colart

Technology Continuity Management Strategy

1.0

Claudio Toledo/Stuart Cooney

Document Approval			
Name	**Signature**	**Role**	**Date**
Toby Russell		CTO	18/3/2020
Stuart Cooney		Head of Infrastructure	18/2/2020

Document Owner			
Name	**Signature**	**Role**	**Date**
Stuart Cooney		Head of Infrastructure	

Review				
Review Date	**Name**	**Role**	**Next Review Date**	**Comments**
18/3/2020	Claudio Toledo	Head of Project Management	20/3/2020	Version 1.0 Published

Contents

Foreword

We strongly believe that business continuity forms part of the overall management strategy of the company. It is vital that we create and maintain good working practices within a safe environment for all our employees and clients.

With the understanding and participation of every member of staff, we can ensure that our Business Continuity strategy is an effective part of company culture.

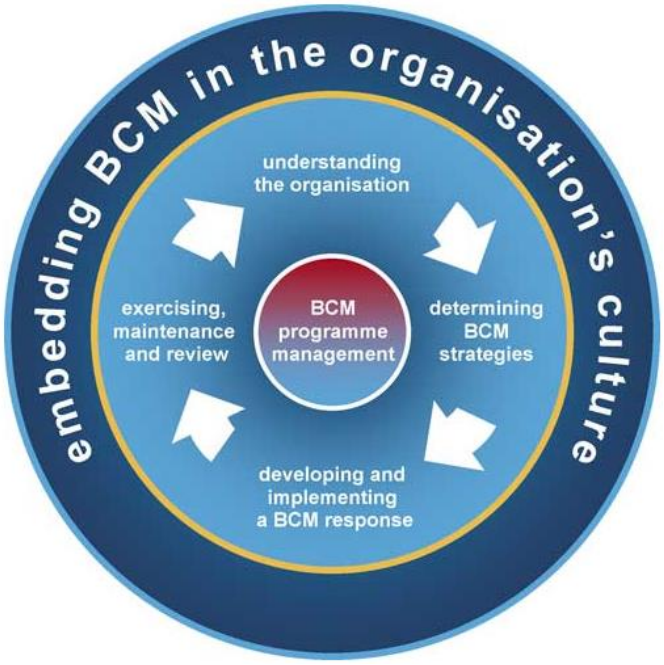
Toby Russel, CTO

Introduction

Business Continuity Management (BCM) is the process involved in creating a system of prevention and recovery from potential threats to the company. It involves defining any and all risks that can affect the company's operation, making it an important part of the organization's risk management strategy, providing an effective response that safeguards the interests of its major stakeholders.

It was written based on good practice guidelines and BS25999 by the BSI (British Standards Institution). This document intends to focus on strategy and guidance for technology continuity as a part of the company wide business continuity strategy.

Find out more at:
https://en.wikipedia.org/wiki/BS_25999



Scope

This document has the main objective to elucidate such plan and formalise how and what to proceed with during a technical disruption.

The purpose of this document is to:

1. Provide a technical disaster response strategy for Colart.
2. Outline the adopted strategic, tactical and operational response strategy.

3. Provide sufficient information to plan for a restore for lost services following an incident or crisis.

Site Tiering

Sites within Colart are tiered in the following mannor below. This document will refer to sites and systems appropriately according to this tiering.

Tier 1 – This site holds critical global business systems and would cause major disruption to the business in the event of a major outage. This is classed as a "service supplier".

Tier 2 – This site will hold critical local systems and would cause major disruption locally and not necessarily globally in the event of a major outage. This is classed as a "local service supplier".

Tier 3 – This site holds no critical systems and will cause no significant disruption to the wider business in the event of major outage. This is classed as a "service consumer".

This technical business continuity is structured as follows:

Part 1: People	Contact names and telephone numbers for: - Internal staff by department - Supplier contacts (where necessary)
Part 2: Technology Recovery Processes and Components	Provides detailed information on the IT and systems involved in the delivery of the services.
Part 3: Risk Management	Risk assessment and plans
Part 4: Other Relevant Information	Additional useful and supporting paperwork Forms and check list

Part 1 – People.

The Gold, Silver and Bronze Concept

Gold, Silver, and Bronze are titles of functions commonly adopted by each of the Emergency Services and the response structures of many organisations. They are role related - not rank related. To ensure that only the required response personnel are involved when a disaster is reported, an additional decision process (filtration) has been added to the front of the Gold, Silver and Bronze concept known as the duty manager responder process.

Gold	Gold is the command in overall charge of the response from a strategic stance. This will be comprised of members of the SLT.
Silver	Silver will focus on the scene, take charge and will be the designated crisis management team.
Bronze	Bronze will control and deploy their resources. They will be the designated incident management team.

Gold Response Team

The Gold team focuses on the required response & recovery strategy. The Gold team is responsible for formulating the response and recovery strategy for the business when an incident occurs. The gold team has overall command of the resources of the organisation, and once agreed the activities required, communicates strategic directives to the Silver team. The Gold team should not communicate directly with the Bronze Team.

