape1)	Tape3 Off-site (Tape2)	Tape4 Off-site (Tape3)	Tape5 Off-site (Tape4) Return(Tapes6-9,10)	
Week2		Tape6 Off-site(Tape5)	Tape7 Off-site (Tape6)	Tape8 Off-site (Tape7)	Tape9 Off-site (Tape8)	Tape10 Off-site (Tape9) Return(Tapes1-4)	
Week3		Tape1 Off-site(Tape10)	Tape2 Off-site(Tape1)	Tape3 Off-site (Tape2)	Tape4 Off-site (Tape3)	Tape11 Off-site (Tape4) Return(Tapes6-9)	
Week4		Tape6 Off-site(Tape11)	Tape7 Off-site (Tape6)	Tape8 Off-site (Tape7)	Tape9 Off-site (Tape8)	Tape12 Off-site (Tape9) Return(Tapes1-4,12)	
Week5	Repeat Week1						

Table 22: Backup Schedule

IT Asset	Aggregated Recovery Priority
Hardware	
Tech-Laptop1 (identical 2 tech-laptop2)	H
Tech-Laptop2 (identical 2 tech-laptop2)	H
Desktop-Sales1	H
Desktop-Sales2	H
Secretary Desktop PC	M
Owner Laptop,	M
Financial control application server	M

Internet Router	M
Office-PBX	H
Back office Application	
Financial control	M
Email	H
office productivity applications (As part of the system backup)	H
Medical-Equipment-problem-diagnosis-application-vendor1	H
Medical-Equipment-problem-diagnosis-application-vendor2	H
Client Facing Application	
web site	M
Corporate Financial Data	M
supplier agreements and contact information	M
funding agreements	M
order progress tracking	M
Expedited Service Customer database	H
Technicians work Planning	H
Expedited Support/repair request reports	H
Spare part requests	H
Medical equipment service manuals	H
Customer Request tracking database	M
Normal Support/repair request reports	M
Medical equipment brochures and technical specifications	M

Table 23: IT Assets covered by this backup plan

Main-Site Backup Log							
Date	Type	Media Type /Media ID	Verified-OK	Test Restore	Shipped Offsite	Returned for reuse	Operator name &signature
3/1/2010	Full	Tape12	Yes		4/1/2010		
4/1/2010	Incremental	Tape1	Yes		5/1/2010	15/1/2010	
5/1/2010	Incremental	Tape2	Yes		6/1/2010	15/1/2010	
6/1/2010	Incremental	Tape3	Yes		7/1/2010	15/1/2010	
7/1/2010	Incremental	Tape4	Yes		8/1/2010	15/1/2010	
8/1/2010	Full	Tape5	Yes		11/1/2010		
11/1/2010	Incremental	Tape6	Yes		12/1/2010		
12/1/2010	Incremental	Tape7	Yes		13/1/2010		
13/1/2010	Incremental	Tape8	Yes		14/1/2010		
14/1/2010	Incremental	Tape9	Yes		15/1/2010		
15/1/2010	Full	Tape10	Yes		18/1/2010		
18/1/2010	Incremental	Tape11	Yes				

Table 24: Backup Log

Annex F - IT Infrastructure Diagram

Include a network diagram that clearly shows the network architecture and hardware components.

(Control HN.1.1.1)

Annex G - IT Site Recovery Plan

In case the primary IT site becomes inaccessible or inoperable a new location will need to be activated for disaster recovery of the IT systems.

Depending on the risk profile of the organization an IT Disaster Recovery (DR) Site (F.1.1.6) and even a Secondary Disaster Recovery Site (F.1.1.8) may have already been identified and prior arrangements for their use might be already established.

The procedure of the activation of the Disaster Recovery Site must be documented and special attention to procedures for avoiding multiple usage conflicts must be given (SP.5.5).

For each hardware and application the recovery location options must be identified. While some of the IT systems will need to be located at the critical business function recovery site (e.g. printers and workstations) others can be restored at remote locations.

Per Asset Site Recovery Plan			
Asset	**Recovery Priority**	**Selected Recovery site provider / Recovery model**	**Disaster Recovery Procedure**

Per Asset Site Recovery Plan			
Asset	Recovery Priority	Selected Recovery site provider / Recovery model	Disaster Recovery Procedure

Table 25: Per Asset Site Recovery Plan

Selecting the recovery site

Depending on the recovery needs several models of recovery site are available that will allow recovery times ranging from seconds to days. The lower the recovery time the higher the technology and communication expenses will be. The different site models are briefly described in Table 26.

