

## Board of Management

### Finance & Physical Resources Committee

<b>Date of Meeting</b>	<b>Wednesday 23 May 2018</b>
<b>Paper No.</b>	<b>FPRC4-M</b>
<b>Agenda Item</b>	<b>15</b>
<b>Subject of Paper</b>	<b>Business Continuity Management Review</b>
<b>FOISA Status</b>	<b>Disclosable</b>
<b>Primary Contact</b>	<b>Paul Clark, College Secretary/Planning Fares Samara, VP Infrastructure</b>
<b>Date of production</b>	<b>8 May 2018</b>
<b>Action</b>	<b>For Discussion</b>

#### Recommendations

1. To consider the review of business continuity with findings and recommendations as submitted to the Audit Committee on 16 May 2018.
2. To recommend to SMT the consideration and implementation of an appropriate action plan.

## Board of Management Audit Committee

<b>Date of Meeting</b>	<b>Wednesday 16 May 2018</b>
<b>Paper No.</b>	<b>AC4-I</b>
<b>Agenda Item</b>	<b>10</b>
<b>Subject of Paper</b>	<b>Business Continuity Management Review</b>
<b>FOISA Status</b>	<b>Disclosable</b>
<b>Primary Contact</b>	<b>Paul Clark, College Secretary/Planning Fares Samara, VP Infrastructure</b>
<b>Date of production</b>	<b>8 May 2018</b>
<b>Action</b>	<b>For Discussion and Decision</b>

### 1. Recommendations

1. To consider the review of business continuity with findings and recommendations.
2. To recommend to SMT the consideration and implementation of an appropriate action plan.

## **2. Purpose of report**

2.1 The purpose of this report is to provide the Committee with a report of an external review of Business Continuity Management at the College, undertaken in March 2018 by Ashton Resilience for the College's insurers, UMAL.

## **3. Context**

3.1 The College's Business Continuity Planning arrangements were developed at merger, in consultation with Marsh Consulting. This plan consisted of a Business Continuity Plan, focusing upon emergency response and crisis management, and a series of business recovery plans covering all 12 college locations and operations.

3.2 The Business Continuity Plan (BCP) has been regularly updated, and utilised on five occasions since November 2017 in response to various emergency situations: loss of water; unattended package; loss of power; severe weather; and marine engine breakdown. In each case the BCP emergency response plan was found to be effective. BCP reviews have been undertaken following these incidents, and various improvements made. The BCP was last subject to a full review by SMT in November 2017.

3.3 In March 2018, by arrangement with the infrastructure team, a review of business continuity management was undertaken on behalf of the College insurers (UMAL) by Ashton Resilience. The review looked at the activities and operations of the College, its current recovery capability, and the degree to which BCM has been implemented. A draft report was forwarded to the College on 16 April 2018, with detailed findings and recommendations.

3.4 The report found that the College had a "well-developed operational response to incidents, however there was a need for all departments "to develop, implement and maintain a functional recovery process". All elements of incident management are graded "Good" in the Report. However, the Business Recovery Plans, previously developed for the former College campus sites, have still to be developed for the new campuses.

3.5 The high priority recommendations from the report reflect this shortcoming, and point to the need for a wide ranging business/service impact analysis for key college processes, including recovery time objectives, and recovery resources, dependencies and strategies for the restoration of College operations.

3.6 Following this analysis, new departmental business continuity plans require to be developed to cover all critical areas of College activity.

3.7 An early draft action plan has been created (appendix 2) to cover the report recommendations. This has yet to be discussed and approved at senior level.

## **4. Impact and implications**

4.1 Failure of business continuity is a strategic risk to the College with a wide range of possible consequences associated with operational failures. These failures may result from a loss of resources, such as facilities and physical resources, or staff/students due to a health and safety incident (e.g. 'flu pandemic).

4.2 These consequences include, but are not limited to, strategic failures represented by most of the College's strategic risks and strategic aims. These include failures to support student success and duty of care, negative impact upon College reputation, performance, IT security, and failure to maintain the College's long-term financial stability. The consequences of such failures may be wide-ranging and significant.

4.3 A College-wide business impact analysis, together with business recovery plan development for all operations, comprises a significant programme of work. This would involve estates/infrastructure teams, and key managers in each area of operation to identify recovery requirements across a range of timescales and scenarios. It may be that a specialist consultancy requires to be engaged to ensure swift completion of the high priority recommendations, with financial cost attached.

4.4 Regional and sectoral considerations are included in the process of risk management, and are reflected in the College's risk management documentation.