Gold Team Members:

Gold		
Name	**Role**	**Phone**
Toby Russell	CTO	T +44 208 424 3352
Gail Pasquier	CCO	T + 44 208 424 3282
Mark Barratt	COO	T +44 2084243331
Jonathan Spight	CFO	T +44 20 8424 3318
Jane Beeston	CPO	T +86 166 2102 0747
Dennis Van Shie	CEO	T +44 208 424 3295

Silver Response Team

The Silver team manages the incident. The Silver team is responsible for the dissemination of directives communicated by the gold team. Silver is then responsible for converting these directives to realistic activities which are then communicated to the Bronze team. As Silver sits in the middle of the process, they are able to challenge the directives communicated by the gold team if the information they are receiving from Bronze deems it necessary. The Silver team should not become personally involved with activities close to the incident but remain detached. Typically, the Silver team will be operational directors / senior management / site managers.

Silver Team Members:

Silver			
Site	**Name**	**Role**	**Contact**
UK LD9 Data Centre	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
UK London	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
UK Kidderminster	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Shane Williams	Site Supervisor	+44 156 275 6743
UK Lowestoft	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Mark Brindle	Site Manager	T +44 150 252 5808
UK Minehead A	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Adrian Ryan	General Manager	T +44 1643 707659
UK Minehead B	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407

	Adrian Ryan	General Manager	T +44 1643 707659
UK - Elephant	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Toby Russell	CTO	T +44 2084 243 250
	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
FR Le Mans	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Patrick Ollier	Director of Applications	T + 33 2 43 83 83 07
	Dominique Murzeau	General Manager	T +33 2 43 83 83 27
	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
FR Paris	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Anne Marie Joannes	Marketing Director	T +33 629203585
	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
DE Maintal	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Piet Van Nassu	Commercial Director	T + 49 6109764661
	Stuart Cooney	Head of Global Infrastructure	T + 44 782 461 9668
NL Breda	Dan Ruzzak	Head of Service Desk	T + 44 738 446 0407
	Jasper Van der Wuff	Commercial Director	+31 854855466

Bronze Response Team

The Bronze team conduct the activities required. The Bronze team is responsible for conducting the activities required as communicated by the silver team. Typically, these are the people who are at/near the scene of the incident and are able to effectively communicate events as they unfold. Bronze is also able to challenge the activities communicated by Silver if they are deemed to be unrealistic.

Bronze team members will be organized dependent on the nature of the issue and will include (but not exclusively) technical engineers and associated members of staff.

Part 2: Technology Recovery Processes

Outage Levels

In most circumstances, it is anticipated that regular business response procedures will be able to deal with a Level 1 incident, with minimum disruption to overall service. Incidents relating to the loss of systems will be dealt with as detailed further below. In all incident levels a Bronze team will be built appropriate to the incident/level of outage.

Level 1 - Loss of services = < 8 hours	Issue communicated to all affected users via Mission Control Squad email. Regular updates to be communicated throughout lifespan of issue.
Level 2 - Loss of services =>8 hours & =< 48 hours	Issue communicated to all affected users (and wider staff if deemed appropriate by Gold/Silver team) via Mission Control Squad. If system affected is business critical a decision is to be undertaken by a member of the Gold team as to whether disaster recovery is to be instigated (where possible). If issue is none system specific and rather a local business unit electrical or network based issue (not affecting applications, servers, etc) a decision is to be made if members of staff can be relocated on a temporary measure (ie from another business location or at home via VPN).

Level 3 - Loss of services for => 72 hours	For the purpose of this plan, loss of service for more than 72 hours month will imply that a catastrophic event has occurred ie: total destruction of the building due to flooding or fire. In this case, the Strategic team will review a more permanent solution involving full disaster recovery/moving the service to an alternate site.

Technological Emergency

Technological Emergencies refer to interruptions in the technical aspects of operations. They includes but are not exclusive to:

- System/application outages
- Electrical outages (causing system disruption)
- Network failure
- Any other equipment failure

In the event of technical emergency, direct line managers or superiors are to be notified immediately. It is then the responsibility of the member of staff notified of the outage to inform a member of the Gold or Silver team to assess the issue and instigate the business continuity playbook or disaster recovery.

Types of Emergency

Electrical

Tier 1

Where N+1 power exists, in the event of 1 power feed failing the second feed will automatically take over and provide relevant power until such a time that the primary feed is bought back on line.

Where only UPS exists (Le Mans) this will hold power for approximately "xx" hours. It is to be assessed during the outage if power is likely to be bought back online within an adequate time scale as not to cause further disruption. If power is not able to be restored adequately then it the responsibility of a member of the Gold or Silver response teams to instigate DR.

Tier 2/3

All branch offices are equipped with a UPS that will hold a small amount of charge for communications equipment in the event of power failure.