Implementation of the site models can follow the traditional path of identifying a suitable physical location that may be available either for free, if the company already rents or owns diverse locations, or for a renting fee.

Recent trends of outsourcing and virtualization allow for remote provisioning of physical space or virtual computing resources as part of a contractual agreement. The provisioning time for physical hosting or virtualized services is usually much sorter and cost effective. A brief description of the different provisioning models is provided in Table 27. The user of such services should be informed about variations of risk levels emanating from the different provisioning models and technologies used[10]. To this extent users should seek to understand the peculiarities of each service through consultation with the individual providers.

Redirecting communication feeds and supplies

Arrangements for transferring the telecommunication services, supplies and spare parts delivery to an alternate (disaster recovery) site must be documented. This, for example, may include redirection of internet based services to other providers, change of DNS records, redirection of voice and FAX telephone numbers, etc.

Recovery Site Models		
Recovery site model	Description	Time to service recovery
Dual active IT sites	The applications / services are provided concurrently from two distinct IT sites. When one of the service nodes fails the one still operational has enough resources to service the load of the failed node.	Almost instant
Hot DR Site	The applications / services are replicated from the main site to the hot site (almost) in real time. The hot site is ready to be activated from within few minutes to a few hours after the main site failure.	A few minutes to hours
Worm DR site	Replicates the hardware and network architecture of the main site. Restoration of applications and data is required to make the site fully	From several hours to the order of 1-2 days

[10] For more information on the risks of cloud based services (Saas, Paas and IaaS) and their impact on SMEs consult the ENISA study available at http://www.enisa.europa.eu/media/press-releases/enisa-clears-the-fog-on-cloud-computing-security-1

Recovery Site Models		
Recovery site model	**Description**	**Time to service recovery**
	operational.	
Cold DR Site	Provides only the space and HVAC required for IT operations. All technology equipment has to be procured, consequently may take a few days to activate that type of sites depending on the availability of the equipment in the suppliers stock.	Several days

Table 26: Recovery Site Models

Site Provider types			
Site provider	**Description**	**Time to implement**	**Supported Site models**
Company owned remote facility	Provided there is enough distance between the two IT sites it can be a cost efficient solution as the physical space comes for free. Depending on the size, the cost of duplicating power, HVAC and environmental controls can still be quite expensive.	Medium to High	Dual Active to cold
Reciprocal agreements	Mutual aid arrangements with other companies. It is a low cost means to secure a DR site, but may not work as expected due to lack of space or events that affect both companies.	Medium	Hot to cold
DR site provider	A solution with varying cost (on average high) depending on the availability and space requirements. It provides a well designed and implemented environment for IT installations and some space for operational personnel.	Medium	Hot to cold
Co-location center / rack space provider	Renting of rack space where physical servers can be installed. In this case the equipment must still be procured. It is the responsibility of the customer to install Since no space is available for operational personnel and systems administration , n most cases these tasks have to be performed remotely.	Low to Medium	Dual Active to cold
Infrastructure as a service	Renting of virtual machine resources. The infrastructure provider has a complete hardware infrastructure and can provide the required hardware resources and network architecture and connectivity. The provisioning of the infrastructure can be completed in fractions of the time require to procure physical equipment. It is the responsibility of the customer to install and manage the operating systems and applications. Operation of the infrastructure is	Low to medium	Dual Active to worm

Site Provider types			
Site provider	**Description**	**Time to implement**	**Supported Site models**
	only possible remotely.		
Software as a service	A complete solution offered by third party provider for a specific application. Email service, web hosting, PBX, CRM, groupware applications are common examples of applications offered as a service. The customer has to deal only with high level administration of the service such as adding users and assigning rights. Operation of the infrastructure is only possible remotely. Usually all required functions are provided through a user friendly interface.	Low	Dual Active to worm

Table 27: IT Site/Infrastructure Provider types

Annex H – Vendor SLAs

Attach printed copies of the SLAs relevant for the recovery of the organization in case of a business continuity event.