### **Appendices:**

**Appendix 1: Strategic Review of Business Continuity: Report**

**Appendix 2: Draft Action Plan**

**REPORT FOR**

**CITY OF GLASGOW COLLEGE**

**STRATEGIC REVIEW OF  
BUSINESS CONTINUITY  
MANAGEMENT**

<b>Project Name:</b>	UMA062 – Strategic Review of Business Continuity Management		
<b>Document Name:</b>	Report		
<b>Version Control:</b>	<b>Version</b>	<b>Date</b>	<b>Change</b>
	0.1	26/03/18	Initial draft sent to Paul Clark
	0.2	11/04/18	Feedback on draft report received from Paul Clark
	1.0	16/04/18	Updated version based on feedback and report published
<b>Author:</b>	Chris Lintern, Ashton Resilience		
<b>Distribution:</b>	Fares Samara, Vice Principal Infrastructure Paul Clark, College Secretary / Planning Fergal McCauley, Head of Facilities Management Derek Mason, UMAL		

## CONTENTS

<b>1. Introduction</b>	<b>1</b>
1.1 Background	1
1.2 The Strategic Review	1
1.3 Summary of Findings	1
1.4 Recommended Next Steps	1
<b>2. Review Criteria</b>	<b>2</b>
2.1 Components of Business Continuity Management (BCM)	2
<b>3. Findings and Recommendations</b>	<b>3</b>
3.1 Category 1: Responding effectively to <i>major incidents</i>	3
3.2 Category 2: Recovering operations following a <i>disruption</i>	6
3.3 Category 3: Maintaining the integrity of organisational resilience	12
<b>4. What is Business Continuity Management</b>	<b>15</b>

## 1. INTRODUCTION

### 1.1 Background

On 16<sup>th</sup> March 2018, Chris Lintern of Ashton Resilience completed a Strategic Review of Business Continuity Management (BCM) for the City of Glasgow College. This Strategic Review is available to members of the U.M. Association Limited and is intended to assist members to improve their risk profile through effective contingency planning.

### 1.2 The Strategic Review

A Strategic Review is a rapid and cost-effective assessment of the College's business continuity management requirements and capabilities. The review looked at the activities and operations of the College, its current recovery capability and the degree to which BCM has been implemented.

Our approach is based on a proven methodology and followed the process summarised below:

Assessing:	Using a series of structured interviews with senior managers we assessed the College's BCM requirements and the current status of each component of BCM. See Section 2.2 for a definition of the status.
Analysing:	By comparing the current status of each component with good practice benchmarks, we identified the gaps that need to be addressed in order to ensure organisational <i>resilience</i> <sup>1</sup> . Recommendations to fill these gaps are set out in Section 3.
Reporting:	This report sets out the findings of the Analysis and recommended actions to improve BCM. Recommendations are prioritised according to the scale shown in Section 2.3.

### 1.3 Summary of Findings

The City of Glasgow College has a structured approach to incident management and a well-developed operational response to incidents, but it does not have a functioning business continuity management system.

All departments need to develop, implement and maintain a functional recovery process. This can be completed through first conducting a business impact analysis then documentation of business continuity (or 'business recovery') plans, based upon coherent recovery strategies.

Since essential components of a formal business continuity management system have not been developed at the College, the resilience of the College's *critical activities* cannot be assured.

The high priority recommendations in this report are that the City of Glasgow College should:

- Conduct a business impact analysis and service impact analysis for key processes right across the College.
- Identify recovery time objectives for critical business activities and IT services.
- Identify recovery resources, dependencies and strategies for operational recovery.
- Complete the creation of new departmental business continuity / recovery plans to cover all critical areas of the College, using the business impact analysis data as the base.

### 1.4 Recommended Next Steps

In order to derive maximum benefit from this Strategic Review and build on existing capability, we recommend that the College initiates a structured implementation project. The recommendations made in this report can be used as the basis for the implementation.