Site Tier	Site	Redundancy
Tier 1	UK LD9 Data Centre	N+ 1 Power N+ 1 Cooling
Tier 1	US Open Data Centre	N+ 1 Power N+ 1 Cooling
Tier 1	Le Mans	N+1 Power N+1 Cooling

Network

LAN

Tier 1 sites operate a network resilience of N+1. In the event of a singular switching device failure, client traffic can be re-routed via other switches. Spare switches are also kept on site where possible in all sites.

WAN

All sites are made fault tolerant with at least 2 independent WAN links including internally managed DIA (direct internet access and vendor managed MPLS). In the event of failure of the primary line, traffic is re-routed to the secondary line to continue service.

In the event of MPLS failure (where DIA and MPLS exist) traffic is re-routed via the internally managed auto VPN.

Network Topologies

These are available on the cloud hosted SharePoint site and made available when necessary. This covers both LAN and WAN topologies.

Systems/Applications

All systems and applications at all 3 Tier 1 sites are hosted on 3 node clusters. Each cluster operates at N+1 redundancy, tolerating 1 node of physical or software failure. Backups are taken daily, weekly and monthly. In the event of total site failure backups can be restored appropriately (please see backup retention form elsewhere in document).

M3
M3 ERP is Colarts most valuable business asset and fundamental to ensuring business operation. In this case M3 is not only backed up locally but is also

replicated in its entirety nightly to a purpose-built co-location site. In the event of total failure of primary Le Mans site M3 can be ran from the co-location site.

Part 4: Other Relevant Information

Impact Mitigation Strategies

Strategies to mitigate the impact of the defined disasters on the company's critical resources should be identified to ensure the continuity of business in the light of specific disasters that may occur. The following are the mitigating strategies implemented to ensure continuity.

Disaster:
Loss of Utility Power/ Power Outages

Critical Resource: Site-Wide

Business Impact: No electricity, impeding the use of all electronic equipment (servers, workstations, etc.)

Mitigating Strategies

- Provision of a/b redundant power feeds (data centers)
- UPS systems are provided appropriately to ensure continuity of supplied power

Monitoring/Maintenance Requirements

- UPS testing – annual
- Testing of failover to a./b power feeds

Disaster:

Loss of WAN (Wide Area Network)

Critical Resource: Site Wide/Global

Business Impact: Loss of connectivity to data centres/hosted applications and other group sites and internet.

Mitigating Strategies

- Provision of 2nd and or 3rd WAN link that will automatically reroute traffic in the event of failure
- Ability to work from other business and non-business unit locations (VPN)

Monitoring/Maintenance Requirements

- Monthly testing of failover to secondary WAN links
- Pro-active alerting from PRTG monitoring platform for all edge devices (routers, firewalls, etc) for packet loss/ping

Disaster:

Loss of LAN (Local area network)

Critical Resource: Site-Wide

Business Impact: Loss of connectivity to local and external networks

Mitigating Strategies

- Provision of N+1 for switching
- Ability to work from home via VPN in the event of total LAN failure
- Spare equipment where available

Monitoring/Maintenance Requirements

- Pro-active alerting from PRTG monitoring platform for all network devices (switches, aps, etc) for packet loss/ping

Disaster

Loss of application services

Critical Resource: Local/Global

Business Impact: Loss of key business applications such as M3

Mitigating Strategies:

- Local and cloud-based backups
- Replication (M3) to co-lo site
- N+1 hardware

Monitoring/Maintenance Requirements

- Pro-active alerting from PRTG monitoring platform for all servers/systems
- Weekly patching off all critical updates

Recovery of Data

This process is to be invoked following the identification that data backup files are required for the restoration of systems/applications.

Data Backups

Data Backups are held in the following locations and contain the below retention periods. Server hosts listed contain multiple vms per node and as such are

Server Hosts	Location	Backup Type	Retention
UK-LD9-NTX1 UK-LD9-NTX2 UK-LD9-NTX3	LD9 Data Centre (local) Azure Cloud (offiste)	Veeam Local Backup Veeam Offsite Cloud Backup	Daily: 3 weeks Monthly: 12 Quarterly: 4 Yearly: 2
US-ODC-NTX1 US-ODC-NTX2 US-ODC-NTX2	ODC Data Centre (local) Azure Cloud (offsite)	Veeam Local Backup Veeam Offsite Cloud Backup	Daily: 3 weeks Monthly: 12 Quarterly: 4 Yearly: 2
FR-LM-VC1 FR-LM-VC2 FR-LM-VC3	Le Mans (local) M3 – Paris Co-Location (offsite) AWS Cloud (offsite)	Veeam Local Backup Veeam Replication Veeam Offsite Cloud Backup	Daily: 3 weeks Monthly: 12 Quarterly: 4 Yearly: 2

The infrastructure team should be utilised for any IT Data backup process or recovery only in the event of an emergency and on instruction from members of the Gold or Silver teams.

Change Management

If a disruption requires an urgent change a retrospective change request is to be submitted via the Jira portal and discussed/recorded after remediation of the incident. All standard requests for change are to be made as per the change management process/policy.

Port Mortem

Once a technical outage is resolved, a post-mortem of the incident will be conducted by all relevant members of the team to ensure lessons learned and to mitigate potential future issues.