Annex I – Critical Application reference documentation index

Critical Application	Document Title	Media / Format	Location
Financial Control Application	Backup & Restore Guide	CD-Rom / PDF	BC Tools Set

Annex J – Critical Business Function Profiles

Critical Business Function Profile Card			
Critical Business Function	Finance	Recovery Priority	Medium
Who controls the function	Company owner		
Who is responsible for delivering the function?	Company owner : Funds management Secretary : orders & invoicing / scheduling of product deliveries Accountant : legal accounting obligations		
Who is the user? (Who benefits / needs this function? / why is it critical?)	This is a core function of the company used by almost every other function. The most demanding user is the **Expedited service contracts fulfillment** function that requires timely delivery of spare parts. **Customer Relationship Management** is also using the services of this function to fulfill customer orders. In addition prolonged unavailability of this function can starve the business from working capital.		
How is it used?	Orders are placed from customers through salesmen or technicians in the case of spare parts used for repairs. Currently internal emails are exchanged for placing orders. When prior arrangements (including credit) exist with suppliers the order is prepared and sent to the suppliers by the secretary without any further processing. The Orders depending on the supplier may need to be dispatched via FAX or Email and sometimes further details are worked out through phone calls. In other cases the company owner needs to secure a deal and supply adequate cash funds to support the order. The accountant updates/verifies the company records on a weekly basis and is available on call for urgent matters during business hours.		

Critical Business Function Profile Card	
Critical Business Function Name	Expedited Service Contract Fulfillment
Who controls the function (Owner)	Technician1
Who is responsible for delivering the function?	Technician1: Diagnose problem, request spare parts, perform repair Technician2: Diagnose problem, request spare parts, perform repair Salesman1: Receive request, prioritize repairs Salesman2: Receive request, prioritize repairs
Who is the user? (Who benefits / needs this function?)	This function is directly visible to the customers who have opted for the expedited service contract.
How is it used?	Customers call their assigned salesman and report the problem of their equipment. The salesman verifies a contract is in effect and arranges a convenient appointment for the customer after consulting the availability of the technicians. Technicians are informed from the salesman. Occasionally events may require the rescheduling of appointments and the salesman will need to consult with the customer and update the technicians’ schedules. Technicians arrive at the premises of the customer to perform a diagnosis and if possible repair the problem. The technicians usually will need to use their laptop computer that includes the diagnosis software supplied by the vendor of the equipment. If spare parts are needed for the repair, technicians will identify the spare part number in the equipments service manuals and prepare the spare part requests to be implemented by the **finance** function. Eventually when the equipment is repaired a support or repair report is filed by the technicians and forwarded to the sales persons for pricing and further actions as part of the **customer relationship management** function. The information and files generated through the expedited service contract fulfillment process is flowing to the individual employees through emails and complementary

	communication takes place by phone (e.g.: when technicians are at a customer’s premises).

Critical Business Function Profile Card	
Critical Business Function Name	Customer Relationship Management
Who controls the function (Owner)	Company Owner
Who is responsible for delivering the function?	Company owner : Identify new prospective customers, assess customer satisfaction, approve new customer marketing campaigns Saleman1, salesman2 : Receive and respond to customer inquiries (RFIs, RFQs, requests for repairs and maintenance), Follow-up on prospective customers, co-ordinate customer requests fulfillment (from order to vendor up to delivery to client), implement customer marketing campaigns, Analyze sales trends and propose marketing campaigns, price services, equipment and spare parts. Secretary: Receives the phone calls or emails from prospective new customers and assigns them to a salesman.
Who is the user? (Who benefits / needs this function?)	This function is directly visible to all existing customers and new prospective customers that need to place an inquiry or order for a product.
How is it used?	New customers will call the publicly known phone numbers of the company. The phone numbers are advertised in ads placed from time to time in the press. The company web site also lists the phone number and email address the customers may use for contact. Communication from new customers is passed on to the first available salesman. Existing and new customers place their requests and can track the progress of fulfillment by contacting their assigned salesman (phone or email). Salesmen are responsible for co-coordinating the fulfillment of the customers' requests starting from the moment an order is placed with finance and tracking the delivery to the customer as

	well as arranging the installation by the technicians. Finally they have to price the service and request the invoicing of the customer by **Finance**. A similar process is used for handling maintenance and repair requests that are implemented by the technical service function (not covered in the example). Back office information exchange is taking place through email and shared access to word processor documents and spreadsheets.

Annex K – Critical Assets Identification Cards

See separate BCP_AnnexK-AssetIdentificationCards.doc document.

Annex L – Personnel Contact Details

Full listing of personnel contact details will be required for communicating critical business functions alternate locations or arranging work in shifts, or there is a need to communicate with relatives of personnel.

Department	Name	Office Phone	Mobile	Email	Home Land Line

Table 28: Personnel Contact Details