<sup>1</sup> Words shown in italics are defined in Section 5



## 2. REVIEW CRITERIA

### 2.1 Components of Business Continuity Management (BCM)

BCM is more than just a series of plans and documents. It is about making sure that the College can deliver its core activities and continue to operate effectively following a *disruption*. There are many component parts to BCM and some of these are more important than others depending on how they affect the overall *resilience* of the College. We categorise the importance of these components according to the following scale:

<b>Category 1:</b>	<b>Responding effectively to <i>major incidents</i> and threats</b> The first minutes and hours following a <i>major incident</i> are crucial in determining the survival of the College. For this reason, we give priority to this aspect when assessing capability and defining areas for improvement.
<b>Category 2:</b>	<b>Recovering operations following a <i>disruption</i></b> Once the immediate crisis has been contained the focus must be on returning operations to normal levels as soon as possible. We look at the College's requirements and current recovery capability and identify areas for improvement.
<b>Category 3:</b>	<b>Maintaining the integrity of organisational <i>resilience</i></b> The College operates in an ever-changing environment. Response and recovery plans that are valid today will be out of date before too long unless they are maintained, tested and improved. The Strategic Review looks at the existing management systems and recommends improvements to ensure that BCM is embedded within the College's routines and procedures.

### 2.2 Status of Components

Each component of BCM is assigned a status to reflect the extent to which it exists or has been developed within the College. The statuses are:

<input checked="" type="checkbox"/> <b>Good:</b>	The component has been addressed and the current capability contributes to organisational <i>resilience</i> .
<input type="checkbox"/> <b>Average:</b>	The component has been addressed but the current capability falls short of true organisational <i>resilience</i> .
<input type="checkbox"/> <b>Poor:</b>	The component has not been addressed or the level of capability is such that it undermines <i>resilience</i> .

### 2.3 Priority for Implementation Actions

Implementation actions are prioritised on the following scale:

<b>H High:</b>	This action directly affects the College's ability to respond to a <i>major incident</i> or recover from a <i>disruption</i> . High priority actions should be addressed within six months.
<b>M Medium:</b>	Failure to address the action may diminish the College's ability to respond to a <i>major incident</i> or recover from a <i>disruption</i> . Medium priority actions should be addressed within 12 months.
<b>L Low:</b>	This action impacts the ability of the College to manage and maintain the overall effectiveness of business continuity management. Low priority actions should be addressed within 24 months at most.
<b>Q Quick-win:</b>	This action may not have a high importance but, in our opinion, can be addressed relatively easily and will add to the overall improvement of BCM. Quick-wins should be addressed as time and resources allow.

**3. FINDINGS AND RECOMMENDATIONS**

**3.1 Category 1: Responding effectively to *major incidents***

Ref No:	Components	Status	Implementation Actions	Priority
a	<i>Incident</i> Management Team	☑	<p>Members of the College Crisis Management Team and site Emergency Response Teams are detailed within the business continuity plan (BC plan).</p> <p>The plan, however, does not contain specific roles that are required in responding to a major incident, and would benefit from this along with primary and deputy members for each role.</p> <p><b>Recommendation:</b></p> <p>Consider the benefit of introducing a role-based team for managing a major incident, with roles covering IT, Estates, Communications, Secretariat, People, and any other roles relevant within the College. Identify a primary and deputy role-holder for each.</p>	<b>Q</b>
b	<i>Incident</i> management arrangements	☑	<p>Emergency Response Centres are identified within the plan across both campus locations, and members of the Crisis Management Team and site Emergency Response Teams are aware of these locations. The addition of a conference call facility would enable the relevant response team to convene quickly without meeting at a physical location and may reduce the risk of senior management travelling into the College (for example in the event of a severe weather event).</p> <p><b>Recommendation:</b></p> <p>Add conference call details to the BC plan, using a free-to-use facility such as the one provided by whypay.net.</p>	<b>Q</b>

Ref No:	Components	Status	Implementation Actions	Priority
c	<i>Incident Management Plan</i>	☑	<p>The BC plan contains members for both Crisis Management and Site Emergency Response Teams, along with arrangements, resources and actions for incident response.</p> <p>Once the College develops continuity or recovery plans (see 3.2.p below) it may be beneficial to rename the existing Business Continuity Plan to reflect the differences between incident management and business continuity or recovery.</p> <p><b>Recommendation:</b></p> <p>Review the terminology used to describe the response plans once recovery plans have been developed. The current BC plan could be rebadged as "Business Continuity: Incident Control Plan" for clarity.</p>	<b>Q</b>
d	Emergency communications arrangements	☑	<p>A number of ways of sending emergency communications are available to the College during incident response. These include use of the website and social media channels. It is clear how messages are delivered and who is responsible for doing so. The Communications and Marketing team also have a crisis communications plan and access to an external PR Agency who could respond quickly if required.</p>	<b>N/A</b>
e	<i>Incident Management Team training</i>	☑	<p>Training for the Crisis Management and Emergency Response Teams have been planned but superseded by the teams having to respond to disruptive incidents. This has given the teams experience of responding to incidents and of using the documentation.</p> <p>Conducting an annual training session would provide attendees with an opportunity to understand both the documentation and their roles and responsibilities in a safe and supportive environment.</p> <p><b>Recommendation:</b></p> <p>Schedule a training session for Crisis Management and Emergency Response Teams on an annual basis.</p>	<b>L</b>

Ref No:	Components	Status	Implementation Actions	Priority
f	<i>Incident Management Exercise</i>	☑	<p>Scenario exercises for the Crisis Management and Emergency Response Teams have been planned but superseded by the teams having to respond to disruptive incidents. This has given the teams experience of responding to incidents and of using the documentation.</p> <p>Conducting an annual training scenario exercise by way of a desktop walkthrough would provide attendees with an opportunity to further understand both the documentation and their roles and responsibilities in a safe and supportive environment.</p> <p><b>Recommendation:</b></p> <p>Develop and deliver a desktop walkthrough exercise for Crisis Management and Emergency Response Teams on an annual basis and use the feedback from the debrief to update the College's business continuity documentation.</p>	L

**3.2 Category 2: Recovering operations following a *disruption***





Ref No:	Components	Status	Implementation Actions	Priority
a	Corporate ownership of Business Continuity Management	✔	The Vice Principal for Infrastructure is responsible at an Executive level and therefore has corporate ownership of business continuity management within the College.	N/A
b	Operational ownership of business continuity	✔	Operational ownership of business continuity resides with the College Secretary who is responsible for the relevant documentation being kept up to date.	N/A
c	<i>Business Impact Analysis (BIA) to identify critical activities</i>	✘	<p>A business impact analysis (BIA) process was last undertaken at merger, and refers to College activity in the former estates and locations. The BIA does not reflect the current College structure nor the two campus sites it occupies.</p> <p>There is no current documentation which analyses the impact of the loss of key activities within the College. Consequently, the priority of processes and deployment of resources in business recovery is not defined.</p> <p><b>Recommendation:</b></p> <p>Undertake a new BIA and ensure that all areas of the College complete this exercise to fully understand the impact of the loss of processes, and resources required, in the event of a major incident.</p>	H

Ref No:	Components	Status	Implementation Actions	Priority
d	Service Impact Analysis (SIA) to identify critical IT services	!	<p>IT have developed an 'Impact-Risk-Resources' Matrix which identifies how several scenarios would affect both user-facing and enabling services. However, in the absence of a current BIA (see above) this is not based upon defined business processes from across the College and may therefore not reflect the College's priorities.</p> <p><b>Recommendation:</b> In conjunction with the BIA exercise (see 3.2.c), undertake an SIA to align the business processes with the IT service requirements. This will derive user-driven recovery time and recovery point objectives (RTOs and RPOs) and can be the basis of any IT service prioritisation required in a major incident.</p>	M
e	<i>Risk Assessment</i> to identify risks of operational <i>disruption</i>	✓	Risk assessments are undertaken on a regular basis across the College and this is managed by the VP Infrastructure via the Health and Safety Compliance Manager. The strategic risk register includes business continuity risks.	N/A
f	<i>Recovery time objectives</i> defined for <i>critical activities</i>	✗	<p>Up-to-date recovery time objectives for critical activities have not been defined across the College as the BIAs have not been recently updated.</p> <p><b>Recommendation:</b> As an outcome of the business impact analysis exercise (see 3.2.c) confirm the business process recovery time objectives and define critical activities.</p>	H

Ref No:	Components	Status	Implementation Actions	Priority
g	<i>Recovery time objectives</i> defined for critical IT services	!	<p>Recovery time objectives have not been formally adopted, although critical data centre operations are managed through an established service contract with a third party. Target response and fix periods are identified through this contract.</p> <p>As these are not based on an SIA, the recovery time objectives are therefore based on IT's perception of criticality to the College.</p> <p><b>Recommendation:</b></p> <p>As an outcome of the SIA (see 3.2.d) confirm the critical IT services and their recovery time objectives.</p>	M
h	Recovery resources defined for operational recovery	⊗	<p>Recovery resources have not been defined for all departments because a BIA has not been recently completed.</p> <p><b>Recommendation:</b></p> <p>Ensure that the BIA process is completed (see 3.2.c) to capture the necessary detail of recovery resources required for operational recovery.</p>	H
i	Recovery resources defined for IT service recovery	!	<p>Recovery resources are defined for a number of IT services; however, these are not aligned with an SIA, as one has not been completed. As a result, resources may not be aligned to the College's critical processes.</p> <p><b>Recommendation:</b></p> <p>As an outcome of the SIA (see 3.2.d) ensure that recovery resources are defined for the most critical IT services.</p>	M
j	Recovery dependencies identified	⊗	<p>Recovery dependencies have not been identified by all areas of the College as a BIA has not been completed. Dependencies should be identified and documented as part of the BIA process.</p> <p><b>Recommendation:</b></p> <p>Ensure that the BIA process is completed (see 3.2.c) to capture both internal and external recovery dependencies.</p>	H

Ref No:	Components	Status	Implementation Actions	Priority
k	Critical periods identified	!	<p>Critical periods within the College are generally well understood and reflect the academic calendar. Any additional critical periods would be captured within the BIA process.</p> <p><b>Recommendation:</b> Critical periods should be identified as part of the BIA process and then documented within updated business continuity plans. This will ensure that recovery resources can be prioritised in case of need.</p>	M
l	<i>Business continuity strategy</i> developed	!	<p>The College business continuity plan outlines the strategy which comprises the following five elements:</p> <ul style="list-style-type: none"> <li>• Risk Identification, Impact Analysis, and Management</li> <li>• Emergency Response and Incident Control</li> <li>• Disaster Recovery</li> <li>• Business Recovery Planning</li> <li>• Ongoing Review and Audit Test</li> </ul> <p>The plan includes approval dates (the most recent of which was November 2017 by the SMT).</p> <p>The strategy should detail how the College will recover from a disruptive event which can only be done once all areas have completed a BIA.</p> <p><b>Recommendation:</b> Once a BIA has been completed, update the strategy to include how the College will recover from a major incident.</p>	M
m	IT continuity strategy developed	!	<p>IT's overall continuity strategy is to support the College business continuity plan. There is no formal IT continuity strategy.</p> <p><b>Recommendation:</b> Formally document the IT continuity strategy.</p>	L







Ref No:	Components	Status	Implementation Actions	Priority
n	Business continuity recovery arrangements		<p>Recovery arrangements have not been formally documented because a BIA has not recently been completed.</p> <p><b>Recommendation:</b> Identify recovery requirements as part of the BIA. Formalise and document recovery arrangements in conjunction with the update of the strategy and business recovery plan rollout (see 3.2.l and 3.2.p respectively).</p>	H
o	IT continuity arrangements		<p>Recovery arrangements exist for a number of systems and services within disaster recovery plans. Plans have not been completed for all IT services although these are in the process of being written.</p> <p><b>Recommendation:</b> Ensure that disaster recovery plans are completed for all IT services.</p>	M
p	<i>Business Continuity (Recovery) Plans</i>		<p>The College BC plan is essentially a tool to aid senior management through the management of a major incident. There are no current and up to date business recovery plans at the College which focus on the continuation of critical activities and the resources required.</p> <p><b>Recommendation:</b> Once the BIA has been completed, use this as the basis to formalise and document BC plans for all departments across the College.</p>	H
q	IT Continuity Plans		<p>Several disaster recovery plans exist but plans have not been completed for all IT services, although these are in the process of being written.</p> <p><b>Recommendation:</b> Ensure that disaster recovery plans are completed for all IT services.</p>	M

Ref No:	Components	Status	Implementation Actions	Priority
r	Key suppliers dependency and capability	!	<p>Some key suppliers and their recovery capability have been identified by several departments, including IT, Facilities and Communications and Marketing. Other departments have not identified their key suppliers' recovery capabilities and may not know how third parties would be able to continue providing key services to the College in the event of a major incident.</p> <p><b>Recommendations:</b></p> <ul style="list-style-type: none"><li>• Ensure that key suppliers are identified as part of the BIA process.</li><li>• Instigate a process of assessing key supplier recovery capability as part of formal due diligence across the College.</li></ul>	M

### 3.3 Category 3: Maintaining the integrity of organisational resilience

Ref No:	Components	Status	Implementation Actions	Priority
a	Business continuity policy	✓	A business continuity policy is documented within the College business continuity plan.	N/A
b	Calendar of planned business continuity activities	✗	No calendar of planned business continuity activities currently exists. <b>Recommendation:</b> Develop a calendar of planned business continuity activities and monitor alignment with it.	Q
c	Business Continuity <i>Exercise</i>	✗	No up to date BC plans are currently in place. There have therefore been no BC exercises conducted to test their effectiveness. <b>Recommendation:</b> Once BC plans have been created, arrange dates in the BC calendar (see 3.3.b) for an exercise to test the plans. Ensure that this exercise takes place annually to check the adequacy of the BC plans. An exercise of this nature would be a pre-arranged desktop walkthrough and attendees would be aware of the exercise, rather than a 'real-life', surprise mock incident. This is both because College management have managed a number of real incidents in recent years, and because of the risks involved in undertaking a 'real-life' mock incident.	M
d	IT Continuity <i>Exercise</i>	!	Service continuity testing has been carried out as part of acceptance criteria for new build handover. Testing, validation and review will be integral to the BC/DR measures currently under development within IT. <b>Recommendation:</b> Ensure that regular IT continuity exercises are scheduled to validate the content of the IT recovery plans when these have been documented.	M

Ref No:	Components	Status	Implementation Actions	Priority
e	Training for <i>business continuity plan</i> owners		<p>No training has been carried out for business recovery plan owners. This can only be completed once these plans have been created and plan owners have been assigned.</p> <p><b>Recommendation:</b> Once departmental business recovery plans have been formalised, arrange training dates in the BC calendar (see 3.3b) for all plan owners.</p>	<b>M</b>
f	Staff awareness activities		<p>All employees are made aware of business continuity plans and processes that are in place within the College.</p> <p><b>Recommendation:</b> Once departmental business recovery plans have been created, ensure that College employees are aware of these plans and how they would be used in the event of an incident.</p>	<b>Q</b>
g	Log of BC preventative and corrective actions		<p>Whilst a formal log of preventative and corrective actions does not exist, there is a detailed 'lessons learned' process which is undertaken as part of the response to each College incident. This process identifies how the BC plan should be updated.</p> <p><b>Recommendation:</b> Once departmental business continuity / recovery plans have been developed, ensure that there is a central log of preventative and corrective actions maintained across the College.</p>	<b>Q</b>
h	Roles and responsibilities assigned		<p>BC management is included or implied within a number of role descriptions but in all who have a role within business continuity across the College.</p> <p><b>Recommendation:</b> Include BC management within role descriptions of all staff with a BC role. This will include plan owners once BC plans have been developed across all areas of the College.</p>	<b>Q</b>

Ref No:	Components	Status	Implementation Actions	Priority
i	Risk Register updated with <i>risk assessment</i> output	✔	A Strategic Risk Register exists within the College and regularly includes operational risk or business continuity-related output.	N/A
j	BCM considered in new projects	!	Business continuity management is considered either formally or informally within new projects and several examples can be provided. <b>Recommendation:</b> Formally include business continuity on a project checklist or equivalent to ensure that it is considered in all new projects.	Q

#### 4. WHAT IS BUSINESS CONTINUITY MANAGEMENT

Business continuity management (BCM) is an operational framework that seeks to:

- Improve an organisation's *resilience* against *disruption*.
- Deliver the capability to manage a business *disruption*; and
- Provide a method of restoring operations following a *disruption*.

BCM applies to all organisations regardless of size, sector, aims or objectives. It is part of the overall risk management framework of the organisation and focuses on continuity of product and service delivery. The interests of all relevant stakeholders are taken into account and protected. BCM is an important element of good operational management and the benefits of an effective BCM programme include:

- Protection of stakeholder interests and preservation of organisational value.
- Reduction in exposure to particular risks and protection of physical and knowledge assets.
- Improved security and a reduction in downtime.
- Better compliance with regulation and legislation.

#### The BCM Lifecycle

The BCM lifecycle comprises six elements as illustrated opposite. These elements are applicable to organisations of all sizes and in all sectors although the scope and structure of implementation will vary. However, all elements will have to be undertaken to ensure a workable system is implemented. A brief description of each element follows:

##### 1. Programme management

Enables business continuity capability to be both established and maintained in a manner that is appropriate to the organisation.

##### 2. Understand the organisation

Provides information to prioritise activities and understand the resources that support these activities. This will help to determine the selection of appropriate BCM strategies.

##### 3. Determine the BCM strategies

A range of response strategies are evaluated and the most appropriate strategy chosen for each activity. The goal is to ensure recovery of operations to a minimum level within agreed timeframes.

##### 4. Develop and implement the BCM response

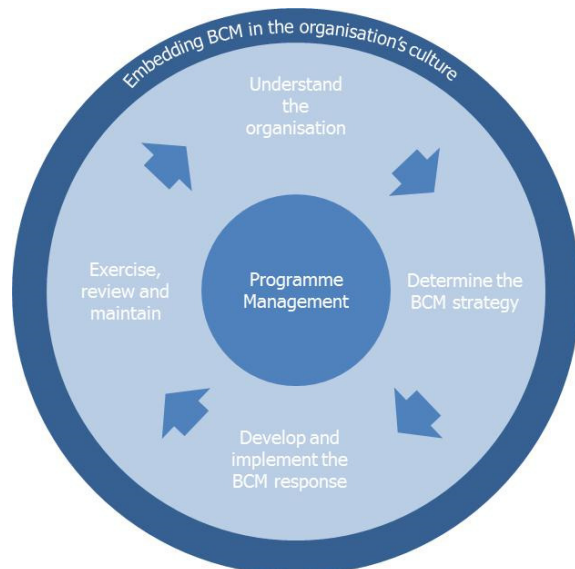
Results in the creation of a management framework and structure for *major incident* management, business continuity and IT continuity.

##### 5. Exercise, review and maintain

Leads to the organisation being able to demonstrate that strategies and plans are workable as well as being able to identify and implement improvements.

##### 6. Embedding BCM in the organisation's culture

Enables BCM to become part of the organisation's core management systems and operational procedures.



## TERMS & DEFINITIONS

### **Business continuity plan (BCP)**

Documented collection of procedures and information that is developed, compiled and maintained in readiness for use following a *disruption* to enable an organization to continue to deliver its *critical activities* at an acceptable pre-defined level. Note – for clarity, as the College has a document referred to as a business continuity plan primarily for incident management purposes, these plans have been termed business recovery plans.

### **Business continuity strategy**

The approach by an organisation that will ensure its recovery and continuity in the face of an incident or other *major incident* or business *disruption*.

### **Business impact analysis (BIA)**

The process of analysing business functions and the effect that a business *disruption* might have upon them.

### **Critical activities**

Those activities which have to be performed in order to deliver the key products and services which enable an organisation to meet its most important and time-sensitive objectives.

### **Disruption**

An event, whether anticipated or not, which causes an unplanned, negative deviation from the expected delivery of products or services according to the organisation's objectives.

### **Exercise**

An activity in which the *Incident Management Plan*, *business continuity plan(s)* and IT continuity plan is rehearsed in part or in whole to ensure that the plan contains the appropriate information and produces the desired result when put into effect.

### **Major incident**

A situation that might be, or could lead to, a business *disruption*, loss, emergency or crisis.

### **Incident Management Plan**

A clearly defined and documented plan of action for use at the time of a *major incident*, typically covering the key personnel, resources, services and actions needed to implement the *major incident* management process.

### **Recovery time objective (RTO)**

The target time set for:

- Resumption of performance of an activity after a *major incident*; or
- Recovery of an IT system or application after a *major incident*.

### **Resilience**

The ability of an organization to resist being affected by a *major incident*.

### **Risk assessment**

The overall process of risk identification, analysis and evaluation.

City of Glasgow College: Business Continuity Management Action Plan

Category	Ref No:	Components	Implementation Actions	Priority	Owner
1: Responding effectively to major incidents	a	Incident Management Team	Consider the benefit of introducing a role-based team for managing a major incident, with roles covering IT, Estates, Communications, Secretariat, People, and any other roles relevant within the College. Identify a primary and deputy role-holder for each.	Quick	PC
1: Responding effectively to major incidents	b	Incident management arrangements	Add conference call details to the BC plan, using a free-to-use facility such as the one provided by whypay.net.	Quick	PC/KempA
1: Responding effectively to major incidents	c	Incident Management Plan	Review the terminology used to describe the response plans once recovery plans have been developed.	Quick	PC/FS (ref. Ashton Resilience glossary)
1: Responding effectively to major incidents	e	Incident Management Team training	Schedule a training session for Crisis Management and Emergency Response Teams on an annual basis.	Low	PC/MT
1: Responding effectively to major incidents	f	Incident Management Exercise	Develop and deliver a desktop walkthrough exercise for Crisis Management and Emergency Response Teams on an annual basis and use the feedback from the debrief to update the College's business continuity documentation.	Low	PC/MT
2: Recovering operations following a disruption	c	Business Impact Analysis (BIA) to identify critical activities	Undertake a new BIA and ensure that all areas of the College complete this exercise to fully understand the impact of the loss of processes, and resources required, in the event of a major incident.	High	FS/SMT/ External consultant via Procurement?
2: Recovering operations following a disruption	d	Service Impact Analysis (SIA) to identify critical IT services	In conjunction with the BIA exercise (see 3.2.c), undertake an SIA to align the business processes with the IT service requirements. This will derive user-driven recovery time and recovery point objectives (RTOs and RPOs) and can be the basis of any IT service prioritisation required in a major incident.	Medium	FS/SMT/ External consultant
2: Recovering operations following a disruption	f	Recovery time objectives defined for critical activities	As an outcome of the business impact analysis exercise (see 3.2.c) confirm the business process recovery time objectives and define critical activities.	High	FS/SMT/ External consultant
2: Recovering operations following a disruption	g	Recovery time objectives defined for critical IT services	As an outcome of the SIA (see 3.2.d) confirm the critical IT services and their recovery time objectives.	Medium	FS/SMT/ External consultant
2: Recovering operations following a disruption	h	Recovery resources defined for operational recovery	Ensure that the BIA process is completed (see 3.2.c) to capture the necessary detail of recovery resources required for operational recovery.	High	FS/SMT/ External consultant
2: Recovering operations following a disruption	i	Recovery resources defined for IT service recovery	As an outcome of the SIA (see 3.2.d) ensure that recovery resources are defined for the most critical IT services.	Medium	FS/SMT/ External consultant
2: Recovering operations following a disruption	j	Recovery dependencies identified	Ensure that the BIA process is completed (see 3.2.c) to capture both internal and external recovery dependencies.	High	FS/SMT/ External consultant
2: Recovering operations following a disruption	k	Critical periods identified	Critical periods should be identified as part of the BIA process and then documented within updated business continuity (recovery) plans. This will ensure that recovery resources can be prioritised in case of need.	Medium	FS/SMT/ External consultant
2: Recovering operations following a disruption	l	Business continuity strategy developed	Once a BIA has been completed, update the strategy to include how the College will recover from a major incident.	Medium	PC/FS
2: Recovering operations following a disruption	m	IT continuity strategy developed	Formally document the IT continuity strategy.	Low	FS/KA
2: Recovering operations following a disruption	m	Business continuity recovery arrangements	Identify recovery requirements as part of the BIA. Formalise and document recovery arrangements in conjunction with the update of the strategy and business continuity plan rollout (see 3.2.l and 3.2.p respectively).	High	FS/SMT/ External consultant
2: Recovering operations following a disruption	o	IT continuity arrangements	Ensure that disaster recovery plans are completed for all IT services.	Medium	FS/KA
2: Recovering operations following a disruption	p	Business Continuity Plans	Once the BIA has been completed, use this as the basis to formalise and document BC plans for all departments across the College.	High	Consultant/ SMT?
2: Recovering operations following a disruption	q	IT Continuity Plans	Ensure that disaster recovery plans are completed for all IT services.	Medium	FS/KA
2: Recovering operations following a disruption	r	Key suppliers dependency and capability	Ensure that key suppliers are identified as part of the BIA process.	Medium	Consultant/SMT
2: Recovering operations following a disruption	r	Key suppliers dependency and capability	Instigate a process of assessing key supplier recovery capability as part of formal due diligence across the College.	Medium	Consultant/SMT
3: Maintaining the integrity of organisational resilience	b	Calendar of planned business continuity activities	Develop a calendar of planned business continuity activities and monitor alignment with it.	Quick	PC/MT
3: Maintaining the integrity of organisational resilience	c	Business Continuity Exercise	Once BC plans have been created, arrange dates in the BC calendar (see 3.3.b) for an exercise to test the plans. Ensure that this exercise takes place annually to check the adequacy of the BC plans.	Medium	PC/MT
3: Maintaining the integrity of organisational resilience	d	IT Continuity Exercise	Ensure that regular IT continuity exercises are scheduled to validate the content of the IT recovery plans when these have been documented.	Medium	FS/KA
3: Maintaining the integrity of organisational resilience	e	Training for business continuity plan owners	Once BC plans have been formalised, arrange training dates in the BC calendar (see 3.3b) for all plan owners.	Medium	SMT
3: Maintaining the integrity of organisational resilience	g	Log of BC preventative and corrective actions	Once departmental business continuity / recovery plans have been developed, ensure that there is a central log of preventative and corrective actions maintained across the College.	Quick	?
3: Maintaining the integrity of organisational resilience	h	Roles and responsibilities assigned	Include BC management within role descriptions of all staff with a BC role. This will include plan owners once BC plans have been developed across all areas of the College.	Quick	PC/JM
3: Maintaining the integrity of organisational resilience	j	BCM considered in new projects	Formally include business continuity on a project checklist or equivalent to ensure that it is considered in all new projects.	Quick	FS/LS